Admin Tools Gebruikers Handleiding

Nicholas K. Dionysopoulos

Admin Tools Gebruikers Handleiding

Nicholas K. Dionysopoulos

Publication date January 2011

Abstract

Dit boek behandelt het gebruik van de Admin Tools website beveiliging component, module en plugin bundel voor Joomla! ™ powered websites. Beiden, de gratis Admin Tools Core en de abonnement gebaseerde Admin Tools Professional edities zijn volledig afgedekt.

Table of Contents

Chapter 1. Aan de slag

1. Wat is Admin Tools?

Admin Tools is een software bundel die bestaat uit een Joomla! component, een module en een plug-in met als voornaamste doel de veiligheid en de prestaties van uw website te verbeteren, evenals de beheerder van deze website het leven een stuk makkelijker te maken door het automatiseren van algemene taken.

Admin Tools maakt gebruik van een native Joomla! component en plugin en is 100% compatibel met Joomla! 1.5, Joomla! 1.6, Molajo en Nooku Servers. Het is niet nodig om php.ini bestanden te bewerken, geen noodzaak om welke vorm van server-side configuratie dan ook uit te voeren en geen behoefte de Joomla! core aan te passen of bestanden te verplaatsen.

Admin Tools kenmerken in een notendop:

- Joomla! core updater [updating-joomla], om uw Joomla! installatie up-to-date te houden. Als Akeeba Backup 3.1 of hoger geïnstalleerd is, kan het automatisch een back-up van uw website maken voordat u hem update. Een pictogram in de Admin Tools controle paneel pagina zorgt ervoor dat u nooit een update zal vergeten.
- Permissions Instellingen [fixing-permissions], zodat u nooit met bestanden of mappen met 0777 permissies komt te zitten. U kunt de permissies per map of zelfs per bestand aanpassen.
- Administrator wachtwoord bescherming [admin-pw-protection], om een extra laag van wachtwoord beveiliging toe te voegen, voordat iemand toegang krijgt tot uw back-end beheerder omgeving
- Administrator query string bescherming, zodat het beheerder back-end gebied alleen zichtbaar is als iemand een geheime URL parameter ingeeft, dat wil zeggen http://www.voorbeeld.com/administrator?geheime_parameter (alleen in de Professional versie van de Web Applicatie Firewall [web-application-firewall])
- .htaccess maker [htaccess-maker], staat u toe een .htaccess bestand op maat te maken die uw website beveiligd, verbetert en vrijwel alle vingerprinting en de meest voorkomende hacker aanvallen blokkeert (alleen de Professional versie).
- Off-Line bij noodgevallen mode [emergency-offline-mode], die *echt* uw website off-line haalt, in tegenstelling tot Joomla!'s off-line functie die alleen de component output verbergt.
- Web applicatie firewall [web-application-firewall], met een aantal belangrijke functies (alleen in de Professional versie):
  - Staat toegang tot de Administrator back-end toe, met alleen specifieke IP adressen, of blokkeert specifieke IP adressen
  - Staat geen toegang tot uw website toe voor specifieke IP adressen, of blokkeert IP adressen (IP blacklisting)
  - Anti-spam op basis van een aanpasbare lijst van woorden
  - SQLi Schild, ontwijkt veel SQL injectie aanvallen
  - Kwaadaardige user agent filtering
  - CSRF / Anti-Spam (omgekeerde CAPTCHA) bescherming
  - Slecht gedrag integratie
  - Project Honeypot IP blacklisting (HTTP:BL) integratie

  - Geographische blokkering: Blokkeert bezoekers van de site op basis van het land of continent waar ze vandaan komen
  - Automatische blokkering voor IP adressen die herhaaldelijk de beveiligingsuitzonderingen triggeren
  - DFI (Direct file inclusion) detectie
  - Uploads scanner (Upload Schild) blokkeert geüploade bestanden met verdachte namen of met PHP code in zich
  - Bescherming tegen de meest voorkomende XSS aanvallen (XSS Schild)
  - Verschillende opties om te verbergen dat uw server gebruik maakt van PHP en Joomla!
  - Joomla!'s verborgen functies uitschakelen, alleen nuttig voor debugging van websites die gebruikt kunnen worden voor vingerprinting aanvallen
- Eén klik reparatie en optimalisatie van database tabellen [database-tools]
- Sessies wissen [database-tools]
- Tijdelijke map opschoner [cleantmp]
- Geplande onderhoudswerkzaamheden [system-plugin] (sessie tabel optimalisatie, sessie wissen, cache verloop, cache wissen) zonder de noodzaak van een CRON job (alleen in de Professional versie)
- Aangepaste URL redirecties [url-redirection] (alleen in de Professional versie)
- Link migratie, dat wil zeggen: Het automatisch herschrijven van URL's die verwijzen naar een oud domein, om ze naar een nieuw domein te laten verwijzen, zeer nuttig na de migratie van uw website van het ene naar het andere domein, of van de ene map naar de andere.
- E-mail notificatie bij een succesvolle beheerder back-end login (alleen in de Professional versie)
- Wachtwoordbescherming [password-protecting-admintools] voor elke combinatie van functies die u wilt beschermen, voordat u de website overdraagt aan uw klant
- Integratie met Joomla! 1.6 ACL en aangepast, per gebruiker ACL voor Joomla! 1.5

De gehele bundel is gelicentieerd onder de GNU General Public License (GPL) versie 3 of - naar uw keuze - iedere latere versie uitgegeven door de Free Software Foundation. In gewoon Nederlands betekent dit dat u het kan installeren op een onbeperkt aantal domeinen en voor zo lang als u wilt. We zijn ervan overtuigd dat vrijheid en veiligheid hand in hand moeten gaan om effectief te zijn.

Note

Tenzij anders vermeld, zijn de vermelde functies beschikbaar in zowel de Professional als de Core releases

1.1. Disclaimer

Beveiligingstoepassingen -als Admin Tools- zijn simpelweg ontworpen om de veiligheid van uw website te verbeteren, het is echter niet ten alle tijden onkwetsbaar voor hackpogingen. Het zal het echter wel veel moeilijker maken voor een potentiële aanvaller om informatie van uw site te verkrijgen, en het zal hen veel moeite kosten uw website te hacken, er is niets dat een volhardende cracker kan stoppen uw website te hacken. Als u bijvoorbeeld een verouderde Joomla! installatie heeft, of een kwetsbare component is geïnstalleerd op uw website, is er niets en, maar dan ook NIETS, dat een hacker kan stoppen een succesvolle aanval op uw website uit te voeren. We zijn ons ervan bewust

dat ook andere ontwikkelaars hun producten op de markt zetten als een "complete bescherming" voor uw website, dat is echter gewoon technisch onmogelijk.

Laat me proberen u een voorbeeld te geven. Denk aan een kogelvrij vest, gedragen door militair personeel over de hele wereld. Kunnen deze militairen nog steeds worden dood? Ja, dat kan. Terwijl het kogelvrije vest ze beschermt tegen de meest voorkomende aanvallen (directe schoten gericht op de romp) het zal hen echter niet beschermen tegen schoten die van zijwaarts komen, high-power close range schoten of explosies. Het is hetzelfde met beveiligingssoftware, het is niets anders dan een kogelvrij vest. Het zal meest voorkomende aanvallen blokkeren, maar kan niet alle aanvallen stoppen. Een vastberaden cracker is als een zelfmoordterrorist: als hij besluit je te pakken te nemen, er is er maar zoveel dat je kunt doen om jezelf te beschermen.

U bent uiteindelijk zelf verantwoordelijk voor de veiligheid van uw website, gebruik uw gezond verstand bij beveiligingszaken. Installatie en configuratie van Admin Tools is niets anders dan een dergelijke gezond verstand praktijk. Er wordt op zijn minst verwacht dat u regelmatig back-ups maakt, opgeslagen op een veilige locaties buiten uw server, en opletten voor afwijkend gedrag op uw website.

Tot slot, zijn wij wettelijk verplicht om uw aandacht te vestigen op de garantie en aansprakelijkheidsbepalingen, in de artikelen 15 tot en met 17 van de licentie van de software, voor uw gemak hier gekopieerd:

15. Disclaimer van de garantie.

ER IS GEEN GARANTIE VOOR HET PROGRAMMA, VOOR ZOVER TOEGESTAAN OP GROND VAN TOEPASSELIJK RECHT. BEHALVE WANNEER ANDERS BEPAALD OP SCHRIFT VAN DE AUTEURSRECHTHOUDERS EN/OF ANDERE PARTIJEN IS HET PROGRAMMA "ZOALS HET IS" ZONDER ENIGE GARANTIE, EXPLICIET OF IMPLICIET, INCLUSIEF, MAAR NIET BEPERKT TOT, DE GARANTIES VAN VERKOOPBAARHEID EN GESCHIKTHEID VOOR EEN BEPAALD DOEL. HET VOLLEDIGE RISICO MET BETREKKING TOT DE KWALITEIT EN DE PRESTATIES VAN HET PROGRAMMA LIGT BIJ GEBRUIKER. MOCHT HET PROGRAMMA DEFECTEN VERTONEN, DAN ZIJN DE KOSTEN VAN ALLE NOODZAKELIJKE ONDERHOUD, REPARATIE OF CORRECTIEVE HANDELINGEN VOOR REKENING VAN GEBRUIKER.

16. Beperking van aansprakelijkheid.

IN GEEN GEVAL, TENZIJ VEREIST IN HET TOEPASSELIJK RECHT OF SCHRIFTELIJK OVEREENGEKOMEN ZAL DE AUTEURSRECHTHOUDER, OF ENIGE ANDERE PARTIJ DIE HET PROGRAMMA WIJZIGT EN/OF UITBRENGT ALS HIERBOVEN TOEGESTAAN, AANSPRAKELIJK ZIJN VOOR SCHADE, INCLUSIEF ENIGE ALGEMENE, BIJZONDERE, INCIDENTELE SCHADE UIT HET GEBRUIK OF HET NIET KUNNEN GEBRUIKEN VAN HET PROGRAMMA (INCLUSIEF MAAR NIET BEPERKT TOT HET VERLIES VAN GEGEVENS OF HET ONNAUWKEURIG MAKEN VAN GEGEVENS OF VERLIEZEN GELEDEN DOOR U OF DERDEN OF HET NIET SAMENWERKEN VAN HET PROGRAMMA MET ANDERE PROGRAMMA'S), ZELFS ALS DE HOUDER OF EEN ANDERE PARTIJ OP DE HOOGTE IS GESTELD VAN DE MOGELIJKHEID VAN SCHADE.

17. Interpretatie van de artikelen 15 en 16.

Als de afwijzing van garantie en beperking van aansprakelijkheid als bovenstaande niet kan worden gegeven volgens lokale wettelijke effecten en hun voorwaarden, is herziening van rechterlijke instanties en de lokale wetgeving van kracht, een absolute verklaring van afstand van alle burgerlijke aansprakelijkheid die deze wetgeving het meest benadert in verband met het Programma, tenzij er een garantie of aanname van aansprakelijkheid een kopie van het Programma begeleidt in ruil voor een vergoeding.

1.2. De filosofie

Ik heb helaas vastgesteld dat sommige mensen mijn artikelen over beveiliging --de meesten van hen schreven meer dan een jaar voor Admin Tools zelfs maar zo veel als een aantekening in mijn kladblok was-- als hypocriet en een

nauwelijks verhulde poging om Admin Tools op de markt te zetten. Wat zeg je?! In tegenstelling tot de meeste mensen *Ik meen altijd wat ik schrijf en schrijf wat ik meen*. Als ik agressief de markt wilde betreden met Admin Tools, zou ik nooit een grondig beveiligingsartikel hebben geschreven, laat staan PHP en .htaccess code weg hebben geven zonder veiligheidsvraagstukken te hebben besproken. Ik zou de stappen van de antivirus jongens volgen, het verspreiden van angst, onzekerheid en twijfel bij de gebruikers, en gebruik maken van hun kwetsbare positie om ze op te lichten. In de loop der tijd heb ik echter meer dan bewezen dat ik niet dat soort persoon ben, daarom voel ik me gedwongen om hun lasterlijke en onrechtvaardige aanvallen tegen mijn jarenlange filosofie over software en informatie te beantwoorden.

Het ultieme goed in een functionele samenleving, is vrijheid. Gebruikers hebben recht op vrijheid van keuze, dat is waarom ik Vrije en Open Source Software maak. Gebruikers hebben recht op gratis toegang tot kennis, dat is waarom ik artikelen schrijf en ze beschikbaar maak onder een vrije of publieke domein licentie.

Dit zijn de twee basisingrediënten van mijn filosofie als professionele ontwikkelaar en lange tijd lid van de FOSS beweging. Admin Tools is niet de bedoeld als de enige ware manier om dit soort beveiligingsverbeteringen in Joomla! te bereiken. Feitelijk, heb ik alle functionaliteit uitgebreid in diverse artikelen en blogs gedocumenteerd, en heb ik geschreven in het Joomla! Community Magazine en op mijn eigen site. Al mijn artikelen dateren van vóór de integratie van deze functies binnen Admin Tools. Admin Tools is een software product dat streeft naar het automatiseren van die vervelende taken, waardoor niet technische gebruikers op hetzelfde niveau van beveiliging staan als de meer technisch onderlegden onder ons. Het tegenovergestelde van wat in Wiki pagina berichten vol met vage adviezen staat. Ik geef gebruikers de vrijheid om te kiezen, en zal ze die vrijheid nooit ontnemen. Als u de Professional versie niet wilt kopen, is alles wat u moet weten gedetailleerd beschreven op het open Internet door ondergetekende. Er zijn ook concurrerende oplossingen die verschillende stukjes van de Admin Tools functionaliteit hebben, maar die zijn ook veel duurder dan de gratis Admin Tools Core release. Bovendien, streef ik ernaar om Admin Tools te verrijken met voorgestelde functies door u, de gemeenschap van Joomla! gebruikers en ontwikkelaars, dat is waar de meeste van de nieuwe functies vanaf versie 1.1 uit voortkomen. Als u Admin Tools helemaal niet wilt gebruiken, zelfs de eeuwig vrije Core release, vind ik dat ook prima, de instructies om hetzelfde niveau van bescherming te bereiken is altijd daar.

Nu weten u het allemaal en —hopelijk— kunt u vertellen wat marketing is en wat een oprechte betrokkenheid bij het helpen van de wereldwijde gemeenschap van Joomla! gebruikers is.

Peace.

2. Server omgevingseisen

Om te kunnen werken, vereist Admin Tools de volgende server software omgeving:

- Joomla!™ 1.5.0 of later in de 1.5.x reeks. Het is een native component; het heeft geen Legacy modus nodig, maar kan er wel mee werken als het is ingeschakeld.
- PHP 5.2.9 of hoger. Het werkt niet met PHP 4!
- MySQL 4.1 of hogerr. MySQL 5.0 of hoger is aanbevolen voor optimale prestaties.
- Minimaal 16Mb PHP `memory_limit`. Meer is beter.
- De PHP functie `opendir` moet aanwezig zijn.
- De cURL PHP module of fopen() URL wrappers moeten geïnstalleerd zijn om Joomla! update te kunnen laten werken.

Wat de gebruikte browser betreft kunt u de volgende gebruiken:

- Internet Explorer 7, of hoger
- Firefox 3.5, of hoger

- Safari 4, of hoger
- Opera 10, of hoger
- Google Chrome 5 of hoger

In ieder geval moet u ervoor zorgen dat Javascript is ingeschakeld in uw browser, voor de goede werking van de component.

3. Admin Tools Installeren

3.1. Normale installatie

Het installeren van Admin Tools is niet anders dan het installeren van elke andere Joomla!™ extensie op uw website. U kunt de volledige instructies voor het installeren van Joomla!™ extensies lezen op de officiële help pagina [http://help.joomla.org/content/view/1476/235/]. In dit hoofdstuk gaan we ervan uit dat u bekend bent met deze instructies en we zullen ze niet dupliceren.

U kunt de nieuwste installatie pakketten downloaden door het bezoeken van onze website op http://www.akeebabackup.com. Gebruik de Download link in de bovenste werkbalk om de pagina van de officiële releases te openen en zoek het Admin Tools pakket. Klik op "View Releases" en u krijgt een lijst met alle up-to-date releases. Klik op de "View files" van de laatste release om de lijst met bestanden te bekijken. Zoek het item dat u wilt downloaden en klik op "Download file". Pak de ZIP bestanden niet uit!

Log in op uw websites back-end Administrator sectie. Klik op de Extensies, Installeer/Deïninstalleer (Joomla! 1.5) link in het top menu. In deze pagina, vind de Bladeren knop in het Upload Pakket Bestand gebied. Zoek het installatiepakket ZIP bestand dat u eerder had gedownload en selecteer het. Terug op de pagina, klikt u op de Upload Bestand & Installeer knop. Na een korte pauze zal Joomla!™ u vertellen dat de component, de module en de plugin zijn geïnstalleerd.

Als u Admin Tools niet kunt installeren en u ziet berichten over onschrijfbare mappen, het onvermogen om bestanden te verplaatsen, of andere gelijkaardige bestandssysteem gerelateerde foutmeldingen, aarzel dan niet ons om ondersteuning te vragen. Deze fouten komen voort uit uw website instellingen en kan het best worden opgelost door om hulp te vragen in de officiële Joomla!™ forums [http://forum.joomla.org]. (Engels talig) Als u echter, een lege pagina krijgt, een Internal Server Error pagina of een time-out foutmelding, dan kunt u naar de handmatige installatie sectie van deze documentatie gaan.

Zorg ervoor dat de plg_admintools (System - Admin Tools) plugin is geïnstalleerd en gepubliceerd. Zonder, zal de Web Applicatie Firewall functie en een aantal andere aspecten van de component niet werken. Normaal moet deze plugin worden geïnstalleerd en geactiveerd tijdens de installatie van Admin Tools Professional. Feitelijk, wordt de installatie status van Admin Tools' plugin en de module weergegeven na de installatie van de bundel. Als de plugin niet is geïnstalleerd, zult u gewaarschuwd worden als u probeert een eigenschap van het component configureren die op de plugin rust.

3.2. Handmatige installatie

Soms is Joomla!™ niet in staat om ZIP archieven goed uit te pakken, dit is te wijten aan technische beperkingen op uw server. In dat geval kunt u de handmatige installatie procedure volgen.

Eerst moet u het installatie ZIP bestand uitpakken in een submap met de naam `admintools` op uw lokale PC. Then, upload the entire subdirectory inside your site's temporary directory. At this point, there should be a subdirectory named `admintools` inside your site's temporary directory which contains all of the ZIP package's files.

Als u niet zeker weet waar de tijdelijke map van uw website zich bevind, kunt u die opzoeken in de Algemene instellingen, klik op de Server tab en kijk naar de Pad naar temp-map instelling. De standaard instelling is de `tmp` map

onder de root van uw site. Zelden, vooral op geautomatiseerde installaties met behulp van Fantastico, zou het een systeemwijd toegewezen `/tmp` map kunnen zijn. Neem in dit geval contact op met uw host voor instructies, over hoe bestanden te uploaden in deze map, of over het wijzigen van de locatie van uw tijdelijke Joomla!™ map, terug naar de standaard locatie en het schrijfbaar maken van deze map.

Ervan uitgaande dat u deze uploaden stap gehad heeft, klikt u op de Extensies, Installeer/Deïnstalleer (Joomla! 1.5) of Extensies, Manager (Joomla! 1.6) link in het top menu. Op deze pagina, zoekt u de Installeer map edit box in the Installeer vanuit map sectie. Het veld is al ingevuld met het absolute pad naar uw tijdelijke map, bijvoorbeeld `/var/www/joomla/tmp`. Voeg hier `/admintools` toe. Uitgaande van ons voorbeeld, moet het er ongeveer zo uitzien `/var/www/joomla/tmp/admintools`. Klik vervolgens op de Installeer knop.

Als u nog steeds Admin Tools niet kunt installeren en u krijgt foutmeldingen over onschrijfbaar mappen, of het niet kunnen verplaatsen van bestanden of andere gelijkaardige bestandssysteem gerelateerde foutmeldingen, vraag ons dan niet om ondersteuning. Deze fouten komen voort uit uw website opzet en kan het best worden opgelost door om hulp te vragen op de officiële Joomla!™ forums [http://forum.joomla.org].

Zorg ervoor dat de plg_admintools (System - Admin Tools) plugin is geïnstalleerd en gepubliceerd. Zonder, zal de Web Applicatie Firewall functie en een aantal andere aspecten van de component niet werken. Normaal moet deze plugin worden geïnstalleerd en geactiveerd tijdens de installatie van Admin Tools Professional. Feitelijk, wordt de installatie status van de Admin Tools plugin en de module weergegeven na de installatie van de bundel. Als de plugin niet is geïnstalleerd, zult u gewaarschuwd worden zodra u probeert enige eigenschap van het component, die steunt op de plugin, te configureren.

4. Snelle Setup

Important

Dit gedeelte is alleen van toepassing op Admin Tools Professional en heeft uitsluitend betrekking op de beveiligingsfuncties

De fundamentele functionaliteit van Admin Tools Professional is uw website beveiligen. Echter, bij het opzetten van uw website beveiliging is wat tweaken vereist, omdat de ene website andere structuren en behoeften heeft dan de andere. Wanneer u voor het eerst Admin Tools Professional installeert kunt u het gevoel krijgen een beetje overdonderd te worden door de overvloed aan beveiligingsinstellingen. Het goede nieuws echter is dat het opzetten ervan nog niet half zo moeilijk als het lijkt! In deze uitleg gaan we door de basis veiligheidsconfiguratie en wijzen u stap voor stap de weg naar wat te doen.

Ga naar de back-end van uw website en klik op Componenten, Admin Tools, Web Applicatie Firewall, Instellingen en stel de volgende optionele instellingen in:

1. Administrator geheime URL parameter Als u hier "foobar" (zonder de aanhalingstekens) invoert, dan moet u om toegang tot uw website backend te krijgen de volgende URL gebruiken `http://www.example.com/administrator?foobar` dat wil zeggen, voeg een vraagteken en het geheime woord toe. Als u het ?foobar deel niet gebruikt, krijgt u de login pagina niet te zien maar eindigd u altijd op de voorpagina van de site.

2. Geef uw e-mail adres op in de secties E-mail naar dit adres bij een succesvolle back-end login en E-mail naar dit adres bij mislukte administrator login. Admin Tools zal u een e-mail sturen als iemand probeert in te loggen op uw site back-end als een Super Administrator. Het moment waarop u een e-mail ontvangt die niet werd veroorzaakt door een vertrouwd persoon, weet u dat u uw site zo snel mogelijk off-line moet halen. Let wel dit is een zeer nuttige functie! Het zal u een email sturen, zelfs in het onwaarschijnlijke geval dat iemand, bijvoorbeeld, uw WiFi hacked, uw login cookie steelt, en vervolgens uw eigen WiFi verbinding en de login cookie gebruikt om op uw website in te loggen.

3. Stel Verbergen / Aanpassen generator metatag in op `Ja` en geef iets ongewoons in het Genereer een eigen metatag veld in. Ik zet daar meestal iets gekscherends als "Drumlapress" in, dit om te vertroebelen welke CMS ik echt ge-

bruik. Wees creatief en verzin iets aparts! Dit is een lage prioriteitsaanpassing, maar stopt "dork scanning" aanvallen. Ik bedoel dat Joomla! normaal haar naam kenbaar maakt in de (verborgen) generator metatag van elke HTML pagina op uw website. Een aanvaller zoekt naar "dorks" (te compromitteren websites), door te zoeken naar "Joomla! 1.5" op Google. Deze functie verwijdert de generator tag en u bent niet langer gevoelig voor dit soort aanvallen.

4. Vergelijkbaar met het bovenstaande, zet iets in het X-Inhoud codering door HTTP header inhoud voor gzip compressie veld, maar zorg ervoor dat u alleen alfanumerieke tekens gebruikt, dat wil zeggen, gebruik az, AZ en 0-9 zonder spaties. Waarom? Net als Joomla! zijn naam verraad in de metatag, gebeurt er hetzelfde in de HTTP headers wanneer uw website van GZip compressie gebruik maakt. Het instellen van deze optie vervangt de standaard HTTP header. Maak er iets onduidelijk van, zoals "MonkeyWithACaliper" of iets dergelijks.

   ## Note

   Deze functie kan mogelijk niet goed werken met Joomla! 1.5. Dit is een beperking van deze Joomla! versie onder een aantal server omgevingen en website instellingen.

5. Ook PHP heeft een grote mond en profileert zich in de HTTP headers. Dit kan worden gebruikt door aanvallers om op betrouwbare wijze uit te vinden of u een verouderde versie van PHP gebruikt en een aanval op maat lanceren tegen uw website. Stel de X-Gedreven HTTP header voorrang geven (PHP kan als leeg worden getoond) naar iets onduidelijks. Ik gebruik meestal "LotsOfCaffeine" of iets anders cafeïne gerelateerd - u weet wel, een beetje geek humor.

6. Optioneel, maar zeer aan te bevelen, ga naar http://www.projecthoneypot.org/httpbl_configure.php en open een eigen Project Honeypot account. Na uw registratie, bezoekt u opnieuw de URL en u zult een zogenaamde "HTTP:BL key" zien. Kopieer die en plak hem in het Admin Tools Project Honeypot HTTP:BL Key veld. Zet ook HTTP:BL filtering inschakelen op Ja. Waarom? Project Honeypot analyseert de gegevens van een groot aantal sites en identificeert IP adressen die momenteel worden gebruikt door hackers en spammers. Deze Admin Tools functie integreert met Project Honeypot, en onderzoekt de IP adressen van uw bezoekers. Als ze op de zwarte lijst (bekende hacker of spammer) voorkomen, worden ze geblokkeerd voor toegang tot Joomla!.

7. Optioneel, maar zeer aan te bevelen, schakel de IP blokkering van recidivisten in. Deze functie blokkeert IP adressen die herhaalde veiligheidsuitzonderingen op uw website genereren, dat wil zeggen dat er sterke redenen zijn om te vermoeden dat het hier om hackers gaat. Houdt u er rekening mee deze functie niet eerder in te schakelen totdat u zeker weet dat alles soepel loopt, zodat u niet per ongeluk uzelf blokkeert van uw website. Als dat toch gebeurt, kijk dan op https://www.akeebabackup.com/documentation/troubleshooter/atwafissues.html voor meer uitleg (Engels talig).

Een ander ding dat u kunt doen is naar Componenten, Admin Tools, .htaccess Maker gaan en klikken op Opslaan en .htaccess aanmaken. Als u een lege pagina of een '500 Internal Server Error' op uw site krijgt, gebruik een FTP cliënt om het `.htaccess` bestand te verwijderen (als het bestand niet zichtbaar is, upload dan een leeg tekst bestand met de naam `.htaccess`), ga terug naar .htaccess Maker, probeer een aantal opties uit te schakelen en herhaal het hele proces tot uw site weer correct laadt. Voor meer informatie over dit onderwerp, kijk op https://www.akeebabackup.com/documentation/troubleshooter/athtaccess500.html (Engels talig).

