

**AMNESTY
INTERNATIONAL**



Maintain. Protect. Optimise.
Admin Tools  for Joomla!

AMNESTY – INTERNETGROEP

Joomla beveiliging

Donderdag 18 november 2021

Richard de Boer

Joomla beveiliging

Agenda

- Inleiding & aanleiding
- Waarom Admin Tools? - pluspunten
- Installatie / aanmelden na Admin Tools
- Admin Tools gebruiken
- Web Application Firewall
- Logging & Statistics
- Admin Tools E-mails

Maintain. Protect. Optimise.

Admin Tools  for Joomla!

Joomla beveiliging

Inleiding & aanleiding

- In 2019 aantal hack-pogingen groepen sites
- Consequenties voor enkele groepsites
- Ook gevolgen voor Amnesty.nl
 - <groepsite>.amnesty.nl
 - www.amnesty.nl
- WordPress – Wordfence
- Joomla – Akeeba Admin Tools

verdacht / besmet
ook verdacht /besmet!



Joomla beveiliging

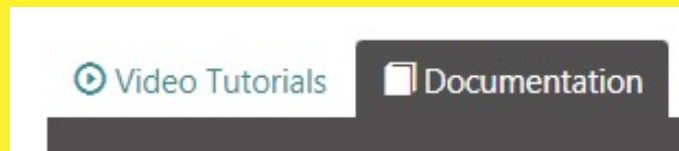
Akeeba Admin Tools



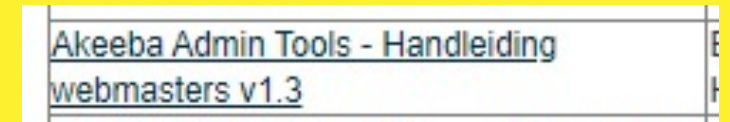
“Admin Tools is een software bundel die bestaat uit een Joomla! component, een module en een plug-in met als voornaamste doel de veiligheid en de prestaties van uw website te verbeteren, evenals de beheerder van deze website het leven een stuk makkelijker te maken door het automatiseren van algemene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



<https://www.akeebabackup.com/support/admin-tools/Tickets.html>



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



Joomla beveiliging

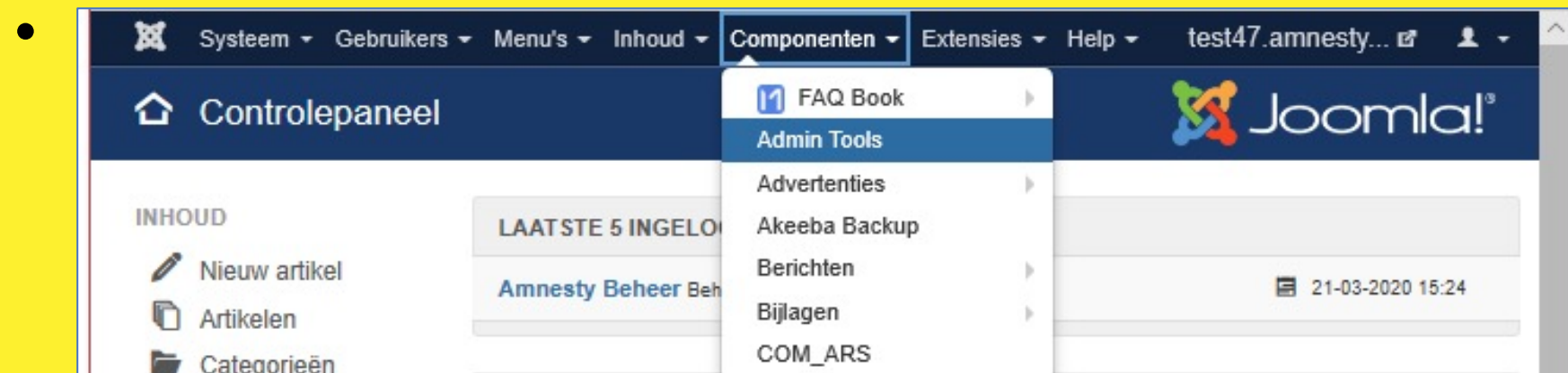
Akeeba Admin Tools - pluspunten

- De Web Application Firewall
- (Automatische) Blokkade van schadelijke IP adressen
- Toestaan veilige IP adressen (voor beheerders, Allow IP List)
- Automatisch controleren van de site (bestanden, rechten, wijzigingen)
- Gedetecteerde meldingen worden gelogd
- Meldingen kunnen worden verstuurd per mail
- Afscherming voor centraal beheer en lokale webmaster

