Joomla!™ security

Willem-Jan ten Wolde

Wie is Willem-Jan?

- Willem-Jan ten Wolde
- 54 jaar, getrouwd met Paula, twee zoons van 17 en 15
- Werkt 4x9 bij NN-group (Nationale-Nederlanden)
  Engineer bij Head Office Functions
  Veel tools/sites in beheer
- WJid: beheer - ontwikkelen - vraagbaak


Security Joomla
Soort gegevens
BIV/CIA rating
Wie heeft er toegang
Pen Test
OWASP Top 10
Simple zelftest
Certificaat
Logfiles check
Provider
SIEM
back-ups
DDOS aanval
live
certificering
Hoe gaat dit bij NN
OSA traject
ISRA
BIA
SRL
TVA
A-OSG
Pen test
Autorisatie matrix
Tools
Akeeba Admintools
Akeeeba Backup
Watchful
CMS configuration file and server details
Core filesystem integrity
File & Folder permissions
Malware scanner
Formulieren
Wel of geen SSL
DTAP/OTAP
Test

Doelgroep en inhoud

- Wie heeft er toegang?
  - Intranet
  - Internet, iedereen of beperkte toegang
- Wat staat er op de site?

Soort gegevens website

- BIV/CIA rating
  Beschikbaarheid en continuïteit
  Integriteit en betrouwbaarheid
  Vertrouwelijkheid en exclusiviteit
  in het Engels:
  Confidentiality
  Integrity
  Availability

- Waarde 1=laag t/m 4=hoog

- Let op: BIV 223 = CIA 322

CIA waarde

	Confidentiality	**I**ntegrity	**A**vailability
1	Public	Nominal	Recoverable
2	Internal	Standard	Cold standby
3	Confidential	Individual	Hot standby
4	Secret	Double intervention	Failsafe

BIV/CIA QUIZ (C = 1,2,3 of 4)

Naam

2

BIV/CIA QUIZ (C = 1,2,3 of 4)

Foto

3

BIV/CIA QUIZ (C = 1,2,3 of 4)

Geslacht

3

BIV/CIA QUIZ (C = 1,2,3 of 4)

BSN

4

BIV/CIA QUIZ (C = 1,2,3 of 4)

Bloedonderzoek

4

Bijzondere persoonsgegevens

- BSN nummer
- Politieke opvattingen of voorkeur
- Religieuze opvattingen of voorkeur
- Gegevens over seksuele geaardheid
- Genetische of biometrische gegevens met het oog op unieke identificatie
- Strafrechterlijke gegevens of veroordelingen, veiligheidsmaatregelingen
- Etnische afkomst
- Lidmaatschap vakbond
- Salarisgegevens
- Paspoortkopie met foto
- Gegevens over gezondheid

Maatregelen

- Afhankelijk van de BIV/CIA neem je maatregelen en je stelt eisen aan de hosting van de site.
- Hoe doet  dit?

Hoe gaat dit bij NN?

- Nieuwe Joomla site PensioenPaniek.nl
- Voordat deze gebruikt mag worden, eerst onderzoek:
  - Wat is de inhoud?
  - Hoe is het gemaakt?
  - Leverancier en Hosting?
- Start van het **ISRA** proces

Het ISRA proces

- **I**nformation **S**ecurity **R**isk **A**ssessment
- Bij NN is dit een Excel sheet met verschillende tabbladen:
- Algemene gegevens
- Beschrijving van de applicatie in Jip en Janneke taal
- BIA (**B**usiness **I**mpact **A**ssessment)

Business Impact Assessment

- Wordt ingevuld door Applicatie eigenaar
- Vragen zoals:
  - Staat er persoonlijke data in, zoals naam, mail adres, geslacht, foto
  - Staan er zaken in die bij diefstal de reputatie kunnen schaden?
  - Kan er fraude mee worden gepleegd,
  - Hoe beschikbaar moet het zijn? 7 x 24
  - Hoe lang mag het niet beschikbaar zijn?
- Daarna goedkeuring van Operational Risk Management en Legal
- Het resultaat is de CIA rating of BIV

Daarna de SRL

- **S**ecurity **R**equirements **L**ist
- Een lijst van 130! vragen afhankelijk van de CIA rating
- Voorbeeldvragen:
  - De applicatie moet toegangscontrole systeem hebben.
  - Wachtwoord: minimum lengte van 10 tekens.
  - Gebruiker moet laatste login datum/tijd zien.
  - Patches moet via een OTAP omgeving worden geïnstalleerd.