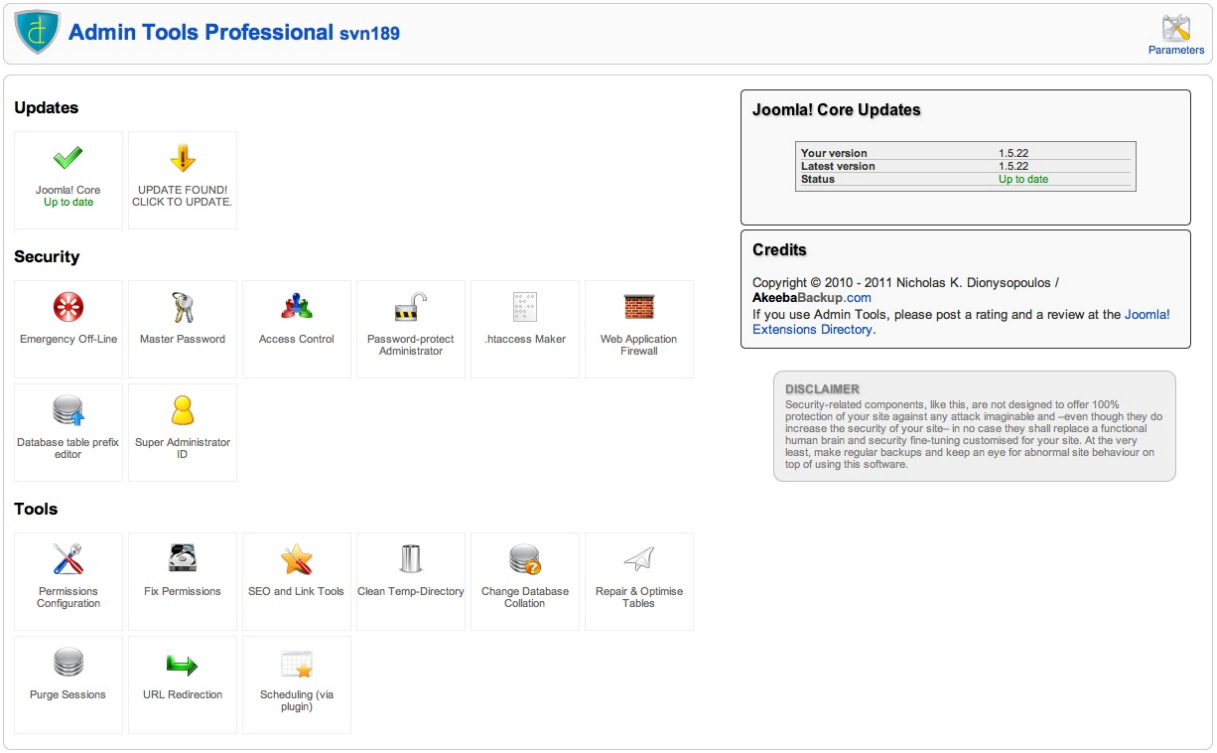
Na het toepassen van al de bovenstaande beveiligingen, is het zeer waarschijnlijk dat een deel van de functionaliteit van uw website niet meer werkt. Dit is normaal. De standaard instellingen zijn zeer restrictief door het ontwerp. Probeer op elke pagina met een probleem, eerst het toepassen van het stap voor stap proces, beschreven in https://www.akeebabackup.com/documentation/troubleshooter/athtaccessexceptions.html (Engels talig).

Als u ergens vastloopt, voel u vrij om op ons support forum te posten of, als u een AKEEBADELUXE abonnement heeft, maak dan een support ticket. Wij zijn hier om te helpen!

Chapter 2. Admin Tools Gebruiken

1. Het Controle Paneel

De hoofdpagina van de component die je toegang geeft tot alle functies wordt het Controle Paneel genoemd.



Het Controle Paneel is verdeeld in twee gebieden, het linker bedieningspaneel met pictogrammen en het rechter met informatie boxen.

In het linker gedeelte heeft u pictogrammen, die de afzonderlijke tools waaruit Admin Tools bestaat, wanneer erop wordt geklikt zullen starten. Elk van deze tools is beschreven in een afzonderlijk deel van deze documentatie.

Klikken op de Instellingen (via plugin) knop, start de System - Admin Tools plugin configuratie pagina in een pop-up dialoog venster. Daarin, kunt u de planning voor Admin Tools hulpprogramma's instellen. Let wel, deze functie is alleen beschikbaar in de Professional editie.

Het Joomla! Core update statuspictogram schakelt tussen een groen vinkje, een uitroepteken/waarschuwingspictogram en een recycle pictogram. Een groen vinkje betekent dat uw website al de nieuwste versie van de Joomla! core heeft geïnstalleerd en er geen verdere actie nodig is. Een uitroepteken betekent dat er een nieuwere versie van de Joomla! core beschikbaar is dan degene die geïnstalleerd is, u dient dan onmiddellijk te upgraden door er op te klikken. Als het verandert in een recycle pictogram, betekent dit dat Admin Tools niet in staat was om de nieuwste vrijgeven informatie van de Joomla! core van de JoomlaCode.org servers op te halen. In dit geval moet u Joomla! handmatig bijwerken op uw website. Meestal kunt u aan uw host vragen hun firewall te openen, zodat uw site de JoomlaCode.org servers via standaard HTTP (poort 80) kan bereiken en de functionaliteit van deze functie kan herstellen.

The topmost right hand information pane displays the Joomla! core update status. "Your version" is the Joomla! version installed on your site. "Latest version" is the latest version of the Joomla! core available for download. "Status", as the name implies, denotes the update status of your Joomla! installation. When it's up to date you don't have to do

anything else. If it notes that an update was found, click on the Joomla! Core update status icon to immediately upgrade to the new release.

Daaronder is er het Credits deelvenster met informatie over deze software. Als u deze software nuttig vind, overweeg dan het doneren van een klein bedrag om de ontwikkeling op gang te door, te klikken op de "PayPal doneren" knop (zichtbaar in de Admin Tools Core release). Uw giften worden veilig afgehandeld door PayPal. We zouden het ook op prijs stellen als u een review in de Joomla! Extensions Directory lijst, over Admin Tools zou willen plaatsen. Volg hiervoor de desbetreffende link in dit venster.

2. Joomla! Updaten

Ongetwijfeld, is één van de meest elementaire website onderhoudswerkzaamheden, die een sterke invloed op de veiligheid heeft, het up-to-date houden van uw Joomla! installatie. Vroeger was dit een vervelende klus: U moest noteren welke Joomla! versie u gebruikte en naar http:// joomla.org/download.html om de laatste versie te vinden en te vergelijken met uw huidige versie. Als er een update was, moest een lange download voor het update-pakket van de Joomla! site halen, lokaal uitpakken, alle bestanden uploaden via FTP en controleren of alles goed werkte. Vermenigvuldigd met tientallen sites beheerd door één enkele sitebouwer, kan dit al snel op een onderhoud nachtmerrie uitlopen. Nu niet meer.

De Admin Tools, Joomla! core update functie maakt het mogelijk deze vervelende procedure te automatiseren. Niet alleen detecteert het de laatste versie en doet de versie vergelijking voor u, maar ook kunt u eerst een back-up maken (optioneel, alleen beschikbaar als Akeeba Backup 3.1 of hoger is geïnstalleerd) en dan uw core installatie upgraden met één enkele klik. Als u denk dat uw core bestanden zijn gecompromitteerd, dan kunt u ze altijd opnieuw overschrijven met een nieuw exemplaar, met ons makkelijk te gebruiken één klik proces.

Important

Admin Tools moet joomlacode.org kunnen bereiken om deze functie te laten werken. Als het een foutmelding geeft die u vertelt dat u Joomla! handmatig moet upgraden, dan kunt u contact opnemen met uw host en hem vragen om poort 80 verbindingen op hun firewall open te zetten voor joomlacode.org. Zorg er ook voor dat uw server ofwel de PHP curl module geïnstalleerd en geactiveerd (bij voorkeur) heeft, of het gebruik van de fopen() URL wrappers toe te staan. Als u niet zeker bent, vraag het dan uw host.

Wanneer u de Joomla! core update tool van Admin Tools start wordt u naar de onderstaande pagina gebracht:

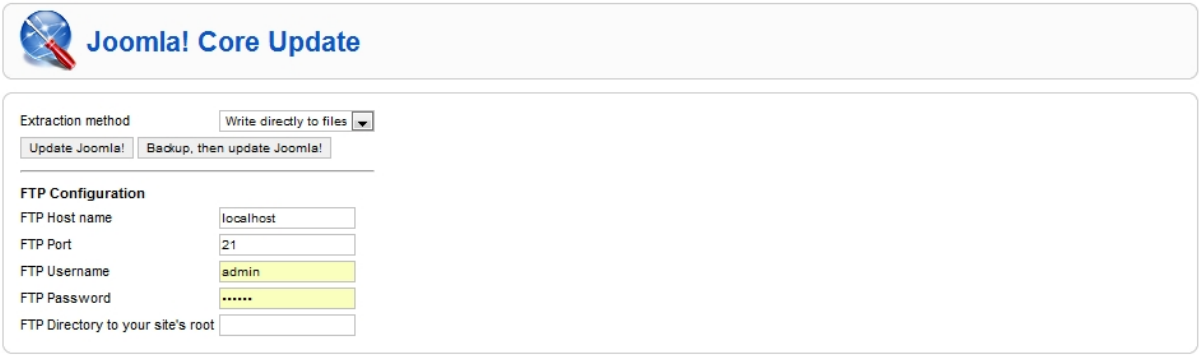
In dit voorbeeld ziet Admin Tools dat de website draait op Joomla! 1.5.15 en de nieuwste versie is 1.5.20. Het geeft u twee opties:

- Upgrade naar 1.5.22. Dit zal het "Stable Patch" pakket downloaden en installeren dat alleen de bestanden aanpast tussen de geïnstalleerde en de nieuwste versie. Dit is de aanbevolen aanpak om een bestaande website te upgraden.
- Herinstalleer 1.5.22. Dit zal het volledige installatie pakket van de meest recente release downloaden en installeren, en alle Joomla! core bestanden overschrijven. Dit is niet aanbevolen, tenzij u een sterke aanwijzing heeft dat er iets

fout is met uw Joomla! core bestanden, bijvoorbeeld bestanden ontbreken of u heeft een vermoeden dat uw website gehacked is. In het laatste geval, is het opnieuw installeren van de core bestanden niet voldoende, je is ook een beveiligingsverificatie van uw website noodzakelijk.

Uiteraard, als er geen update beschikbaar is bijvoorbeeld als u de nieuwste versie al heeft, is alleen de Herinstalleer knop zichtbaar.

Klikken op één van deze knoppen start het downloaden van het desbetreffende installatie pakket. Zodra de download is voltooid, wordt de pre-installatie pagina weergegeven:



De Extractie methode optie bepaalt hoe Admin Tools gaat proberen uw back-up archiefbestanden te overschrijven. De Schrijf direct naar bestanden optie zal proberen om PHP direct de bestanden te laten overschrijven. Dit zal bij de meeste shared hosts niet werken. Daarom raden we aan gebruik te maken van de tweede optie, Upload via FTP, wat gebruik zal maken van FTP om de bestanden te overschrijven. In dit geval moet u de volgende informatie invullen in het onderste deel van de pagina:

FTP Host naam — De host naam van de FTP server van uw website, zonder het protocol. Bijvoorbeeld: `ftp.voorbeeld.com` is *geldig*, `ftp://ftp.voorbeeld.com` is *ongeldig*.

FTP Port — De TCP/IP port van de FTP server van uw website. De standaard waarde is 21. Gebruik alleen een andere instelling als uw host expliciet een niet standaard poort opgeeft.

FTP Gebruiker-snaam — De gebruikersnaam om verbinding te maken van de FTP server.

FTP Wachtwoord — Het wachtwoord om verbinding te maken van de FTP server.

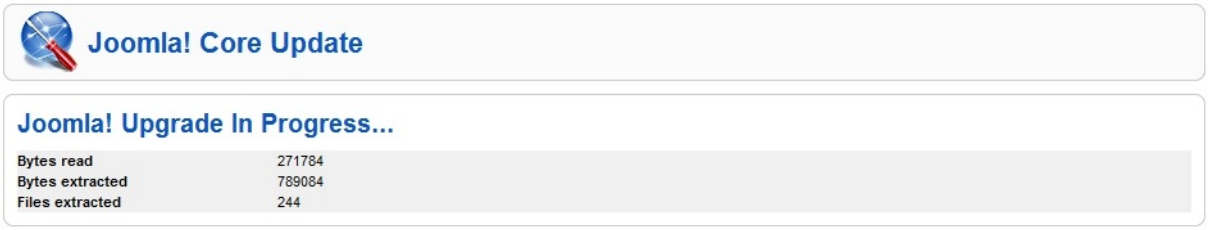
Hoofdmap — De FTP map naar root van uw website. Dit *is niet hetzelfde als de bestandssysteem map* en kan niet automatisch worden bepaald. De eenvoudigste manier om dit te bepalen is om verbinding te maken met uw website met uw favoriete FTP cliënt, zoals FileZilla. Navigeer binnen de root van uw website map. U weet dat u er bent als u de `configuration.php` en mappen zoals `administrator`, `component`, `language`, `includes`, `cache` and `xmlrpc` in die map ziet. Kopieer (in FileZilla het verschijnt op de rechter kolom, boven de map structuur) en plak dat pad in de Akeeba Backup instelling.

Zodra u klaar bent om uw website te upgraden, hwwft u twee opties om dat te doen:

- Update Joomla! zal de update meteen starten.
- Backup, en update Joomla! is alleen beschikbaar als u Akeeba Backup Core of Akeeba Backup Professional, versie 3.1 of hoger heeft geïnstalleerd op uw website. Door op deze knop te klikken wordt u doorgestuurd naar de Backup Nu pagina. U kunt, eenmaal daar het back-up profiel selecteren en de back-up starten. Zodra de back-up is voltooid, zal Akeeba Backup u automatisch terug sturen naar Admin Tools, dat het herstel zal starten. Met deze functie wilden

we ervoor zorgen dat een back-up en dan het upgraden van uw website in slechts twee muisklikken nodig heeft en u er verder niet bij hoeft na te denken.

Wanneer het herstel begint, wordt u de update voortgang getoont:



U kunt zien hoe veel van het installatie pakket is verwerkt (Bytes gelezen), hoeveel gegevens zijn naar de schijf geschreven (Bytes uitgepakt) en ten slotte, hoeveel bestanden er tot nu toe zijn uitgepakt (Bestanden uitgepakt).

Als de update voltooid is dan wordt u doorgestuurd naar het Admin Tools Controle Paneel. Het Joomla! updaten pictogram van Admin Tools verandert in een groen vinkje, en eronder staat "Up-to-date", om aan te geven dat uw Joomla! core nu is bijgewerkt.

Wat te doen bij een foutmelding over een niet compleet of beschadigd archiefbestand?

Als u deze foutmelding krijgt tijdens het bijwerken van de Joomla! core, staat uw server het correct downloaden van het upgrade pakket niet toe. In dit geval gebruik de link naar het Joomla! upgrade pakket in de "Joomla! Core update" pagina om het archiefbestand te downloaden. Upload het daarna naar de tijdelijke map van uw website (zoals gedefinieerd in de Algemene server instellingen van uw site back-end Controle Paneel). Door dit te doen, zal Admin Tools detecteren dat u het handmatig het update-pakket heeft gedownload en zal het niet proberen opnieuw te downloaden wanneer u op de Upgrade knop klikt.

In het geval dat de toegang tot uw site niet mogelijk is na een onderbreking in het update-proces, geen paniek. Ga naar http://joomla.org/download.html en download het nieuwste upgrade pakket. Pak het lokaal uit, upload alle uitgepakte bestanden naar uw website, overschrijf de reeds bestaande bestanden. Dit is het handmatige upgrade proces en zou moeten werken.

Wat moet ik instellen op mijn server om Admin Tools toe te staan de update informatie en upgrade pakketten te downloaden?

U moet ofwel de cURL PHP module geïnstalleerd en geactiveerd, of URL fopen() wrappers hebben. Vraag uw host of ze één van deze opties vrijgeven. Verder moet uw host TCP/IP verbindingen via poorten 80 en 443 toestaan om `joomlacode.org` en `akeebabackup.com` te kunnen benaderen. Bij twijfel, vraag het uw host. De meeste hosts hebben een firewall in gesteld en zij zullen uitzonderingen moeten instellen op uw verzoek om Admin Tools 'update functies goed te laten werken.

Important

Op Windows hosts raden wij het installeren en activeren van de cURL module aan.

Tot slot, zal Admin Tools proberen in de temp map van uw website een schrijfbare submap te creëren, dit is echter niet altijd mogelijk. We raden in ieder geval het hebben van een schrijfbare tijdelijke map aan. Als uw host suPHP

draait is alles wat u moet doen, de permissies van die tijdelijke map op 0755 zetten. U kunt ook één van de volgende alternatieven volgen.

Het eerste alternatief (makkelijker, maar niet aangeraden) is om uw tijdelijke map 0777 permissies te geven. Echter, omdat dit nadelige gevolgen kan hebben voor de veiligheid van uw website, raden we het uploaden van een .htaccess bestand via FTP in deze map aan met de volgende inhoud:

```
order deny, allow
deny from all
allow from none
```

Geef dit bestand 0644 permissies als het is geüpload. Op deze manier is de tijdelijke map world writable gemaakt, maar niet toegankelijke vanaf het web, zodat potentiële hackers niet de "lax permissies exploid" kunnen benutten om uw website aan te vallen.

Het tweede alternatief is veiliger, maar ook meer rommelig. Begin met de "algemene server instellingen" van uw site back-end Controle Paneel en zorg ervoor dat het pad naar de tijdelijke map naar de tmp map van uw website wijst. Let wel, u moet het absolute pad weten naar de map. Als u het niet zeker weet, kunt u het eenvoudig bepalen. Plaats een bestand genaamd `temppath.php` in de root van uw website met de volgende regel als de enige inhoud:

```
<?php echo dirname(__FILE__).DIRECTORY_SEPARATOR.'tmp'; ?>
```

U kunt het benaderen met uw browser, type bijvoorbeeld `http://www.voorbeeld.com/temppath.php`, en het zal het absolute pad naar uw tijdelijke map in een webpagina tonen. Vergeet niet om dit bestand daarna te verwijderen!

Nadat u deze stap gehad heeft, gebruik dan uw FTP cliënt om de `tmp` map volledig te verwijderen van uw website. Installeer daarna Joomla! eXtplorer [http://extensions.joomla.org/extensions/core-enhancements/file-management/2630] en maak een nieuwe `tmp` map in de root van uw website. Als dit niet werkt, kunt u uw host te vragen hoe u uw websites root map tijdelijk "world-writable" kunt maken om die map te creëren. Uw host kan klagen over de veiligheid redenen. Verwijs hem dan naar deze paragraaf. U hoeft de websites root map alleen voor een beperkte tijd schrijfbaar te maken, net lang genoeg om de nieuwe Temp map aan te maken, en vervolgens de permissies op meer veilige instellingen te zetten.

Aangenomen dat u deze map aangemaakt heeft, is die nu eigendom van uw web server gebruiker en is beschrijfbaar. Tot slot, om veiligheidsredenen, wilt u wellicht ook een nieuw .htaccess bestand in die map plaatsen die u met eXtplorer kunt creëren, met de volgende inhoud:

```
order deny, allow
deny from all
allow from none
```

3. De permissies van bestanden en mappen instellen

Zoals elke website beheerder weet, zijn bestanden en mappen permissies de eerste poortwachter op weg naar een gehackte website. 0777 permissies op uw website hebben, is een grote fout en kan fataal zijn voor uw website. Voor meer informatie, lees my blog post [http://www.dionysopoulos.me/blog/777-the-number-of-the-beast] (Engels). In een ideale situatie moet u slechts 0755 permissies voor uw mappen en 0644 voor uw bestanden hebben.

Bij andere gelegenheden, zijn we allemaal wel eens tegen verkeerd geconfigureerde servers aangelopen die nieuw aangemaakte bestanden en mappen onpraktische permissies geeft, bijvoorbeeld 0600. Dit heeft het directe effect dat nieuwe geüploade of aangemaakte bestanden niet toegankelijk zijn vanaf het web. Herstellen van deze permissies is een vervelende klus, op jacht naar de bestanden met FTP en het handmatig veranderen van die permissies. Soms wordt

dit zo vervelend dat we in de verleiding komen om gewoon 0777 permissies geven om alles gedaan te krijgen. Een grote, en fatale vergissing.

De oplossing voor deze permissie problemen is de Herstel Map en Bestandspermissie tool van Admin Tools. Haar missie is zo eenvoudig als maar kan, het zal al uw mappen 0755 permissies en al uw bestanden 0644 permissies geven. Uiteraard heeft dit alleen effect op Linux, Mac OS X, Solaris en andere hosts op basis van UNIX-afgeleide Operating Systems, dat wil zeggen alles behalve servers, draaien op Windows. Als u op een shared host zal u waarschijnlijk Joomla!'s FTP layer willen inschakelen in de Algemene instellingen in de back-end van uw website. Admin Tools zal detecteren dat en wanneer het een bestand of map tegen komt waarvan de permissies niet kunnen worden veranderd door PHP het gebruik zal maken van FTP om deze taak uit te voeren.

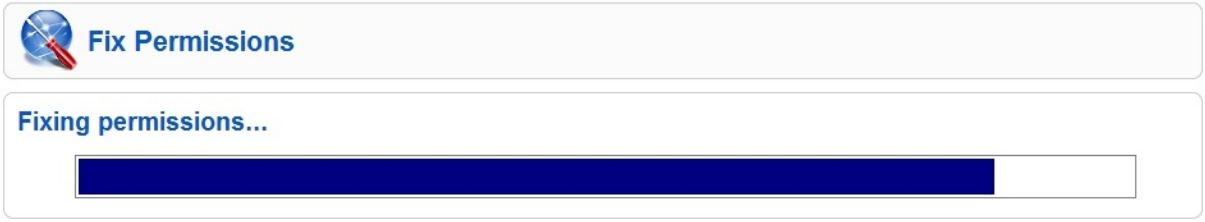
Note

U kunt de rechten per map en het bestand aanpassen met behulp van de Permissie instellingen pagina.

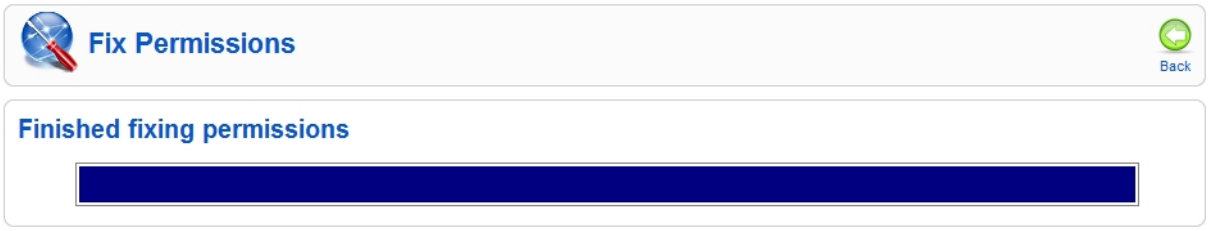
Warning

Het is mogelijk dat -als u de verkeerde soort permissies in Permissie instellingen pagina selecteert- u wordt buitengesloten van uw website en niet meer in staat bent toegang te krijgen via FTP of uw hosting paneel bestandsbeheer. Als dit gebeurt, neem dan contact op met uw host en vraag hem om de permissie problemen van uw website op te lossen.

Wanneer u klikt op de Herstel Map en Bestandspermissies tool ziet u het "Permissies herstellen..." pop-up venster met een voortgangsbalk, die zich vult als Admin Tools de permissies van al uw mappen en bestanden herstelt.



Als de voortgangsbalk is volgelopen, verandert de titel van de pagina in "Permissies herstellen voltooid":



Klik op de Terug knop om terug te keren naar de Controle Paneel pagina.

Waarom zijn er geen permissies veranderd op mijn web-site?

Het is een kwestie van eigendom. Als u bij een host zit die geen gebruik maakt van suPHP, zijn uw bestanden en mappen eigendom van een andere gebruiker dan waar uw webserver onder draait (bijvoorbeeld de apache server van uw host). Het enige wat u dan moet doen is naar de Algemene instellingen pagina van de back-end van uw website gaan, en uw FTP gegevens invoeren en de FTP functie van Joomla! inschakelen. Admin Tools zal het volgende keer dat u probeert permissies te herstellen oppakken en automatisch gebruik maken van de FTP modus wanneer het niet direct permissies kan wijzigen.

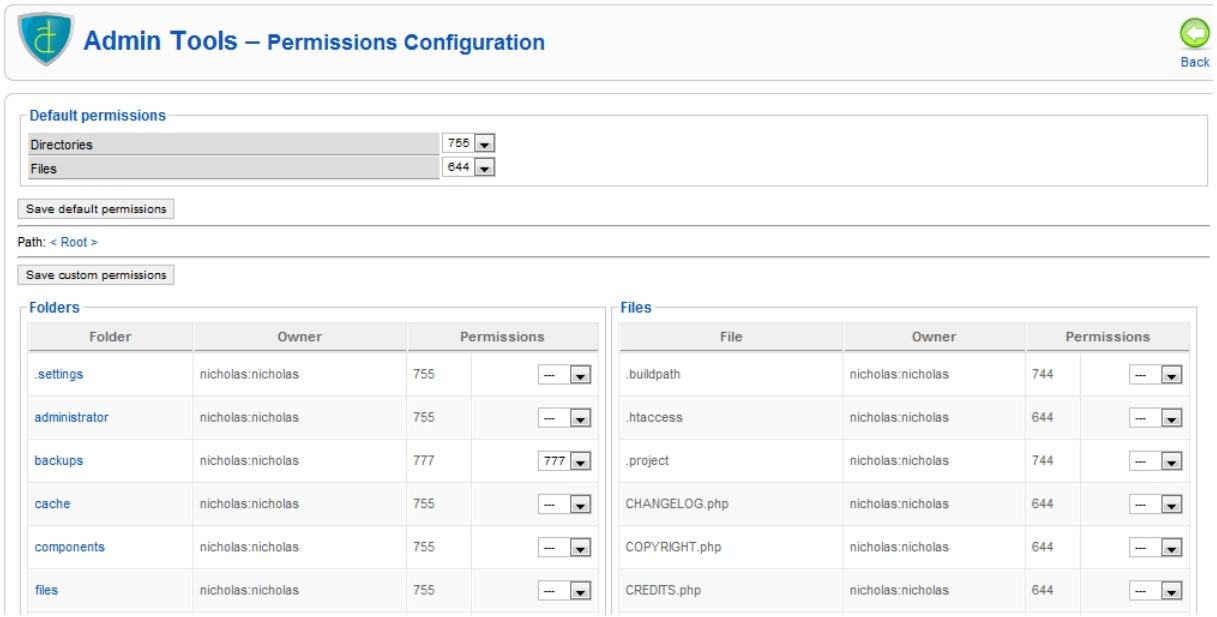
Ik zie veel JFTP foutmeldingen in een rode achtergrond tijdens dat proces. Wat is er mis?

Admin Tools, zoals uitgelegd in de bovenstaande paragraaf, probeert de FTP modus te gebruiken wanneer het niet direct de permissies kan wijzigen. Om deze truc te laten werken, moet uw FTP server het CHMOD commando ondersteunen. Niet alle servers doen dat echter, vooral servers die draaien op Windows, waar geen notie van permissies is. Als u deze lange lijst van JFTP Bad Response berichten krijgt, raadpleeg dan uw host en vraag of hun FTP server het CHMOD commando ondersteunt.

Ten slotte plaatsen sommige hosts mappen in uw web root, die niet bedoeld zijn om direct voor u toegankelijk te zijn, dat wil zeggen een `cgi-bin` of een `stats` map. U kunt de permissies van deze mappen niet veranderen als gevolg van hun eigendom (ze zijn meestal eigendom van een gereserveerde systeem gebruiker of de root gebruiker) en zullen leiden tot een paar JFTP foutmeldingen. Dit is normaal en u hoeft zich daarover geen zorgen te maken.

3.1. Permissies van bestanden en mappen configureren

Standaard zal Admin Tools 0755 permissies voor al uw mappen en 0644 permissies voor al uw bestanden toepassen. Dit is echter niet altijd wenselijk. Soms wilt u configuratiebestanden alleen lezen (0400 of vergelijkbare permissies) maken of een map wijd open (0777) permissies geven. Hoewel dit niet wordt aanbevolen, kan het de enige optie zijn op een aantal shared hosts om een aantal extensies te laten werken. Het meest opvallend is, dat een aantal extensies in staat moeten zijn content aan bestanden toe te voegen —Akeeba Backup bijvoorbeeld moet aan de log en back-up archieven content kunnen toevoegen— dit is onmogelijk via FTP te doen en daarom zijn bredere permissies nodig. Sinds Admin Tools 1.0.b1 kunt u dat doen met behulp van de Permissie instellingen knop in het controle paneel van de component.



Wanneer u deze functie start ziet u een in drie secties verdeelde pagina.

Het bovenste deel, getiteld Standaard permissies, Staat u het instellen van permissies toe, die zullen worden toegepast als er niets anders is geconfigureerd. Gebruik de drop-down lijsten om de standaard permissies voor mappen en bestanden (standaard respectievelijk 755 en 644) te selecteren, gebruik dan de Sla standaard permissies op knop om de instelling toe te passen.

Het middelste gedeelte toont het pad naar de huidige geselecteerde map en staat u toe snel door de mappen navigeren door op hun namen te klikken.