Joomla beveiliging

Installatie / aanmelden

- Installatie door de Internetgroep / webhosting
- Aangepaste Administrator Logging
 - `https://<sitenaam>.amnesty.nl/administrator/index.php?<string>`
 - Bij extra IP beveiliging ook zonder extra string



Password Protection

The administrator of this site has locked down some or all features of Admin Tools with a password. Please supply the password in order to be allowed access to them.

Password:

Security

- Emergency Off Line
- Master Password
- Password protect Administrator
- Jtaccess Maker
- Web Application Firewall
- PHP File Change Scanner
- PHP File Change Scanner Scheduling

Tools

- Permissions Configuration
- Temporary Super Users
- SEO and Link Tools
- Temp and log directory check
- URL Redirection
- Site maintenance scheduling (via plugin)
- Export settings
- Import settings

Quick Setup

You should only run the Quick Setup Wizard once, when you first install Admin Tools. If you run it again it will override all your settings! If you want to adjust the configuration use the other buttons above.



Quick Setup Wizard

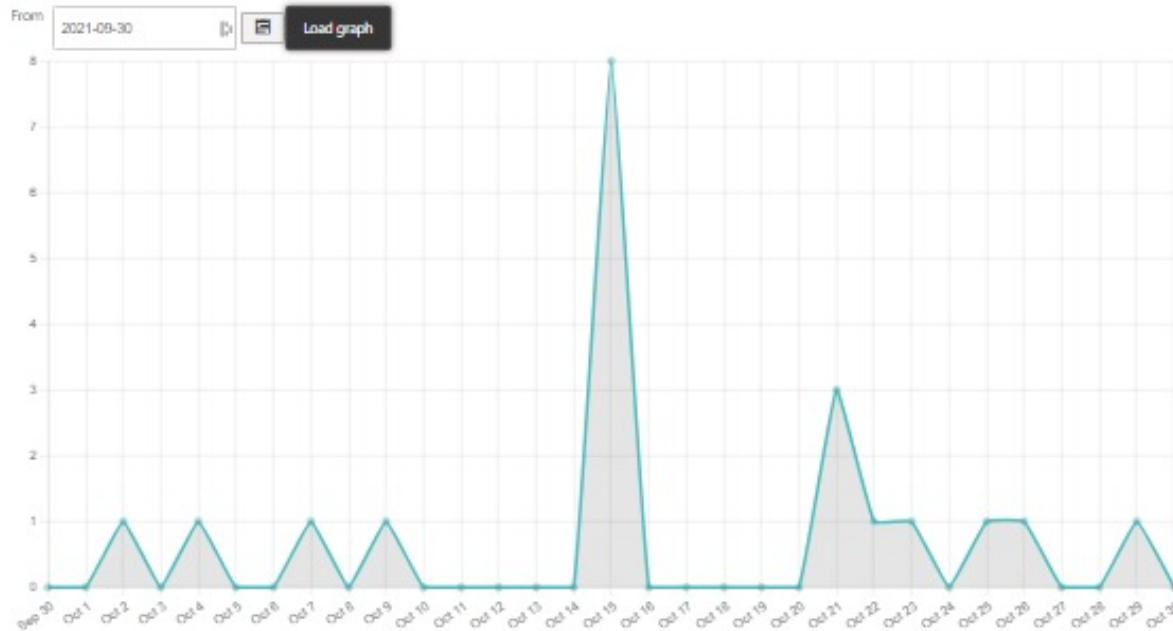
Updates

Admin Tools version 6.1.3 - [CHANGELOG](#)

Copyright © 2010-2021 Nicholas K. Dionysopoulos / [Alakaba Ltd](#)

If you use Admin Tools Professional, please post a rating and a review at the [Joomla! Extensions Directory](#).