Threats & Vulnerabilities Assessment

- Alleen als CIA >= 3
- Infrastructuur: zoals stroomuitval, hardware storing
- Software: onbetrouwbare leveranciers
- Natuur: Aardbeving, storm, overstroming
- Medewerkers: Betrouwbaarheid, aanslagen
- Cyber attack: DDOS attack
- Slechte Processen: responsietijd servicedesk

Een SaaS applicatie?

- Voor de leverancier: ORA en OSA traject
  Outsourcing **R**isk **A**ssessment / **O**utsourcing **S**ecurity **A**rchitecture
  Hier vult de leverancier in wat voor maatregelen hij heeft getroffen voor risico's, bedreigingen. **D**isaster **R**ecovery **P**lan
  Input voor SRL

- Certificeringen
  ISO 9001, ISO 27001
  ISAE 3402, SOC 1 of SOC 2

- Het certificaat, de Statement of Applicability en het auditrapport willen wij inzien. **Input voor SRL**

OSG

- **O**perational **S**ecurity **G**uidelines is een vragenlijst waarin je beschrijft welke maatregelen zijn getroffen die nodig zijn om de risico's te beperken met betrekking tot de CIA rating. **Input is OSA, SRL interviews met leveranciers**

- SIEM = **S**ecurity **I**nformation & **E**vent **M**onitoring

- TSCM = **T**echnical **S**tate **C**ompliance **M**onitoring

- Autorisatie matrix (technisch en functioneel) en ISV

- PEN test (OWASP) / Code review (tools: Fortify code review)

- SAP = **S**ecurity **A**ction **P**lan

Penetration test 1

- **Ethical Hackers** proberen de site te hacken
- Tools om SSL certificaat en headers etc te checken
- Tools om code te checken Fortify code review
- En handmatig hacken (OWASP)

Penetration test 2

Cross Site Scripting (XSS)
SQL Injection
Command Injection
Cross Site Request Forgery (CSRF)
Authentication/Authorization Bypass
Session Management testing, e.g. token analysis, session expiration, and logout effectiveness
Account Management testing, e.g. password strength, password reset, account lockout, etc.
Directory Traversal
Response Splitting
Stack/Heap Overflows
Format String Attacks
Cookie Analysis
Server Side Includes Injection

Remote File Inclusion
LDAP Injection
XPATH Injection
Internationalization attacks
Denial of Service testing at the application layer only
AJAX Endpoint Analysis
Web Services Endpoint Analysis
HTTP Method Analysis
SSL Certificate and Cipher Strength Analysis
Forced Browsing
Exploiting password recovery mechanisms
Accessing unpublished or test APIs
Cache poisoning
Etc…..

Kortom…….

- Veel werk….. Doorloop 8 tot 12 weken
- Veel afstemming
- Veel akkoorden krijgen dat je verder kan.