Het onderste deel is verdeeld in twee panelen, Mappen en Bestanden. Elk paneel bevat de mappen en bestanden in de huidige map. Klikken op de naam van een map laat u navigeren binnen die map. Er zijn drie kolommen naast elke map. De eerste geeft de huidige eigenaar (gebruiker: groepsformaat). De tweede geeft de huidige permissies van die map in het bestandssysteem. De laatste kolom bevat is een drop-down lijst. De standaardinstelling, vertegenwoordigd door streepjes, betekent dat er geen specifieke voorkeur voor deze map / bestand is en de standaard permissies worden toegepast. Als u een aangepaste permissies instelling toepast vergeet dan niet op de Sla aangepaste permissies op knop te klikken voor naar een andere map te navigeren of terug te keren naar de controle pagina, anders zullen uw instellingen verloren gaan.

Important

Geen van deze aangepaste permissie instellingen wordt direct toegepast. U moet eerst de Herstel Permissies opties starten voordat ze worden toegepast. Klik op de Terug knop om terug te keren naar de Controle Paneel pagina waar u deze knop zult vinden.

Als alternatief kunt u op de Opslaan en Toepassen aangepaste permissies knop klikken om onmiddellijk alle aangepaste permissies op te slaan en toe te passen op deze pagina. Als u de permissies niet ziet veranderen, kijk dan in de vorige paragraaf van deze gebruikershandleiding voor meer informatie over wat te doen.

4. De Off-Line bij noodgevallen modus

De Joomla! Off-line functie, die u kunt inschakelen in de Algemene Instellingen van de back-end van uw website, heeft een grote tekortkoming. Het haalt de website NIET ECHT off-line. Alles wat het doet is om de output van de component vervangen door de "off-line" pagina. Dit heeft ernstige gevolgen voor de beveiliging, vooral wanneer het nodig is om uw website off-line te nemen wanneer het gaat om een een inbreuk op de beveiliging (bijvoorbeeld wanner uw site wordt gehacked) of om een belangrijk onderdeel van uw website bij te werken. Voor meer informatie over dit probleem, kunt u lees dit artikel [http://www.dionysopoulos.me/blog/how-offline-is-joomla-offline-mode] (Engels).

De Off-Line bij noodgevallen optie van Admin Tools zorgt ervoor dat u *verkelijk* en *veilig* uw website off-line haalt. Meer specifiek, de 'Off-Line bij noodgevallen' modus voert de volgende acties uit:

- Het maakt —als deze nog niet bestaat— een statische HTML pagina met de naam offline.html in de root van uw website. Deze pagina bevat het off-line bericht dat uw bezoekers te zien krijgen.
- Het maakt een backup van uw het `.htaccess` bestand van uw website, als er al een was onder de naam `.htaccess.eom`.
- Ten slotte, maakt het een .htaccess bestand dat tijdelijk alle toegangspogingen zal omleiden naar de offline.html pagina. Het zal alleen uw IP adres accepteren om toegang te krijgen tot de website.

Om uw website in de 'Off-Line bij noodgevallen' modus te zetten, klikt u op de Off-Line bij noodgevallen knop op de Controle Paneel pagina van Admin Tools. Dit zal u naar de volgende pagina leiden:

Als u op de 'Off-Line bij noodgevallen' knop klikt zal deze optie proberen bovenstaande stappen uit te voeren. Mocht één van deze stappen niet worden uitgevoerd, bijvoorbeeld als gevolg van onvoldoende bestandspermissies, dan kunt u nog steeds uw website in de 'Off-Line bij noodgevallen' modus zetten door doorlopen van de volgende procedure:

1. Bewaar een kopie van het `.htaccess` bestand van uw website, hernoem het bijvoorbeeld naar `htaccess.bak`.

2. Maak een nieuw .htaccess bestand in de root van uw website met de inhoud van wat er wordt weergegeven in het laatste deel van de 'Off-Line bij noodgevallen' modus pagina.

Als uw internet IP adres verandert voordat u de 'Off-Line bij noodgevallen' modus uitschakelt —uw verbinding valt bijvoorbeeld weg of u schakelt naar een andere computer die met het internet verbindt via een andere router—, dan zal u niet in staat zijn om in te loggen op uw website. In dit geval volg onderstaande stappen:

1. Met behulp van een FTP toepassing van uw voorkeur verwijder het .htaccess bestand, of upload een blanco .htaccess bestand dat het oude overschrijft.

2. Ga naar het Administrators back-end van uw website en klik op Admin Tools 'Off-Line bij noodgevallen'. Het klikken op de 'Off-Line bij noodgevallen' knop zal een nieuw `.htaccess` bestand met uw huidige IP adres maken. Uw back-up `.htaccess.eom` bestand zal niet worden overschreven.

Als u uw website terug on-line wilt zetten, ga naar de 'Off-Line bij noodgevallen' pagina en klik op de Set Online knop. Dit zal het off-line `.htaccess` bestand met de inhoud van het `.htaccess.eom` backup bestand overschrijven en het back-up bestand verwijderen. Als dit niet lukt volg dan de onderstaande handmatige procedure.

1. Met behulp van een FTP toepassing van uw voorkeur verwijder het .htaccess bestand, of upload een blanco .htaccess bestand dat het oude overschrijft.

2. Hernoem het `.htaccess.eom` back-up bestand terug naar `.htaccess`

Zal ik FTP kunnen gebruiken, of bestandsbeheer in het controle paneel van mijn host als ik deze functie in-schakel?

Natuurlijk! Deze functie beschermt alleen web (HTTP/HTTPS) toegang. Het kan, en zal geen FTP toegang, of uw hosting controle paneel bestandsbeheer aanraken.

Moet ik altijd gebruik maken van de 'Off-Line bij noodgevallen' modus in plaats van de off-line functie van Joomla!?

Het korte antwoord is eenvoudig, nee. Er zijn veel gevallen waarin de off-line functie van Joomla! is handig, dat wil zeggen wanneer u gewoon de inhoud van uw website niet beschikbaar wilt maken voor willekeurige bezoekers en zoekmachines, terwijl u een nieuwe website bouwt, of deze moet bewerken. De enige gevallen wanneer u de Emergency off-line modus moet gebruiken zijn:

- Als u van mening bent dat uw site gecompromitteerd (gehackt) is. De 'Off-Line bij noodgevallen' modus, maakt het onmogelijk voor de hacker om toegang tot uw website te forceren terwijl u bezig bent om hem te herstellen.

- Bij het updaten van de belangrijkste componenten van uw website, en niet het risico wilt dat een gebruiker een directe link volgt en het proces onderbreekt of vast laat lopen.

In alle andere gevallen is het handiger en voldoende om in de Algemene Instellingen van uw websites back-end de off-line functie van Joomla! zelf te gebruiken.

De offline.html pagina die Admin Tools maakt is afschuwelijk. Kan ik dit veranderen?

Dank u dat u het opmerkt! Natuurlijk kunt u dit veranderen. Upload simpelweg een door uzelf gemaakt offline.html bestand naar de root van uw website. U kunt linken naar JPG, GIF, PNG, BMP, SWF, CSS en JS bestanden —op dezelfde, of een andere server— vanuit de HTML code van dit bestand. Probeer niet te linken naar andere bestandstypes, want dat zal niet werken.

Zal de omleiding naar offline.html mijn SEO ranking niet verpesten?

Nee, de omleiding naar `offline.html` is gemaakt met behulp van de 307 HTTP status code die zoekmachines vertelt dat deze omleiding tijdelijk is, ze zullen de pagina nu niet indexeren, maar later terug te komen wanneer het probleem zal zijn hersteld.

Help! Ik ben buitengesloten van mijn website! Herstel het!

Lees een paar alinea's terug naar boven. U hoeft alleen maar een bestand via FTP te verwijderen.

De omleiding werkt niet! Ik test het vanaf mijn PC en ik kan nog steeds mijn website zien.

Allereerst heb ik een voor de hand liggende vraag: heb je *echt* de beschrijving van deze functie gelezen? U wordt verondersteld uw website alleen te kunnen zien vanaf uw PC. Als u wilt testen of deze functie echt werkt, probeer dan toegang te krijgen tot uw website vanaf een andere computer, aangesloten op het internet via een andere router. Een goed idee is om uw mobiel te gebruiken, zolang het maar een verbinding met het internet via 3G en niet via WiFi. Als u dat doet en nog steeds de omleiding niet ziet gebeuren, zorg er dan voor dat uw server `.htaccess` bestanden ondersteunt en dat het mod_rewrite ingeschakeld heeft. Sommige servers, zoals IIS, ondersteunen helemaal geen `.htaccess` bestanden. Als dit het geval is, raadpleeg dan uw host over het volledig off-line nemen van uw website.

Help! Zodra ik klikte op "Set Off-Line" kreeg ik een witte pagina of Internal Server Error 500 pagina.

Geen paniek! U heeft een oude versie van Apache —1.3 of 2.0— die geen ondersteuning biedt voor een specifieke functie in het `.htaccess` bestand gegenereerd door Admin Tools.U kunt dit probleem eenvoudig omzeilen door het handmatig bewerken van het `.htaccess` bestand in de root van uw website, met behulp van een FTP toepassing. Vervang `[R=307,L]` in de laatste regel met `[R,L]` (verwijder het =307 deel) en sla het bestand op. Dat is alles.

Mijn internetverbinding valt steeds weg. Zal ik voortdurend geblokkeerd worden van mijn website als ik deze functie gebruik?

Het hangt ervan af. Als u een statisch IP adres heeft, nee, u zult nooit geblokkeerd worden. Als u een dynamisch IP adres heeft, weet ik het niet. Toen ik een dynamisch IP adres had keek ik of mijn IP adres niet veranderde als mijn

verbinding minder dan 1-2 minuten weg viel. Het hangt allemaal af van hoe uw ISP IP adressen toekent aan haar klanten. De enige manier om erachter te komen is de harde manier: trial and error.

5. Bescherm uw administrator back-end met een wachtwoord

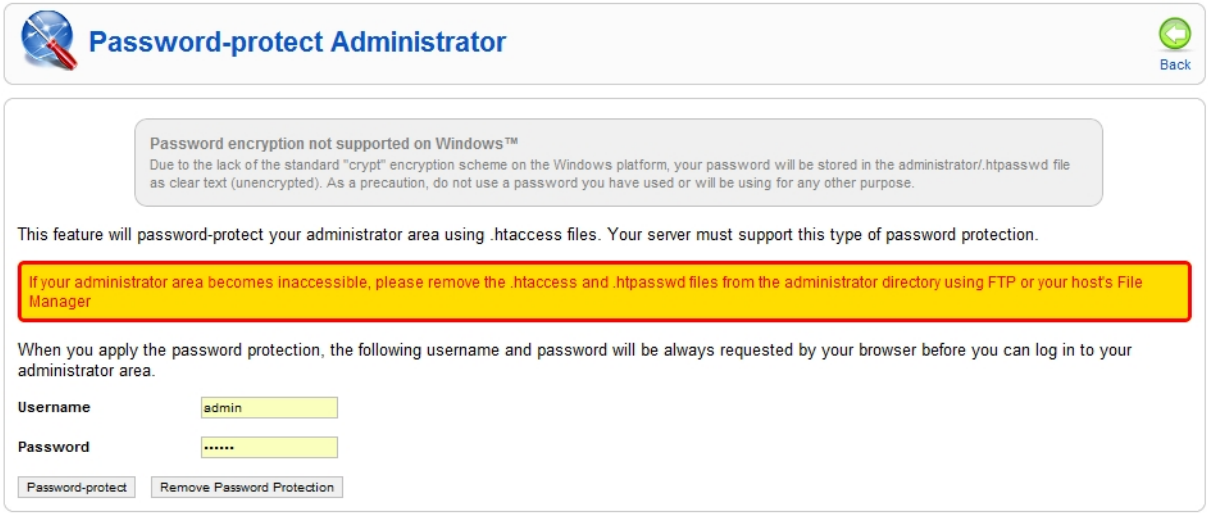
De Admin login wachtwoordbescherming tool van Admin Tools is ontworpen om een extra niveau van bescherming toe te voegen aan de administrator back-end van uw website, het vraagt om een gebruikersnaam en wachtwoord voor toegang tot de administrator login-pagina, of elk ander bestand in de `administrator` map van uw website. Het doet dit door gebruikmaking van Apache .htaccess en .htpasswd bestanden, dus zal niet werken op IIS hosts.

Important

Sommige voorverpakte server bundels, zoals Zend Server CE, en een aantal live hosts staan het gebruik van .htaccess bestanden om een map te beveiligen met een wachtwoord niet toe. Als het een lokale server betreft, bewerk dan uw `httpd.conf` bestand (voor Zend Server CE is bevind het zich in `C:\Program Files\Zend\Apache2\conf` of `C:\Program Files (x86)\Zend\Apache2\conf`) en wijzig alle 'AllowOverride' regels in:

```
AllowOverride All
```

Als u van een live host gebruik maakt, neem dan contact op met uw host over de mogelijkheid u toe te staan deze functie te gebruiken op uw website.



Als u op een server zit die draait op Windows™, ontvangt u een waarschuwing bovenaan de pagina waarin u staat dat het wachtwoord versleuteld wordt opgeslagen op de harde schijf. Dit is te wijten aan het ontbreken van een systeem wijde encryptie mogelijkheid op het Windows platform, waardoor Apache het wachtwoord alleen begrijpt, als het versleuteld of gecodeerd is met een niet standaard encryptie methode, die niet bestaat in PHP.

Warning

Als u uw administrator map met een wachtwoord beschermd op een Linux systeem en, uw website herstelt op een Windows server (een typische live naar local site herstel) zult u van een blanco pagina of een 'Internal Server 500' foutmelding krijgen bij het benaderen van de website. Dit is normaal en verwacht. Het enige wat u hoeft te doen is het verwijderen van de `.htaccess` en `.htpasswd` bestanden van uw administrator map na het herstellen van de website.

Om de wachtwoordbeveiliging toe te passen, voert u een gewenste gebruikersnaam en wachtwoord in en klik op de Beveilig met wachtwoord knop. Na een paar seconden zal uw browser u vragen om de gebruikersnaam het wachtwoord dat u zojuist opgegeven heeft in te voeren. Dit gebeurt ook elke keer als iemand probeert toegang te krijgen van de administrator back-end van uw website. Met andere woorden, u moet de gebruikersnaam en het wachtwoord delen met alle back-end gebruikers van uw website.

Indien u na het toepassen van de beveiliging met een wachtwoord onmiddellijk een lege pagina of een 'Internal Server Error 500' krijgt in plaats van een wachtwoord prompt, is uw server niet compatibel met de wachtwoordbeveiliging optie. In dit geval is de enige manier om de toegang tot de administrator back-end te krijgen het verwijderen van de `.htaccess` en `.htpasswd` bestanden van uw administrator map, met een FTP toepassing of de File Manager in het hosting controle paneel van uw website, te verwijderen. Neem in geval van twijfel contact op met uw host over hoe u dat kunt doen, voordat u probeert de wachtwoordbeveiliging toe te passen. Als deze bestanden niet te zien zijn in uw FTP cliënt, maak dan twee lege bestanden met deze namen, upload ze naar uw website, en overschrijf de bestaande (maar onzichtbare) bestanden. Hiermee verwijdert u de wachtwoordbeveiliging zodat u weer toegang tot uw administrator back-end heeft.

Als u de wachtwoordbeveiliging wilt verwijderen, kunt u zowel de `.htaccess` en de `.htpasswd` bestanden van uw administrator map verwijderen, of klik op de Verwijder wachtwoordbeveiliging knop.

6. De .htaccess maker

Note

Deze optie is alleen beschikbaar in de Professional release.

Een van de belangrijkste aspecten van het beheren van een website gehost op een Apache server is dat u in staat bent uw .htaccess bestand te bewerken. Dit bestand is verantwoordelijk voor vele webserver niveau tweaks, zoals het inschakelen van het gebruik van zoekmachine vriendelijke (SEF) URL's, het blokkeren van de toegang tot systeem-bestanden die niet toegankelijk moeten zijn voor het web, het omleiden tussen pagina's op basis van eigen criteria, en zelfs het optimaliseren van de prestaties van uw website. Aan de andere kant, is leren hoe al deze instellingen te tweaken verwant aan het leren van een vreemde taal en dus niet makkelijk. De .htaccess Maker tool van Admin Tools is ontworpen om u te helpen dergelijk bestanden te maken door gebruik te maken van een wijs-en-klik interface.

Important

Sommige voorverpakte server bundels, zoals Zend Server CE, en een aantal live hosts staan .htaccess bestanden niet toe de server instellingen te overschrijven. Als het een lokale server is, bewerk dan uw `httpd.conf` bestand (voor Zend Server CE bevind die zich in `C:\Program Files\Zend\Apache2\conf` of `C:\Program Files (x86)\Zend\Apache2\conf`) en wijzig alle 'AllowOverride' regels in:

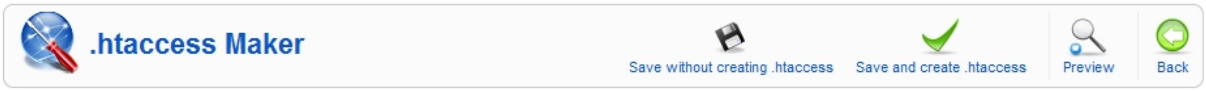
```
AllowOverride All
```

Als u van een live host gebruik maakt, neem dan contact op met uw host over de mogelijkheid u toe te staan deze functie te gebruiken op uw website.

Tip

Als u ooit wilt terugkeren naar een "veilige standaard instelling", zet dan alle opties op deze pagina "Nee" en klik op "Opslaan en .htaccess aanmaken". Dit zal een `.htaccess` bestand maken, dat in wezen hetzelfde is als de standaard bij Joomla! geleverde (`htaccess.txt`).

Het bovenste deel van de .htaccess maker pagina, bevat de standaard werkbalk knoppen die u zou verwachten:



- Opslaan zonder .htaccess aan te maken slaat de wijzigingen die u heeft gemaakt in de opties op deze pagina op, zonder dat een aangepast `.htaccess` bestand wordt gemaakt. Dit kan worden gebruikt wanneer u nog niet heeft besloten over de instellingen van sommige opties, of als u het gegenereerde voorbeeld wilt zien van het `.htaccess` bestand voordat u het opslaat op schijf.

- Opslaan en .htaccess aanmaken is de logische volgende stap naar de 'vorige' knop. Het slaat niet alleen de wijzigingen op die u gemaakt heeft, maar creëert en schrijft ook het nieuwe `.htaccess` bestand naar schijf. Als er al een `.htaccess` bestand op u website bestaat, zal het worden hernoemd naar `.htaccess.admintools` voor het nieuwe bestand naar de schijf wordt geschreven.

- Voorbeeld pops up een dialoogvenster hoe het gegenereerde `.htaccess` bestand eruit ziet zonder het naar schijf te schrijven. Dit dialoogvenster toond de configuratie. Als u enkele instellingen heeft aangepast zullen ze hier niet worden weergegeven totdat u op één van de vorige twee knoppen klikt.

- De Terug knop brengt u terug naar de Controle Paneel pagina.

Onder de werkbalk zijn er vijf panelen met verschillende opties, die hieronder worden beschreven. Voordat u dat doet, zorg dat u de volgende waarschuwing leest en begrijpt. Verzoeken om ondersteuning waaruit blijkt dat u de waarschuwing niet heeft gelezen worden beantwoord met een link terug naar deze pagina.

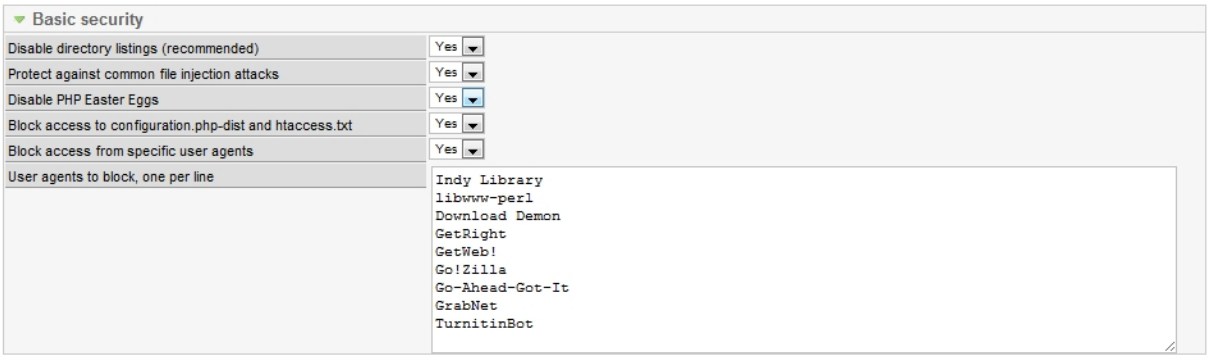
Warning

Afhankelijk van uw webserver instellingen, kunnen sommige van deze opties niet compatibel zijn met uw website. In dit geval krijg u een blanco pagina of een 'Internal Server Error 500' foutmelding wanneer u probeert ongeacht welk deel van uw website te benaderen. Als dit gebeurt, moet u het `.htaccess` bestand uit de root van uw website map verwijderen met behulp van een FTP cliënt of de 'File Manager' functie van uw hosting controle paneel. Omdat sinds Admin Tools 1.2, uw oude `.htaccess` bestand is opgeslagen als `.htaccess.admintools`. U kunt dat bestand terug hernoemen naar `.htaccess` om terug te keren naar de laatst bekende goede staat. Als u niet weet hoe dit werkt, neem dan contact op met uw host voordat u probeert een nieuw `.htaccess` bestand te maken zonder Admin Tools.

Sommige kant en klare server omgevingen, zoals WampServer, schakelen niet standaard de Apache mod_rewrite module in, dit resulteert altijd in een 'Internal Server Error' bij het toepassen van het .htaccess bestand. In dit geval raden we u met klem aan om deze in te schakelen. Op WampServer kunt u klikken op het pictogram in het systeemvak, ga daarna naar Apache, Modules en zorg ervoor dat rewrite_module wordt aangevinkt. Op andere server omgevingen moet u uw httpd.conf bestand bewerken ervoor zorgen dat de LoadModule mod_rewrite regel niet is uitgecommentarieerd (er moet geen hekje aan het begin van de regel staan). Zodra u één van deze veranderingen heeft uitgevoerd, moet u de server opnieuw opstarten om de wijzigingen van kracht te laten worden.

We raden met klem aan te beginnen met alle opties op Nee in te stellen, en ze vervolgens weer één voor één op Ja in te stellen, en elke keer een nieuw .htaccess bestand te creëren. Als u op een bepaalt moment een lege of fout pagina te zien krijgt, zult u weten dat de laatste optie die u probeerde niet compatibel is met uw host. In dat geval verwijdert u het .htaccess bestand, zet u de optie die het probleem veroorzaakte op Nee en gaat u verder met de volgende optie op Ja te zetten. Helaas is er geen andere weg dan met de trial-and-error methode te kijken welke opties compatibel zijn met uw server.

6.1. Basisbeveiliging



Schakel map listings uit (aanbevolen)
: Wanneer uitgeschakeld, kan uw webserver een lijst van de bestanden en submappen van elke map op uw website weergeven als er geen index.html bestand aanwezig is. Dit kan een veiligheidsrisico inhouden, dus u moet deze optie altijd inschakelen (op Ja zetten) als u wilt voorkomen dat dit gebeurt.

Bescherm tegen gemeenschappelijke bestandsinjectie aanvallen
: Veel kwaadwillige hackers proberen kwetsbare extensies op uw website te misbruiken door ze te misleiden en kwaadwillige code te laten toevoegen op de server van de aanvaller. Het inschakelen (op Ja zetten) van deze optie zal uw server beschermen tegen dit soort aanvallen.

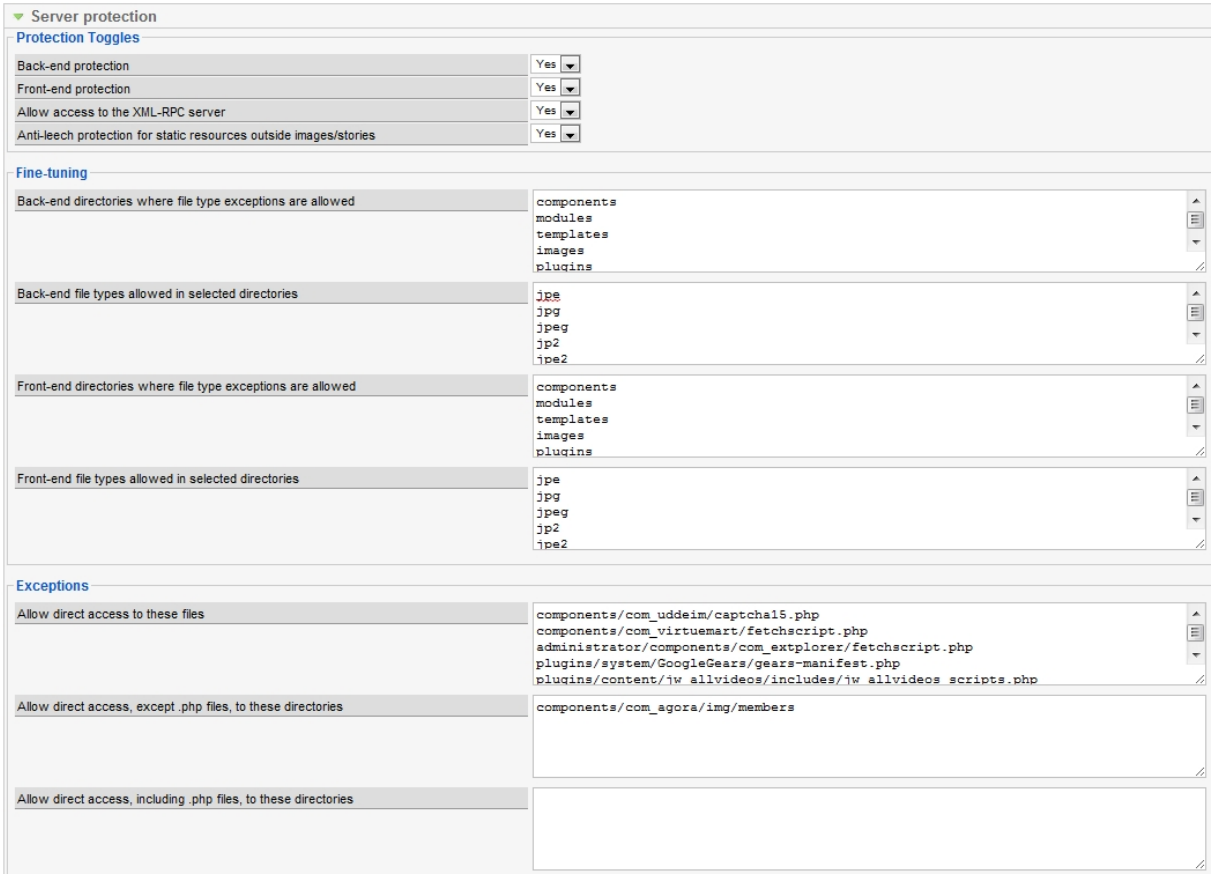
PHP easter eggs uitschakelen
: PHP heeft een leuke en vervelende eigenschap, die bekend staat als "Easter Eggs". Bij het toevoegen van een speciale URL parameter, zal PHP een afbeelding in plaats van de gevraagde feitelijke pagina weergeven. Overwegende dat deze wordt beschouwd als leuk, is het ook een op grote schaal misbruikte methode door aanvallers gebruikt om erachter te komen welke versie uw PHP installatie heeft (deze afbeeldingen zijn in iedere PHP versie anders) een hacker zal nu aanvallen kunnen uitvoeren gericht op uw specifieke PHP versie. Door het activeren van deze optie (op Ja zetten), schakelt u de volledige toegang tot die Easter Eggs uit, en maakt u het nog moeilijker voor de aanvallers de details van uw server te achterhalen.

Blokkeer de toegang tot configuration.php-dist en htaccess.txt
: Deze twee bestanden zijn achtergelaten na een Joomla! installatie of upgrade, en zijn direct toegankelijk via het web. Ze worden gebruikt door aanvallers om te kijken welke Joomla! versie u gebruikt, zodat ze een aanval op maat gericht op uw specifieke Joomla! versie kunnen uitvoeren. Het inschakelen van deze optie "verbergt" deze bestanden voor het benaderen via het web (een 404 Not Found pagina wordt geretourneerd), om aanvallers te laten geloven dat deze bestanden niet bestaan, dit maakt het iets moeilijker voor hen om informatie over uw site te verkrijgen.