Blocked Requests Graph



Blocked requests per type

Joomla beveiliging Control panel








- Security












- Web Application Firewall



Fout ×
You are not authorised to use this feature

Security

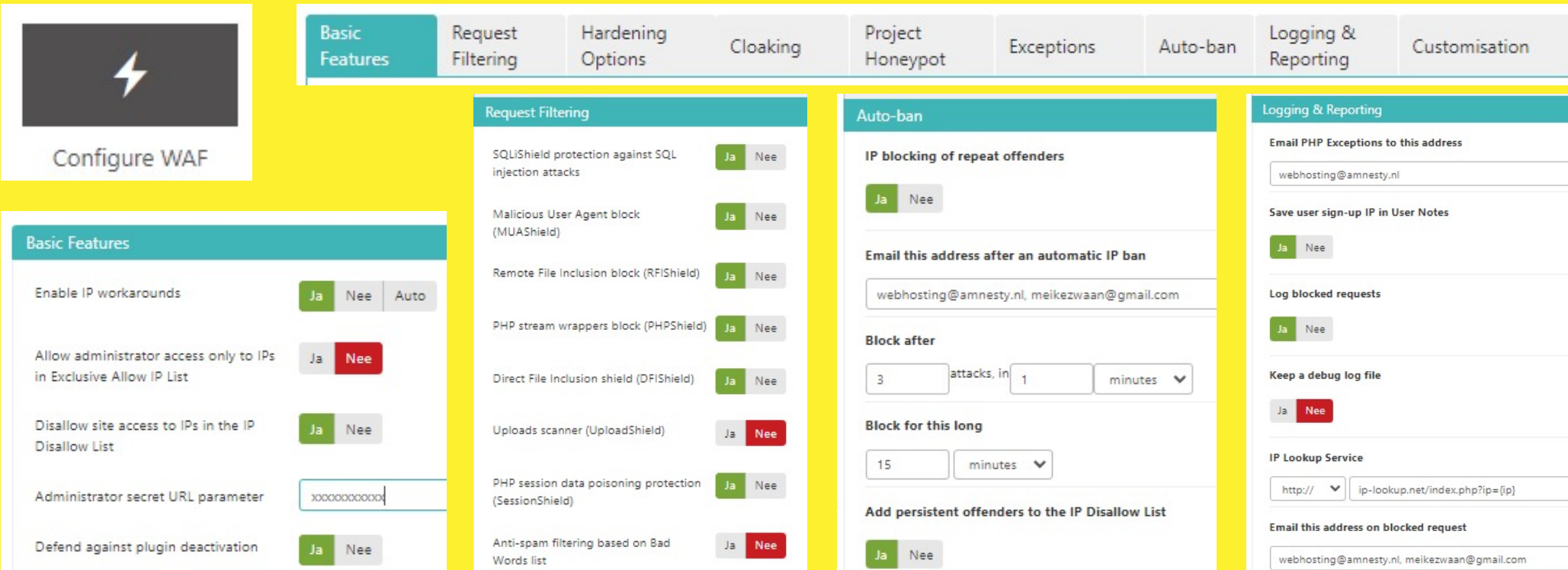
 Emergency Off-Line	 Master Password	 Password-protect Administrator	 .htaccess Maker	 Web Application Firewall	 PHP File Change Scanner	 PHP File Change Scanner Scheduling
---	--	---	--	---	--	---

 Configure WAF	 WAF Exceptions	 WAF Deny List	 Administrator Exclusive Allow IP List	 Site IP Disallow List	 Anti-spam Bad Words	 Blocked Request Log
 Auto IP Blocking Administration	 Auto IP Blocking History	 Unblock an IP	 Email Templates			