De site PensioenPaniek.nl

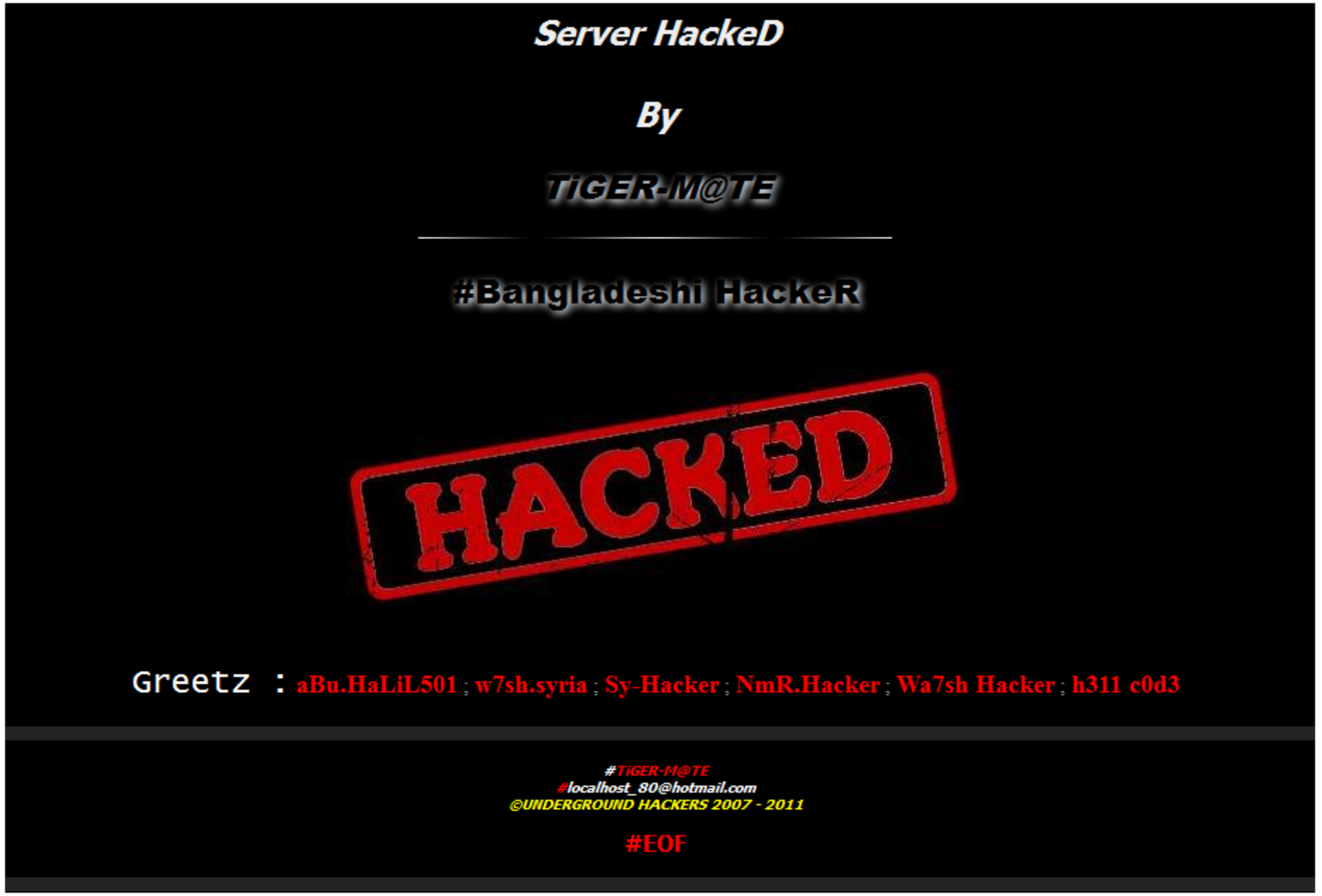
CIA rating: 433

dus https: …..