Blokkeer de toegang van specifieke user agents
: Wanneer ingeschakeld zal het alle pogingen toegang tot uw website te krijgen blokkeren, als remote programma's één van de user agent strings in de Te blokkeren user agents, één per regel lijst staat. Deze functie is ontworpen om uw website te beschermen tegen veel voorkomende bandbreedte slurpende download bots en andere legitieme tools die vaker worden gebruikt voor het hacken van websites, dan hun goedaardig beoogde functionaliteit.

Te blokkeren user agents, één per regel
: De user agent strings die geblokkeerd worden voor toegang tot uw website. U hoeft niet de hele UA string in te voeren, maar een deel ervan is genoeg. De standaardinstelling bevat een aantal gebruikelijke verdachte user agents. Scheid meerdere items door elk item op een nieuwe regel te plaatsen. Let wel dat bij sommige servers met mod_security of mod_evasive geïnstalleerd, een 'Toegang geweigerd' bericht zal worden weergegeven wanneer u probeert de configuratie instellingen op te slaan, als dit veld het woord "Wget" bevat. Als u tegen dit probleem aanloopt is het geen bug in Admin Tools of Joomla!. Het is een op server niveau beschermingsfunctie die ingrijpt. Voorkom het gebruik van het woord Wget en u bent uit de gevarenzone.

6.2. Serverbeveiliging



Dit is de meest gewilde functie van onze software en biedt een bijna alles omvattende bescherming tegen de overgrote meerderheid van de bekende gevaren wanneer ingeschakeld. De missie statement van deze functie kan worden samengevat met één enkele zin: niets op uw site wordt uitgevoerd, tenzij daar toestemming voor geeft. Door het blokkeren van de toegang tot uw front-end en back-end elementen (media-bestanden, Javascript, CSS en PHP-bestanden) wordt het extreem moeilijk, —maar niet ronduit onmogelijk— voor een aanvaller om uw site te hacken, zelfs als hij erin slaagt om een kwetsbaarheid te exploiteren door kwaadaardige PHP code te uploaden naar uw website. Daarnaast zal het directe toegang tot bronnen niet ontworpen voor direct toegankelijkheid vanaf het web niet toestaan, zoals vertaling INI bestanden, die meestal worden gebruikt door aanvallers om uit te zoeken welke Joomla! versie u gebruikt op uw site, om op maat een aanval op uw website uit te kunnen voeren. Aan de andere kant, moet u expliciet de toegang inschakelen tot sommige extensies, bijvoorbeeld PHP bestanden die zijn ontworpen om direct vanaf het web te worden aangeroepen en niet via Joomla!'s hoofdbestand, `index.php` and `index2.php`.

Let wel dat het inschakelen van deze functie, dodelijk kan zijn voor de functionaliteit van een aantal extensies die willekeurig PHP bestandsnamen creëren binnen uw website, zoals RokGZipper. Naar onze bescheiden mening weegt het veiligheidsrisico van het hebben van een niet goed beschermde website, niet op tegen de voordelen van een dergelijke oplossing. Als gevolg hiervan, raden we u aan RokGZipper en andere soortgelijke software met dezelfde dubieuze beveiligingspraktijken uit te schakelen.

Er zijn drie secties voor configuratie instellingen die de functionaliteit van de 'Serverbeveiliging' functie controleren. De eerste is de Schakelt de beveiliging in en uit waarmee u de drie belangrijkste aspecten van deze bescherming kunt in of uitschakelen:

Back-end bescherming	Schakelt directe toegang tot de meeste back-end bronnen uit, behalve die in de uitzonderingen lijsten. Het wordt algemeen aanbevolen om deze optie op aan te zetten om de bescherming van uw

website te verbeteren, tenzij u de administrator wachtwoord beveiligingsfunctie aan heeft staan. In het laatste geval is deze optie overbodig en raden we u aan hem uit te schakelen.

Front-end bescherming
: Schakelt directe toegang tot de meeste front-end bronnen uit, behalve die in de uitzonderingen lijsten. Het wordt algemeen aanbevolen om deze optie aan te zetten om de bescherming van uw website te verbeteren.

Sta toegang tot de XML-RPC-server toe
: Standaard blokkeert de front-end beveiliging ook de toegang tot de xmlrpc map op uw website, die wordt gebruikt voor XML-RPC (Web Services) aanvragen. Als u een extensie geïnstalleerd heeft die vereist dat de Web Services optie is ingeschakeld in uw Algemene Instellingen in de back-end van uw site —zoals bijvoorbeeld de Remote Control plugin van Akeeba Backup, de Blogger service, de Joomla! XML-RPC service of een andere soortgelijke plug-in in de xmlrpc groep— moet u deze optie inschakelen om de toegang op afstand te kunnen laten werken. In alle andere gevallen verzoeken wij u om deze optie uit te schakelen om potentiële exploits te voorkomen.

In de volgende paragraaf wordt Fijnafstemming genoemd en bevat de nodige opties om het gedrag van de bescherming aan uw eigen website aan te passen. Voor het beschrijven van wat elke optie doet, is een kleine uitleg over hoe de bescherming werkt aan de orde. De beschermingscode in het gegenereerde `.htaccess` bestand blokkeert directe web toegang tot alle bestanden. Joomla!'s standaard "toegangspunt" of "hoofd" bestanden, `index.php` en `index2.php`, worden automatisch vrijgesteld van deze regel. Maar uw site bevat ook afbeeldingen, media, CSS en Javascript bestanden in bepaalde mappen. Voor de back-end en front-end bescherming moeten we een aantal mappen waar dergelijke bestanden en de bestandsextensies van die bestanden zijn toegestaan opgeven. Dit is waar het bij deze deze opties allemaal over gaat. De standaardinstellingen bevatten de meest voorkomende bestandstypen die je zou verwachten te vinden, en de standaard mappen waar ze zouden moeten staan op een Joomla! website. U hoeft ze alleen maar wat aan te passen als u meer bestandsextensies wilt toevoegen, of om statische bestanden op andere locaties dan de standaard locatie te hebben.

Back-end mappen waar bestandstype uitzonderingen zijn toegestaan
: Dit is een lijst met back-end mappen (dat wil zeggen, submappen van de administrator map van uw website) waarvan u verwacht dat er mediabestanden aanwezig zijn. Plaats een map op elke regel. Submappen van deze mappen worden automatisch toegevoegd aan de lijst met uitzonderingen, zonder dat hier expliciet op te geven.

Back-end bestandstype toegestaan in de geselecteerde mappen
: De extensies van back-end bestanden die zijn toegestaan doorgelaten te worden door het server beschermingsfilter, zolang de bestandsextensies in de lijst staan. Plaats één extensie per regel, zonder de voorafgaande punt. Bijvoorbeeld, als u toegang tot alle PDF bestanden wilt toestaan moet u "pdf" (zonder de aanhalingstekens) op een nieuwe regel van deze lijst typen om de extensie toe te staan. Let wel dat de bestandsextensies zijn hoofdlettergevoelig. Dit betekent dat de PDF, Pdf, pdf en pDF vier verschillende bestandsextensies zijn voor wat uw webserver betreft. Als vuistregel, typt u de extensies in kleine letters in en zorg ervoor dat de extensies van de bestanden die u upload ook in kleine letters zijn geschreven.

Front-end mappen waar bestandstype uitzonderingen zijn toegestaan
: Dit is een lijst van de front-end mappen (dat wil zeggen, mappen in de root van uw website) waar u mediabestanden verwacht. Plaats één map op elke regel. Submappen van deze mappen worden automatisch toegevoegd aan de lijst met uitzonderingen, zonder dat hier expliciet op te geven.

Front-end bestandstype toegestaan in de geselecteerde mappen
: The extensions of front-end files which allowed to pass through the server protection filter, as long as the files with those extensions are in the list above. Place one file extension per line, without the dot. For example, if you want to allow access to all PDF files you have to type in "pdf" (without the quotes) on a new line of this list. Do note that file extensions are case-sensitive. This means that PDF, Pdf, pdf and pDF are four different file extensions as far as your web server is concerned. As a rule of thumb, type in the extensions in lowercase and make sure that the extensions of the files you upload are also in lowercase.

Tenslotte hebben we de Uitzonderingen sectie. Hierdoor kunnen specifieke bestanden of alle bestanden in bepaalde mappen het server beschermingsfilter passeren zonder verdere vragen. Dit is nodig om verschillende redenen. Om te beginnen, sommige extensies hebben directe toegang tot PHP bestanden nodig, zonder ze door te geven door middel van Joomla!'s hoofdbestanden. Een voorbeeld hiervan is Akeeba Backup Professional's `restore.php` gebruikt in de geïntegreerde herstel functie, omdat het onmogelijk zou zijn om de index.php van een site die in bewerking is terwijl het herstel aan de gang is. Andere belangrijke voorbeelden zijn CSS en javascript minifiers, ofwel opgenomen worden in uw template of geïnstalleerd over uw site. Forum bijlagen maken ook deel uit van hetzelfde probleem, omdat ze de neiging hebben een speciale map voor de bijlagen, en avatar pictogrammen enzovoort te creëren. Bovendien plaatsen sommige extensies PHP bestanden in uw websites `tmp` en `cache` mappen en verwachten dat ze direct toegankelijk zijn vanaf het web. Hoewel dit dom gedrag is, en in strijd met de doelstellingen van het ontwerp van de Joomla! zelf, u nog steeds een manier nodig heeft om er omheen te werken die wij moeten verstrekken. Tot slot, heeft u mogelijk een script van een andere partij (bijv. Coppermine galerij, phpBB forum, WordPress blog, of zelfs een andere Joomla! website in een submap) die niet als een Joomla! extensie geïnstalleerd wordt. De server beschermingsfunctie zal normaal gesproken de toegang daartoe blokkeren en u moet nog steeds een manier om deze beperking heen vinden. Dan is dit de de oplossing:

Sta directe toegang tot deze bestanden toe

Plaats één bestand per regel, die moet worden vrijgesteld van de filtering, dus rechtstreeks toegankelijk vanaf het web. De standaardinstellingen zijn de vereiste uitzonderingen voor de meest gebruikte extensies, zoals UddeIM, VirtueMart, eXtplorer, Phil Taylor's Google Gears plugin, JoomlaWorks' AllVideos plugin, Akeeba Backup Professional en natuurlijk, Admin Tools zelf.

Sta directe toegang, met uitzondering van .php bestanden, in deze mappen toe

Directe toegang tot alle bestanden (behalve .php bestanden) wordt verleend indien ze binnen een van de mappen in deze lijst voorkomen. Normaal gesproken is dit alleen nodig wanneer u een forum heeft en bijlagen, avatars en fotogalerijen mappen, of andere mappen waar u alleen mediabestanden in wilt opslaan wilt toevoegen. Het voorbeeld is het Agora forum gebruikersbestanden. Zoals bij alle soortgelijke opties, voeg één map per regel toe, zonder een slash.

Sta directe toegang, inclusief .php bestanden, in deze mappen toe

Deze optie moet zo min mogelijk worden gebruikt. Elke map die in deze lijst wordt geplaatst is niet langer beschermd door de 'Serverbeveiliging' en kan mogelijk worden gebruikt als een toegangspoort tot het hacken van uw website. Voor zover wij weten zijn er slechts drie gevallen waarin het gebruik ervan te rechtvaardigen is:

- Als u een Joomla!, WordPress, phpBB, Coppermine gallery of enige andere PHP applicatie in een subdirectory van uw site heeft geïnstalleerd. Bijvoorbeeld, als u probeert om een kopie van uw website te herstellen binnen een map met de naam `test` dan moet u `test` in deze lijst opnemen. Dit is het enige te rechtvaardigen scenario dat de veiligheid van uw website niet in gevaar brengt.

- Sommige templates en templatekaders kunnen hun CSS en javscript binnen PHP bestanden wikkelen om ze gecomprimeerd aan uw browser te leveren. Hoewel dit een geldige techniek is, is het mogelijk dat de lijst van PHP bestanden te groot is om op te sporen, en op te nemen in de eerste lijst van de Uitzonderingen sectie. In dit geval kunt u overwegen om de template submap die deze bestanden bevat in deze lijst op te nemen.

- Sommige extensies doen iets doms: ze plaatsen bestanden in uw site's `tmp` of `cache` mappen en verwachten dat ze direct toegankelijk zijn vanaf het web. Dit is duidelijk verkeerd, want deze mappen zijn ontworpen om beschermde systeemmappen te zijn waar rechtstreekse toegang niet mag worden toegestaan, met name omdat ze gevoelige informatie zouden kunnen bevatten. Echter, als u zulke extensies heeft —met name bepaalde Javascript en CSS minifiers— heeft u een manier nodig om directe toegang tot die mappen toe te staan.

  Als u besluit dat gemak voor veiligheid gaat kunnen we u niet tegenhouden. Voeg de tmp en cache map aan deze lijst toe en hoop het beste. U opent een beveiligingsgat op uw website en u doet dat op eigen risico en potentieel gevaar.

> Hoewel het heel verleidelijk lijkt om er een aantal Joomla! systeemmappen in te zetten, zoals componenten en templates, doe het niet. Dat klopt. Doe dat niet. Het is als een kruisraket gebruiken om een mug te doden die zich in dezelfde kamer bevind als u. De mug zal het vrijwel zeker niet overleven, maar u zal zelf mee ten onder gaan. Of, om in informatica termen te blijven, u zal potentiële hackers toestaan eventuele beveiligingslekken te gebruiken waarvoor u nog niet de kans heeft gehad ze te repareren, en kwaadaardige code zullen uploaden en *uitvoeren*. U doodde de mug (het toegangsproblemen dat u had met een extensie), maar u heeft per ongeluk geholpen uw website neer te halen. Au! Zelfs als er een kans bestaat dat dit gebeurt, van ongeveer één op de tienduizend, bent u dan bereid om dat risico te nemen *op uw eigen website*?

Om erachter te komen welke aangepaste uitzonderingen u nodig heeft om toe te voegen op uw site, kijk dan in de Hoe te bepalen welke uitzonderingen nodig zijn sectie hieronder.

Warning

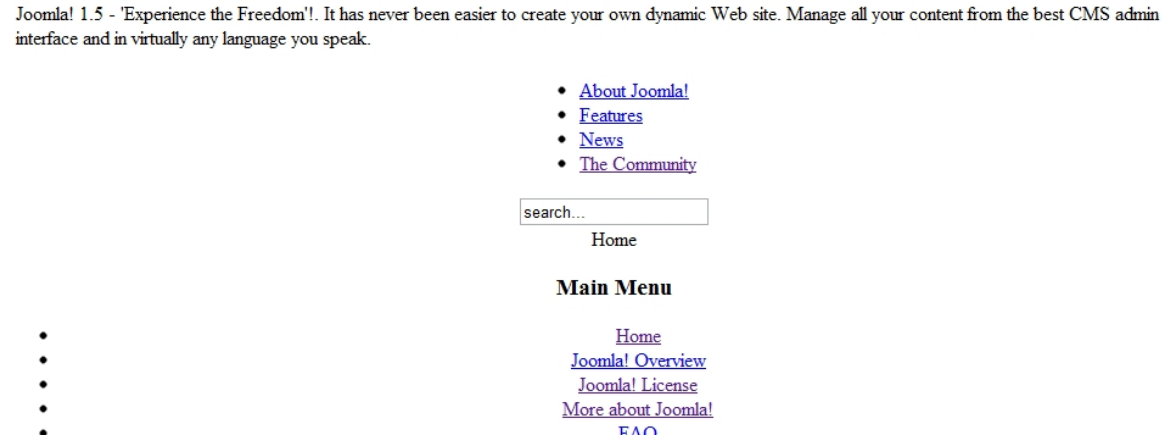
Windows gebruikers let op! *Gebruik geen* Windows pad scheidingsteken (de backslash - \) om mappen te scheiden! We praten over mappen zoals ze in URL's voorkomen, dus u moet altijd gebruik maken van de URL pad scheidingsteken (forward slash - /) in deze instellingen. Met andere woorden: `een/lang/pad` is correct, `een\lang\pad` is FOUT!

6.2.1. Hoe te bepalen welke uitzonderingen nodig zijn

Na het aanbrengen van de Serverbeveiliging script zult u merken dat sommige van uw extensies niet meer goed werken of, erger nog, helemaal niet meer werken. Soms kan het zelfs lijken dat uw website iets mist of als CSS en Javascript niet langer laden. Wees niet bang en niet haast je niet om meteen 'Serverbeveiliging' uit te schakelen. Bepaal eerst welke uitzonderingen nodig zijn, het is eenvoudig en neemt slechts een paar minuten van uw tijd. Ik beloof u, het is net zo spannend, fantasierijk en voldoening gevent als het CSI werk van televisie. Bovendien, als u ze eenmaal bepaalt op één site kunt u ze opnieuw gebruiken op elke websites die deze extensie geïnstalleerd heeft. U zult snel eindigen met uw "master" uitzonderingen lijst die u kunt toepassen op al uw sites zonder er verder bij na te denken.

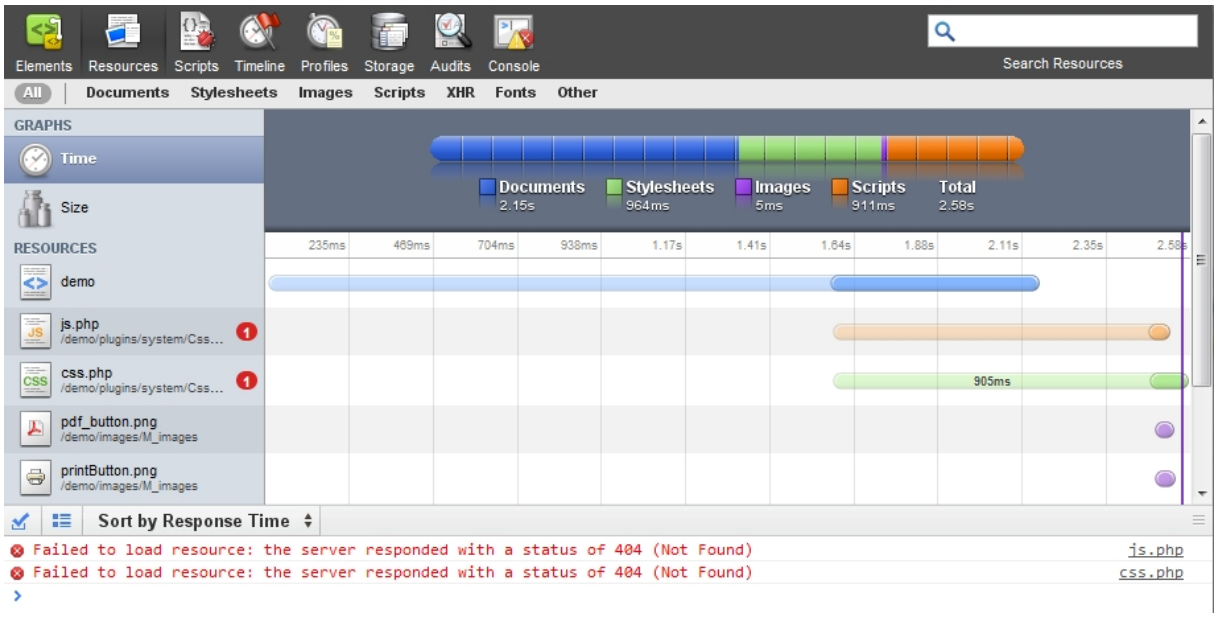
In het volgende voorbeeld gaan we Google Chrome gebruiken om toegangsproblemen te signaleren op een website. Vergelijkbare instrumenten zijn ingebouwd in andere grote browsers, zoals Safari en Internet Explorer 8. Als u gebruik maakt van Firefox kunt u de FireBug installeren en van haar NET paneel gebruik maken om de toegangsproblemen te detecteren.

Onze eerste test case zal een site met de fantastische CssJsCompress JS/CSS minifier plugin geïnstalleerd zijn. De eerste aanwijzing dat er iets mis is gegaan, is dat onze site er uit ziet alsof alle CSS is verdwenen:

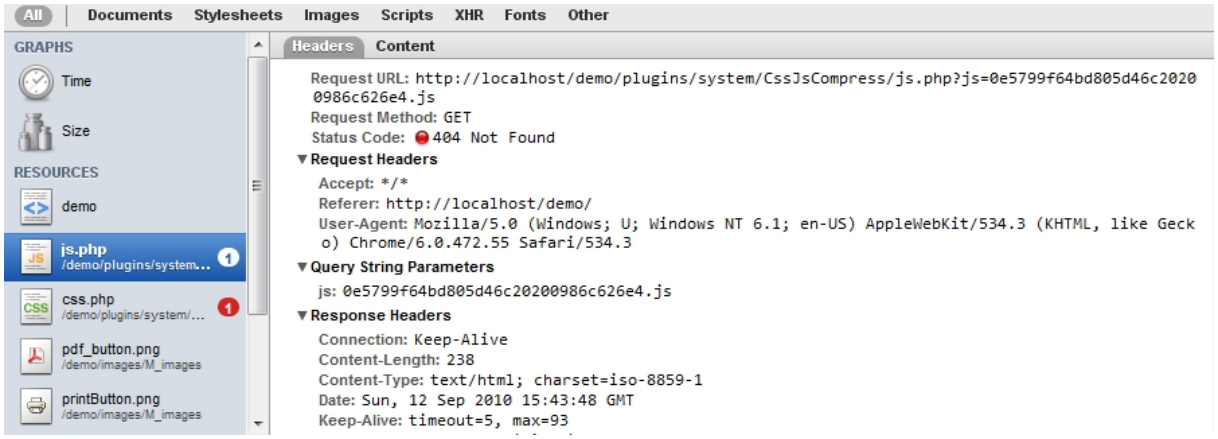


Om te achterhalen wat er fout gaat, moeten we weten welke van de bestanden waarnaar wordt verwezen door de pagina een 404 fout (dit betekent dat ze worden gefilterd door 'Serverbeveiliging'), hun naamgevingspatroon en de locatie

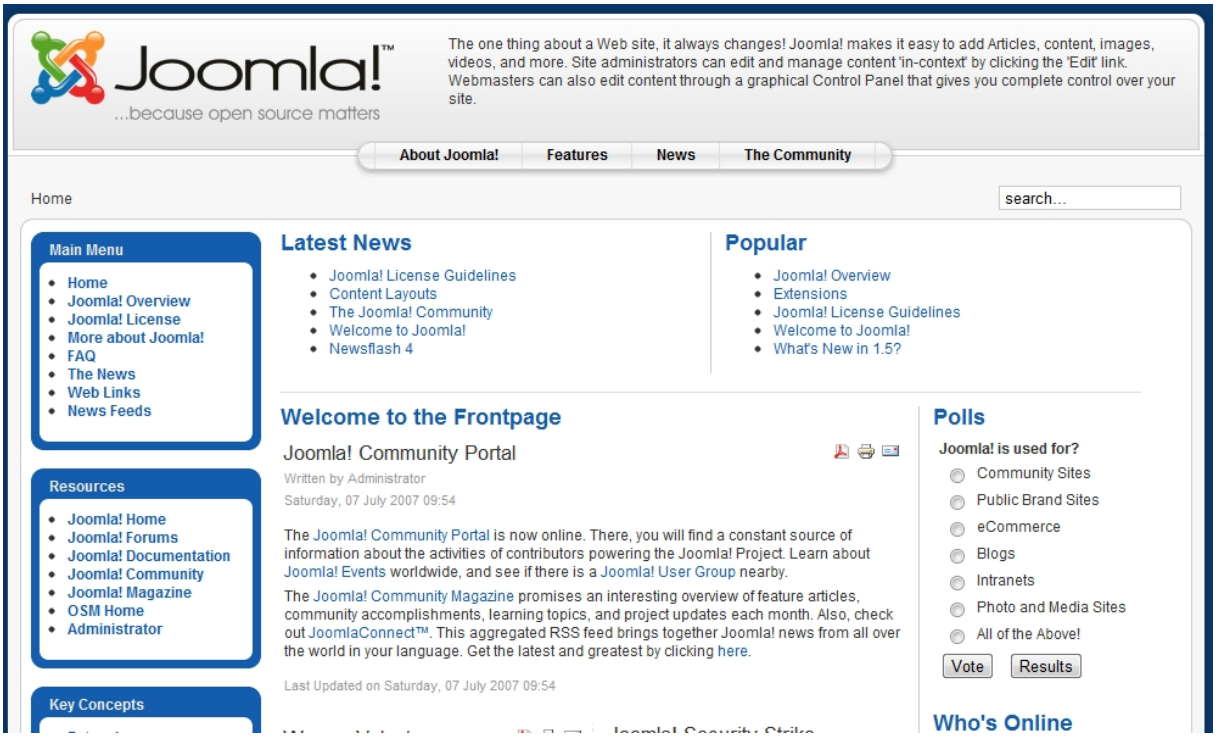
genereren. Aangenomen dat u gebruik maakt van Chrome open het Ontwikkelaar Tools venster door CTRL-SHIFT-J te typen tijdens het bekijken van de gebroken pagina. Klik op het tabblad Bronnen en, indien hierom wordt gevraagd, schakelt u het bijhouden van bronnen voor deze sessie in. De pagina herlaad, en een lijst van bestanden die de browser heeft geprobeerd te benaderen wordt weergegeven:



Het onderste deel van het venster is de console. Het informeert ons vriendelijk dat twee bestanden, js.php en css.php, niet konden worden geladen met de status van 404. Bingo! We vonden de daders, laten we nu eens kijken waar ze vandaan komen. Klik op de js.php link in de console. Het bovenste deel van het venster wordt gewijzigd om wat debug info over dat bestand te tonen:



Het interessante deel is de aangevraagde URL: `http://localhost/demo/plugins/system/CssJsCompress/js.php?js=0e5799f64bd805d46c20200986c626e4.js`. Zoals u al raadde, het deel na het vraagteken is een URL parameter en kan worden verwijderd. We houden dan het volgende over: `http://localhost/demo/plugins/system/CssJsCompress/js.php`, maar we weten dat http://localhost/demo de basis URL is van onze website. Verwijder het en u houd over: `plugins/system/CssJsCompress/js.php`. Hebbes! Is er een kans dat dit bestand een variabele naam kan hebben? Nee. Bestaat het bestand in ons bestandssysteem? Ja. Dit betekent dat dit precies het bestand is dat we moeten plaatsen in onze Sta directe toegang tot deze bestanden toe lijst. Voeren we precies hetzelfde proces uit voor de css.php dan komen we op nog een ander bestand dat we moeten uitsluiten: `plugins/system/CssJsCompress/css.php`. Let op de hoofdletters, OK? Kopiëer en plak de bestanden in de uitzonderingen optie en regenereer het `.htaccess` bestand dit, zal onze website weer goed laden:



Dat gezegd hebbende, zult u soms een lange lijst van moeilijk te raden bestandsnamen vinden, iets als js-abc123456789fed0.php en dergelijken. Als de bestandsextensie is alles behalve .php dan kunt u de extensie toevoegen aan de front-end of back-end toegestane bestandstypen lijst en de map in de respectievelijke lijst met mappen waar bestandstype uitzonderingen zijn toegestaan. Als de schuldigen PHP bestanden zijn, heeft u twee opties: stoppen met het gebruik deze extensie of voeg de map toe in de "Sta directe toegang, met uitzondering van .php bestanden, in deze mappen toe" lijst.

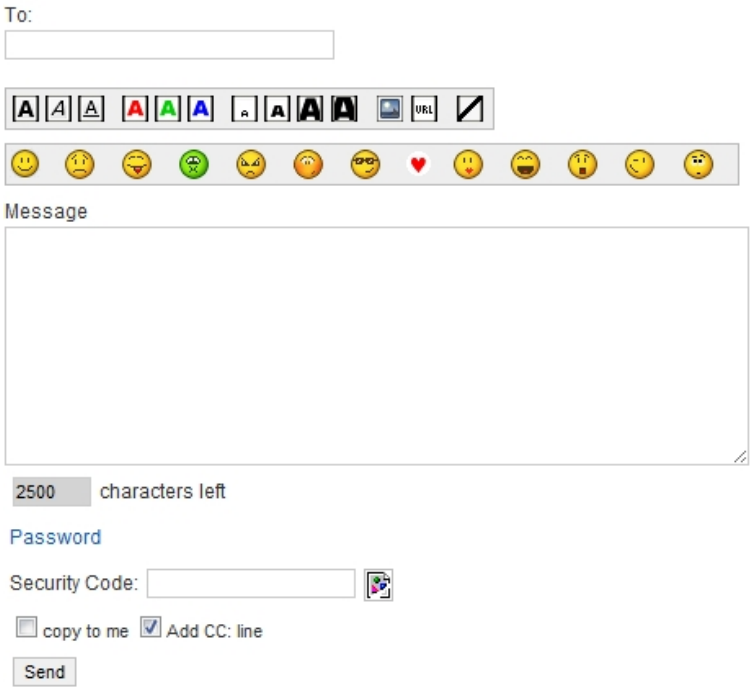
Hoe zit het met een ander voorbeeld?