Joomla beveiliging

Configure Web Application Firewall

- Basis configuratie voor je gedaan



The screenshot displays the Joomla! WAF configuration interface. At the top, there is a navigation bar with tabs for: Basic Features, Request Filtering, Hardening Options, Cloaking, Project Honeypot, Exceptions, Auto-ban, Logging & Reporting, and Customisation. The 'Basic Features' tab is active, showing several settings with 'Ja' (Yes) or 'Nee' (No) buttons. A 'Configure WAF' button with a lightning bolt icon is visible in the top left. Below the navigation bar, the 'Request Filtering' tab is active, showing settings for SQLiShield, MUAShield, RFIShield, PHPShield, DFIShield, UploadShield, SessionShield, and Bad Words list. The 'Auto-ban' tab is also active, showing settings for IP blocking, email notifications, and block duration. The 'Logging & Reporting' tab is active, showing settings for email notifications, log blocked requests, and IP lookup service.

Basic Features

- Enable IP workarounds: Ja Nee Auto
- Allow administrator access only to IPs in Exclusive Allow IP List: Ja Nee
- Disallow site access to IPs in the IP Disallow List: Ja Nee
- Administrator secret URL parameter:
- Defend against plugin deactivation: Ja Nee

Request Filtering

- SQLiShield protection against SQL injection attacks: Ja Nee
- Malicious User Agent block (MUAShield): Ja Nee
- Remote File Inclusion block (RFIShield): Ja Nee
- PHP stream wrappers block (PHPShield): Ja Nee
- Direct File Inclusion shield (DFIShield): Ja Nee
- Uploads scanner (UploadShield): Ja Nee
- PHP session data poisoning protection (SessionShield): Ja Nee
- Anti-spam filtering based on Bad Words list: Ja Nee

Auto-ban

- IP blocking of repeat offenders: Ja Nee
- Email this address after an automatic IP ban:
- Block after: attacks, in minutes
- Block for this long: minutes
- Add persistent offenders to the IP Disallow List: Ja Nee

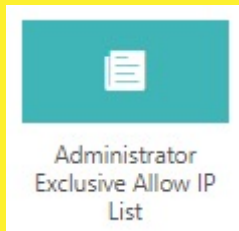
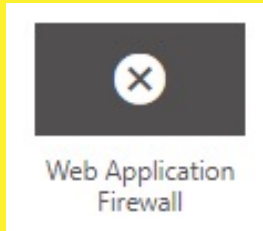
Logging & Reporting

- Email PHP Exceptions to this address:
- Save user sign-up IP in User Notes: Ja Nee
- Log blocked requests: Ja Nee
- Keep a debug log file: Ja Nee
- IP Lookup Service:
- Email this address on blocked request:

Joomla beveiliging

Extra IP beveiling administrators

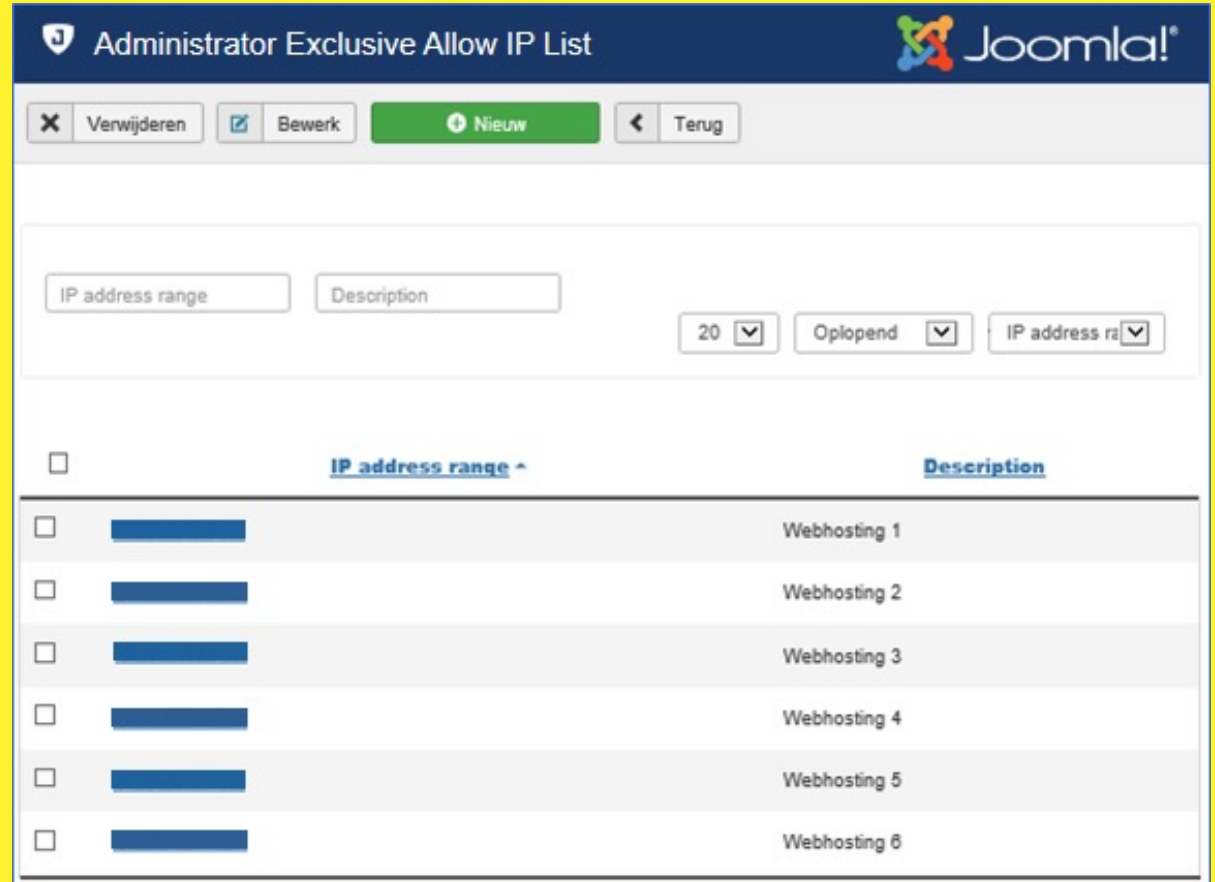
•



Allow administrator access only to IPs in Exclusive Allow IP List Ja Nee

 The Administrator Exclusive Allow IP List feature is not enabled
The IP addresses you enter below will **not** be taken into account until you enable the "Allow administrator access only to IPs in the Exclusive Allow IP List" option in the Configure WAF page.

• Even aanvragen bij [webhosting](#)