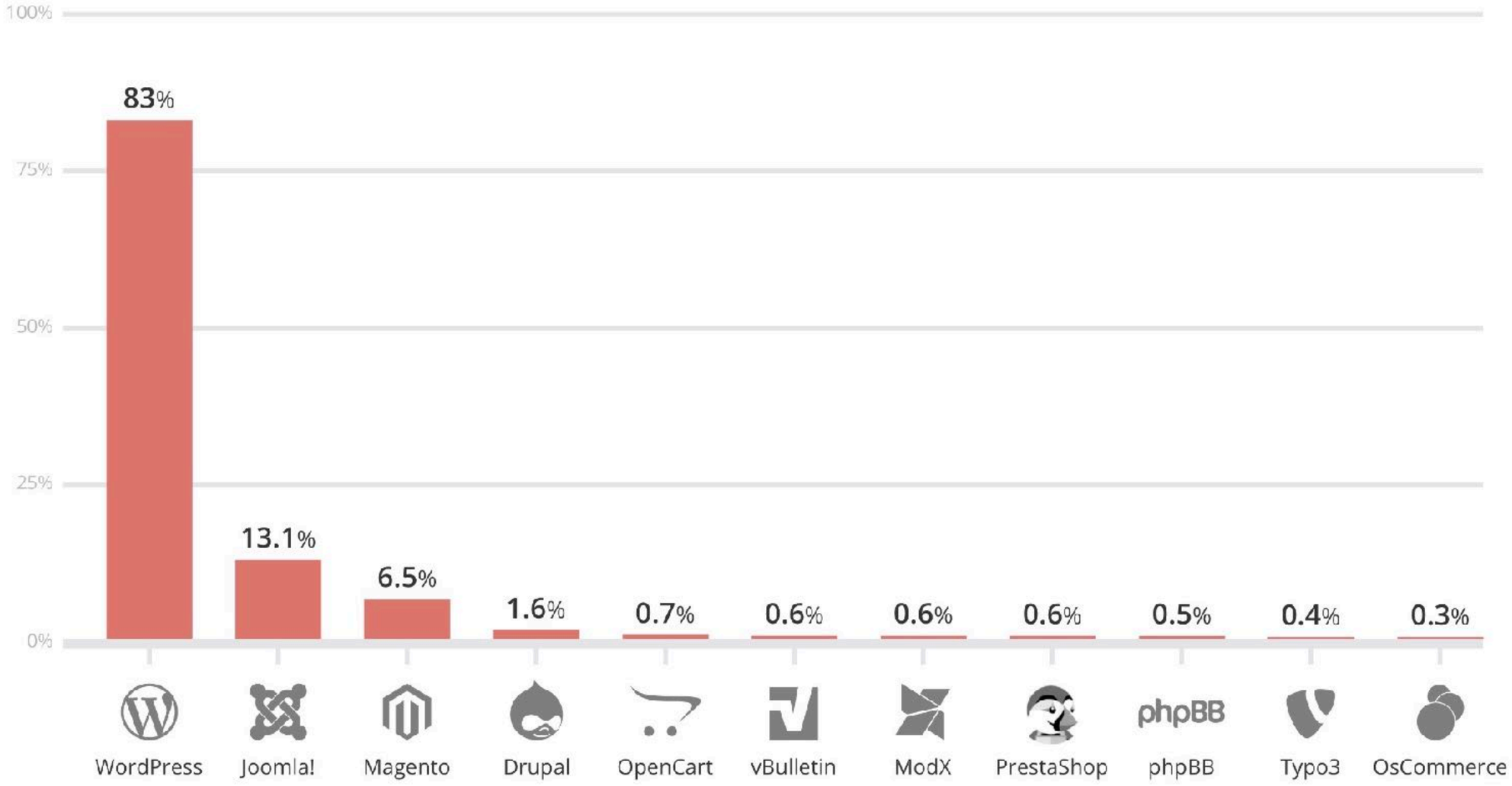
Hosting en SSL

- een SSL Certificaat zijn er drie opties;
  - Domein verificatie (DV)
  - Organisatie verificatie (OV)
  - Uitgebreide verificatie (EV)
- Algemene verordening gegevensbescherming (AVG) Daarin staat onder meer dat jij, als beheerder van de persoonsgegevens van je klanten, verantwoordelijk bent voor het beveiligen van deze gegevens.

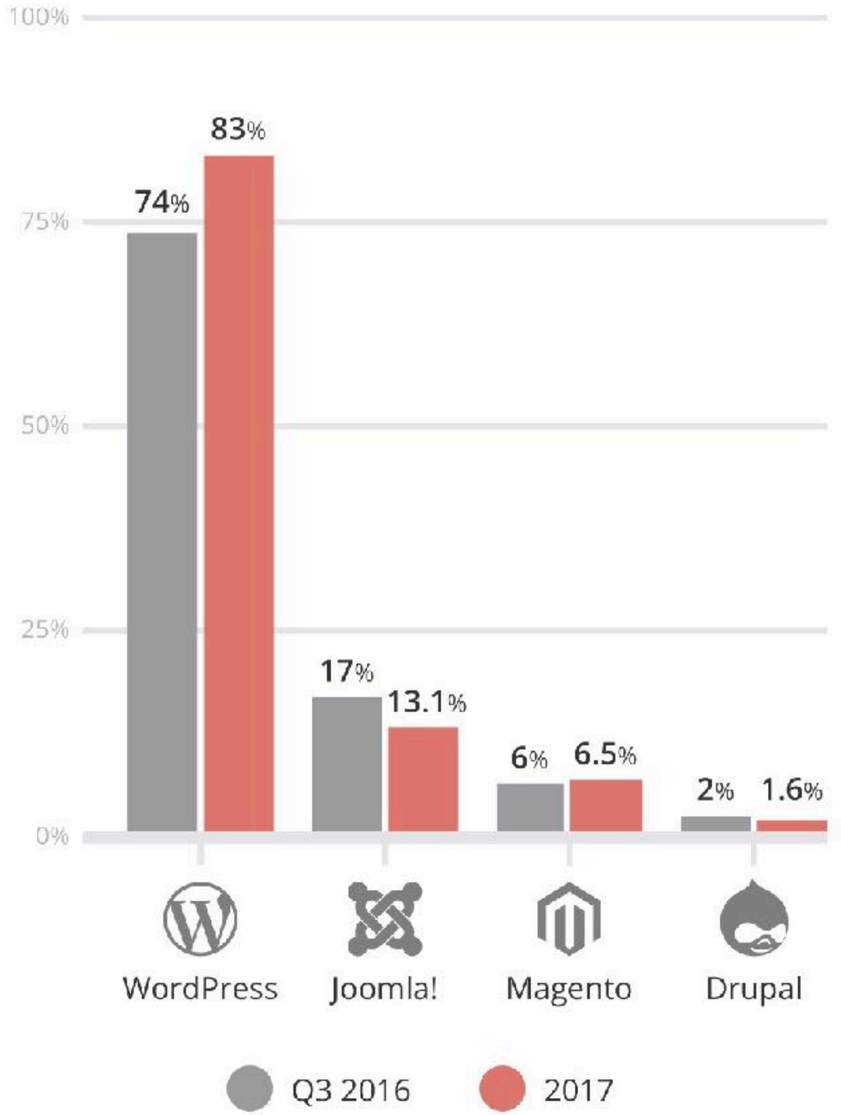
- Een site onder https kan nog steeds gehackt worden!



