Handleiding voor Amnesty Webmasters

Versie	**1.2**
Auteur	**Webhosting Amnesty NL**
Datum	**22-07-2020**
Online laatste versie:	

https://internetgroep.amnesty.nl/images/downloadables/Akeeba_Admin_Tools_-_Handleiding_Amnesty_Webmasters.pdf

Wijzigingen

Versie	Datum	Wijzigingen
0.3	01-04-2020	Email berichten toegevoegd
0.4	13-04-2020	Paginanummers toegevoegd. H3 Extra beveiliging IP Whitelist toegevoegd. Webhosting groep veranderd in team.
0.5	22-05-2020	Tekstverbeteringen Brigitte Voerman
1.0	23-05-2020	H5 Email berichten vertaald naar het Nederlands. H5.1 List of blocking reasons toegevoegd. Link naar “Online laatste versie” toegevoegd.
1.1	20-06-2020	Nieuwe versie Admin Tools 5.7.3. Administrator IP White vervangen door Administrator Exlusive Allow IP List, Site IP Blacklist vervangen door Site IP Disallow List, Sercurity Exceptions Log vervangen door Blocked Request Log.
1.2	22-07-2020	H5, Aanpassing/verminderen van Email berichten.

Inhoud

1. Inleiding

In de zomer van 2019 zijn een aantal WordPress sites van de Amnesty groepen geïnfecteerd en benaderd. Hiermee liepen niet alleen de groepensites gevaar, maar ook www.amnesty.nl omdat al deze sites gebruik maken van hetzelfde domein. Ook www.amnesty.nl werd hiermee als site "besmet" verklaard. De WordPress sites zijn toen beveiligd met de plugin Wordfence. Daarna zijn we ook op zoek gegaan naar een betere beveiliging van de Joomla websites bij Amnesty. Daarbij hebben we gekozen om gebruikt te maken van de **Akeeba 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."

Enkele belangrijke functies van de Admin Tools zijn:

- De Web Application Firewall
- Blokkade van IP adressen met verkeerd gedrag, ook automatisch (IP Disallow list)
- Extra beveiliging door een lijst met IP adressen die toegang krijgen tot de website (Exclusive Allow IP List)
- Controleren van bestanden en rechten van je website en automatisch aanpassen
- Uitgebreide logging van de door de Web Application Firewall gedetecteerd meldingen (Security Exceptions Log)
- Gebruik van Email templates voor het automatisch versturen van deze Firewall meldingen
- Database Tools
- Het kunnen afschermen van de Admin Tools instellingen via een Master Password
- De mogelijkheid om specifieke onderdelen beschikbaar te stellen aan alle administrators

Er zijn twee versies: Core (gratis) en Professional (betaald). De Webhosting Amnesty NL heeft voor de betaalde Professional versie gekozen.

1.1. Installatie door Webhosting Amnesty NL

De Internetgroep / Webhosting Amnesty NL zorgt voor de installatie van de Akeeba Admin Tools en ook voor de basis configuratie en instelling. Dit hoeft een lokale webmaster dus niet zelf te doen. De lokale webmaster / administrators hebben wel toegang tot bepaalde onderdelen van de Admin Tools en kunnen ook de uitgebreide logging (Security Exceptions Log) bekijken.

1.2. Aangepaste Administrator Login

Normaal kun je het Administrator deel van de website benaderen via de URL:

https://<groepensite>.amnesty.nl/administrator

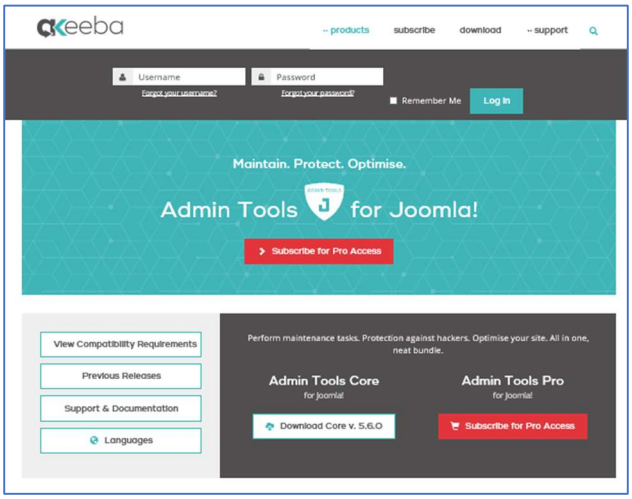
Potentiële hackers weten dit ook en zullen hiermee proberen toegang te krijgen tot de site. Eén van de beveiligingsopties van de Admin Tools is om deze toegang ook te verbergen door er een eigen (geheime) tekst aan toe te voegen. We hebben gekozen voor de tekst "am1961" en de URL wordt dan:

https://<groepensite>.amnesty.nl/administrator/index.php?am1961

Bij de oude- of een andere URL word je gewoon doorverwezen naar de homepagina van de site en wordt er gelijk een interne melding van gemaakt (zie verderop).

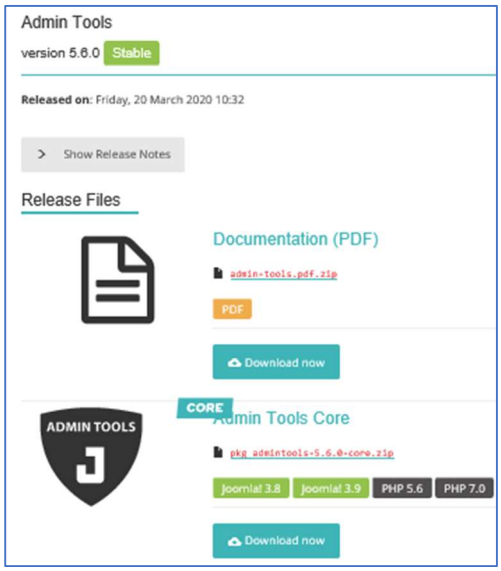
1.3. Documentatie

De uitgebreide informatie over de Admin Tools vind je bij de leverancier:
https://www.akeebabackup.com/products/admin-tools.html

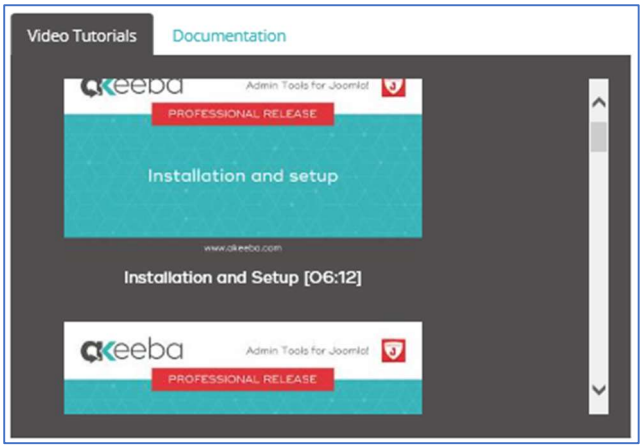


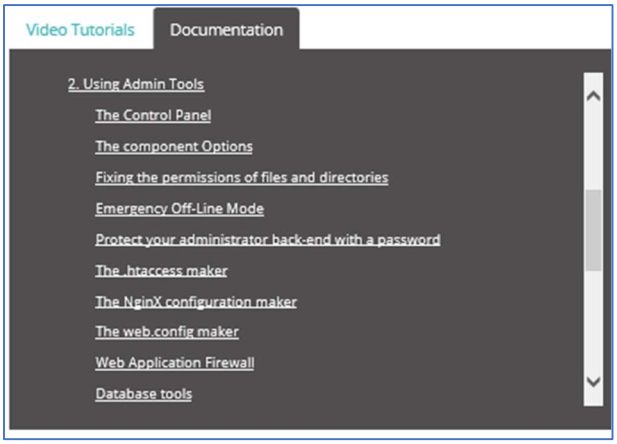
Een uitgebreid PDF document van de laatste versie (hier v.5.6.0) vind je bij de downloads:
https://www.akeebabackup.com/download.html

Kies voor [All Files], waar je het PDF document als een ZIP-file kunt downloaden.