Het vorige voorbeeld was dood eenvoudig te herkennen omdat de pagina eruit zag als een grote puinhoop die ons meteen op het spoor van de schuldige zette. Dit is niet altijd het geval. Soms stopt een optie van een extensie op onverklaarbare wijze met werken. In dit test geval zullen we gebruik maken van de extensie UddeIM. Dit was een real-world probleem waarmee ik te maken had, en dit is het verhaal over hoe ik dit heb opgelost.

Note

Een uitzondering voor UddeIM is reeds aanwezig in de standaard configuratie. Omwille van het documenteren van de procedure verwijderde ik het, om aan te tonen wat er gaande is en hoe het te repareren.

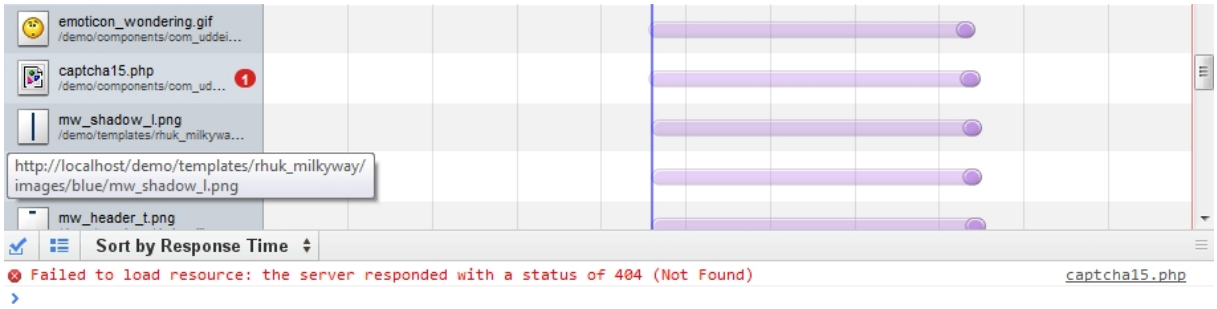
Na de installatie van de 'Serverbeveiliging' begonnen gebruikers te klagen dat ze mij geen berichten via UddeIM meer konden sturen. In het begin begreep ik niet waarom, want ik kon het zonder enig probleem gebruiken. Toen besloot ik om een eenvoudige onbevoegde geregistreerde gebruiker aan te maken, met de bedoeling een bericht naar mijzelf te sturen om dit te testen. En ik vond het probleem:



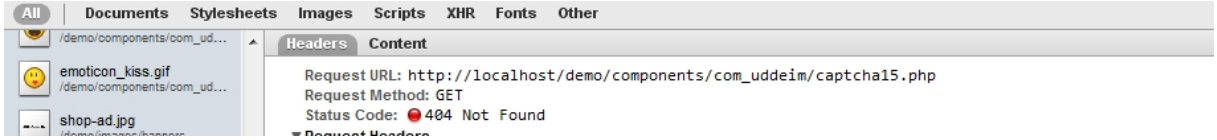
Tip

Als u probeert een probleem te vinden dat gevolgen heeft voor uw gebruikers maar niet voor uzelf, probeer dan altijd een gebruiker met dezelfde rechten als een getroffen gebruikersaccount te gebruiken. Idealiter, log in met de account van de rapporterende gebruiker —met zijn toestemming omdat u zijn wachtwoord moet veranderen—, om het probleem zelf te ondervinden. Ik deed dit stukje ervaring op, op de moeilijkste manier.

Ziet u de gebroken afbeelding link naast 'Beveiliging Code'? Dit is de plek waar een CAPTCHA weergegeven moet worden - maar alleen voor geregistreerde gebruikers. Hm ... Waarom wordt het weergegeven? Tijd om de Developer Tools in de browser weer te gebruiken. En hier is wat het zegt:



Er is een captcha15.php bestand niet geladen. Juist. Maar waar is het te vinden? Laten we op de bestandsnaam klikken in de console om erachter te komen:



Zo daar is het! `components/com_uddeim/captcha15.php`. Voeg dit toe aan de Sta directe toegang tot deze bestanden toe uitzonderingen lijst, en genereer een nieuw `.htaccess` bestand en laten we het resultaat bekijken:

Dat was het! Probleem opgelost.

6.3. Aangepaste .htaccess regels

Soms moet u gewoon toe regels op maat aan .htaccess toevoegen, regels die verder gaan dan wat .htaccess Maker kan bieden. Dergelijke voorbeelden kunnen bijzondere richtlijnen zijn die uw host zei in uw .htaccess bestand toe te voegen om bijvoorbeeld naar PHP5 om te schakelen, of als u het standaard foutmeldingsdocument van uw server wilt wijzigen en ga zo maar door. Als u een gevorderde gebruiker bent kunt u ook uw eigen geavanceerde regels verder aanpassen om het gedrag van de Serverbeveiliging aan te passen. Met de twee opties in deze sectie kunt u om dat doen.

De inhoud van het Aangepaste .htaccess regels bovenaan in het bestand tekstgebied zal worden uitgevoerd bovenin het .htaccess bestand, net na de 'RewriteEngine On' richtlijn. U moet aangepaste uitzonderingsregels en in het algemeen, alles wat wellicht nog voor de bescherming en de veiligheidsregels moet worden uitgevoerd hier ingeven.

De inhoud van het Aangepaste .htaccess regels onderaan in het bestand tekstgebied worden toegevoegd aan het eind van het .htaccess bestand. Dit is de plek om dingen zoals richtlijnen om PHP5 in te schakelen en eventuele optimalisaties die alleen moeten worden uitgevoerd nadat het verzoek is doorgegeven via de beveiliging en server beschermingsregels.

6.4. Optimalisatie en hulpprogramma

Deze sectie bevat richtlijnen die van utilitaire waarde zijn en u tijd besparen:

Forceer uitvoeren van index.php voor index.html	Sommige servers proberen om index.html te verwerken voor index.php. Dit heeft tot gevolg dat het proberen om root toegang tot uw website te krijgen, zal bijvoorbeeld `http://www.voorbeeld.com`, eerst proberen een index.html aanroep af te handelen. Als dit bestand niet bestaat, zal het pas proberen om index.php af te handelen. Echter, al onze Joomla! websites verwerken alleen de index.php, dus deze controle vertraagt onnodig elke pagina aanvraag. Deze regel werkt om dit probleem heen. Let wel dat sommige servers dit niet toestaan, en het kan resulteren in een lege pagina of een 'Internal Server Error' pagina.
Stel standaard verlooptijd in op 1 uur	Als uw server mod_expires heeft geïnstalleerd en geactiveerd, zorgt deze optie ervoor dat alle bestanden en pagina's die op de site worden afgehandeld een verlooptijd van 1 uur hebben, dit betekent dat de browser niet zal proberen ze te laden via het netwerk voordat een uur verstreken is. Dit is een zeer wenselijke eigenschap, want het versnelt uw website.
Automatisch comprimeren statische bronnen	Inschakelen van deze optie instrueert de server platte tekst te sturen, HTML, XML, CSS, XHTML, RSS en Javascript pagina's en bestanden naar de browser na hen te comprimeren met gzip. Dit vermindert de hoeveelheid overgedragen gegevens en versnelt de website. Aan de andere kant zouden een aantal zeer oude webbrowsers, zoals Internet Explorer 6, moeite kunnen hebben met het laden van de website.
Index.php omleiden naar de website's root	Normaal gesproken, uw site benaderen als `http://www.voorbeeld.com` en `http://www.voorbeeld.com/index.php` zal resulteren in dat dezelfde pagina wordt geladen. Behalve voor cosmetische redenen voor dit gedrag, kan het ook slecht zijn voor zoekmachine optimalisatie (SEO), omdat zoekmachines dit zien als twee verschillende pagina's met dezelfde inhoud ("duplicate content"). Inschakelen van deze optie zal verzoeken naar index.php, zonder extra parameter, omleiden naar de root van uw website en dit probleem negeren.

Leid www en niet www adressen om

De meeste webservers zijn ontworpen om www en niet www URL's op dezelfde manier te behandelen. Bijvoorbeeld, als uw website `http://www.voorbeeld.com` is, zullen de meeste servers ze ook weergeven als ze `http://voorbeeld.com` worden genoemd. Dit heeft vele bijwerkingen. Om te beginnen, als een gebruiker de website met www benaderd, in logt en dan de niet-www site bezoekt is hij niet meer ingelogd, waardoor een functioneel probleem met gebruikers van uw site ontstaat. Bovendien gelden de 'duplicate content' regels ook in dit geval. Daarom raden we u aan de omleiding instellingen van deze optie in te schakelen. De verschillende instellingen zijn:

- Niet omleiden. Er wordt niet omgeleid (schakelt deze functie uit)
- Leid niet www om naar www. Verzoeken aan de niet www site zullen worden omgeleid naar de www site, bijvoorbeeld `http://voorbeeld.com` zal worden omgeleid naar `http://www.voorbeeld.com`.
- Leid www om naar niet www. Verzoeken aan de www site zullen worden omgeleid naar de niet www site, bijvoorbeeld `http://www.voorbeeld.com` zal worden omgeleid naar `http://voorbeeld.com`.

Deze (oude) domeinnaam omleiden naar de nieuwe

Soms moet u uw website te migreren naar een nieuw domein, zoals wij destijds migreerde van joomlapack.net naar akeebabackup.com. Meestal gebeurt dit transparant, met beide domeinen wet dezelfde site gekoppeld op hosting niveau. Echter, terwijl een bezoeker de nieuwe domeinnaam opent, wordt in de adresbalk van zijn browser nog steeds de oude domeinnaam weergegeven, en zoekmachines zullen denken dat u een 'duplicate content' website hebt ingesteld, en verzend de resultaten naar het donkerste gat van de zoekmachine. Niet goed! Dus, u zou er beter aan doen het oude domein naar het nieuwe domein om te leiden met een 301 omleiding om zowel gebruikers als zoekmachines te waarschuwen voor de naamswijziging van uw domein. Dit is wat deze optie doet. U kunt meerdere oude domeinen ingeven gescheiden door komma's. Bijvoorbeeld:

```
joomlapack.net, www.joomlapack.net
```

zal alle toegangspogingen naar joomlapack.net en www.joomlapack.net omleiden naar het nieuwe domein.

Forceer HTTPS voor deze URL's (domeinnamen uitsluiten)

Onder normale omstandigheden moet Joomla! in staat zijn om automatisch bepaalde menu items om te leiden naar een beveiligd (HTTPS) adres. Dit is echter niet mogelijk als de HTTPS domeinnaam en de HTTP domeinnaam niet hetzelfde zijn, zoals gangbaar bij tal van shared hosts. Sinds Admin Tools aangepaste HTTPS domeinnamen ondersteunt kunt u deze functie gebruiken om het gebrek aan functionaliteit in Joomla! zelf op te heffen. Gebruik één URL per website exclusief http:// en uw domeinnaam. Bijvoorbeeld, als u `http://www.voorbeeld.com/eshop.html` naar `https://www.voorbeeld.com/eshop.html` wilt omleiden moet u `eshop.html` in een nieuwe regel van dit veld zetten. Makkelijk, vind je niet?

6.5. Systeem instellingen

Warning

Als u een back-up van uw site maakt en die wilt herstellen op een nieuwe host MOET u deze configuratie parameters veranderen om uw nieuwe server configuratie handmatig weer te geven. In feite, moet u uw.htaccess bestand verwijderen, en de parameters wijzigen, en Admin Tools een nieuw .htaccess bestand laten maken voordat de front-end u uw site kunt gebruiken.

Dit laatste hoofdstuk bevat alle mogelijkheden die .htaccess maker laat weten, dat de meest elementaire informatie met betrekking tot uw website, die gebruikt wordt om de regels voor een aantal van de opties in de vorige paragraaf aan te maken.

Hostnaam voor HTTPS verzoeken (zonder https://)	Geef de domeinnaam voor veilige (HTTPS) verbindingen. Standaard neemt Admin Tools aan dat het hetzelfde is als het domein van uw website, maar u moet het wel controleren omdat het anders zijn kan op sommige hosts, in het bijzonder op shared hosts. Gebruik geen https:// prefix, alleen de domeinnaam en het pad naar uw website. Bijvoorbeeld, als het adres `https://www.voorbeeld.com/joomla` is, type dan `www.voorbeeld.com/joomla`.
Hostnaam voor HTTP verzoeken (zonder http://)	Geef de domeinnaam voor veilige (HTTP) verbindingen. Standaard neemt Admin Tools aan dat het hetzelfde is als het domein van uw website, maar u moet het wel controleren omdat het anders zijn kan op sommige hosts, in het bijzonder op shared hosts. Gebruik geen http:// prefix, alleen de domeinnaam en het pad naar uw website. Bijvoorbeeld, als het adres `http://www.voorbeeld.com/joomla` is, type dan `www.voorbeeld.com/joomla`.
Volg symlinks (kan leiden tot een lege pagina of een 500 Internal Server Error)	Deze optie voegt de "Options + FollowSymLinks" richtlijn aan uw .htaccess bestand toe. Op sommige hosts is dit al vastgelegd in de systeem wijde configuratie en is het u niet toegestaan om deze optie in te stellen. In feite, op die servers en alleen op die servers, krijgt u een '500 Internal Server Error' of een lege pagina als u dat doet. Op servers die het niet server breed hebben opgezet, moet u het het inschakelen voor de juiste werking van uw Joomla! website.
Basis map van uw website (/ voor de root van de domeinnaam)	Dit is de map waarin uw website is geïnstalleerd. Bijvoorbeeld als deze is geïnstalleerd in een map met de naam `joomla` en u benaderd het met een URL vergelijkbaar met `http://www.voorbeeld.com/joomla` dan moet u hier `/joomla` in typen. Als uw site is geïnstalleerd in de root van uw domein, moet u gebruik maken van een forward slash in dit veld: `/`

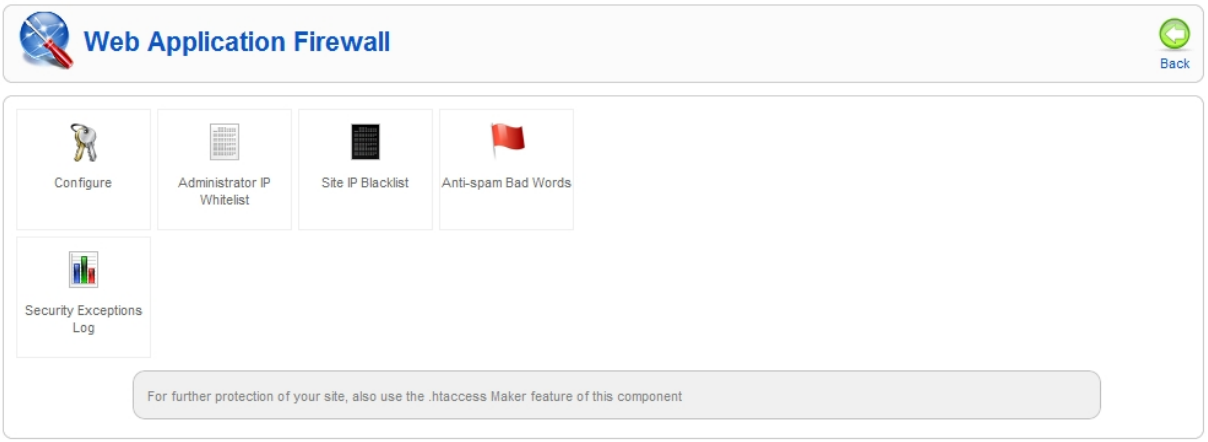
7. Web Applicatie Firewall

Note

Deze optie is alleen beschikbaar in de Professional release.

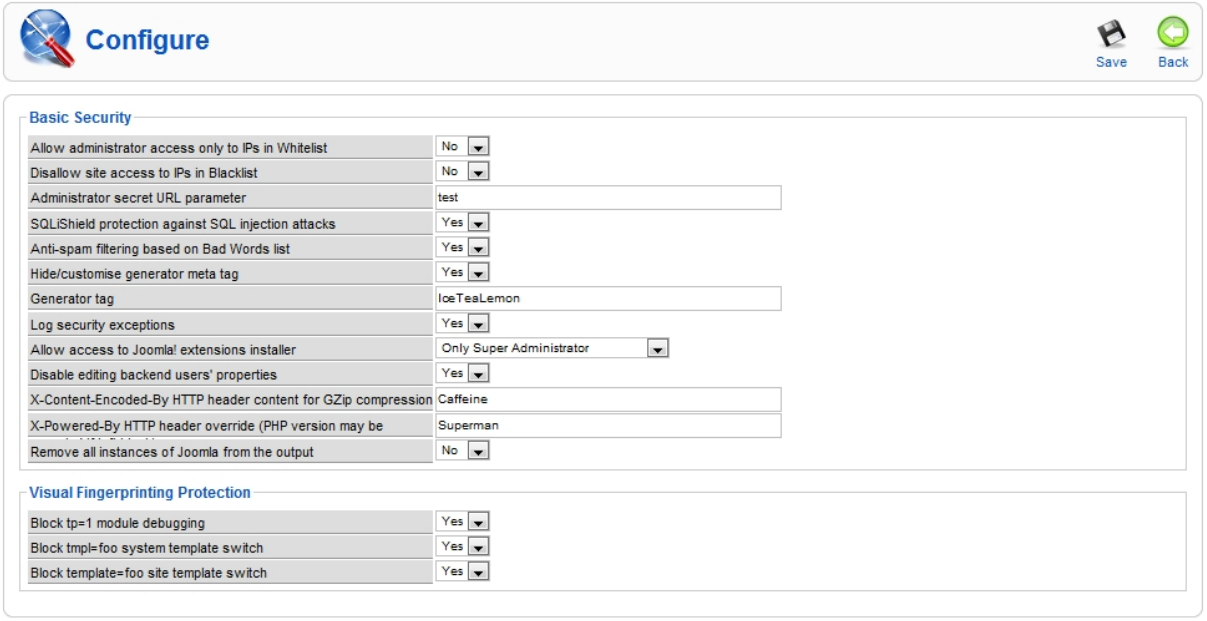
De Web Applicatie Firewall optie van Admin Tools is ontworpen om in real-time bescherming te bieden tegen de meest voorkomende fingerprinting aanvallen, gebruikt door aanvallers om informatie over uw site te verzamelen om een aanval op maat, en de meest voorkomende overige aanvallen uit te voeren. De real-time bescherming wordt uitgevoerd door de "System - Admin Tools" plugin (`plg_admintools`). Voordat u Admin Tools WAF instelt moet u ervoor zorgen dat de plugin is gepubliceerd en deze voor het eerst wordt uitgevoerd, dat wil zeggen het moet eerst in het sorteer menu voorkomen. Deze voorwaarden worden automatisch toegepast wanneer u de Admin Tools bundel installeert. Echter, als u meer systeem plugins heeft geïnstalleerd moet u ervoor zorgen dat plg_admintools wordt gepubliceerd vóór alle andere systeem plugins. Zo niet, dan zal de aangeboden bescherming niet grondig zijn.

Wanneer u de Web Applicatie Firewall functie van Admin Tools start, wordt de WAF Controle Paneel pagina weergegeven:



Door te klikken op een pictogram start u de respectievelijke sub-tool. De Terug knop rechts bovenaan in de werkbalk brengt u terug naar de Controle Paneel pagina.

7.1. Instellingen



Deze sub-tool is waar alle configuratie fijn afstemming van de firewall plaatsvindt. Standaard zijn geen van deze opties ingeschakeld tijdens de installatie. U moet hen handmatig inschakelen. Zodra u tevreden bent met uw opties klikt u op Opslaan om de wijzigingen op te slaan en terug te keren naar de WAF Controle Paneel pagina, of Terug om terug te keren zonder op te slaan.

Important

Als u iets verkeerd doet en u zich per ongeluk buitensluit van het administrator back-end gebied van uw site, geen paniek! Lees deze paragraaf over het herkrijgen van toegang.

Het eerste deel van de WAF configuratie is de Basisbeveiliging, en bevat de volgende opties:

Aangepast bericht
: Standaard maakt Admin Tools gebruik van een generiek bericht ("Denk je dat het lukt?"), wanneer een beveiligingsuitzondering optreedt. Gezien het feit dat dit misschien niet precies het soort bericht is dat u aan uw bezoekers wilt tonen, laten we het u hier aanpassen. Typ gewoon het bericht in dat moet worden getoond aan bezoekers van de website, wanneer een beveiligingsuitzondering zich voordoet, bijvoorbeeld "We hebben gedetecteerd dat u mogelijk een veiligheidsrisico overtreding veroorzaakt door uw verzoek. Ga terug naar de vorige pagina en probeer het opnieuw."

Laat Administrator toegang alleen toe van IP adressen in de whitelist
: Wanneer ingeschakeld, zullen alleen IP adressen in de Whitelist (zie de volgende hoofdstukken van deze documentatie over het configureren ervan) worden toegestaan op het administrator back-end gedeelte van de site. Alle andere pogingen om toegang tot de administrator pagina's te krijgen wordt doorgestuurd naar de startpagina van de website. Wees voorzichtig bij het gebruik van deze functie! Als u uw eigen IP nog niet heeft toegevoegd aan de Whitelist wordt u buitengesloten van de administrator omgeving!

Important

Vanaf Admin Tools 2.1.7, ongeacht of deze optie is ingeschakeld, IP adressen toegevoegd aan de administrator IP whitelist worden volledig ge-whitelist wat Admin

Tools betreft. Dit betekent dat er geen beveiligingsmaatregel zal worden toegepast tegen deze IP adressen. Plaats dus uitsluitend zeer goed vertrouwde IP adressen in deze lijst! Als een aanval tegen uw site vanaf een IP uit de whitelist wordt gelanceerd, zal het niet worden geblokkeerd door Admin Tools!

Blokkeer website toegang voor IP adressen in de blacklist

Wanneer ingeschakeld, als het IP adres van de bezoeker in de Blacklist is opgenomen (zie de volgende hoofdstukken van deze documentatie over het configureren ervan) zullen zij meteen een 403 Forbidden foutmelding krijgen wanneer zij proberen uw website te benaderen.

Administrator geheime URL parameter

Normaal gesproken, heeft u toegang tot het administrator back-end van uw website met behulp van een URL als bijvoorbeeld `http://www.voorbeeld.com/administrator`. Potentiele hackers weten dat ook en zullen proberen uw administrator back-end op dezelfde manier te benaderen. Vanaf dat punt kunnen ze proberen om met bruteforce aanvallen (automatisch raden uw gebruikersnaam en wachtwoord) zich in te loggen of gewoon gebruik maken van het feit dat een administrator back-end bestaat, om daaruit af te leiden dat uw website onder Joomla! draait om het aan te vallen. Door hier een woord in te invoeren, bent u verplicht dat op te nemen als een URL parameter om uw administrator back-end te kunnen benaderen. Bijvoorbeeld, als u het woord *test* hier ingeeft, kunt u alleen uw administrator back-end benaderen met een URL vergelijkbaar met `http://www.voorbeeld.com/administrator?test` . Alle andere pogingen om administrator back-end toegang te krijgen worden omgeleid naar de startpagina van de website. Als geen gebruik wilt maken van deze functie, kunt u dit veld leeg laten.

Important

De geheime URL parameter *moet* met een letter beginnen. Als het met een cijfer begint, krijgt u onmiddlijk een foutmelding als "IIlegal variable _files of _env of _get of _post of _cookie of _server of _session of globals passed to script" wanneer u probeert uw administrator back-end te benaderen. Het moet ook alleen maar kleine letters, hoofdletters, ASCII-tekens en cijfers (az, AZ, 0-9) bevatten om de meest uitgebreide compatibiliteit met alle mogelijke combinaties van browsers en servers te garanderen.

E-mail naar dit adres bij een succesvolle back-end login

Vul een e-mail adres in waar een melding naar wordt verstuurd wanneer iemand succesvol inlogt op de administrator back-end van uw website. Als u deze functie niet wilt gebruiken, laat het veld dan leeg. Als u een e-mail adres invult, telkens als iemand zich aanmeldt in het administrator back-end zal er een e-mail worden verstuurd naar dit e-mailadres met vermelding van de gebruikersnaam en sitenaam. Hierdoor krijg u direct een melding bij onverwachte administrator back-end logins die een teken kunnen zijn van een gehackte website. In dat onwaarschijnlijke geval, moet u direct inloggen op uw site back-end omgeving, en naar Extensies, Admin Tools gaan en klikken op de Off-line bij noodgevallen modus knop. Hierdoor wordt de toegang van de hacker tot uw hele website geblokkeerd en geeft u ruim de tijd om uw website en de extensies te upgraden, evenals het wachtwoord (en misschien de gebruikersnaam) te wijzigen van de gecompromitteerde Super Administrator account. Voor een maximale beveiliging, moet u na het opnieuw on-line zetten van uw website, eerst uitloggen, uw browser cookies en cache opschonen, en opnieuw inloggen.

E-mail naar dit adres bij mislukte administrator login

Vul een e-mail adres in dat een melding ontvangt wanneer iemand probeert in te loggen op uw site's administrator back-end, maar de toegang is geweigerd. Als u deze functie niet wilt gebruiken, laat het veld dan leeg. Als u een e-mail adres invult, zal telkens als iemand zonder succes probeert in te loggen op de administrator back-end een e-mail worden verzonden naar dit e-mailadres met vermelding van de gebruikersnaam en sitenaam. Hierdoor krijg u direct een melding bij onverwachte administrator back-end logins die een teken kunnen zijn van een gehackte website. In dat onwaarschijnlijke geval, moet u direct inloggen op uw site back-end omgeving, en naar Extensies, Admin Tools gaan en klikken op de Off-line bij noodgevallen modus knop. Hierdoor wordt de toegang van de hacker tot uw hele website geblokkeerd en geeft u ruim de tijd om uw website en de extensies te upgraden, evenals het wachtwoord (en misschien de gebruikersnaam) te

wijzigen van de gecompromitteerde Super Administrator account. Voor een maximale beveiliging, moet u na het opnieuw on-line zetten van uw website, eerst uitloggen, uw browser cookies en cache opschonen, en opnieuw inloggen.

SQLi Schilt, bescherming tegen SQL injectie aanvallen

Wanneer ingeschakeld, zal Admin Tools proberen gemeenschappelijke SQL injectie aanvallen tegen uw site te detecteren en ze te blokkeren. Let wel, dit is geen waterdichte oplossing. Sommige aanvallen kunnen er nog steeds doorkomen en er is een zeer kleine kans op false positives, dat wil zeggen, waarbij legitieme verzoeken geïdentificeerd worden als SQLI aanvallen.

Cross Site Scripting blokkering (XSS Schild)

Wanneer ingeschakeld, zal Admin tools proberen gemeenschappelijke cross site scripting (XSS) aanvallen te detecteren tegen uw site te detecteren en ze te blokkeren. De filtering is in staat om veel van dit soort aanvallen te detecteren, bestaande uit kwaadaardige Javascript en PHP code, maar het kan niet uitputtend. Hackers vinden elke dag nieuwe soorten aanvallen. U wordt geadviseerd om met gezond verstand uw veiligheidspraktijken (zoals het direct bijwerken van al uw extensies en templates naar hun nieuwste releases) te volgen bovenop het gebruik van deze functie.

Schadelijke user-agent blokkeren (MUA Schild)

Veel hackers zullen proberen om toegang tot uw site te krijgen met een speciaal geprepareerde browser om kwaadaardige PHP code te sturen in de 'user agent' string (een klein stukje tekst in de header, gebruikt om de browser aan uw server te beschrijven). Het idee is dat buggy log verwerkingssoftware het zal parsen en de hacker de controle geeft over uw website. Wanneer deze functie is ingeschakeld kan Admin Tools dergelijke aanvallen detecteren en de aanvraag blokkeren.