Infected Websites Platform Distribution - 2017



CMS Infection Comparison - 2017



Maatregelen nemen

- De maatregelen kunnen afhankelijk zijn van CIA rating
- Je moet maatregelen nemen op site en bij hosting
- Kunnen ze worden genomen bij de hosting partij?
- Dus *geen* cheaphosting.nl voor 1 euro / maand
  Inclusief domeinnaam

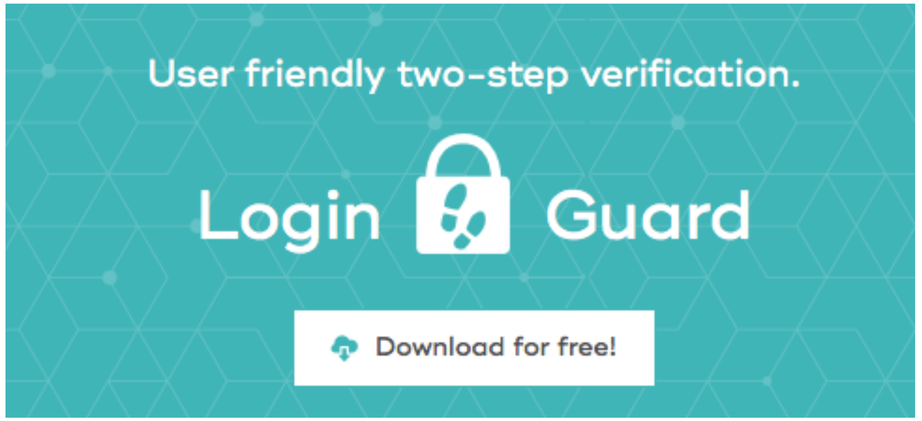
Hoe beginnen?

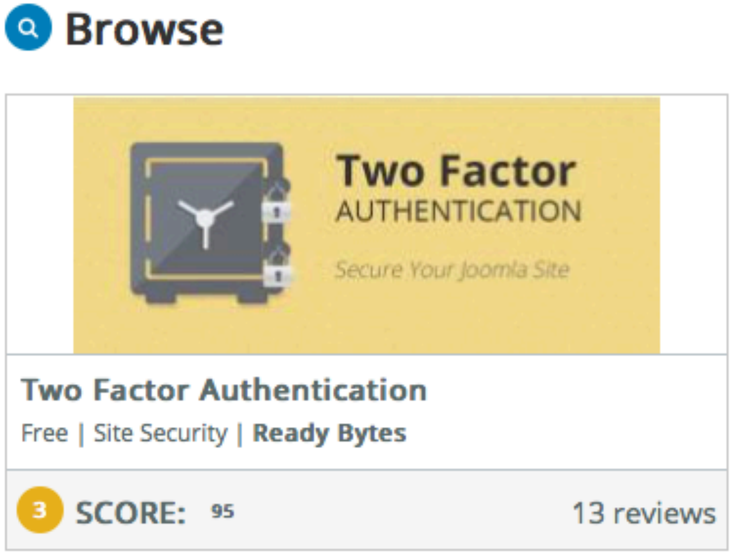
- Begin met verschillende omgevingen:
  - Ontwikkel
  - **Test**
  - Acceptatie
  - **Productie**
- **test.pensioenpaniek.nl (sub domein)**
- testpensioenpaniek.nl (apart domein)
- pensionpaniek.nl/test (sub directory)
- Of met WAMP/XAMP lokaal op de pc.