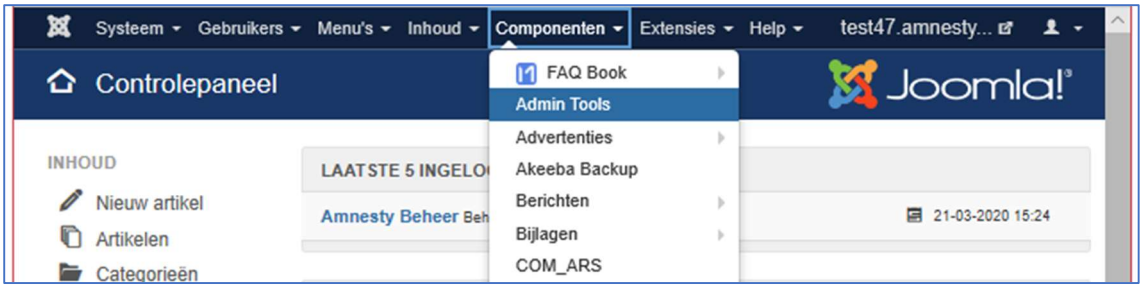
Verdere online documentatie kun je ook vinden bij:
https://www.akeebabackup.com/support/admin-tools/Tickets.html
Hier vind je Video Tutorials en ook de online versie van de PDF. In dit document wordt hier regelmatig naar verwezen voor meer informatie over een onderdeel.





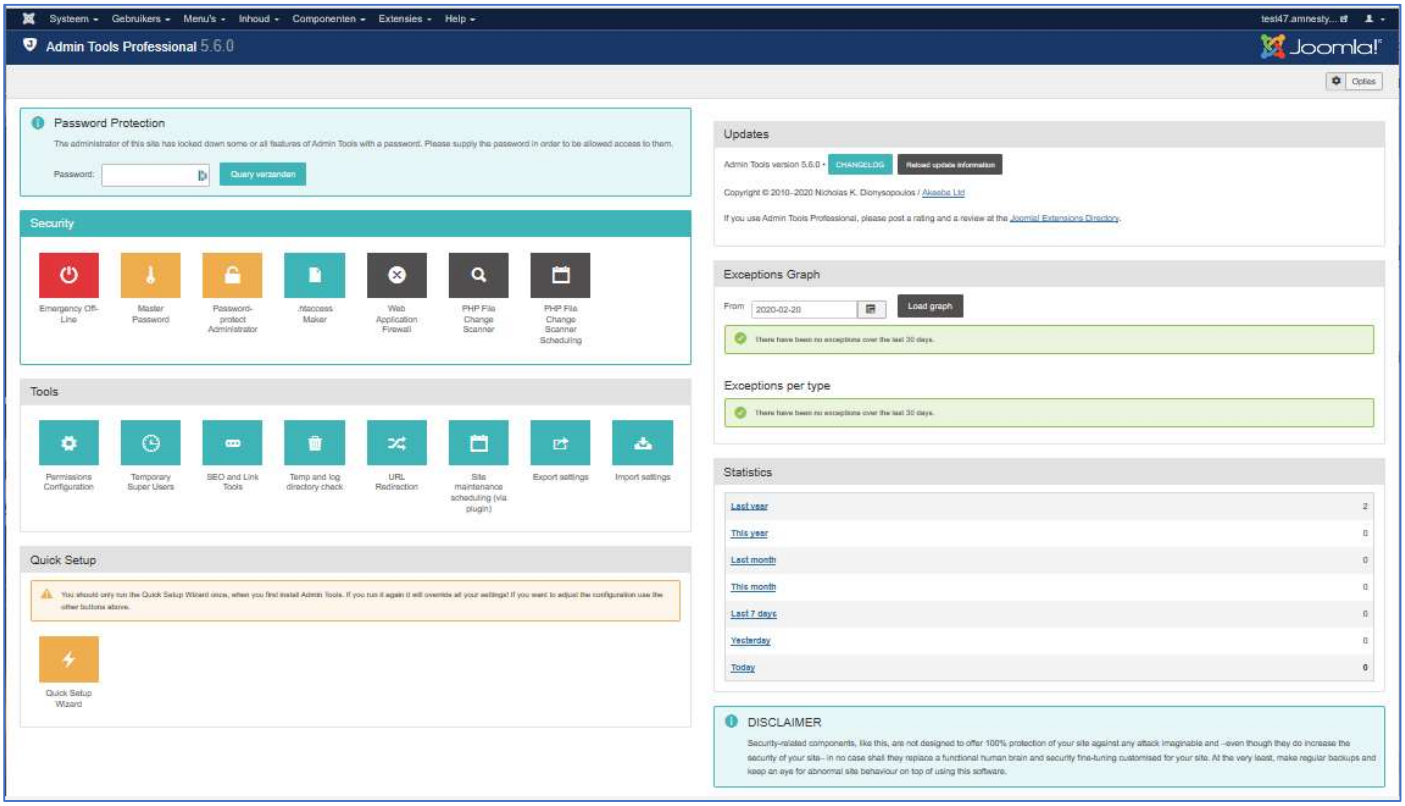
2. De Admin Tools gebruiken

Als men via de Admnistrator Login ingelogd is in het beheer gedeelte van de website kan men de Admin Tools vinden bij de Componenten: **Menu | Componenten | Admin Tools**.



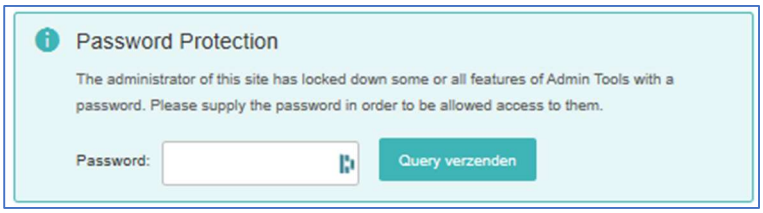
2.1. Control Panel

Het totale scherm voor de Admin Tools ziet er dan voor de Amnesty Webmasters als volgt uit en wordt het Control Panel genoemd:



Het Control Panel is opgebouwd uit een aantal onderdelen.

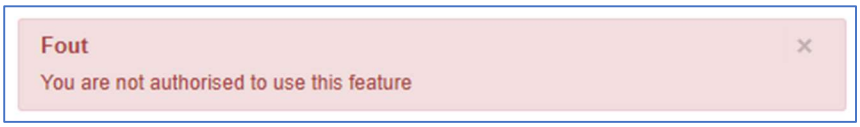
2.2. Password Protection



Omdat de Joomla sites waar deze Admin Tools geïnstalleerd zijn allemaal bij Amnesty hosten wordt het hosting deel door de Webhosting Amnesty NL team uitgevoerd. Dit team beheert dus de basis installatie van Joomla zelf, de database onderdelen en ook de bestandsstructuur. Het is dus niet nodig dat een lokale webmaster deze onderdelen nog eens beheert en controleert. Voor een aantal onderdelen van de Admin Tools is dat ook niet gewenst. De Admin Tools biedt de mogelijkheid deze onderdelen af te schermen met een wachtwoord (Master Password). Het

Webhosting Amnesty NL team heeft daarvoor gekozen en alleen specifieke onderdelen vrijgegeven voor de webmasters / administrators. Dit Master Password is dus alleen in beheer bij de Webhosting team.

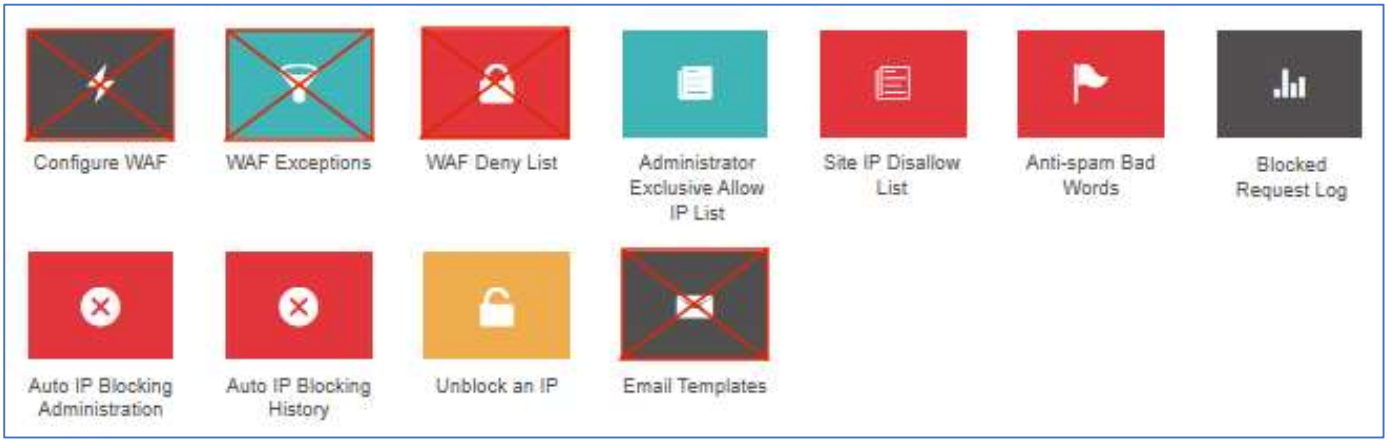
Helaas blijven veel iconen van een onderdeel wel staan, terwijl daar toch geen rechten voor zijn. Dan krijgt men onderstaande melding. Deze iconen krijgen in de afbeeldingen verderop een rood kruis.