CSRF / Anti-spam formulierbeveiliging (CSRF Schild)

Eén van de grootste problemen met betrekking tot web formulier achtige login formulieren, contact formulieren, e.d. is dat ze kunnen worden uitgebuit door geautomatiseerde scripts (bots). Dit wordt meestal uitgevoerd om spam berichten of brute-force wachtwoorden te verzenden. Admin Tools heeft twee methoden om een dergelijk misbruik, afhankelijk van de instelling van deze optie te voorkomen:

- `Nee`. Hiermee schakelt u deze functie uit.
- `Basis`. Voert basis referer filtering uit. Als de browser van de bezoeker meldt dat de vorige pagina niet tot uw site behoorde, zal Admin Tools de verwerking van het formulier blokkeren. Dit is genoeg om script kiddies en simpele spam bots tegen te gaan, maar zal niets doen tegen meer ernstige aanvallen.
- `Uitgebreid`. Bovenop de basis bescherming, zal Admin Tools automatisch een verborgen veld injecteren op alle formulieren. Spambots, zullen meestal proberen om alle velden op een formulier, inclusief de verborgen velden in te vullen. Wanneer dit gebeurt, zal Admin Tools het verzoek blokkeren. Dit is een betere methode, maar het is veel trager en niet aanbevolen voor high-traffic (enkele tienduizenden bezoekers per dag) websites.

Bestandsinjectie op afstand blokkering (RFI Schild)

Sommige hackers zullen proberen om een kwetsbare extensie dwingen PHP code direct vanaf hun server te laten laden. Dit wordt gedaan door het sturen van een http(s):// of ftp:// URL in hun verzoek, verwijzend naar hun kwaadaardige site. Wanneer deze optie is ingeschakeld, zal Admin Tools van dergelijke gevallen proberen om de externe URL op te halen en de inhoud ervan te scannen. Als het blijkt PHP code te bevatten, zal het verzoek geblokkeerd worden.

Important

Als uw site witte pagina's begint te geven bij het indienen van een URL in uw site front-end, schakelt u deze optie dan uit. De witte pagina betekent dat uw server niet gevoelig is voor dit soort aanvallen en geeft dit niet juist door aan Admin Tools wanneer daarom wordt gevraagd. In dit geval, crasht Admin Tools terwijl het probeert de inhoud van de remote locatie te scannen, waardoor de witte pagina fout wordt veroorzaakt. Het uitschakelen van deze optie is een dergelijk geval, en vormt geen gevaar voor de veiligheid.

Directe bestandsinjectie blokkering (DFI Schild)

Sommige hackers proberen kwetsbare componenten te verleiden tot het laden van willekeurige bestanden. Afhankelijk van het kwetsbare component, wordt het bestand ofwel letterlijk uitgevoerd of geparsed als een PHP bestand. Dit laat aanvallers toe gevoelige informatie over uw site openbaar te maken, of kwaadaardige code te uploaden naar uw site en uit te voeren via een andere kwetsbare vector, bijvoorbeeld een ongefilterde upload van uitvoerbare PHP code. Wanneer deze optie is ingeschakeld, zal Admin Tools zoeken in de request parameters naar iets dat lijkt op een pad. Als er een wordt gevonden, wordt deze gescand. Als het blijkt PHP code te bevatten, wordt het verzoek afgewezen.

Uploads scanner (Upload Schild)

Wanneer deze optie is ingeschakeld, zal Admin Tools alle bestanden die zijn geüpload door Joomla! proactief scannen. Als één van deze bestanden zelfs maar één enkele regel PHP code bevat, wordt het verzoek geblokkeerd. Dit kan sommige soorten erg gevaarlijke aanvallen voorkomen, zoals het uploaden van kwaadaardige PHP code verpakt in avatar afbeeldingen. Let wel dat niet alle servers deze functie ondersteunen. Als de geüploade bestanden map wordt geblokkeerd door 'open_basedir' restricties, zal er geen scanning plaatsvinden. Bij twijfel, vraag uw host of ze 'open_basedir' restricties hebben die de toegang tot de PHP upload map blokkeren. Als de host bevestigend antwoord, zal deze Admin Tools functie niet werken, tenzij deze beperking wordt opgeheven.

Warning

NIET ALLE COMPONENTEN STAAN ADMIN TOOLS TOE OM HUN UPLOADS TE SCANNEN! Sommige componenten maken geen gebruik van Joomla!'s index.php toegangspunt bestand. In plaats daarvan gebruiken ze hun eigen toegangspunt bestand. Aangezien deze uploads niet via de Joomla! toepassing gaan, zal de Admin Tools code niet worden uitgevoerd en deze geüploade bestanden worden niet gescand. In dit geval, als de component kwetsbaar is bevonden, is uw website nog steeds in gevaar. Wij stellen voor het gebruik van dergelijke componenten vermijden. Hoe weet u dat? Dat is eenvoudig. Als u gebruik maakt van de front-end bescherming optie van .htaccess Maker en u moest een uitzondering voor een component toevoegen, maakt het geen gebruik van Joomla!'s index.php en is in potentie kwetsbaar voor dit soort code upload aanvallen.

Anti spam filtering gebaseerd op slechte woorden lijst

Wanneer ingeschakeld, worden alle aanvragen die ten minste één woord uit de slechte woorden lijst bevat (apart geconfigureerd, zie de volgende alinea's) geblokkeerd. Standaard is de slechte woorden lijst leeg, u moet het configureren van uw site afstemmen op de behoeften. Een goed idee is om de farmaceutische, luxe horloges en schoenen merknamen te nemen, omdat dit het merendeel van commentaar en contact spam op websites is.

Verbergen / Aanpassen generator metatag

Alle Joomla! installaties stellen de meta-tag generator tag in, een stukje HTML code in de header van alle pagina's, om bekend te maken dat uw site op Joomla! draait. Deze informatie wordt gecached door zoekmachines en wordt gebruikt door de aanvallers om te bepalen of uw site op Joomla! draait bij het zoeken naar potentiële doelwitten. Het uitschakelen van de generator tag vereist normaal het wijzigen van Joomla! core bestanden. In plaats daarvan kunt u deze optie inschakelen en een aangepaste waarde ingeven voor de generator tag in de volgende optie. Wees inventief! Gebruik iets raars, zoals 'Een miljoen apen met typemachines' of 'loop op water', of door het toekennen van de naam van een andere CMS, zoals "Drupal" of "WordPress".

Genereer eigen metatag

Als de vorige optie is ingeschakeld, is dit wat de generator meta tag waarde zal zijn.

Log beveiligingsuitzonderingen

Voorgesteld wordt om deze optie in te schakelen. Wanneer ingeschakeld, alle mogelijke inbreuken op de beveiliging —geblokkeerd door Admin Tools— zullen worden vastgelegd in de database en ter beschikking worden gesteld onder de Log beveiligingsuitzonderingen tool.

Het inschakelen van deze optie zal ook een bestand genaamd `admintools_breaches.log` in uw website's `logs` map. Dit bevat alle debug details die Admin Tools detecteerd wanneer het een 403 error betreft. Voeg dit log bestand, of tenminste dat deel dat relevant is voor de 403 error pagina die u ontvangt, bij uw verzoek om ondersteuning, om u beter van dienst te kunnen zijn. Hou er rekening mee dat uw logs map beschrijfbaar MOET zijn om het logbestand te kunnen produceren.

E-mail naar dit adres bij beveiligingsuitzonderingen

Vul een e-mail adres in waar een melding naar wordt verstuurd wanneer er een beveiligingsuitzondering op uw website plaats vind. Een "Beveiligingsuitzondering" is alles wat Web Applicatie Firewall triggert. Dit is handig om een waarschuwing vooraf te krijgen in het geval een bot probeert om een reeks aanvallen op uw website uit te voeren.

Sta toegang tot Joomla! extensies installer toe

Deze opties bepaalt wie toegang heeft tot Joomla!'s extensies installer. Als u zich hier nog niet van bewust bent, zowel Super Administrators als regelmatige Beheerders hebben toegang tot deze optie. Gezien het feit dat de extensies installer kan worden gebruikt om uitvoerbare code in te voeren, en database SQL commando's uit kan voeren op uw website, kan deze optie worden benut door insider aanvallen. In feite, hoeft een potentiële aanvaller slechts een Administrator account te compromitteren om "eigenaar" (wreck havoc on) van uw site te worden. Het Joomla! beveiligingsteam is zich bewust van deze claim, compleet met gedetailleerde instructies die deze techniek demonstreren, maar toch we hebben besloten om het af te doen als een "non issue". Ik ben 'liever safe dan sorry' en ik wed dat u dat ook wilt. Dit is de reden waarom deze optie bestaat en de volgende mogelijke instellingen heeft:

- **Administrators en hoger (standaard)**. Zowel Administrators als Super Administrators hebben toegang tot de Joomla! Extensies Installer. Dit is het standaard, onveilige, Joomla! gedrag.
- **Alleen Super Administrators**. Administrators hebben geen toegang tot de extensies installer, alleen Super Administrators hebben toegang. Dit is de aanbevolen instelling.
- **Niemand**. Volledig vergrendelen van de extensies installer, niemand heeft toegang, tenzij deze optie wordt gewijzigd in een lagere instelling.

Bewerken back-end gebruikers eigenschappen uitschakelen

Wanneer ingeschakeld, zullen pogingen de instellingen van een bestaande of een nieuwe manager te wijzigen, of het maken van een nieuwe Administrator of Super Administrator account mislukken.

X-Inhoud codering door HTTP header inhoud voor gzip compressie

Wanneer u de GZip compressie inschakelt in de Algemene Configuratie van uw website, voegt Joomla! een onzichtbare HTTP header met reclame over haar naam toe. Hoewel u deze niet ziet, kunnen aanvallers met hun tools het wel zien. Ze kunnen eruit afleiden dat uw site een potentieel doelwit is voor hun aanvallen. Hier iets anders invoeren zal de scan tools voor de gek houden en aanvallen tegen gaan. Wees creatief als het op het verzinnen van een tekst gaat!

X-Gedreven HTTP header voorrang geven (PHP kan als leeg worden getoond)

Net als Joomla!, PHP is 'hoofd over klif' in het ijdelheid spel. Alle PHP sites bevatten een onzichtbare HTTP header reclame, niet alleen het feit dat u PHP draait, maar zelfs de PHP versie die u gebruikt! Dit is waardevolle informatie om een potentiële aanvaller, vooral als uw host een verouderde versie van PHP (FYI, dat is een angstaanjagende 90% van de live hosts onder onze gebruikers) heeft. Wees creatief! Gebruik iets geks en onverwachts.

Verwijder alle voorkomende tekst 'Joomla' van de uitvoer

Gebruik deze optie met UITERSTE VOORZICHTIGHEID. Wanneer ingeschakeld, zal dit alle voorkomende gevallen van de woorden "Joomla!" en "Joomla" strippen uit de HTML uitvoer van uw webpagina's. Als uw site naam, map naam of een SEF URL pad het woord "Joomla" bevat zal het uw website breken. Dit betekent ook dat als u probeert deze optie te gebruiken met een site die gebruik maakt van de standaard Joomla! voorbeeld inhoud, u op ram koers ligt en een gebroken

website het gevolg zal zijn. U bent gewaarschuwd. In alle andere gevallen moet het veilig zijn deze optie in te schakelen, omdat het ervoor zorgt dat u niet per ongeluk sporen achter laat die kunnen worden gebruikt door een potentiële aanvaller om af te leiden dat uw website op Joomla! draait.

Het tweede deel heet Visuele fingerprinting beveiliging en bevat opties om een aantal debugging functies van Joomla! uit te schakelen die routinematig worden uitgebuit door aanvallers op zoek naar Joomla! websites om hun aanvallen tegen te laten plaatsvinden. Het idee is dat potentiële aanvallers geautomatiseerde tools gebruiken om duizenden websites te scannen, en probeert te identificeren wie van hen Joomla! draait. Met behulp van deze opties, de opties in de vorige paragraaf en de .htaccess Maker functie, zullen uw site onzichtbaar maken voor dergelijke fingerprinting (scanning) aanvallen door middel van 'cloaking'.

Blokeer tp=1 module debugging

Weneer u `?tp=1` toevoegd aan een URL naar een Joomla! website zal het al de module posities op de pagina weergeven. Voor een live voorbeeld, veel plezier met www.joomla.org?tp=1 [http://www.joomla.org?tp=1]. Het inschakelen van deze optie zal deze verborgen Joomla! functie uitschakelen.

Important

Deze beperkingen ZIJN NIET VAN TOEPASSING op Super Administrators die zijn ingelogd op de front-end van de website! Bovendien werkt deze functie niet onder Joomla! 1.6 en hoger omdat deze geen gebruik maaken van de tp=1 functie om module posities te tonen, in plaats daarvan heeft Joomla! 1.6 en hoger een Algemene Configuratie optie in de back-end.

Blokkeer tmpl=foo systeem template wisseling

Een van de minder bekende Joomla! kenmerken zijn de systeem templates. Wanneer een fout optreedt of u uw website off-line haalt, laadt Joomla! de desbetreffende systeem template. Door het toevoegen van de naam van de template in de URL, bijvoorbeeld `?tmpl=offline` stelt u in staat deze sjablonen te testen, zonder dat hij daadwerkelijk een fout zal produceren of uw site off-line zal halen. Voor een live voorbeeld, veel plezier met http://www.joomla.org/?tmpl=offline. Het inschakelen van deze optie zal deze verborgen Joomla! functie uitschakelen. Hou er rekening mee dat tmpl=system en tmpl=component altijd moeten worden toegestaan, omdat ze benodigd zijn om een aantal extensies te kunnen laten werken.

Lijst van toegestane tmpl= sleutelwoorden

De lijst van tmpl sleutelwoorden die toestemming moeten hebben van uw site, als een door komma's gescheiden lijst. Op zijn minst MOET u system en component in de lijst Zetten, anders zal Joomla! niet goed werken. Standaardwaarden: `component,system`

Blokkeer template=foo website template wisseling

Nog een verborgen Joomla! functie is de mogelijkheid om tussen geïnstalleerde templates schakelen door het toevoegen van speciale URL parameters. Bijvoorbeeld, als u de JA Purity template toe wilt passen, voeg dat de parameter `?template=ja_purity` toe. Voor een live voorbeeld, veel plezier met http://www.joomla.org/?template=ja_purity. Het inschakelen van deze optie zal de verborgen Joomla! functie uitschakelen.

Project Honeypot integratie stelt u in staat om de spam bestrijding dienst 'Project Honeypot' te integreren. 'Project Honeypot' is een collectieve inspanning om spammers, e-mail harversters en crackers op te sporen. De HTTP:BL service staat deelnemers toe aan de hand van IP adressen queries van hun bezoekers, erachter te komen of het een kwaadwillende gebruiker betreft. Als u deze functie is ingeschakeld, zal Admin Tools het IP-adres van elke bezoeker controleren en bij 'Project Honeypot, én als het een kwaadwillende gebruiker betreft, zal Admin Tools hem blokkeren. U hebt de volgende opties:

HTTP:BL filtering inschakelen

Hiermee schakelt u de volledige functie aan en uit.

Project Honeypot HTTP:BL Key

Vul uw HTTP:BL sleutel in. U kunt zich aanmelden voor 'Project Honeypot' en krijg dan uw sleutel op http://www.projecthoneypot.org/httpbl_configure.php.

Minimaal te blokkeren dreigingswaardering (0-255, standaard 25)	Project Honeypot maakt gebruik van een logaritmische "threat rating" om de mogelijkheid te onderzoeken of een specifiek IP adres aan een spammer toebehoord. Deze optie bepaalt het minimale dreigingsniveau dat een IP adres moet hebben voordat het geblokkeerd wordt. Een waarde van 25 betekent dat deze IP 100 spam berichten heeft ingediend op Project Honeypot's spam vangende honeypots en is meestal een veilige indicatie dat het hier een spammer betreft. Let wel dat de rating logaritmische is. Een waarde van 50 betekent 1000 spam berichten en een waarde van 75 betekent een miljoen spam berichten. Stel dit niet in op waarden boven de 50, want u zal spammers waarschijnlijk nooit helemaal kunnen uitbannen.
Maximum leeftijd van geaccepteerde HTTP:BL resultaten	Project Honeypot rapporteert wanneer de laatste keer was dat een IP werd betrapt op het verzenden van spam berichten. Hoe langer dit geleden is (hoe hoger de leeftijd is), hoe kleiner de kans is dat dit IP nog steeds wordt gebruikt door een spammer. U kunt hier kiezen wat de maximale meld leeftijd moet zijn om te worden geblokkeerd. De standaard waarde van 30 betekent dat de IP's die in de afgelopen 30 dagen een spam bericht hebben ingediend zullen worden geblokkeerd.
Blokkeer ook verdachte IP adressen, niet alleen bevestigde spammers	Soms is Project Honeypot niet zeker of een IP tot een spammer behoort, of het is een ongelukkige kerel die op de verkeerde link heeft geklikt. In dit geval is het IP gemarkeerd als "verdacht". Het standaard gedrag is deze IP adressen niet te blokkeren. Echter, als u veel spam ontvangt is het een goed idee om deze functie in te schakelen en zelfs "verdacht" IP's te blokkeren. Uiteindelijk, zullen ook sommige ongelukkige gebruikers per ongeluk geblokkeerd worden, dus gebruik deze optie met de nodige voorzichtigheid!

Slecht gedrag integratie stelt u in staat de Slecht Gedrag filtering algoritmen in te schakelen. In het kort, deze algoritmes proberen spammers en hackers op basis van de manier waarop ze proberen uw website te benaderen, ze te blokkeren voordat ze enige schade aan uw website kunnen aanrichten. U hebt de volgende opties:

Slecht gedrag filter inschakelen	Schakelt deze functie aan/uit
Strikte Modus	Wanneer ingeschakeld, wordt het filter strenger. Aan de andere kant, kan het per ongeluk toegang van legitieme bots afsnijden, als zoekmachine indexers van specifieke zoekmachines. Over het algemeen raden u aan deze functie uit te schakelen.
Whitelist IP adressen (komma gescheiden lijst)	Geef een lijst van IP adressen die niet mogen worden geblokkeerd door Slecht Gedrag filtering. Wij raden het toevoegen van het IP adres van PayPal's IPN (66.211.170.66) aan deze lijst.

Tot slot kunt u eenvoudig Auto-ban recidivisten gebruiken. Met deze functie kunt u automatisch IP's bannen die veiligheidsuitzonderingen activeren. Dit kan een effectieve maatregel blijken te zijn tegen kwaadwillende gebruikers die proberen uw site te testen op kwetsbaarheden. U MOET het loggen van veiligheidsuitzonderingen voor deze functie inschakelen om deze te laten werken. U kunt de volgende opties instellen om te bepalen hoe Admin Tools zich zal gedragen in deze gevallen:

IP blokkering van recidivisten	Indien ingesteld op ja, zal het IP adres van recidivisten automatisch worden gebanned op basis van de rest van de instellingen.
Deze IP adressen nooit blokkeren	Voer een door komma's gescheiden lijst van IP adressen in, die nooit automatisch moeten worden geblokkeerd. Een dergelijke lijst kan er bijvoorbeeld als volgt uitzien: `127.0.0.1, 123.124.125.126`

Tip

Als u de whitelist functie gebruikt om toegang tot de administrator back-end van uw site om specifieke IP adressen toe te staan, worden deze IP adressen automatisch toegevoegd aan de lijst van veilige IP adressen die nooit automatisch zullen worden geblokkeerd.

Important

Vanaf Admin Tools 2.1.7, zijn IP's die zijn toegevoegd aan deze lijst volledig gewhitelist. Dit betekent dat er geen beveiligingsmaatregel zal worden toegepast tegen deze IP adressen. Plaats dus uitsluitend zeer goed vertrouwde IP adressen in deze lijst! Als een aanval tegen uw site vanaf een IP uit de whitelist wordt gelanceerd, zal het niet worden geblokkeerd door Admin Tools!

E-mail naar dit adres als een IP automatisch wordt gebanned	Admin Tools kan een e-mail versturen wanneer een IP adres automatisch wordt gebanned, vul in dit veld een e-mail adres in dat een melding ontvangt wanneer een auto ban plaatsvindt. Dit staat u bijvoorbeeld toe, te bepalen of een IP adres regelmatig wordt geblokkeerd, in welk geval het een goed idee kan zijn om het in de permanente IP blacklist op te nemen. Laat dit veld leeg (standaard) om deze functie uit te schakelen.
Blokkeer na	Kies hoeveel aanvallen, binnen hoeveel tijd moeten plaatsvinden. Als u deze bijvoorbeeld op 3 aanvallen in 1 uur zet, zal Admin Tools een IP adres bannen waarvan minstens drie aanvallen zijn geblokkeerd in het laatste uur.
Blokkeer voor de duur van	Hoe lang de blokkering zal duren. Als u de instelling op 1 zet, zal de toegang vanaf dit IP adres één hele dag (24 uur) worden geblokkeerd.
Toon dit bericht aan geblokkeerde IP adressen	Stelt u in staat om een specifiek bericht weer te geven aan geblokkeerde IP adressen. U kunt bijvoorbeeld uitleg geven aan de gebruiker dat zijn IP is geblokkeerd, omdat er verdachte activiteiten werden gedetecteerd die afkomstig waren van zijn IP adres.

Warning

De blacklist maakt geen onderscheid. Als u bijvoorbeeld probeert uw administrator back-end te benaderen zonder een geheim woord zal uw IP adres geblokkeerd worden en u zult niet in staat zijn om uw eigen website te benaderen. In dat geval volg de handmatige override procedure om Admin Tools plug-in uit te schakelen en weer toegang tot uw website te krijgen, ga naar de 'Auto-ban recidivisten' functie en schakel deze uit.

7.1.1. Help, ik ben buiten gesloten van de administrator back-end van mijn website!

Het is mogelijk om per ongeluk uzelf buiten te sluiten van de administrator back-end, met name bij het gebruik van IP whitelisting of IP blacklisting opties van de Web Applicatie Firewall. De eenvoudigste manier om dit probleem te omzeilen is met behulp van een FTP toepassing of uw hosting controle paneel, File Manager om een bestand te hernoemen.

Ga naar de `plugins/system/admintools` map op uw website. U ziet daar een bestand `main.php` genaamd. Hernoem het naar `main-disable.php`. Dit zal de Web Applicatie Firewall uitschakelen en voorkomen dat deze wordt uitgevoerd, u kunt uw site back-end weer benaderen. Nadat u de oorzaak van het probleem heeft opgelost, vergeet dan niet het bestand `main-disable.php` te hernoemen naar `main.php`, anders laat u uw website onbeschermd!

7.2. WAF Uitzonderingen

Op deze pagina kunt u uitzonderingen op de WAF regels voor het filteren instellen. Waarom dit nodig is? Sommige componenten zijn ontworpen om goed en veilig gegevens te gebruiken en parsen, die toch de WAF regels triggeren. De meeste, meestal een component accepteren een absoluut pad naar bestanden op uw server, of kunnen complexe data parsen die in de regel leiden tot het triggeren van het WAF XSSSchild filter. Zonder uitzonderingen in te stellen, zouden deze componenten worden geblokkeerd en u zou niet in staat zijn om uw site goed te gebruiken. De oplossing is om de 'WAF filters' uit te schakelen, maar dit eindigt in het verlagen van de beveiliging van uw website. Met behulp

van het 'WAF Uitzonderingen' overzicht kunt u fijn-afstemmen welke componenten, weergaven en query parameters in de "veilige lijst" zijn opgenomen en nooit geblokkeerd mogen worden.

Note

WAF Uitzonderingen is een zeer nuttige en krachtige tool. Het is ook mogelijk dat u te veel beveiligingen toe past, die dan potentiële beveiligingsproblemen en gaten in de firewall openen. Wees zeer voorzichtig bij het gebruik ervan.

WAF Uitzonderingen worden gedefinieerd door het specificeren van een combinatie van drie dingen:

- *Component*. Op welk component de uitzondering van toepassing is. Bijvoorbeeld, als u filtering voor een query parameter in JCE wilt uitschakelen moet u dit op `com_jce` zetten. Als u wilt dat de uitzonderingen van toepassing zijn op alle componenten, maakt niet uit wat, laat dit dan leeg.

- *Toon*. Elke component heeft een of meerdere vertoningen. Als u SEF uitschakelt ziet u iets als `index.php?option=com_foobar&view=example&id=`1. Let op het view=example deel in deze URL; dit vertelt Joomla! dat de te tonen naam (bijvoorbeeld het gebied van de component die we willen gebruiken) is example. Zoals u misschien al heeft geraden, met de 'toon' optie in een WAF Uitzondering kunt u de doelstelling van de uitzondering op precies één maal bekijken instellen. Als u dit leeg laat, zal de uitzondering overeenkomen met alle weergaven.

  ### Important

  Joomla! vertaalt SEF URL's intern voor niet-SEF URL's! Dus, zelfs als u Joomla's SEF URL's gebruikt of een derde partij SEF extensie, de tonen en query parameters zijn altijd ingesteld - u kan ze gewoon niet zien. Het wordt sterk aanbevolen om SEF uit te zetten bij het opzetten van WAF Uitzonderingen om fouten te voorkomen.

- *Query Parameter*. Alles na het vraagteken in een niet-SEF URL heet de URL query. U zult ziet veel sleutel/waarde paren zien, zoals `id=1`, `category=1:test` en dergelijken. Het woord aan de linker kant van het 'is gelijk' (=) teken heet *Query Parameter*. De gelijknamige parameter in WAF Uitzonderingen staat u toe te richten op een zeer specifieke parameter query. Als u deze leeg laten, zullen alle query parameters worden afgestemd.

  ### Warning

  U kunt niet alle drie de opties blanco laten. Dat zou overeenkomen met alle componenten, met alle vertoningen en alle query strings of, met andere woorden, ELKE PAGINA die u benaderd. Dit zou impliceren dat het WAF zou effectief worden uitgeschakeld. Admin Tools detecteert een poging om dat te doen en zal niet toestaan dat u een dergelijke wijziging uitvoert.

WAF uitzonderingen begrijpen

De beste manier om WAF uitzonderingen te begrijpen, is door een aantal praktische voorbeelden.

Welke-component uitzondering. Stel component in op `com_jce`, laat weergave en query parameter leeg. Dit vertelt WAF dat als het een verzoek ziet voor JCE's hulpprogramma component (com_jce) het WAF moet uitschakelen, ongeacht welke weergave of query parameters zijn ingesteld. In wezen is WAF uitgeschakeld voor het gehele JCE component.

Uitzonderen van een enkele component weergave. Laten we zeggen dat we WAF willen uitschakelen voor alle front-end logins om te voorkomen dat door een complex wachtwoord een 403 fout wordt gegenereerd voor onze gebruikers. Front-end logins worden afgehandeld door de login com_user te weergave. Dus stel uw component gewoon in op `com_user`, en weergave op `login` en laat de query parameter leeg. WAF is nu uitgeschakeld voor de login / log uit pagina van uw website.

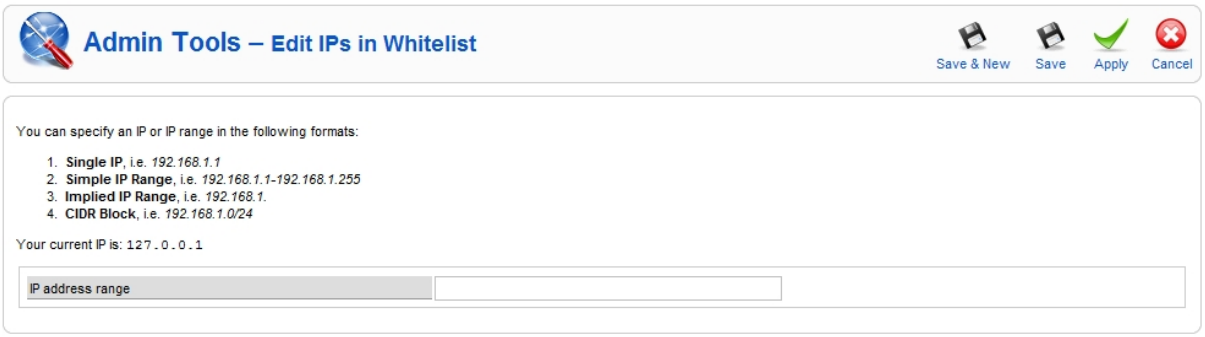
Uitzonderen van een query parameter van een specifieke component en weergave. Laten we zeggen dat we een com_foobar component hebben waarvan de test weergave accepteert en een pass parameter. Sterke wachtwoorden kunnen per ongeluk WAF activeren. Maak gewoon een nieuwe uitzondering waar component is `com_foobar`, weergave is `test` en query parameter is `pass`. WAF WAF zal zich niet bezig houden met deze specifieke query parameter op dat specifieke component en weergave, maar zal worden getriggert door onveilige inhoud doorgegeven in een andere query parameter op die bepaalde weergave.