Installatie van Joomla (nieuwste)

- Creëer een nieuwe accounts voor een user (jezelf) en administrator. Gebruik ***niet*** de naam admin
- Gebruik een sterk wachtwoord dus: J8F4B6(e@s%nRQ
  Gebruik een password manager. (1Password)
- Installeer Akeeba Admintools en Backup (koop beide)
- Gebruik MFA van Joomla (multi factor authenticatie)
  Zit standaard (sinds 3.2) in Joomla of gebruik ….

multi factor authenticatie





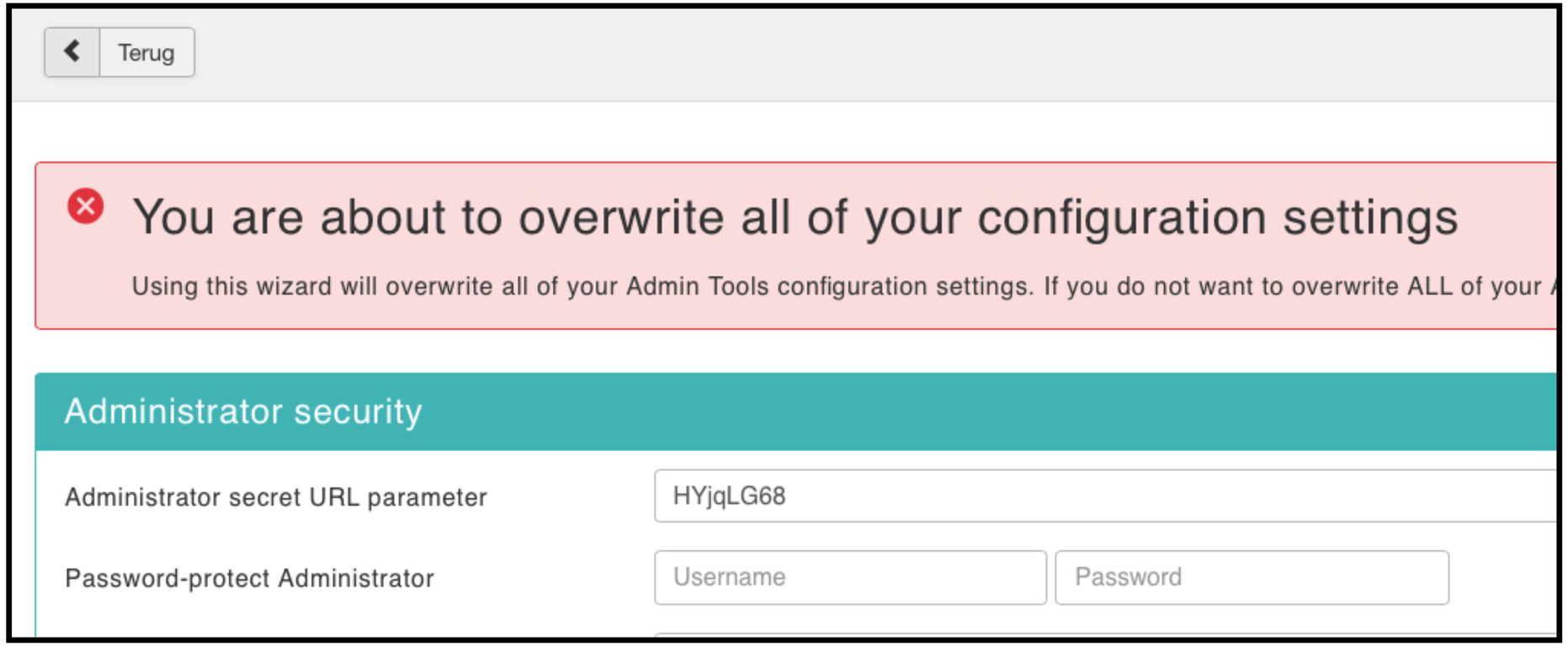
Beheer en monitor

- Installeer updates van Joomla en Extenties (Watchful)
- Gebruik alleen noodzakelijke extenties en templates
- Monitor de site (Admintools en Watchful)
- Controleer de permissies (Admintools en Watchful)
  PHP files – 644
  Config Files – 644
  Other folders – 755