2.3. Security

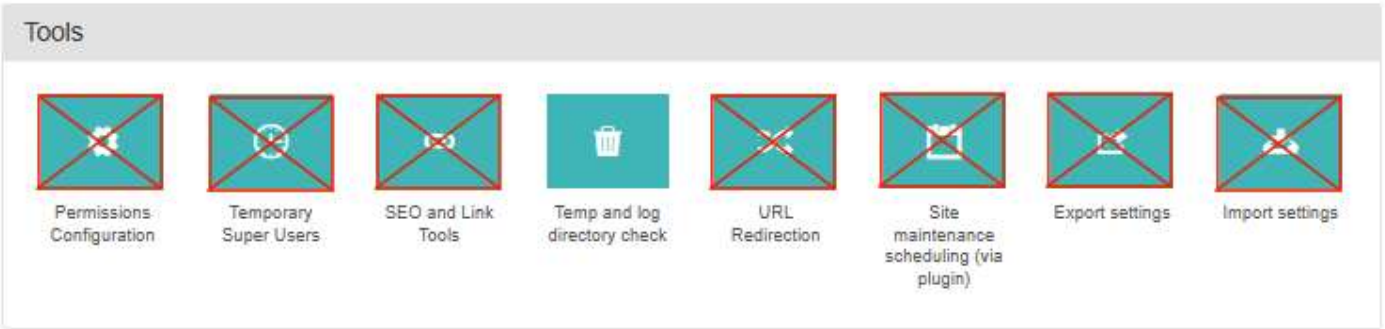
Naam	Betekenis	Autorisatie	Online beschrijving
Emergency Off-line	De website off-line zetten ingeval van een (beveiligings-)probleem. Waarschuw ook de Webhosting team als je hier gebruik van moet maken!	Webmaster	Online beschrijving
Master Password	Het afschermen van Admin Tools instellingen en het afschermen van gebruik van eventuele onderdelen voor andere administrators met een wachtwoord.	Webhosting	
Password protect Administrator	Zetten van een extra username password op de administrators accounts.	Webhosting	
.htaccess Maker	Het toevoegen van (standaard)opties aan het .htaccess bestand.	Webhosting	
Web Application Firewall	Instellingen mogelijkheden van de Web Application Firewall (vervolgscherm 2.4).	Webmaster	Online beschrijving
PHP File Change Scanner	Uitvoeren van security scan van de PHP files van de Joomla omgeving.	Webhosting	
PHP File Change Scanner Scheduling	Automatisch schedulen van de PHP File Change Scanner.	Webhosting	

2.4. Web Application Firewall



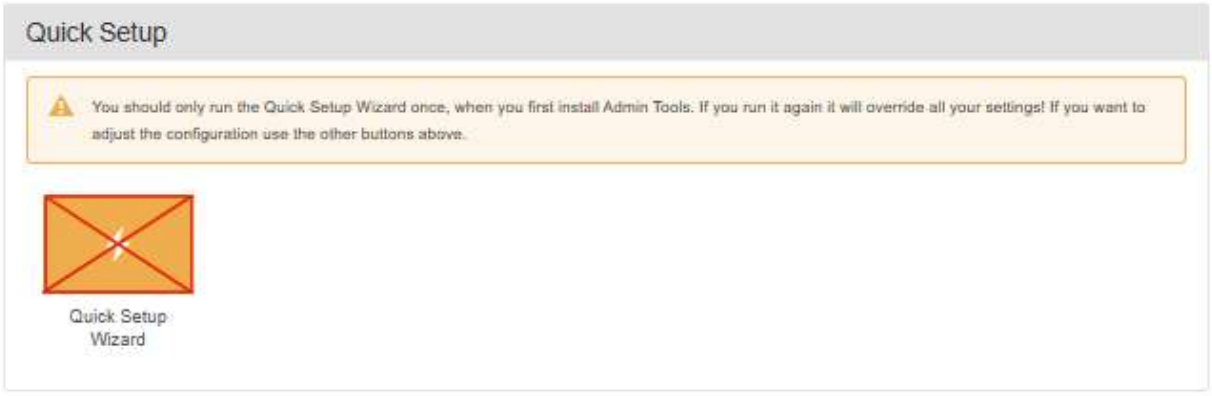
Naam	Betekenis	Autorisatie	Online beschrijving
Configure WAF	Alle basis instellingen van de Web Application Firewall.	Webhosting	
WAF Exeptions	Mogelijkheid om uitzonderen voor de Firewall toe te voegen.	Webhosting	
WAF Deny List	Extra mogelijkheid van toevoegen van filter/ blokkeer opties voor de Firewall.	Webhosting	
Administrator Exclusive Allow IP List	Bijhouden van een lijst van IP-nummers die altijd toegang hebben tot het beheren van de website. Hierin worden o.a. de IP-nummers van het Webhosting team ingezet.	Webmaster	Online beschrijving
Site IP Disallow List	Het kunnen beheren van de IP nummers die geblokkeerd moeten worden.	Webmaster	Online beschrijving
Anti-spam Bad Words	Lijst met woorden die niet gebruikt mogen worden op de website (dan 403 error). B.v. als er openbaar tekst ingevoerd kan worden.	Webmaster	Online beschrijving
Blocked Request Log	De logging van de Firewall exceptions, de reden van blokkeren. Zie ook H3. Logging: Securirty Graph en Security Exceptions Log.	Webmaster	Online beschrijving En ook H3.
Auto IP Blocking Administration	De lijst van IP-nummers die herhaald worden geblokkeerd.	Webmaster	Online beschrijving
Auto IP Blocking History	History van automatisch geblokkeerde IP nummers.	Webmaster	Online beschrijving
Unblock an IP	De mogelijkheid om een onterecht geblokkeerd IP nummer weer toe te staan.	Webmaster	Niet gevonden …
Email Templates	De email berichten/templates die worden gebruikt voor het versturen van fout boodschappen. Bepaalt ook waarvoor wel of niet email wordt verstuurd.	Webhosting	

2.5. Tools en Quick Setup



Naam	Betekenis	Autorisatie	Online beschrijving
Permission Configuration	Het aanpassen van de rechten per directory en bestand.	Webhosting	
Tempory Super Users	Niet gevonden in handleiding … Tijdelijk aanmaken van Super Users?	Webhosting	
SEO and Link Tools	Bij verplaatsing van site's herstellen van aanwezige links.	Webhosting	
Temp and log directory check	Controleert de aanwezigheid van de temp locatie.	Webmaster	Niet gevonden …
URL Redirection	Het aanmaken van (verkorte) URL's voor het gebruik in de website.	Webhosting	

Site maintenance scheduling (via plugin)	Zetten van achtergrond taken voor de System - Admin Tools plugin.	Webhosting	
Export settings	Keuze van settings voor de export file.	Webhosting	
Import settings	Selecten van de import file voor het overschrijven van de Admin Tools settings.	Webhosting	



Naam	Betekenis	Autorisatie	Online beschrijving
Quick Setup Wizard	Normaal alleen gebruikt direct na installatie om een groot aantal basisinstellingen te zetten. Button blijft wel staan na gebruik.	Webhosting	

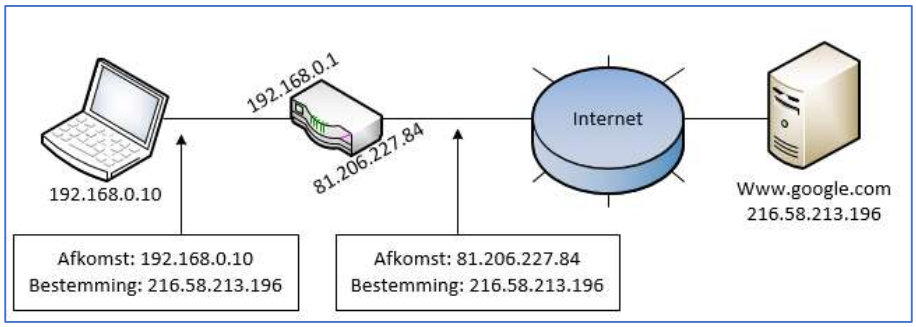
3. Extra beveiliging door gebruik van de “Administrator Exclusive Allow IP List”

Er is nog een mogelijkheid om gebruik te maken van een extra beveiligingsoptie van de Admin Tools en dat is de “Administrator Exclusive Allow IP List”. Het is voor het Webhosting team eigenlijk onmogelijk om dit voor alle groepen te gaan beheren. We vragen dan ook de lokale webmasters om deze “Exclusive Allow IP List” voor de lokale groep te gaan beheren. Als je de enige administrator bent dan gaat het dus maar om één adres. Zijn er meerdere administrators dan zul je de verschillende IP-adressen van je groep dus moeten verzamelen.