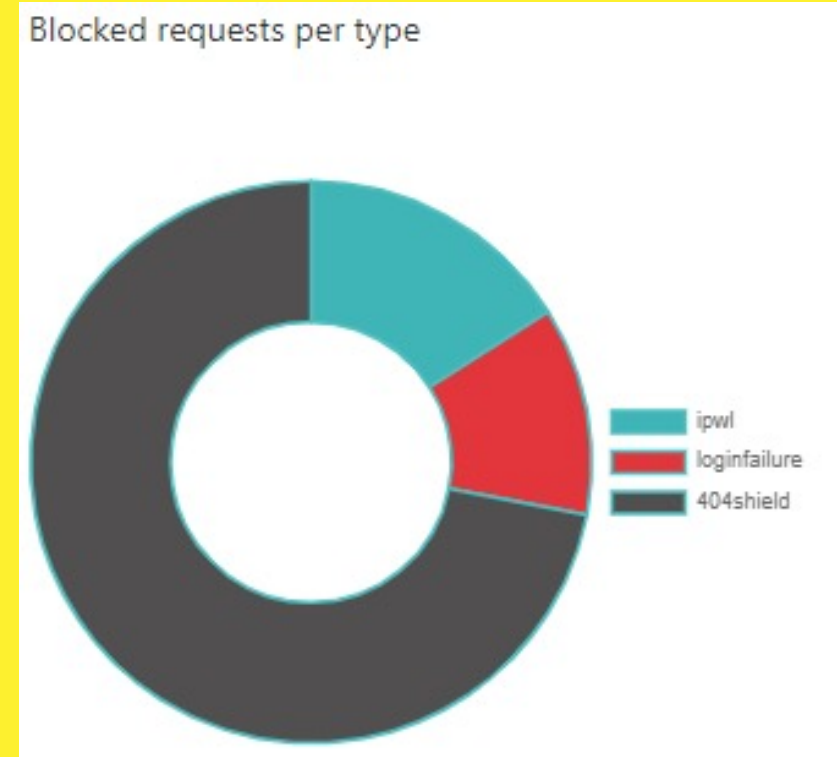
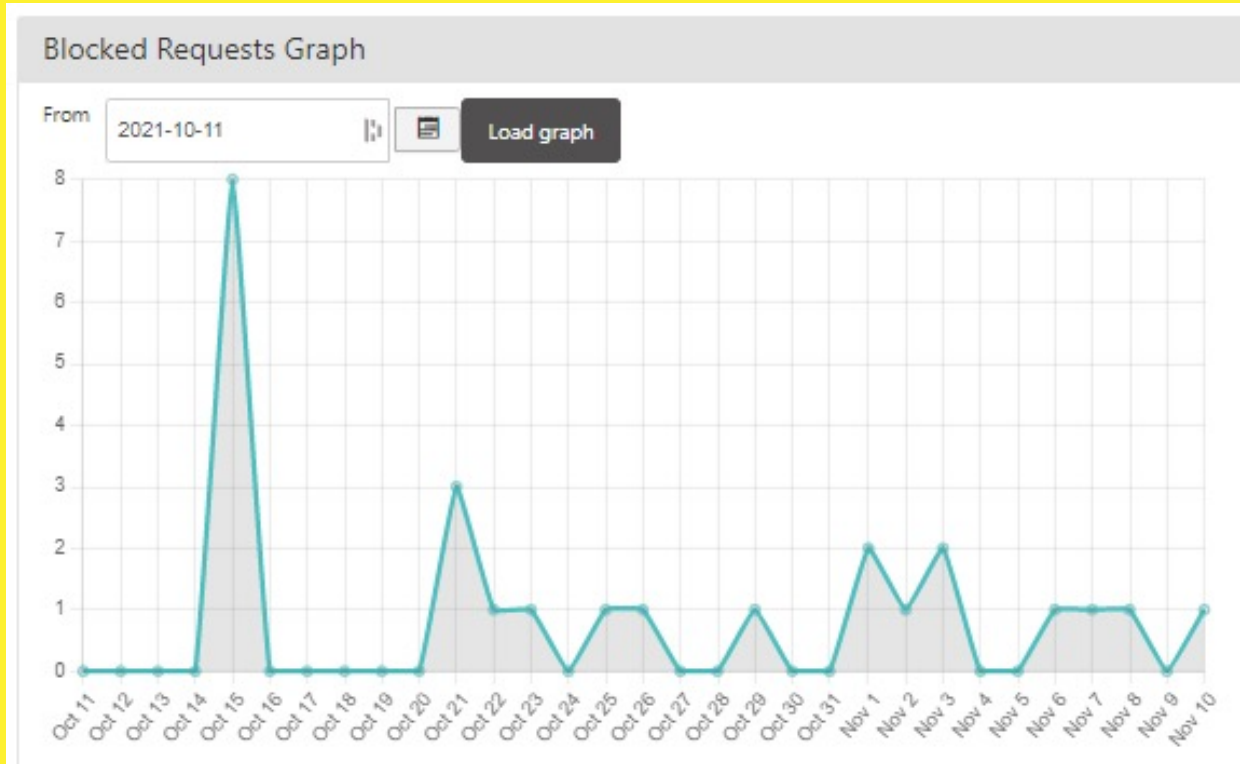


The screenshot shows the Joomla! Administrator Exclusive Allow IP List configuration page. At the top, there are navigation buttons: 'Verwijderen', 'Bewerk', 'Nieuw', and 'Terug'. Below these are input fields for 'IP address range' and 'Description', along with dropdown menus for '20', 'Oplopend', and 'IP address range'. The main content area is a table with columns for 'IP address range' and 'Description'. The table contains six rows, each representing a webhosting provider, with checkboxes in the first column and IP address ranges in the second column.