Uitzonderen van een query parameter in alle componenten en weergaven. Laten we zeggen dat u veel 403 fouten op uw site ziet omdat verschillende componenten een wachtwoord query parameter gebruiken om wachtwoorden te aanvaarden en, zoals hierboven vermeld, kan leiden tot het triggeren van WAF bij complexe wachtwoorden. In plaats van jacht te maken op alle weergaven van alle componenten, kunt u gewoon component en weergave leeg laten de query parameter op `password` zetten Van nu af aan, wanneer WAF een wachtwoord parameter ziet langskomen in Joomla! zal het niet proberen om de beschermingsfilters ertegen toe te passen. Als andere query parameters binnenkomen met het verzoek van de gebruiker zullen ze worden gefilterd en, indien zij onveilige inhoud bevatten, wordt het verzoek toch geblokkeerd.

7.3. Administrator IP Whitelist

Op deze pagina kunt u de IP Whitelist beheren, de lijst van IP adressen of IP blokken die de toegang tot de administrator back-end van uw site definiëren. Het management gebeurt met behulp van de standaard Joomla! knoppen op de werkbalk. Klikken op een item, of het aanvinken van de box en klikken op Wijzigen zal u toelaten om de invoer te bewerken. Klikken op de Nieuw knop zal u toelaten een IP/IP bereik toe te voegen. Aanvinken van één of meerdere items in de lijst en klikken op Verwijder reactie zal deze van de lijst verwijderen.

The Edit/Add page looks like this:



Tip

Uw huidige IP adres wordt weergegeven direct boven het invoerveld. Zorg ervoor dat het de eerste is om toe te voegen zodat u uzelf niet buitensluit van de administrator back-end van uw website!

In het IP adres range veld kunt u een IP of IP range op één van de volgende manieren invoeren:

- Een enkele IP, b.v.b. 192.168.1.1

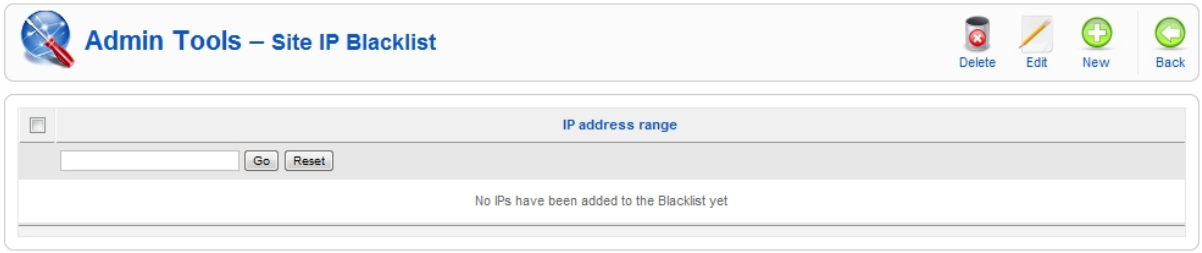
- Een simpele IP range, b.v.b. 192.168.1.1-192.168.1.255
- Een impliciete IP range, b.v.b. 192.168.1. voor alle IP's tussen 192.168.1.1 en 192.168.1.255, of 192.168. voor alle IP's van 192.168.0.1 tot 192.168.255.255.
- Een CIDR block [http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing], b.v.b. 192.168.1.1/8. Als u niet weet wat dit is, vergeet het dan, u zult het waarschijnlijk niet nodig hebben.
- Een Subnet Mask [http://en.wikipedia.org/wiki/Subnetwork] notatie, b.v.b. 192.168.1.1/255.255.255.0

Hou er rekening mee dat Admin Tools alleen IPv4 IP-adressen ondersteunt. IPv6 wordt (nog) niet ondersteund, tot dusver is er nog weinig ondersteuning van commerciële hosts.

Tip

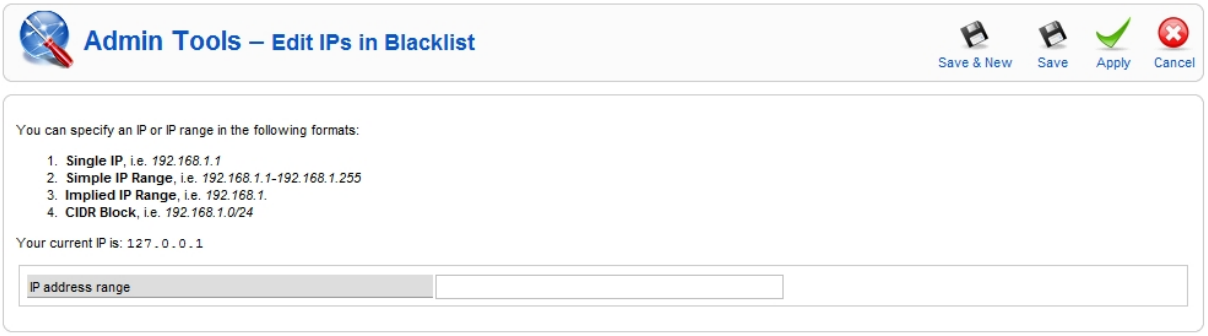
U kunt gebruik maken van de Opslaan & Nieuw om snel meerdere items toe te voegen zonder terug te hoeven gaan naar de administratie pagina en steeds op Nieuw te moeten klikken.

7.4. Website IP Blacklist



Op deze pagina kunt u de IP Blacklist beheren, de lijst van IP adressen of IP blokken die geen toegang tot de website hebben definiëren. Het management gebeurt met behulp van de standaard Joomla! knoppen op de werkbalk. Klikken op een item, of het aanvinken van de box en klikken op Wijzigen zal u toelaten om de invoer te bewerken. Klikken op de Nieuw knop zal u toelaten een IP/IP bereik toe te voegen. Aanvinken van één of meerdere items in de lijst en klikken op Verwijder reactie zal deze van de lijst verwijderen.

The Edit/Add page looks like this:



Tip

Uw huidige IP adres wordt weergegeven direct boven het invoerveld. Zorg ervoor dat het de eerste is om toe te voegen zodat u uzelf niet buitensluit van de administrator back-end van uw website!

In het IP Address Range veld kunt u een IP of IP range op één van de volgende manieren invoeren:

- Een enkele IP, b.v.b. 192.168.1.1

- Een simpele IP range, b.v.b. 192.168.1.1-192.168.1.255
- Een impliciete IP range, b.v.b. 192.168.1. voor alle IP's tussen 192.168.1.1 en 192.168.1.255, of 192.168. voor alle IP's van 192.168.0.1 tot 192.168.255.255.
- Een CIDR block [http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing], b.v.b. 192.168.1.1/8. Als u niet weet wat dit is, vergeet het dan, u zult het waarschijnlijk niet nodig hebben.
- Een Subnet Mask [http://en.wikipedia.org/wiki/Subnetwork] notatie, b.v.b. 192.168.1.1/255.255.255.0

Hou er rekening mee dat Admin Tools alleen IPv4 IP-adressen ondersteunt. IPv6 wordt (nog) niet ondersteund, tot dusver is er nog weinig ondersteuning van commerciële hosts.

Tip

U kunt gebruik maken van de Opslaan & Nieuw om snel meerdere items toe te voegen zonder terug te hoeven gaan naar de administratie pagina en steeds op Nieuw te moeten klikken.

7.5. Anti-spam Slechte woorden

Op deze pagina kunt de lijst van 'Slechte woorden' beheren. Het gebruik ervan zal worden verboden op de site. Als een query één van de woorden uit deze lijst bevat, zal dit resulteren in een 403 fout en het zal optioneel worden in uw Beveiligings uitzonderingen log. U kunt gebruik maken van de standaard Joomla! knoppen op de werkbalk om de lijst te beheren. Alle woorden zijn hoofdlettergevoelig, dit betekent dat ze niet worden uitgefilterd als ze niet overeenkomen met de kleine letters en hoofdletters van de woorden in de lijst.

Note

Sommige servers bevatten reeds een server-side filter om gemeenschappelijke spam woorden te vermijden. Als u een foutmelding krijgt, —meestal een 403 error of een fout met de opmerking dat u een ongeldig verzoek heeft— terwijl u probeert een woord op te slaan, raak niet in paniek. Het is uw server filter kicking in. Laat het woord dat u wilde toevoegen gewoon weg, omdat het al effectief gefilterd wordt door uw server!

7.6. Beveiligings uitzonderingen log

Een firewall is niets waard als het de pogingen om het te negeren niet kan loggen. Meestal zult u dezelfde soort aanvallen zien, over en weer komend van de zelfde IP adressen. Met behulp van deze log viewer faciliteit kunt u een duik in het logboek nemen, de IP's spotten en ze noteren, zodat u ze kunt bannen (ze in de Blacklist zetten).

Onder elke IP staat een link Toevoegen aan Black List of Verwijder van Black List. Klikken op de 'Toevoegen aan Black List' link voegt het IP adres van het betreffende record aan de IP Black List toe, en dat IP zal geen toegang meer tot uw website hebben. De 'Verwijder van Black List' link verwijdert het IP adres van de Black List.

7.7. Geografische blokkering

Verschillende gebruikers hebben gevraagd om een consistente manier om bezoekers uit bepaalde landen of werelddelen te blokkeren. Hoewel dit geen beveiliging toevoegt –zou een slimme cracker zich alleen maar verstoppen achter een anonieme proxy- het kan nog steeds nuttig zijn voor inherent regionale websites, zoals e-shops in staat stellen zaken te doen met alleen een handvol vertrouwde landen.

In de interface pagina van de Admin Tools 'Geografische Blokkering' kunt u selecteren welke landen en/of continenten u wilt blokkeren. Als het respectievelijke vakje aangevinkt is, wordt het geblokkeerd. Wanneer u klaar bent met het selecteren van de continenten of landen die u wilt blokkeren, klikt u op Opslaan.

Vergeet niet dat Admin Tools de MaxMind GeoLite database gebruikt om IP adressen te koppelen aan landen. Deze lijst is niet statisch, dat wil zeggen dat hij in de loop der tijd kan veranderingen. We raden u aan de maandelijks nieuwste versie te downloaden van MaxMing GeoLite database [http://www.maxmind.com/app/geoip_country] in binair formaat, van http://geolite.maxmind.com/download/geoip/database/GeoLiteCountry/GeoIP.dat.gz. Pak het gedownloade gecomprimeerde bestand uit met behulp van gunzip op Linux, 7-Zip op Windows of BetterZIP op Mac OS X. Het zal resulteren in een bestand met de naam `GeoIP.dat`. Upload het naar uw website in de `administrator/components/com_admintools/assets/geoip` map en overschrijf het bestaande bestand.

Important

Hoofdletter gevoeligheid is belangrijk! U moet het bestand uploaden als `GeoIP.dat`, en niet `geoIP.dat` of `geoip.dat`.

Zal ik deze functie gebruiken?

We zijn ervan overtuigd dat het geografisch blokkeren helemaal niets toevoegt aan de veiligheid van uw website. De meeste mensen denken "cool, ik kan die Russische spammers blokkeren". Niets is echter minder waar. De intelligente spammers en crackers gebruiken niet één enkele computer in hun eigen land om hun aanvallen op andere sites te lanceren. Ze zijn meestal onder controle van een botnet, een verzameling besmette computers over de hele wereld die doen wat ze opgedragen wordt. Gebruik makend van een dergelijk botnet, kunnen ze een spam operatie lanceren, waarvan het verkeer afkomstig is uit verschillende landen van over de hele wereld, zelfs het land waar u woont. Slimme crackers bovendien zullen nooit hun echte IP adres gebruiken om u aan te vallen. Ze maken meestal gebruik van een anonieme proxy of van het TOR netwerk. Het directe effect is dat het verkeer schijnbaar uit een ander land of uit een verscheidenheid van verschillende landen afkomstig is.

Dan is er ook nog de nauwkeurigheid factor. MaxMind claimt een nauwkeurigheid van 99%. Op een site met 10.000 bezoekers per dag wordt dit vertaald naar 100 bezoekers per dag die afkomstig zijn uit een ander land dan ze in werkelijkheid doen. Het dit klinkt misschien niet als een big deal, maar stel je hebt een e-shop en verliest hierdoor potentiële klanten. Dan wordt het opeens wel een big deal.

Al met al adviseren wij gezond verstand. IP filtering is als een uitsmijter bij de deur. U zou niet verwachten een uitsmijter naast de deur van uw bakkerij te vinden. Zo ook, overdrijf niet met geografisch blokkeren. Gebruik het spaarzaam.

8. Database tools

Let op, deze tools zijn te vinden in Admin Tools 'Controle Paneel' pagina sinds Admin Tools 1.0. In oudere versies stonden deze tools in een aparte pagina.

De database is het belangrijkste onderdeel van onze websites. Het bevat alle gegevens en de meeste configuratie opties, dat wil zeggen, alles wat onze website maakt tot wat het is. Echter, omdat de gegevens worden geschreven naar en verwijderd uit de database, worden de database tabellen steeds trager of zelfs beschadigd. Het is het hetzelfde als wat er gebeurt met het fragmenteren van harde schijven. Eén tabel, berucht om steeds zeer snel gefragmenteerd te te raken is de 'sessies tabel'. In feite, elke keer als een gast gebruiker uw site bezoekt of een gebruiker inlogt en weer uit logt van uw website wordt deze tabel steeds meer gefragmenteerd, tot op een dag, niemand zich meer kan aanmelden bij uw website, zelfs uzelf niet. Dit is een zeer veel voorkomend probleem, vooral op websites met veel verkeer.

Met een harde schijf weet u dat u altijd kan defragmenteren met bijvoorbeeld chkdisk of fsck (afhankelijk van uw Operating System). Voor databases moet u een zeer tijdrovend proces doorlopen met behulp van een database beheer tool, zoals phpMyAdmin, voor het herstellen en optimaliseren van elke tabel apart. Admin Tools hulpmiddelen voor databases zijn hier om dit lastige proces voor u te automatiseren!

Er zijn twee tools beschikbaar:

- Repareer en optimaliseer database tabellen doorloopt een reparatie en optimalisatie proces op alle database tabellen van uw website. Als het proces bij het eerste gebruik, langere tijd blijft hangen, probeer het dan opnieuw uit te voeren. Het gebruikelijke probleem is dat de Joomla! sessies tabel zo gefragmenteerd is dat PHP times out, wachtend op uw database server om deze tabel te optimaliseren.

- Sessies legen zal alleen de sessies tabel (volledig) legen en optimaliseren. Bij dit proces zal iedereen worden uitgelogd van de website, behalve uzelf als Super Administrator. Gebruik deze optie spaarzaam en alleen wanneer u ernstige problemen waarneemt wanneer gebruikers proberen in te loggen op de website.

Een verkorte versie van het optimalisatie proces, alleen het aanpakken van de sessies tabel, kan worden gepland te starten op een tijdschema, door gebruik te maken van de parameters van de "System - Admin Tools" plugin van de Professional versie.

9. Wijzig uw database tabellen prefix

Standaard wordt Joomla! geïnstalleerd met een database tabel prefix jos_ genaamd, tenzij u specifiek een andere prefix kiest. Helaas, weten hackers dat ook, en verwachten dat u de standaard instelling zo heeft gelaten, en passen hun aanvallen in die zin op aan. Voor meer informatie over de problemen van het gebruik van de standaard database tabel prefix kunt u mijn artikel lezen in Joomla! Community Magazine [http://magazine.joomla.org/issues/Issue-Aug-2010/item/108-the-prefix-has-nothing-to-do-with-telephony] (Engels). Admin Tools maakt het doodeenvoudig om deze prefix met één enkele klik, on-the-fly, te wijzigen.

Important

Maak een back-up van uw site en *haal uw site off-line* voordat u verder gaat. In het onwaarschijnlijke geval van een server crash, midden in het proces zal u de back-up nodig hebben om uw website te herstellen. U kunt altijd gebruik maken van de gratis Akeeba Backup [http://www.akeebabackup.com] component om een volledige website back-up te maken, of phpMyAdmin te gebruiken om uw database tabellen te exporteren.

De interface van deze functie is zeer eenvoudig. In het "Huidige prefix" tekstvak bovenaan kunt u zien wat uw huidige prefix is. In het "Nieuwe prefix" tekstvak eronder kunt de nieuw te gebruiken database tabel prefix invoeren. Standaard bevat dit velt een willekeurig aangemaakte prefix. U kunt natuurlijk ook een andere, door uzelf bedachte prefix invoeren. Prefixes moeten aan de volgende regels voldoen:

- Het moet bestaan uit 3 tot 6 kleine onbeklemtoonde letters of cijfers (az, 0-9), gevolgd door een underscore (_).
- Het mag geen gereserveerde prefix zijn zoals, jos_ of bak_.
- Het kan niet hetzelfde zijn als de huidige prefix.
- Het mag niet al in gebruik zijn voor een tabel in de database. Bijvoorbeeld, als u gebruik maakt van de prefix foo_ moet u ervoor zorgen dat er geen tabel in uw database gebruikt wordt waarvan de naam begint met foo_.

Maak u geen zorgen dat u het verkeerd zal doen. Admin Tools zal u waarschuwen. U moet er ook voor zorgen dat aan de volgende voorwaarden wordt voldaan:

- Uw `configuration.php` bestand in uw website's root moet beschrijfbaar zijn.
- Als alternatief, moet u Joomla!'s FTP opties inschakelen in de Algemene instellingen van uw back-end, en ervoor zorgen dat u uw gebruikersnaam en wachtwoord heeft opgeslagen.

Als Admin Tools detecteert dat het, het configuration.php bestand niet kan bijwerken zal het u waarschuwen en de database tabel prefix wijziging afbreken.

Wanneer u klaar bent, klik op de Verander prefix knop. Dit zal uw `configuration.php` bestand updaten met de nieuwe prefix en het ALTER TABLE commando in uw database uitvoeren om al uw Joomla! tabellen te hernoemen, inclusief de tabellen die gebruikt worden door geïnstalleerde extensies. Als het hernoemen niet lukt, zal Admin Tools proberen alle veranderingen terug te draaien.

Het wordt aanbevolen om de oude gebruikersaccount degraderen naar het 'Geregistreerd' niveau. Om dat te doen, volg deze eenvoudige procedure:

1. Bewerk de oude gebruikersaccount en zet geblokkeerd op 'Nee' en de gebruikersgroep op 'geregistreerd'. Pas de wijzigingen toe.
2. Bewerken de gebruikersaccount nog een keer en zet geblokkeerd op 'Ja'. Tot slot, de wijzigingen opslaan.

Dit is noodzakelijk voor Joomla! om niet met een foutmelding te komen van 'Kan Super Administrator niet uitschakelen'.

Waarom kan mijn database tabellen hernoemen?

Admin Tools moet twee zeer belangrijke MySQL commando's kunnen starten om te kunnen werken. De ene is SHOW TABLE STATUS en de andere is ALTER TABLE. Het is mogelijk dat door de configuratie van uw host, het uw database gebruiker niet is toestaat om één of beide opdrachten uit te voeren. In geval van twijfel, raadpleeg uw host. Post hiervoor niet op ons forum voor ondersteuning, we kunnen niet raden of dit het geval is, en zullen u dan toch aanraden uw host te raadplegen.

10. Wijzig uw database collatie

Er zijn momenten waar u een website op een server wilt installeren of herstellen en u beseft dat tegen de tijd dat u halverwege de aanpassingen bent, accenten en internationale tekens niet zullen werken. Vaker wel dat niet, gebeurt dit met een extensie die u installeert. De verklaring is eenvoudig. Uw database collatie is waarschijnlijk de MySQL standaard (latin1_swedish_ci), terwijl Joomla! vraagt om UTF-8 tekenset codering. Aan de andere kant kunnen sommige lokalisaties, zoals Japans en Russisch behoefte hebben aan een andere tekenset codering dan UTF-8 om goed te kunnen werken, met hun speciale characters.

In beide gevallen, is het wijzigen van uw database collatie makkelijk, maar het veranderen van de collatie van de tabellen die reeds in de database zijn gemaakt, is een groter probleem. Dit is waarin de Admin Tools 'Wijzig Database Tekst Codering' functie uitblinkt. Met één klik zal het uw database collatie veranderen en al uw collatie tabellen.

Important

U moet ervoor zorgen dat uw database gebruiker voldoende privileges om ALTER DATABASE en ALTER TABLE commando's te kunnen uitvoeren. In geval van twijfel, raadpleeg uw host. Post hiervoor niet op ons forum voor ondersteuning, we kunnen niet raden of dit het geval is, en zullen u dan toch aanraden uw host te raadplegen.

De interface is zeer eenvoudig en recht vooruit. In de drop-down lijst selecteert u de gewenste collatie. Standaard is utf8_general_ci (de UTF-8 collatie vereist door Joomla!) geselecteerd. Klik daarna op de Toepassen knop.

11. Uw Super Administrator ID aanpassen

Standaard maakt Joomla! 1.5 bij de installatie een Super Administrator gebruiker aan met een gebruikers-ID van 62 en een gebruikersnaam van admin. Joomla! 1.6 creëert zo'n gebruiker met een ID van 42 en een gebruikersnaam van uw keuze. In beide gevallen kan het hebben van een bekende gebruikers-ID gevaar opleveren voor de veiligheid van uw website. Het creëren van een eerste nieuwe gebruiker zal respectievelijk een ID van 63 of 43 geven enzovoort, dat is een hacker's op één na beste gok om te knoeien met uw website. De echte oplossing is het creëren van een Super Administrator gebruiker met een ID in het 1-61 (Joomla! 1.5) of 1-41 (Joomla! 1.6) bereik. Voor meer informatie over de bezorgdheid over de veiligheid van de standaard Super Administrator ID, kijk eens naar mijn Joomla! Community Magazine artikel [http://magazine.joomla.org/issues/Issue-Sept-2010/item/148-62-reasons-to-fire-your-super-admin] (Engels).

De 'Admin Tools' Super Administrator ID aanpassen functie staat u toe dit probleem met één enkele klik op te lossen. Zodra u op de knop klikt, is dit wat er gebeurt:

- Er wordt een nieuwe gebruiker aangemaakt met een willekeurig ID in het 1-61 (Joomla! 1.5) of 1-41 (Joomla! 1,6) bereik, met dezelfde gebruikersnaam en hetzelfde wachtwoord als de standaard Super Administrator account, dat wil zeggen gebruikers met ID 62 (Joomla! 1.5) of ID-42 (Joomla! 1.6).
- De oude gebruiker z'n e-mail adres, gebruikersnaam en wachtwoord zijn volledig willekeurig gegenereerd, om per ongeluk gelijke logins onder dit account te voorkomen.
- De oude gebruiker is geblokkeerd, zodat niemand meer kan inloggen met dat account

Vergeet niet om uit te loggen van de administrator back-end van uw site, en vervolgens opnieuw in te loggen na het toepassen van deze verandering. Als u dit niet doet, zal u zien dat niets wil laden of dat hele pagina's van opties leeg blijven. *Dit is normaal en verwacht*. Daarom hebben we u in de eerste plaats gezegd uit te loggen van de administrator back-end.

Important

We raden met klem aan de oude gebruiker te bewerken en te degraderen naar de "Geregistreerd" groep. Door de introductie van de aanpasbare ACL in Joomla! 1.6 kunnen we deze stap niet betrouwbaar op een geautomatiseerde manier uitvoeren.

I have not a Super Administrator with ID 62, but Admin Tools still complains

The detection is based on a quite different method than what you might think. Admin Tools checks if there is a user with an ID lower than 62 (Joomla! 1.5) or 42 (Joomla! 1.6). If it's not found, it supposes that you are using the default Super Administrator ID. The reason for this strange check is the compatibility of the component with Joomla! 1.6. In

Joomla! 1.6 there is no hard-coded Super Administrator group. Moreover, it's perfectly possible to set the ACLs of any group in such a way that it is almost equivalent with a Super Administrator, making a proper check quite impossible.

Deze functie lijkt geen verandering te hebben gemaakt op mijn site?

Let op: deze functie werkt op het principe van het kopiëren en wijzigen van gebruiker accounts. Kortom, de gebruiker met ID 62 of 42 (afhankelijk van uw Joomla! Versie) is gekopieerd en een ID lager dan 42 toegewezen. Daarna is de oorspronkelijke gebruiker uitgeschakeld, en wordt de gebruikersnaam en e-mail verminkt met behulp van een willekeurige string en het wachtwoord is volkomen willekeurig gegenereerd. Als de gebruiker met de standaard ID (62 of 42) geen Super Administrator was, u had het bv. handmatig uitgeschakeld, is er geen effectieve verandering op uw website.

12. SEO en Link Tools

Dit gedeelte van Admin Tools bevat handige tools om uw website's SEO te verbeteren en uw site links te verwerken. De lijst van functies in deze sectie wordt met der tijd nog verder uitgebreid.

Link migratie

Wanneer u uw website verhuist tussen hosts, kan u eindigen met gebroken intra-site links. Meestal wordt dit veroorzaakt door het gebruik van absolute links of het verplaatsen van de site naar een map met een andere naam dan voorheen.

In het eerste geval, laten we zeggen dat u uw website wilt verplaatsen van `www.voorbeeld.com` naar `www.voorbeeld.org`. Als u de links zou kopiëren van de adresbalk van uw browser en ze in uw content of menu's zou plakken, zit u vast aan een heleboel links die verwijzen naar de www.voorbeeld.com domeinnaam, bijvoorbeeld `http://www.voorbeeld.com/eenpagina.html`. Het vinden en veranderen van al die links is een enorme klus, vooral als u duizenden content items heeft.

In het laatste geval, wat het meest voorkomende is, verloopt het typische scenario als volgt. U ontwikkeld uw website lokaal, en benaderd hem als `http://localhost/mijnsite`. Dan verplaatst u uw website naar een live server met een adres als `http://www.voorbeeld.com`. Plotseling zijn al uw links en afbeeldingen gebroken! Waarom? Alle WYSIWYG Joomla! editors creëren relatieve URL's. Bijvoorbeeld, het linken naar `images/stories/image.jpg` geeft een link als `/mijnsite/images/stories/image.jpg` in de HTML bron code van uw content. Als u goed naar deze URL kijkt, zal u meteen de /mysite prefix opvallen. Dit werkt prima op uw lokale server, omdat uw website in de /mijnsite map van uw web root staat, maar breekt op de live website wanneer u wilt herstellen naar het web root zelf! Nogmaals, het vinden van al die referenties en ze veranderen is een enorme klus.

Enorme klus? Dat is het niet meer! De Admin Tools Link Migratie functie komt u te hulp. Zet eerst de Link migratie inschakelen optie op Ja om deze functie in te schakelen. In the Oude locaties tekst gebied zal u de domeinnamen of submappen waar uw site zich bevind moeten invoeren, één op elke regel invoeren. Bijvoorbeeld, als uw website werd gehost op `http://www.voorbeeld.com`, moet u invoeren `www.voorbeeld.com` op één regel (zonder de http:// of https:// prefix!). Als u om relatieve URL's wilt heen werken, geeft dan de volledige URL en directory in, één op elke regel, bijvoorbeeld. `http://localhost/mijnsite` op één regel, en `/mijnsite` op een volgende regel. Admin Tools zal zijn magische werk doen, en al uw URL's migreren en naar uw nieuwe site laten wijzen, wanneer Joomla! on-the-fly uw site pagina's genereert.

Important

Vergeet niet uw Joomla! cache en uw browser cache te legen na het inschakelen van deze functie om de veranderingen in uw browser te zien als u uw website pagina's herlaadt.