Voor informatie over een IP-adres zie b.v.:

https://solidbe.nl/nl/tech/networking/ipv6-in-een-notendop/#hoofdstuk7 of
https://www.vpngids.nl/privacy/anoniem-browsen/wat-is-mijn-ip/

“Als u een Internetabonnement voor thuis afsluit, krijg u van uw internetprovider een router. Deze router communiceert met het internet via een wereldwijd uniek IPv4 adres. Binnenshuis communiceert de router met een privé IPv4 adres. Alle apparaten die intern functioneren communiceren met elkaar via privé IP adressen, zonder tussenkomst van een router. Alle apparaten, die naar internet verbinden, moeten via de router gaan.”



De Admin Tools biedt nu de mogelijkheid om alleen bekende IP-adressen toe te laten tot het administrator deel van de website en alle andere IP-adressen te blokkeren voor toegang als administrator. Dit is natuurlijk nog een mooie extra beveiliging van je website! Het gaat dan om het IP-adres waarmee je toegang krijgt tot het internet. Hierboven is dat het adres 81.206.227.84. Zolang je bij dezelfde provider blijft en hetzelfde netwerkkastje (mediabox, router)

blijft gebruiken blijft dit normaal een vast adres. Het adres van je PC/Laptop (hierboven 192.168.0.10) kan soms wel vaker veranderen, maar dat geeft dus niet.

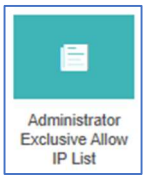
Je kunt op verschillende manieren bepalen met welk IP-adres je toegang hebt tot het internet (dus bovenstaand adres 81.206.227.84).

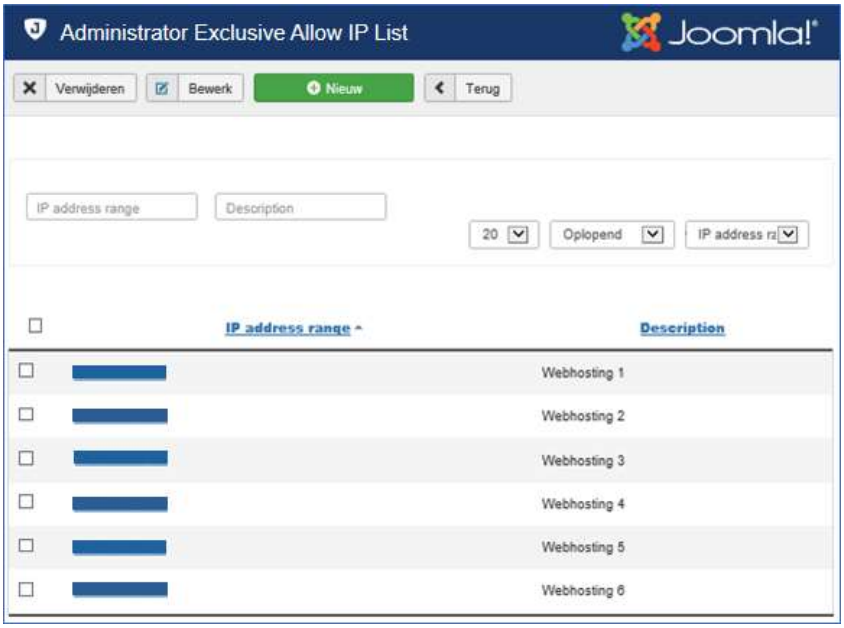
- *Bepalen IP-adres via Admin Tools zelf*

Start de Admin Tools op:

Menu | Componenten | Admin Tools

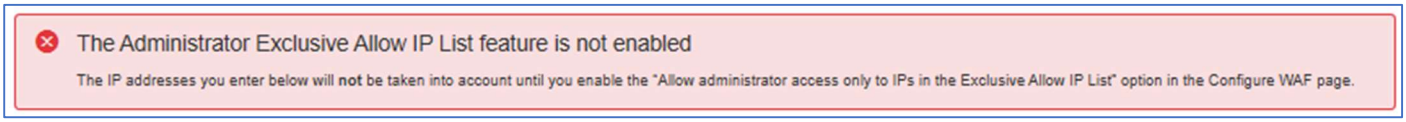
Kies in **Security** de **Web Application Firewal**
Kies dan voor **Administrator Exclusive Allow IP List**





Je ziet hierboven al de IP-adressen staan van het Webhosting team. Deze adressen moet je dus laten staan!

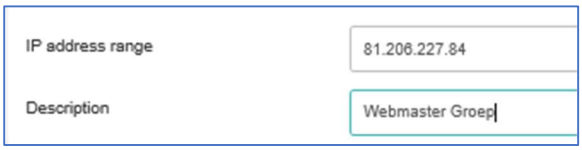
Als de extra beveiligingsoptie nog niet aan staat krijg je nog onderstaande melding te zien:



Als je nu kiest voor een [Nieuw] IP-adres toe te voegen dan krijg je:

In rood zie je dan je eigen IP-adres staan!

Daaronder kun je dan gelijk het IP-adres toevoegen. Kies een herkenbare naam bij “Description” en kies voor [Opslaan & sluiten]



- *Bepalen IP-adres via diverse websites.*

Als iemand niet direct zelf bij de Admin Tools kan komen (b.v. een andere beheerder van je groep) dan zijn er ook diverse websites waarbij je eenvoudig het IP-adres kunt zien.

https://www.watismijnipadres.nl/ Geeft gelijk je IP adres.

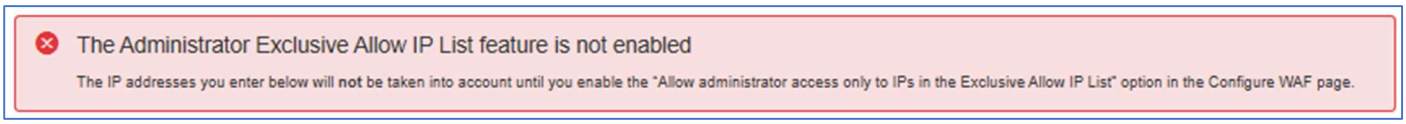
http://ip.kliksafe.nl/ Geeft gelijk je IP adres.

https://www.speedtest.net/ Deze test eventueel ook je internetsnelheid.

In het gedeelte hierboven zie je hoe je het IP-adres dan aan de “Administrator Exclusive Allow IP List” toevoegt.

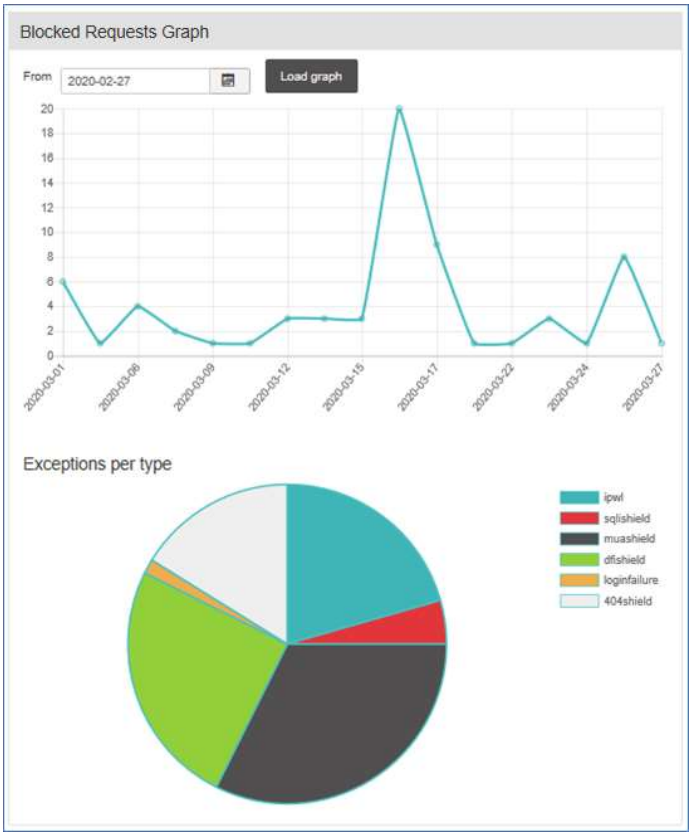
Als alle IP-adressen van alle gebruikers die van het administrator deel van de website gebruik maken zijn toegevoegd, kan het Webhosting team deze extra beveiligingsoptie aanzetten, zodat alleen IP-adressen van de “Exclusive Allow IP List” toegang krijgen en anderen geblokkeerd worden. Tijdens de inrichting van de Admin Tools zal het Webhosting team vragen of jij de IP-adressen voor je eigen groep wilt beheren. Wil je dat niet, dan kunnen we deze extra beveiliging dus niet aanzetten.