<input type="checkbox"/>	IP address range ^	Description
<input type="checkbox"/>	[Redacted]	Webhosting 1
<input type="checkbox"/>	[Redacted]	Webhosting 2
<input type="checkbox"/>	[Redacted]	Webhosting 3
<input type="checkbox"/>	[Redacted]	Webhosting 4
<input type="checkbox"/>	[Redacted]	Webhosting 5
<input type="checkbox"/>	[Redacted]	Webhosting 6

Joomla beveiliging



















Logging & Statistics 1



Joomla beveiliging

Logging & Statistics 2

Statistics	
Last year	524
This year	186
Last month	20
This month	9
Last 7 days	6
Yesterday	1
Today	1

<input type="checkbox"/> Date	IP address	Reason	Target URL
<input type="checkbox"/> 2021-11-10 16:44:05 CET	  37.0.11.64	404 Shield	https://internetgroep.amnesty.nl/wp-admin/css/
<input type="checkbox"/> 2021-11-08 05:02:15 CET	  35.225.94.95	404 Shield	https://internetgroep.amnesty.nl/wp-login.php
<input type="checkbox"/> 2021-11-07 16:50:15 CET	  94.212.194.253	Login failure	https://internetgroep.amnesty.nl/service2/webhostin
<input type="checkbox"/> 2021-11-06 04:32:30 CET	  165.227.115.229	404 Shield	https://internetgroep.amnesty.nl/wp-login.php
<input type="checkbox"/> 2021-11-03 18:13:58 CET	  156.146.49.139	404 Shield	https://internetgroep.amnesty.nl/wp-login.php
<input type="checkbox"/> 2021-11-03 02:00:57 CET	  67.205.3.168	404 Shield	https://internetgroep.amnesty.nl/wp-login.php
<input type="checkbox"/> 2021-11-02 18:02:32 CET	  159.89.1.19	404 Shield	https://internetgroep.amnesty.nl/wp-login.php
<input type="checkbox"/> 2021-11-01 12:16:13 CET	  154.21.208.153	404 Shield	https://internetgroep.amnesty.nl/wp-login.php
<input type="checkbox"/> 2021-11-01 03:59:08 CET	  164.68.110.108	404 Shield	https://internetgroep.amnesty.nl/wp-login.php

Joomla beveiliging

Admin Tools E-mail

<input type="checkbox"/> Reason	Subject	Gepubliceerd	Language
<input type="checkbox"/> all	Admin Tools melding voor [SITENAME]	✓	Alle
<input type="checkbox"/> user-reactivate	Admin Tools melding_Gebruiker geblokkeerd voor [SITENAME]	✓	Alle
<input type="checkbox"/> adminloginfail	Admin Tools melding_Mislukte administrator login [USER] voor [SITENAME]	✓	Alle
<input type="checkbox"/> adminloginsuccess	Admin Tools melding voor [SITENAME] Administrator [USER] login	✗	Alle
<input type="checkbox"/> ipautoban	Admin Tools melding_IP [IP] geblokkeerd voor [SITENAME]	✓	Alle
<input type="checkbox"/> configmonitor	Admin Tools melding_Configuratie wijziging [AREA] voor [SITENAME]	✓	Alle
<input type="checkbox"/> criticalfiles	Admin Tools melding_Bestandswijzigingen voor [SITENAME]	✓	Alle
<input type="checkbox"/> superuserslist	Super Users were added to [SITENAME]	✓	Alle
<input type="checkbox"/> rescueurl	Admin Tools melding_Rescue URL verzoek voor [SITENAME], gebruiker [USER]	✗	Alle
<input type="checkbox"/> criticalfiles_global	Admin Tools melding_Bestandswijzigingen voor [SITENAME]	✓	Alle

Do not send email notifications for these reasons

SQLi Shield ✕

tmpl= in URL ✕

template= in URL ✕

MUA Shield ✕

SessionShield ✕

DFIShield ✕

404 Shield ✕

[Microsoft Word - Akeeba Admin Tools - List of blocking reasons.docx](#)

Joomla beveiliging

Admin Tools E-mail

Maintain. Protect. Optimise.