Tools

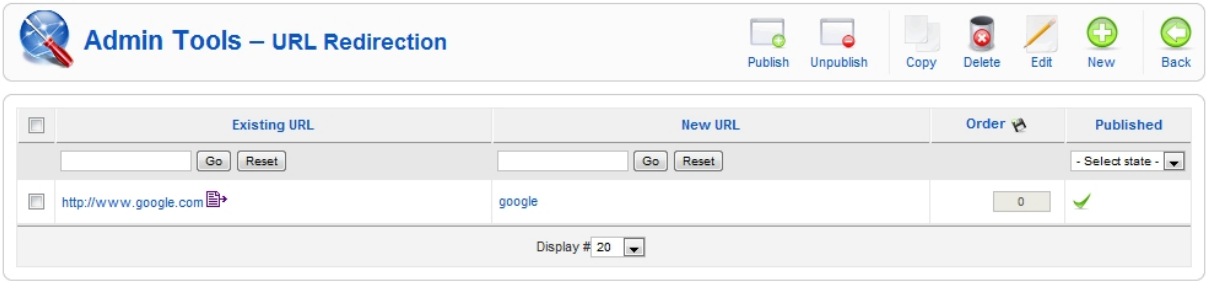
Wanneer u uw website via SSL benaderd (HTTPS) zou u met verschillende browsers eindigen met een "gedeeltelijk gecodeerde pagina" waarschuwing. Dit gebeurt omdat sommige resources, zoals Javascript, CSS of externe pagina's (kaarten, kalenders) geladen in IFRAME's opgevraagd kunnen worden via HTTP. Het is meestal erg moeilijk om ze allemaal op te merken en ze te veranderen. Sommige zijn ronduit onmogelijk om te veranderen, tenzij u de code van de extensie die ze produceert bewerkt. Met Admin Tools is dat niet meer het geval. Schakel gewoon de Converteer alle links naar HTTPS wanneer de website wordt benaderd over SSL optie in en Admin Tools zal alle HTTP URL's automatisch converteren naar HTTPS URL's wanneer uw site wordt benadert via SSL (HTTPS). Dit zorgt ervoor dat de "deels gecodeerde pagina" waarschuwingen eindelijk tot het verleden behoren.

13. URL Omleiding

Note

Deze functie is alleen beschikbaar in de Professional versie

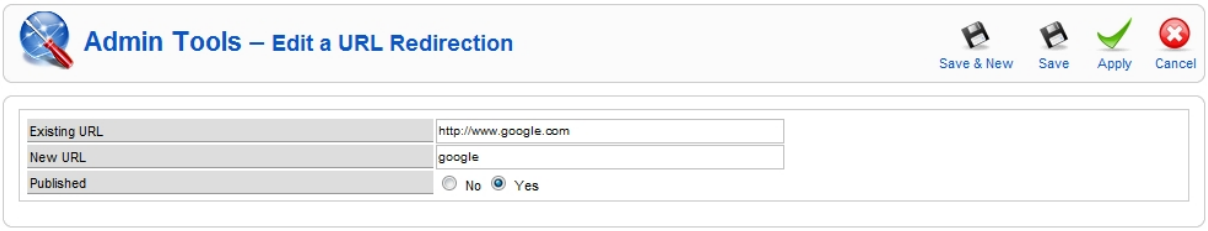
Soms moet u korte, makkelijk te onthouden URL's creëren om een aantal pagina's van uw website. die Joomla!'s mede oprichter Brian Teeman PEF (Pub Ear Friendly) noemt. Waarschijnlijk om iemand te vertellen dat `http://www.voorbeeld.com/downloads` te bezoeken, veel makkelijker is dan iemand te vertellen om `http://www.voorbeeld.com/index.php?option=com_downloads&view=repository&task=list` of zelfs `http://www.voorbeeld.com/site-resources/download.html` te bezoeken. De andere keren dat u graag een korte URL wilt gebruiken om een externe site te benaderen, maar om redenen van privacy geen gebruik wilt maken van gratis diensten, zoals bit.ly, ow.ly, t.co of tinyurl.com. Bied Admin Tools de uitkomst! Met de aangepaste URL omleiding functie kunt u al het bovenstaande doen met een belachelijk eenvoudige interface



De omleiding beheer pagina toont u een lijst van de aangepaste URL omleidingen gedefinieerd op uw websites. Elk onderdeel bestaat uit de volgende informatie:

- De uiterst linkse checkbox. De werkbalk operaties zullen alleen gelden voor de aangevinkte items.
- Bestaand URL. De URL waar uw bezoekers vandaan zullen worden omgeleid. Erop klikken zal de URL in een nieuw venster openen, zodat u een voorbeeld van het resultaat kunt zien.
- Nieuw URL. Het relatieve pad op uw site die de omleiding triggert. Bijvoorbeeld, als uw site te bereiken is op `http://www.voorbeeld.com/joomla` en in dit veld staat `search/google`, dan zullen alle verzoeken naar `http://www.voorbeeld.com/joomla/search/google` worden omgeleid naar 'Bestaand URL' met een 301 (Permanent verplaatst) HTTP status code, om het zoekmachine vriendelijk te houden. Klikken op de weergegeven waarde opent de Bewerken/Toevoegen pagina, zodat u de invoer kunt bewerken.
- Volgorde. De volgorde waarmee de aangepaste omleidingen zullen worden verwerkt.
- Gepubliceerd. Wanneer niet gepubliceerd, zal de omleiding niet plaatsvinden. Handig om tijdelijk een omleiding te voorkomen zonder deze te verwijderen.

Bij het toevoegen van een nieuwe vermelding of het bewerken van een bestaand item, verschijnt de volgende pagina:



Er zijn drie velden die kunnen worden bewerkt:

Bestaand URL
: Een bestaande URL op uw website, of een link naar een externe pagina.

  Bij gebruik van een URL in uw eigen hoeft u niet de URL naar de root van uw website bij te voegen. Gebruik in plaats daarvan het relatieve pad. Bijvoorbeeld, het gebruik van `index.php?option=com_frontpage` is voldoende om de front-end component weer te geven. U kunt zowel een index.php URL als een SEF URL (zolang SEF URL's is ingeschakeld in uw Algemene Configuratie in de back-end!) gebruiken.

  De grootste kracht van deze functie is de mogelijkheid om externe links in te geven. Zo kunt u `http://www.google.com` invoeren om uw bezoekers om te leiden naar de Google zoek pagina. Met behulp van deze krachtige functie kunt u uw eigen URL verkort service op uw domein instellen!

Nieuw URL
: Het relatieve pad dat de omleiding triggert. Bijvoorbeeld, als uw site toegankelijk is als `http://www.voorbeeld.com/joomla`, zal het invoeren van `google` in dit veld de URL `http://www.voorbeeld.com/joomla/google` omleiden naar de URL die u hebt ingevoerd in het 'bestaand URL' veld hierboven. U kunt ook gebruik maken van submappen in uw pad, bijvoorbeeld `search/external/google`.

Gepubliceerd
: Wanneer niet gepubliceerd, zal de omleiding niet plaatsvinden. Handig om tijdelijk een omleiding te voorkomen zonder deze te verwijderen.

Gebruik de Opslaan knop om de wijzigingen op te slaan en terug te keren naar de URL omleiding beheer pagina, Opslaan & Nieuw om de wijzigingen op te slaan en te beginnen met het invoeren van gegevens voor een nieuwe omleiding, Toepassen om de wijzigingen op te slaan en terug te keren naar deze bewerken pagina en Annuleren om alle wijzigingen te negeren en terug te keren naar de 'URL omleiding' beheer pagina.

14. Uw tijdelijke bestanden map opschonen

Uw Tijdelijke bestanden map (de *Temp map* in uw Algemene Instellingen back-end pagina) is de map waar Joomla! en haar extensies alle tijdelijke bestanden bij het installeren van software of andere soorten van bestandsbewerking uitvoert, opslaat. Een probleem met deze map is dat bestanden er soms in kunnen achterblijven, bijvoorbeeld na een mislukte update. Dit veroorzaakt niet alleen een ruimte probleem —omdat deze bestanden waardevolle schijfruimte gebruiken— maar kan ook uw website's veiligheid in gevaar brengen omdat deze bestanden mogelijk gevoelige informatie kunnen bevatten, of uitvoerbare PHP bestanden kunnen zijn. Hoewel dit laatste probleem kan worden tegen gegaan door gebruik te maken van de front-end bescherming modus in de .htaccess Maker functie van Admin Tools Professional, is de juiste oplossing om periodiek de inhoud van die map te wissen.

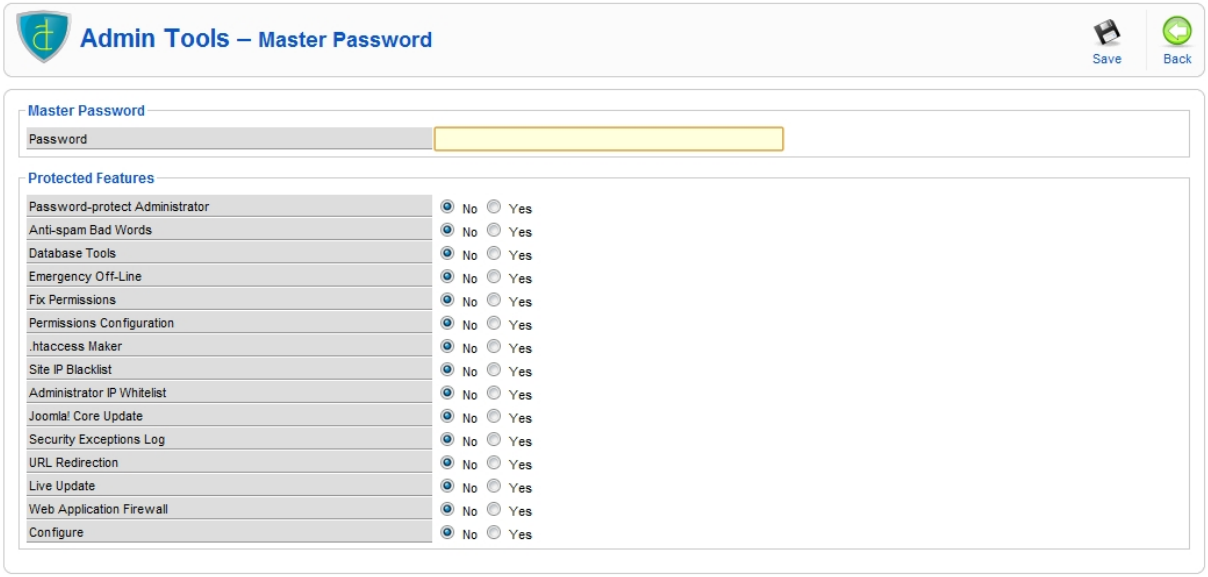
Admin Tools Core en Admin Tools Professional beschikken beiden over de Temp map opschonen functie die dit voor u doet in één enkele klik! Meer specifiek zal het automatisch alle bestanden en mappen van uw Temp map wissen, behalve `index.html` en `.htaccess`, als dergelijke bestanden in de temp map bestaan.

15. Admin Tools gebruik beschermen met een wachtwoord

Warning

DIT IS GEEN BEVEILIGINGSFUNCTIE **HET MASTER WACHTWOORD IS ONGECODEERD OP UW SITE OPGESLAGEN**. Wij beschouwen deze functie als een eenvoudige manier voor u om te voorkomen dat uw cliënten wijzigingen in de configuratieparameters aanbrengen waardoor ze de website per ongeluk zouden kunnen breken. DEZE FUNCTIE IS NIET ONTWORPEN OM TE VOORKOMEN DAT EEN KWAADAARDIG EN/OF WELINGELICHT KWAADWILLENDE PERSOON TOEGANG HEEFT TOT ADMIN TOOLS.

Soms bent u niet de enige beheerder van een website, bijvoorbeeld wanneer er een groot administratie team is, of wanneer u de website bouwt voor een klant. In zulke gevallen hoeft u niet iedereen met back-end toegang toe te staan Admin Tool instellingen te wijzigen. In plaats van de traditionele 'alles of niets' toegangscontrole opgelegd door Joomla! gebruikersgroepen, stelt Admin Tools u in staat om de toegang tot enkele of alle functies met behulp van een "master wachtwoord" toe te kennen. Het idee is dat voordat een gebruiker in staat is om een van de beschermde functies te gebruiken, hij het "master wachtwoord" in moet geven op de Admin Tools 'controle paneel' pagina.



Als u op de Master Wachtwoord knop klikt in het Admin Tools Controle Paneel gaat u naar de Master Wachtwoord pagina waar u zowel het master wachtwoord kunt ingeven en kunt selecteren welke functies u wilt beschermen.

Bovenaan de pagina kunt u een Master Wachtwoord instellen. Als u de wachtwoord beveiliging wilt uitschakelen, laat dit veld dan gewoon leeg.

In het gedeeltte direct eronder kunt u kiezen welke functies zullen worden beschermd. Stel de pull-down optie naast elke functie die u wilt beschermen in op "Ja" voordat u op de Opslaan knop gebruikt. Functies gemarkeerd als "Nee" zijn voor alle back-end gebruikers toegankelijk (managers, administrators en Super Administrators). Functies gemarkeerd met "Ja" zijn alleen beschikbaar voor gebruikers die een geldig wachtwoord in het Controle Paneel pagina hebben ingevoerd. Dit betekent dat zelfs Super Administrators niet in staat zijn om de beveiligde toegang tot de functies te benaderen zonder het leveren van een geldig wachtwoord.

Als u snel alle functies wilt beveiligen, klikt u op de Alles knop bovenaan de lijst. Omgekeerd, zal klikken op de Geen knop de Master Wachtwoord bescherming op alle functies uitschakelen.

Ik ben mijn wachtwoord vergeten, wat nu?

De enige manier om achter uw wachtwoord te komen is om direct uit de database te lezen. Gebruik de database management tool van uw host, —meestal is dat phpMyAdmin— om de inhoud van uw site's jos_admintools_storage tabel (waar *jos_* de prefix is). Vind het enige record in de tabel (de *key* waarde is "cparams") en kijk in de inhoud van de *value* kolom. Het bevat een lange tekst. Op een gegeven moment zie u iets als `"masterpassword":"mypassword"`. Het *mypassword* deel is uw Master Wachtwoord.

16. Gebruikers toegangscontrole

Admin Tools is in staat om op een verscheidenheid van op Joomla! gebaseerde CMS systemen te draaien, inclusief Joomla!™ 1.5, Joomla! 1.6, Nooku Server en Molajo. Sinds versie 2.0, is het standaard beperkt tot gebruikers met Super Administrator rechten.

Dat gezegd hebbende, hebben veel web professionals gevraagd naar een manier om Admin Tools te configureren op een manier die het mogelijk maakt voor hun klanten om specifieke functies te beheren, zonder de noodzaak van een Master Wachtwoord. Om op deze behoefte in te gaan, is Admin Tools uitgerust met een fijnmazige toegangscontrole (ACL) sinds versie 2.0. De exacte ACL methode is specifiek voor het platform waarop het draait.

16.1. Joomla! 1.5, Nooku Server en andere Joomla! 1.5 distributies

Wanneer Admin Tools draait onder Joomla! 1.5, Nooku Server of een andere CMS distributie op basis van Joomla! 1.5, zijn er twee niveaus van toegangscontrole: component toegang en per gebruiker ACL (controle) instellingen.

Het eerste niveau van toeganscontrole bepaalt wie er überhaupt toegang tot de Admin Tools component heeft, dat wil zeggen, wie kan de interface zien. Om dit te configureren, gaat u naar het Componenten, Admin Tools menu en klikt u op de Gebruikers Toegangscontrole knop. Zie de Minimum toegangsniveau optie bovenaan de pagina. Elk van de drie opties in het pull-down menu rechts ervan heeft de volgende bedoeling:

Super Administrator	Alleen Super Administrators hebben toegang tot de component
Administrator	Alleen gebruikers in de Administrator of Super Administrator groep hebben toegang tot de component
Beheerder	Elke gebruiker met back-end toegang (Beheerder, Administrator of Super Administrator) heeft toegang tot de component

Houdt u er rekening mee dat deze instelling voorrang heeft boven de per-gebruiker ACL. Dit betekent dat als u deze instelling naar Super Administrator zet, een beheerder niet in staat zal zijn om Admin Tools te gebruiken, zelfs als u hem alle permissies verleent in de per-gebruiker ACL instellingen.

Het tweede niveau van toegangscontrole is de per-gebruiker ACL. Standaard kan de Super Administrator alles doen, Administrators hebben geen toegang tot beveiligingsinstellingen en Beheerders kunnen alleen gebruik maken van enkele handige functies. Met deze functie kunt u fijnmazige controle hebben over wat elke gebruiker wel en niet kan doen. Om dit te configureren, gaat u naar het Componenten, Admin Tools menu en klikt u op de Gebruikers Toegangscontrole knop. U ziet een lijst met alle gebruikers met back-end toegang (Beheerders, Administrators en Super Administrators). In elke regel, ziet u de volgende kolommen:

Gebruikersnaam	De gebruikersnaam waarop deze regel van toepassing is
Groep	Tot welke gebruikersgroep (Beheerder, Administrator, Super Administrator) deze gebruiker behoort

Hulpprogramma
: Een groen vinkje betekent dat de gebruiker, gebruik kan maken van de hulpprogramma functies van Admin Tools. Een witte X in een rode achtergrond betekent dat hij geen toegang tot deze functies heeft. De betrokken functies zijn: het opschonen van de tijdelijke map, toegang tot de componenten (Controle Paneel), Off-line bij noodgevallen, de vaststelling en het configureren van permissies, Joomla! core update, URL omleidingen, SEO en link tools.

Onderhoud
: Een groen vinkje betekent dat de gebruiker, gebruik kan maken van de database onderhoud kenmerken van Admin Tools. De betrokken functies zijn: het veranderen van de Administrator gebruikers-ID, het veranderen van de database collatie, het veranderen van de database prefix, sessie opruimen en tabel optimalisatie.

Beveiliging
: Een groen vinkje betekent dat de gebruiker, gebruik kan maken van de beveiligingsfuncties van Admin Tools. De betrokken functies zijn: toegangscontrole, Administrator wachtwoord bescherming, Web Applicatie Firewall setup en de bijbehorende tools (anti-spam slechte woorden filteren, Geografisch blokkeren, IP white en black list, log view), .htaccess Maker en Master wachtwoord.

16.2. Joomla! 1.6/1.7+ en andere Joomla! 1.6/1.7+ distributies

Joomla! 1.6 is uitgerust met zijn eigen zeer krachtige en ietwat complexe ACL systeem. Admin Tools is ontworpen om hier optimaal gebruik van te maken. Voor de ACL setup, gaat u naar Componenten, Admin Tools klikt u op de Opties knop in de werkbalk. Klik dan op de Permissies tab. Elke gebruikersgroep kan worden ingesteld met de volgende permissies:

Configureer (bovenaan)
: Biedt toegang tot de Component Parameters knop. Dit is een core Joomla! privilege.

Component toegang
: Spreekt voor zich. Als een gebruiker niet over deze bevoegdheid beschikt, zal hij geen toegang tot componenten hebben! Dit is een core Joomla! privilege.

Hulpprogramma
: De gebruiker kan gebruik maken van de hulpprogramma functies van Admin Tools. De betrokken functies zijn: het opschonen van de tijdelijke map, toegang tot de componenten (Controle Paneel), Off-line bij noodgevallen modus, de vaststelling en het configureren van permissies, Joomla! core update, URL omleidingen, SEO en link tools.

Onderhoud
: De gebruiker kan gebruik maken van de database onderhoud kenmerken van Admin Tools. De betrokken functies zijn: het veranderen van de Administrator gebruikers-ID, het veranderen van de database collatie, het veranderen van de database prefix, sessie opruimen en tabel optimalisatie.

Beveiliging
: De gebruiker kan gebruik maken van de beveiligingsfuncties van Admin Tools. De betrokken functies zijn: toegangscontrole, Administrator wachtwoord bescherming, Web Applicatie Firewall setup en de bijbehorende tools (anti-spam slechte woorden filteren, Geografisch blokkeren, IP white en black list, log view), .htaccess Maker en Master wachtwoord.

We zullen niet dieper op de details van de ACL instellingen in Joomla! 1.6 ingaan. Indien u meer informatie wilt over hoe het Joomla! 1.6 ACL systeem werkt, raadpleeg dan de Joomla! 1.6 documentatie of vraag het op het Joomla! forum (Engels).

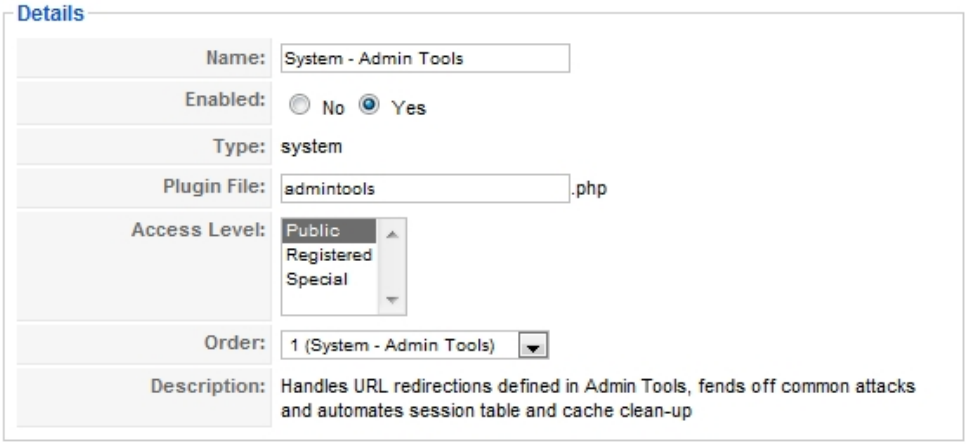
17. De "System - Admin Tools" plugin

Note

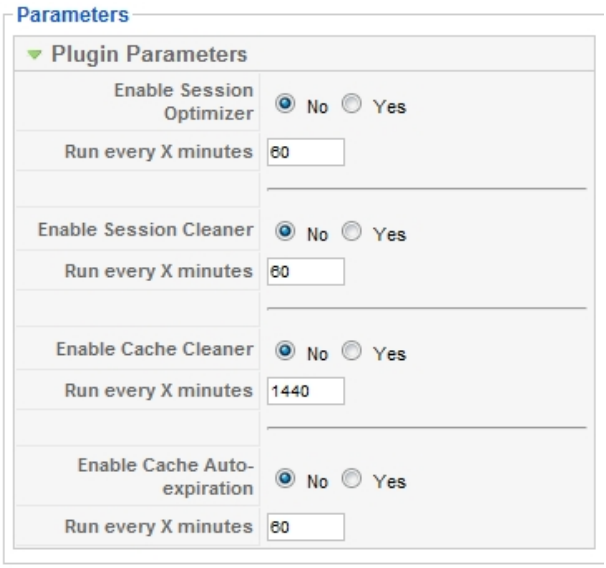
De planningsfuncties van deze plugin zijn alleen beschikbaar in de Professional versie. In de core versie moet de plugin worden ingeschakeld om de SEO en Link functies te laten werken.

De "System - Admin Tools" plugin, of `plg_admintools` in het kort, heeft een dubbele rol in de Professional versie van Admin Tools. Aan de ene kant is het noodzakelijk voor de goede werking van de 'Web Applicatie Firewall' en 'URL omleidingen' functies van Admin Tools. Aan de andere kant kunt u de verschillende aspecten van het onderhoud van uw website plannen.

U kunt de plugin configuratie parameters benaderen via de Extensies, Pluginbeheer menu optie in uw back-end. Zoek het System - Admin Tools item in de lijst en klik erop. De standaard Joomla! plugin configuratie pagina opend zich.



Aan de linkerkant van de administrator omgeving vindt u de standaard Joomla! instellingen. Zorg er eerst voor dat de Geactiveerd optie op Ja is ingesteld. De plugin wordt altijd automatisch als eerste in de system plugin lijst opgenomen en kan niet worden verplaatst. Dit is noodzakelijk voor een juiste werking.



De rechterkant is de plaats waar alle belangrijke functies kunnen worden gepland. U hebt de volgende opties:

Schakel Sessie Optimaliseren in
: Wanneer ingeschakeld, wordt de sessie Optimalisatie gepland om automatisch te worden uitgevoerd. Deze functie zal de sessies tabel van Joomla! herstellen en optimaliseren.

Elke X minuten uitvoeren
: Hoe vaak de sessies optimaliseren functie moet worden uitgevoerd, in minuten

Schakel Sessie Cleaner in	Wanneer ingeschakeld, wordt de sessie cleaner gepland om automatisch te worden uitgevoerd. Deze functie zal de sessie tabel volledig wissen en optimaliseren. Kijk uit! Dit zal automatisch alle gebruikers van uw website uitloggen! Gebruik dit alleen op websites waarvan u niet verwacht dat er gebruikers zijn ingelogd, bijvoorbeeld een bedrijfspresentatie website.
Elke X minuten uitvoeren	Hoe vaak de sessies cleaner functie moet worden uitgevoerd, in minuten
Schakel Cache Cleaner in	Wanneer ingeschakeld, zal de cache cleaner worden gepland om automatisch te worden uitgevoerd. Deze functie zal proberen de Joomla! cache volledig te wissen. Dit is niet mogelijk in sommige gelegenheden, vooral als u een cache adapter gebruikt die geen ondersteuning biedt voorn het cache wissen.
Elke X minuten uitvoeren	Hoe vaak de cache cleaner functie moet worden uitgevoerd, in minuten
Schakel Cache Auto-verloop in	Wanneer ingeschakeld, zal de cache auto verloop functie worden gepland om automatisch worden uitgevoerd. Deze functie zal proberen vervallen en oude items te verwijderen uit de cache van Joomla!. In tegenstelling tot de ingebouwde Joomla! functie, zal het proberen deze bewerking in alle caches te draaien. Dit is niet mogelijk in sommige gelegenheden, vooral als u een cache adapter heeft die geen ondersteuning biedt voor automatisch verlopen controle.
Elke X minuten uitvoeren	Hoe vaak de cache auto-verloop functie moet worden uitgevoerd, in minuten

Alle verloop opties zijn 'naar beste vermogen' gepland. Dit betekent dat zij zullen proberen om elke X minuten draaien, maar alleen zolang er bezoekers verkeer is om het de functie triggeren. In alle andere gevallen zal de uitvoering ervan worden uitgesteld tot er bezoekers verkeer gedetecteerd werd.

Appendix A. GNU General Public License versie 3

Versie 3, 29 Juni 2007

Omwille van juridische redenen zijn onderstaande licentie voorwaarden niet uit het Engels vertaald.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program—to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger

that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

“This License” refers to version 3 of the GNU General Public License.

“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

“The Program” refers to any copyrightable work licensed under this License. Each licensee is addressed as “you”. “Licensees” and “recipients” may be individuals or organizations.

To “modify” a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example,

Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a. The work must carry prominent notices stating that you modified it, and giving a relevant date.

b. The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to “keep intact all notices”.

c. You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d. If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a. Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b. Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c. Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d. Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e. Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A “User Product” is either (1) a “consumer product”, which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling.

In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, “normally used” refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

“Installation Information” for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

“Additional permissions” are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a. Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b. Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c. Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d. Limiting the use for publicity purposes of names of licensors or authors of the material; or

e. Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f. Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction,

each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is “discriminatory” if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PER-

MITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

```
one line to give the program's name and a brief idea of what it does.
Copyright (C) year name of author

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program.  If not, see http://www.gnu.org/licenses/.
```

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

```
program Copyright (C) year name of author
This program comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.
This is free software, and you are welcome to redistribute it
```

```
under certain conditions; type 'show c' for details.
```

The hypothetical commands '`show w`' and '`show c`' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an “about box”.

You should also get your employer (if you work as a programmer) or school, if any, to sign a “copyright disclaimer” for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see http://www.gnu.org/licenses/.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read http://www.gnu.org/philosophy/why-not-lgpl.html.

Appendix B. GNU Free Documentation License

Version 1.3, 3 November 2008

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A “Transparent” copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not “Transparent” is called “Opaque”.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The “Title Page” means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, “Title Page” means the text near the most prominent appearance of the work’s title, preceding the beginning of the body of the text.

The “publisher” means any person or entity that distributes copies of the Document to the public.

A section “Entitled XYZ” means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as “Acknowledgements”, “Dedications”, “Endorsements”, or “History”.) To “Preserve the Title” of such a section when you modify the Document means that it remains a section “Entitled XYZ” according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document’s license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled “Endorsements”. Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled “Endorsements” or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version’s license notice. These titles must be distinct from any other section titles.

You may add a section Entitled “Endorsements”, provided it contains nothing but endorsements of your Modified Version by various parties — for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled “History” in the various original documents, forming one section Entitled “History”; likewise combine any sections Entitled “Acknowledgements”, and any sections Entitled “Dedications”. You must delete all sections Entitled “Endorsements”.

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an “aggregate” if the copyright resulting from the compilation is not used to limit the legal rights of the compilation’s users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document’s Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled “Acknowledgements”, “Dedications”, or “History”, the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See Copyleft [http://www.gnu.org/copyleft/].

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License “or any later version” applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free

Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

```
Copyright © YEAR YOUR NAME

Permission is granted to copy, distribute and/or modify this document under the
terms of the GNU Free Documentation License, Version 1.3 or any later version
published by the Free Software Foundation; with no Invariant Sections, no
Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in
the section entitled "GNU Free Documentation License".
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with… Texts." line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts
being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.