Zolang onderstaande melding ziet, staat deze extra beveiliging dus nog niet aan!

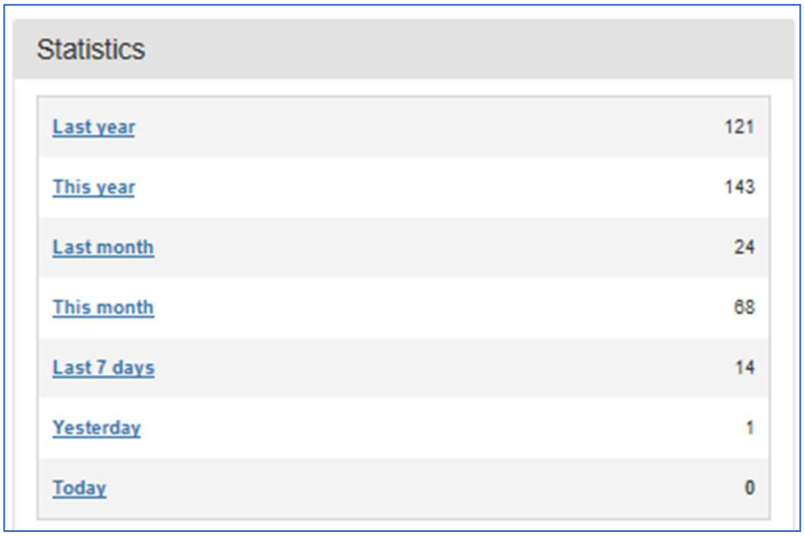


4. Logging: Blocked Requests Graph en Blocked Request Log

De Admin Tools houdt een uitgebreide logging bij van alle gedetecteerde meldingen van de Web Application Firewall. In het hoofdscherm van de Admin Tools: het Control Panel zijn deze al zichtbaar in een grafiek: de Blocked Request Graph. Hier een voorbeeld van de meldingen van de website van de internetgroep.

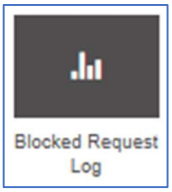


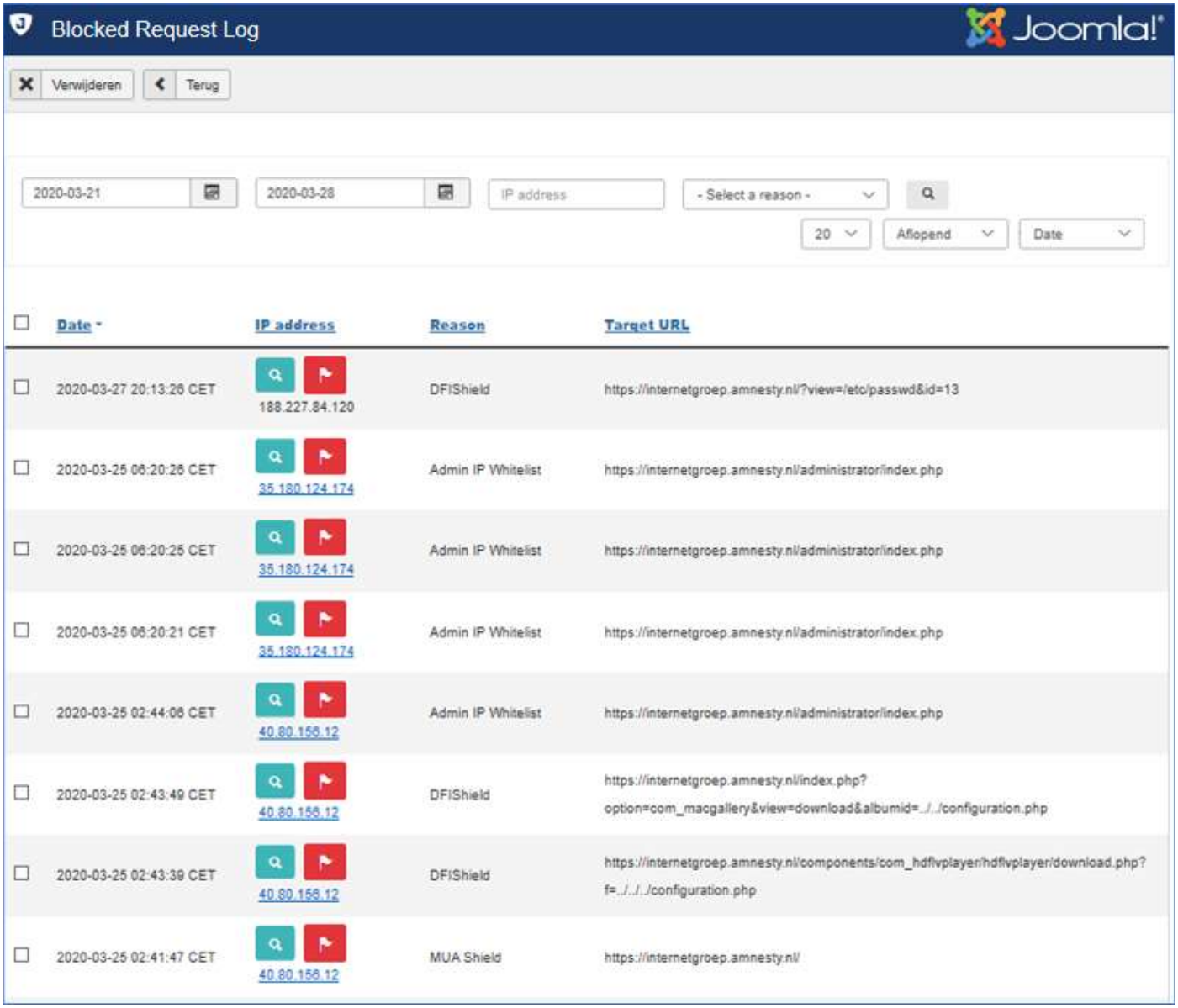
Via dit hoofdscherm / Control Panel kan men ook meer gedetailleerde gegevens krijgen:



Als men één van de linkjes kiest, krijgt men een overzicht voor een bepaalde periode.
Men kan ook gebruik maken van de Web Application Firewall en het icoon daar.

Web Application Firewall:

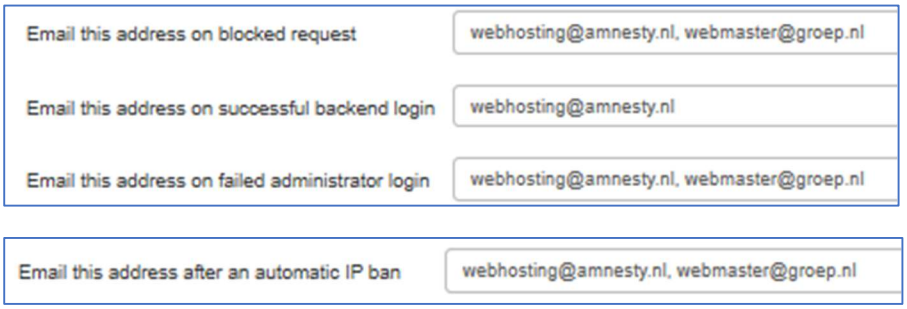




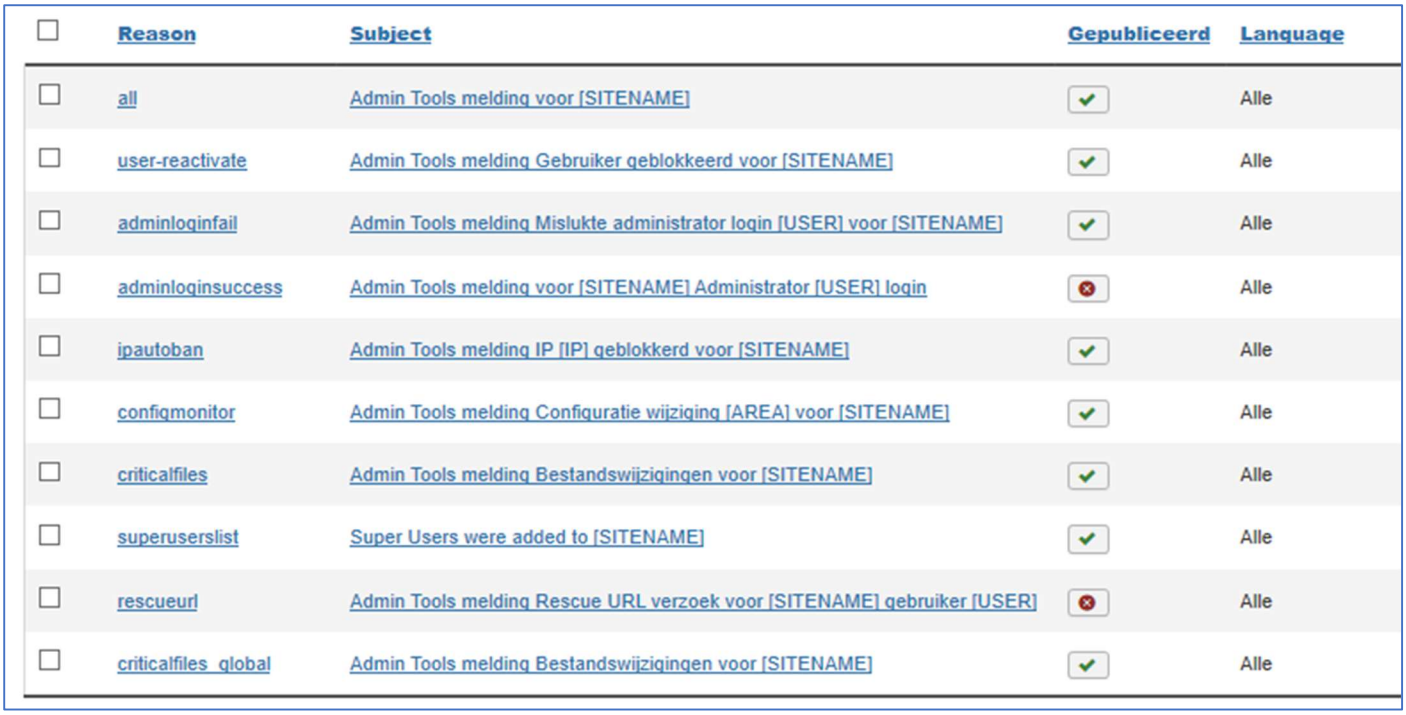
Bij de List of blocking reasons vind je de betekenis van de reden van blokkeren.

5. Email berichten

Alle door Admin Tools gedetecteerde meldingen kunnen ook -vrijwel direct- per Email verzonden worden. Standaard wordt gekozen om alle meldingen naar het Webhosting team te sturen. Maar om ook de lokale groep op de hoogte te houden van alle meldingen wordt er gekozen om de mails ook te sturen naar de bij ons bekende webmaster.



Voor het versturen van de Email berichten gebruikt de Admin Tools “templates” met in het bericht de juiste informatie over de melding. Zo zijn er de volgende templates:



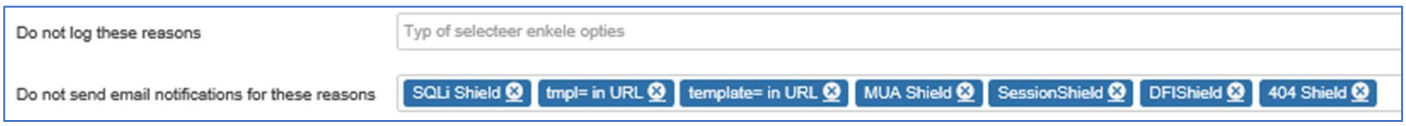
Reason	Subject	Gepubliceerd	Language
all	Admin Tools melding voor [SITENAME]	✓	Alle
user-reactivate	Admin Tools melding Gebruiker geblokkeerd voor [SITENAME]	✓	Alle
adminloginfail	Admin Tools melding Mislukte administrator login [USER] voor [SITENAME]	✓	Alle
adminloginsuccess	Admin Tools melding voor [SITENAME] Administrator [USER] login	✗	Alle
ipautoban	Admin Tools melding IP [IP] geblokkerd voor [SITENAME]	✓	Alle
configmonitor	Admin Tools melding Configuratie wijziging [AREA] voor [SITENAME]	✓	Alle
criticalfiles	Admin Tools melding Bestandswijzigingen voor [SITENAME]	✓	Alle
superuserslist	Super Users were added to [SITENAME]	✓	Alle
rescueurl	Admin Tools melding Rescue URL verzoek voor [SITENAME] gebruiker [USER]	✗	Alle
criticalfiles_global	Admin Tools melding Bestandswijzigingen voor [SITENAME]	✓	Alle

Per template kan gekozen worden of deze gebruikt wordt (Gepubliceerd) of niet. Standaard worden dus alle templates gebruikt, behalve de “adminloginsuccess”. We hebben er dus gekozen om niet alle succesvolle administrator logins te melden. Als een groep behoefte heeft om wel een melding te krijgen van alle succesvolle administrator logins dan kunnen we dit eventueel wel aanzetten. In de eerste afbeelding zie je dat we een aparte email adres voor de succesvolle logins kunnen opgeven. Stuur dan even een verzoek naar webhosting@amnesty.nl met het Email adres waar de meldingen dan naar toe mogen.

Na een paar maanden proefdraaien (april t/m juli 2020) blijken er via de eerste template “Admin Tools melding voor [SITENAME] voor bepaalde “reasons” toch wel heel veel Email meldingen worden verstuurd. Vooral 2 items blijken voor veel Email verkeer te zorgen:

- 404 Shield: Er wordt naar (bekende) webpagina's gevraagd, die er niet zijn (404 foutmelding). B.v. naar WordPress pagina's op een Joomla site.
- SQLi Shield: Poging tot invoegen van data in de MySQL database, b.v. Usernames en paswoorden.

Het is mogelijk om bepaalde meldingen wel in de logging te laten komen, maar daarvan geen Email melding te versturen. We hebben daarom nog eens kritisch gekeken welke meldingen we eigenlijk wel willen versturen en welke niet. We hebben gekozen om de volgende reasons uit te zetten:



Dus alle meldingen komen wel in de logging, maar van 7 “reasons” worden geen Email berichten meer verstuurd.

Ook als je toch liever helemaal geen meldingen van Admin Tools wilt ontvangen kun je een verzoek sturen naar webhosting@amnesty.nl.

In hoofdstuk 5.1 geven we de Akeeba uitleg over de reasons, onze eigen korte verklaring en de reden om wel of niet Email te verzenden.
In hoofdstuk 5.2 geven we een aantal voorbeelden van de Admin Tools Email berichten.
In hoofdstuk 5.3 geven we de volledige Akeeba List of blocking reasons.

5.1. Keuzes voor verzenden via Email van Admin Tools meldingen.

Keuzes voor verzenden van Email meldingen via template “Admin Tools melding voor [SITENAME] voor bepaalde “reasons”:

Email J/N	Reason	Akeeba List of blocking reasons	Korte verklaring webhosting	Motivatie verzenden Email J/N
J	**Admin Query String**	Someone tried to access your site's administrator section but he didn't provide the secret URL parameter. Admin Tools blocked him and prevented him from seeing the login page at all.	Poging tot gebruik van /administrator of /administrator/index.php?< foute string> om in te loggen op de site.	Komt ook nog wel regematig voor. Geeft wel poging tot inloggen/hacking aan. Eigen webmaster en webhosting kent de secret URL: J
J	**Admin Exlusive Allow IP List**	Someone tried to access your site's administrator section but his IP was not in the Administrator Exclusive Allow IP List. Admin Tools blocked him and prevented him from seeing the login page at all.	Het gebruik van de Exlusive Allow IP lijst staat aan en iemand probeert in te loggen die niet op de lijst staat.	Komt ook nog wel regematig voor. Geeft wel poging tot inloggen/hacking aan. Eigen webmaster en webhosting staan op de Allow IP lijst: J
J	**Login failure**	Someone tried to log in in the front- or back-end of your site with the wrong username and/or password.	Voor back-end wordt juiste secret string gegeven of staat op de Exclusive Allow IP lijst, maar wordt verkeerde password gegeven. Of verkeerd password voor front-end van site.	Foute inlogpoging. Kan foutje van webmaster of webhosting zijn. Als veel voorkomt wil je dat weten: J
N	**404 Shield**	Configure WAF, 404 Shield, blocked by Admin Tools wp-admin.php wp-login.php wp-content/* wp-admin/* This feature 404 will block irregular "Page not found"requests which typically indicate that your site is beingtargeted by an automatic vulnerability scanner or hackingtool. For example, someone trying to access the folder wp-admin on your Joomla site is irregular sincethat folder is the administration area of WordPress.	Er wordt naar (bekende) webpagina's gevraagd, die er niet zijn (404 foutmelding). B.v. naar WordPress pagina's op een Joomla site.	Eigenlijk wel ongewenst, maar het zijn er te veel en men kan er weinig aan doen: N
N	**SQLi Shield**	Configure WAF, SQLiShield protection, blocked by Admin Tools. But what is a SQLi attack? Database queries are also called SQL queries An attacker can exploit this mistake by sendingdata which have the effect of terminating the developer'sdatabase query and starting a new one which either dumpsprivileged data -such as usernames and passwords- or modifiesdata into the database - such as adding a new Super User underthe control of the attacker. This class of attacks is calleda n SQL Injection, or SQLi for short, since the attacker"injects" his own code into a SQL query running on thesite.	Poging tot invoegen van data in de SQL database, b.v. Usernames en passworden.	Eigenlijk wel ongewenst, maar het zijn er te veel en men kan er weinig aan doen: N
N	**MUA Shield**	Configure WAF Malicious User Agent block (MUA), blocked by Admin Tools. Many hackers will try to access your site using a browser configured to send malicious PHP code in its useragent string (a small piece of text used to describe the browser to your server). The idea is that buggy log processing software will parse it and allow the hacker to gain control of your website. When enabled, this feature allows Admin Tools to detect such attacks and block the request.	Poging om via een browser om stukjes ongewenste PHP code mee te sturen.	Komt beperkt voor. Gekozen om de meldingen uit de logging te halen.

N	**tmpl= in URL**	Configure WAF, Block tmpl=foo system template, blocked by Admin Tools. One of the lesser known Joomla! features are its system templates. The value of the tmpl keyword tells Joomla which .php file in the template's folder it will use to render thepage. For example, ?tmpl=component tells Joomla to use the component.php file. Of and by itself this feature is not dangerous.However, hackers have realized that this feature is being abused by badly architectured plugins and components beyond the intended purpose in Joomla itself. The downside is that it may open a security hole, e.g. if the code parsing the tmpl keyword in a third party extension gets confused by certain types of data and executes arbitrarycode or does something unintended. For this reason Admin Tools has the Block tmpl=foo system template switch feature which will block any request that does not have one of the expected tmpl keywords for your site.	Bij sommige third party producten kan het gebruik van het oproepen van een tmpl (?tmpl=<template>) security problemen geven, zodat deze geblokkeerd worden. Er wordt ook een lijst met juiste tmpl (component, system, raw, koowa) ingesteld.	Komt beperkt voor. Gekozen om de meldingen uit de logging te halen.
N	**template= in URL**	Confiugure WAF, template=foo site tempate, blocked by Admin Tools. Another Joomla! hidden feature is the ability to switch between installed templates by passing a special URL parameter called "template". Enabling this option will turn off this hidden Joomla! feature.	Het is in Joomla mogelijk om in 1 site van meerder templates gebruik te maken en dus van buiten uit, via de URL te switchen. Dit gaat niet goed voor sommige third party producten en wordt geblokkeerd.	Komt beperkt voor. Gekozen om de meldingen uit de logging te halen.
N	**DFIShield**	Configure WAF , Direct File Inclusion (DFI), blocked by Admin Tools. Some hackers try to trick vulnerable components intoloading arbitrary files. Depending on the vulnerablecomponent, the file will either be output verbatim or parsedas a PHP file. This allows attackers to disclose sensitive information about your site or run malicious code uploaded to your site through another vulnerable vector, e.g. anunfiltered upload of executable PHP code. When this option isenabled, Admin Tools will search the request parameters foranything which looks like a file path. If one is found, itwill be scanned. If it is found to contain PHP code, the request will be rejected.	Er wordt geprobeerd gebruik te maken van bestaande files op systeem om te combineren met webpagina's.	Komt beperkt voor. Gekozen om de meldingen uit de logging te halen.
N	**Session Shield**	PHP session data poisoning protection(SessionShield). Prevents malicious input data which can be used to trickPHP's internal session handler into executing arbitrary code when it's restoring the user session. The PHP session unserializer has a major bug which makesit misinterpret stored session data if they contain specificcharacter combinations, overwriting the legitimate sessiondata with the attacker-defined contents. Combined with someother features of PHP this can lead to the execution ofarbitrary PHP code. In short, attackers can send malicious data in one page load and get arbitrarycode to execute in the next page load. This featureof Admin Tools detects and blocks this kind of malicious data.CAUTION: It may block some legitimate requests as well.	Er wordt geprobeerd data/gegevens van de ene pagina mee te sturen als data naar een volgende pagina, wat niet gewenst is.	Komt beperkt voor. Gekozen om de meldingen uit de logging te halen.
J	**<overigen>**	Diversen, zijn nog niet voorgekomen!		Overige Reasons/codes zijn nog niet voorgekomen, standaard aan laten staan: J

Daarnaast zijn er nog een aantal andere Email templates die ook Email berichten kunnen versturen:

Email J/N	Template	Template omschrijving	Motivatie verzenden Email J/N
J	**user-reactivate**	Admin Tools melding Gebruiker geblokkeerd voor [SITENAME]	Nog niet voorgekomen: J
J	**adminloginfail**	Admin Tools melding Mislukte administrator login [USER] voor [SITENAME]	Mislukte login doorgeven aan webmaster en webhosting: J
N	**adminloginsuccess**	Admin Tools melding voor [SITENAME] Administrator [USER] login	Template staat standaard uit. Kan op verzoek van webmaster aangezet worden: N
J	**ipautoban**	Admin Tools melding IP [IP] geblokkerd voor [SITENAME]	Webmaster en webhosting laten zien dat er redenen zijn om te blokkeren: J
J	**configmonitor**	Admin Tools melding Configuratie wijziging [AREA] voor [SITENAME]	Wijzingen in de instellingen van Joomla, melden aan de webmaster en webhosting: J
J	**criticalfiles**	Admin Tools melding Bestandswijzigingen voor [SITENAME]	Vaak Joomla of plugin updates, melden aan webmaster en webhosting: J
N	**rescueurl**	Admin Tools melding Rescue URL verzoek voor [SITENAME] gebruiker [USER]	Template staat standaard uit. Ingewikkelde proces voor "rescue" optie. Alleen voor webhosting: N
J	**criticalfiles_global**	Admin Tools melding Bestandswijzigingen voor [SITENAME]	Vaak Joomla of plugin updates, melden aan webmaster en webhosting: J

5.2. Voorbeelden van Email berichten

Admin Tools melding voor [SITENAME]

Van: test47.amnesty.nl <webhosting@amnesty.nl>
Verzonden: woensdag 20 mei 2020 21:19
Aan: Richard de Boer <r.deboer@amnesty.nl>
Onderwerp: Admin Tools melding voor test47.amnesty.nl

Hallo webmaster,

Er is een Admin Tools beveiligingsmelding voor de website **test47.amnesty.nl** met de volgende details:
IP adres: **123.456.78.9** (IP Lookup: IP Lookup)
Reden: **Admin Exclusive Allow IP List**

Zie voor de reden ook de List of blocking reasons.

Met vriendelijke groet,
Webhosting Amnesty NL
webhosting@amnesty.nl

Je krijgt deze mail omdat je de administrator bent van test47.amnesty.nl en omdat webhosting het ontvangen van deze mails zo voor je ingesteld heeft.

Zie ook 5.1. List of blocking reasons voor de lijst met redenen.

Admin Tools medling voor [SITENAME] Administrator [USER] login

Deze template staat dus normaal niet aan!

Van: test47.amnesty.nl <webhosting@amnesty.nl>
Verzonden: dinsdag 19 mei 2020 21:40
Aan: Richard de Boer <r.deboer@amnesty.nl>
Onderwerp: Admin Tools melding voor test47.amnesty.nl Administrator Beheer@Amnesty20 (Webhosting Amnesty <webhosting

Hallo webmaster,

Er is een Admin Tools beveiligingsmelding voor de website **test47.amnesty.nl** voor de gebruiker **Beheer@Amnesty20 (Webhosting Amnesty)**. De gebruiker is succesvol ingelogd in het administrator gedeelte van je website. Meer informatie:

Gebruiker: Beheer@Amnesty20 (Webhosting Amnesty)
IP adres: 123.456.78.9 (IP Lookup)
Browser User Agent string: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko

Als dit een onverwachte inlog melding is controleer dan je website en bij problemen waarschuw het webhosting team.