Admin Tools  for Joomla!

VAN	ONDERWERP	VERZONDEN
Alphen a/d Rijn	Admin Tools melding IP 217.160.192.178 geblokkeerd voor Alphen aan den Rijn	zo 7-11-2021 22:22
intrnetgroep.amnesty.nl	Admin Tools melding voor Internetgroep Amnesty NL	zo 7-11-2021 16:50
Culemborg Amnesty	Admin Tools melding Configuratie wijziging Algemene instellingen voor Culemborg...	zo 7-11-2021 12:27
Culemborg Amnesty	Admin Tools melding Bestandswijzigingen voor Culemborg-Amnesty	zo 7-11-2021 12:27
alkmaar	Admin Tools melding voor alkmaar	zo 7-11-2021 11:40
alkmaar	Admin Tools melding voor alkmaar	zo 7-11-2021 11:27
alkmaar	Admin Tools melding voor alkmaar	zo 7-11-2021 11:26
Amnesty Heerhugowaard	Admin Tools melding IP 54.147.178.243 geblokkeerd voor Heerhugowaard	za 6-11-2021 21:57
leiden.amnesty.nl	Admin Tools melding IP 138.201.203.132 geblokkeerd voor Leiden	za 6-11-2021 20:55
leiden.amnesty.nl	Admin Tools melding IP 138.201.203.132 geblokkeerd voor Leiden	za 6-11-2021 20:36
leiden.amnesty.nl	Admin Tools melding IP 138.201.203.132 geblokkeerd voor Leiden	za 6-11-2021 20:05
leiden.amnesty.nl	Admin Tools melding IP 138.201.203.132 geblokkeerd voor Leiden	za 6-11-2021 19:49
test46	Joomla! Update available for test46 – https://test46.amnesty.nl/administrator/	za 6-11-2021 12:59
Amnesty Heerhugowaard	Admin Tools melding IP 54.147.178.243 geblokkeerd voor Heerhugowaard	vr 5-11-2021 21:04
Amnesty Wierden	Admin Tools melding voor Amnesty Wierden	vr 5-11-2021 17:43
test46	Joomla! Update available for test46 – https://test46.amnesty.nl/administrator/	vr 5-11-2021 15:55
beheer.amnesty.nl	Admin Tools troubleshooting information	vr 5-11-2021 15:55
beheer.amnesty.nl	User Beheer@Amnesty20 (Amnesty Beheer <webhosting	vr 5-11-2021 15:54
test38.amnesty.nl	User Beheer@Amnesty20 (Amnesty Beheer <webhosting	vr 5-11-2021 15:50
beheer.amnesty.nl	Critical file modified on test42	vr 5-11-2021 14:47
beheer.amnesty.nl	Joomla! update beschikbaar voor test42-https://test42.amnesty.nl/administrator/	vr 5-11-2021 14:45
beheer.amnesty.nl	User Beheer@Amnesty20 (Amnesty Beheer <webhosting	vr 5-11-2021 14:45
test35.amnesty.nl	Admin Tools melding Bestandswijzigingen voor test35	vr 5-11-2021 14:41
Amnesty Wierden	Admin Tools melding IP 80.127.235.158 geblokkeerd voor Amnesty Wierden	vr 5-11-2021 12:16

Email this address after an automatic IP ban

Email this address on blocked request

Email this address on failed administrator login

webhosting@amnesty.nl, meikezwaan@gmail.com

Aan NLD - INB - Webhosting

Hallo webmaster,

Er is een Admin Tools beveiligingsmelding voor de website **alkmaar** met de volgende details:
IP adres: **82.169.215.68** (IP Lookup: [IP Lookup](#))
Reden: **Admin Query String**

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 alkmaar en omdat webhosting het ontvangen van deze mails zo voor je ingesteld heeft.

Joomla beveiliging



Vragen?