Met vriendelijke groet,
Webhosting Amnesty NL
webhosting@amnesty.nl

You are receiving this automatic email message because you are an administrator in *test47.amnesty.nl*. Do not reply to this email, it's sent from an unmonitored email address.

Admin Tools melding IP [IP] geblokkeerd voor [SITENAME]

Van: test47.amnesty.nl <webhosting@amnesty.nl>
Verzonden: woensdag 20 mei 2020 22:10
Aan: Richard de Boer <r.deboer@amnesty.nl>
Onderwerp: Admin Tools melding IP 123.456.78.9 geblokkerd voor test47.amnesty.nl

Hallo webmaster,

Er is een Admin Tools beveiligingsmelding voor de website test47.amnesty.nl. Het IP adres 123.456.78.9 is nu geblokkeerd voor toegang tot je website. Meer informatie:

IP adres: 123.456.78.9 (IP Lookup: IP Lookup)
Reden: Auto-banned IP address
Geblokkeerd tot: 2020-05-20 20:25:13

Als dit je eigen IP adres is en je hebt geen toegang meer tot je website neem dan contact op met het webhosting team.

Met vriendelijke groet,
Webhosting Amnesty NL
webhosting@amnesty.nl

Je krijgt deze mail omdat je de administrator bent van test47.amnesty.nl en omdat webhosting het ontvangen van deze mails zo voor je ingesteld heeft.

Admin Tools melding Configuratie wijziging[AREA] voor [SITENAME]

Van: test47.amnesty.nl <webhosting@amnesty.nl>
Verzonden: dinsdag 19 mei 2020 19:50
Aan: Richard de Boer <r.deboer@amnesty.nl>
Onderwerp: Admin Tools melding Configuratie wijziging Algemene instellingen voor test47.amnesty.nl

Hallo webmaster,

Er is een Admin Tools beveiligingsmelding dat er enkele configuratie wijzigingen zijn aangebracht voor de de website **test47.amnesty.nl** in het onderdeel: **Algemene instellingen**

IP adres: **123.456.78.9** (IP Lookup: IP Lookup)
User Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko

Mogelijk heb je zelf een wijziging aangebracht.
Als het webhosting team een wijzing heeft aangebracht gebruiken ze normaal de IP adressen:
123.456.78.9, 123.456.78.9, 123.456.78.9, 123.456.78.9, 123.456.78.9, 123.456.78.9

Met vriendelijke groet,
Webhosting Amnesty NL
webhosting@amnesty.nl

Je krijgt deze mail omdat je de administrator bent van test47.amnesty.nl en omdat webhosting het ontvangen van deze mails zo voor je ingesteld heeft.

Admin Tools melding Bestandswijzgingen voor [SITENAME]

Van: test47.amnesty.nl <webhosting@amnesty.nl>
Verzonden: dinsdag 19 mei 2020 19:50
Aan: Richard de Boer <r.deboer@amnesty.nl>
Onderwerp: Admin Tools melding Bestandswijzigingen voor test47.amnesty.nl

Hallo webmaster,

Er is een Admin Tools beveiligingsmelding dat er enkele belangrijke bestanden zijn gewijzigd voor de de website **test47.amnesty.nl**. Het gaat om de bestanden:

- **configuration.php**

De bestanden kunnen o.a. gewijzigd zijn door de volgende redenen:

- Veranderingen in de Joomla Global Configuration
- Updates van Joomla (door het Webhosting team)
- Updates van site templates

Met vriendelijke groet,
Webhosting Amnesty NL
webhosting@amnesty.nl

Je krijgt deze mail omdat je de administrator bent van test47.amnesty.nl en omdat webhosting het ontvangen van deze mails zo voor je ingesteld heeft.

5.3. List of blocking reasons

Online versie bij Akeeba: https://www.akeebabackup.com/documentation/admin-tools/waf-log.html#waf-log-reasons

List of blocking reasons 20-06-2020

The block reasons, listed in the log and optionally sent to you by email are the following. The "Code" is what you need to enter in the "Do not log these reasons" or "Do not send email notifications for these reasons" options in WAF configuration to prevent these security exceptions from being logged or trigger an email respectively.

404 Shield
Code: `404shield`
See the Configure WAF page, **404 Shield**. The request was blocked by Admin Tools.

Admin Query String
Code: `adminpwp`
Someone tried to access your site's administrator section but he didn't provide the secret URL parameter. Admin Tools blocked him and prevented him from seeing the login page at all.

Admin Exclusive Allow IP List
Code: `ipwl`
Someone tried to access your site's administrator section but his IP was not in the Administrator Exclusive Allow IP List. Admin Tools blocked him and prevented him from seeing the login page at all.

Site IP Disallow List
Code: not applicable
Someone tried accessing the front- or back-end of your site but his IP is in the IP Disallow List. Admin Tools blocked him and didn't allow him to see the content of your site.

SQLi Shield
Code: `sqlishield`
See the Configure WAF page, **SQLiShield protection against SQL injection attacks**. The attack was blocked by Admin Tools.

Bad Words Filtering
Code: `antispam`
The request contains one of the Bad Words you have defined and was blocked by Admin Tools.

tp=1 in URL

Code: not applicable
Only for Joomla! 1.5, see the respective option in the Configure WAF page. The attack was blocked by Admin Tools.

tmpl= in URL

Code: `tmpl`
See the Configure WAF page, **Block tmpl=foo system template switch**. The attack was blocked by Admin Tools.

template= in URL

Code: `template`
See the Configure WAF page, **Block template=foo site template switch**. The attack was blocked by Admin Tools.

MUA Shield

Code: `muashield`
See the Configure WAF page, **Malicious User Agent block (MUAShield)**. The attack was blocked by Admin Tools.

CSRF Shield

Code: `csrfshield`
See the Configure WAF page, **CSRF/Anti-spam form protection (CSRFShield)** . The attack was blocked by Admin Tools.

Bad Behaviour

Code: not applicable
See the Configure WAF page, **Bad Behaviour integration**. The attack was blocked by Admin Tools. NO LONGER PRESENT SINCE ADMIN TOOLS 2.5.3

RFIShield

Code: `rfishield`
See the Configure WAF page, **Remote File Inclusion block (RFIShield)**. The attack was blocked by Admin Tools.

DFIShield

Code: `dfishield`
See the Configure WAF page, **Direct File Inclusion shield (DFIShield)**. The attack was blocked by Admin Tools.

UploadShield

Code: `uploadshield`
See the Configure WAF page, **Uploads scanner (UploadShield)**. The attack was blocked by Admin Tools.

XSSShield

Code: `xssshield`
(Only on older sites) **Cross Site Scripting block (XSSShield)**. The attack was blocked by Admin Tools. This has been removed in Admin Tools 3.6.7 as it was throwing too many false positives (legitimate requests being blocked).

Spammer (via HTTP:BL)

Code: `httpbl`
See the Configure WAF page, **SQLiShield protection against SQL injection attacks**. The attack was blocked by Admin Tools.

Login failure

Code: `loginfailure`
Someone tried to log in in the front- or back-end of your site with the wrong username and/or password.

Two-factor Auth Fail

Code: `securitycode`
Someone tried to log in the back-end of your site but provided the wrong Two Factor Authentication code. Please note that this feature has been removed since Admin Tools 3.5.0. If you see it, it probaby comes from an old version of Admin Tools.

Backend Edit Admin User

Code: `nonewadmins`

Someone tried to create or edit an administrator user from the backend of your site. In this context "administrator user" means any user who belong in one or more User Groups that gives them backend login privileges. In a default Joomla! installation these are the users belonging to the Manager, Administrator and Super User groups.

Frontend Edit Admin User

Code: `nonewfrontendadmins`

Someone tried to create or edit an administrator user from the frontend of your site. In this context "administrator user" means any user who belong in one or more User Groups that gives them backend login privileges. In a default Joomla! installation these are the users belonging to the Manager, Administrator and Super User groups.

Configuration Editing

Code: `configmonitor`

Someone tried to change either the Global Configuration of Joomla! itself or the configuration (Options) of a component. Please consult the additional information saved with this security exception to understand which configuration was attempted to be changed. The change may have originated from the backend or the frontend of your site.