Beheer en monitor

- Extra beveiliging in URL Administrator (Admintools)
- https://www.example.com/administrator/index.php?HYjqLG68
- Handig of niet…
- Hoe gaat dit?


Quick Setup
You should only run the
run it again it will overri
other buttons above.
Quick Setup
Wizard


Terug
You are about to overwrite all of your configuration settings
Using this wizard will overwrite all of your Admin Tools configuration settings. If you do not want to overwrite ALL of your
Administrator security
Administrator secret URL parameter
HYjqLG68
Password-protect Administrator
Username
Password


UPDATE

Beheer en monitor

- Gebruik SEF (search engine friendly)
- Gebruik .htaccess (Apache) (lokale kopie maken)
- Maak regelmatig backup’s en TEST (Akeeba back-up, Watchful)
- Scheidt de back-up van de site (Dropbox, Amazon S3, OneDrive, etc)
- Gebruik een WAF Web Application Firewall (Admintools)
- Klopt de configuratie nog (Admintools, Watchful)
- Test met een tool zoals https://observatory.mozilla.org

Home FAQ Statistics About

Observatory by Mozilla has helped over 125,000 websites by teaching developers, system administrators, and security professionals how configure their sites safely and securely.

Scan your site

wjid.nl

Scan Me

- [ ] Don't include my site in the public results
- [x] Force a rescan instead of returning cached results
- [ ] Don't scan with third-party scanners

OBSERVATORY
by mozilla

Home FAQ Statistics About

HTTP Observatory | TLS Observatory | SSH Observatory (Beta) | Third-party Tests

Scan Summary

B

Host:	wjid.nl
Scan ID #:	6335679
Start Time:	January 10, 2018 9:51 PM
Duration:	6 seconds
Score:	75/100
Tests Passed:	10/11

Recommended Change

Initiate Rescan

You're doing a wonderful job so far!

Did you know that a strong Content Security Policy (CSP) policy can help protect your website against malicious cross-site scripting attacks?

- Mozilla Web Security Guidelines (Content Security Policy)
- An Introduction to Content Security Policy
- Google CSP Evaluator
- Mozilla Laboratory CSP Generator

Once you've successfully completed your change, click Initiate Rescan for the next piece of advice.

Test Scores

Test	Pass	Score	Explanation
Content Security Policy	✖	-25	Content Security Policy (CSP) header not implemented
Cookies	✔	0	All cookies use the `Secure` flag and all session cookies use the `HttpOnly` flag
Cross-origin Resource Sharing	✔	0	Public content is visible via cross-origin resource sharing (CORS) `Access-Control-Allow-Origin` header
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)
HTTP Strict Transport Security	✔	0	HTTP Strict Transport Security (HSTS) header set to a minimum of six months (15768000)
Redirection	✔	0	Initial redirection is to https on same host, final destination is https
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)
Subresource Integrity	–	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin
X-Content-Type-Options	✔	0	X-Content-Type-Options header set to `"nosniff"`
X-Frame-Options	✔	0	X-Frame-Options (XFO) header set to `SAMEORIGIN` or `DENY`
X-XSS-Protection	✔	0	X-XSS-Protection header set to `"1; mode=block"`

HTTP Headers & Content Security

securityheaders.io

B

Host:	wjid.nl
Complete Results:	https://securityheaders.io/?followRedirects=on&hide=on&q=wjid.nl

Security Report Summary

B

Site:	https://wjid.nl/
IP Address:	83.137.198.9
Report Time:	10 Jan 2018 20:54:01 UTC
Report Short URL:	Feature disabled.
Headers:	✔ X-Frame-Options ✔ Strict-Transport-Security ✔ X-Content-Type-Options ✔ X-XSS-Protection ✖ Content-Security-Policy ✖ Referrer-Policy

Grade History

Date	Score	Grade
December 16, 2017 3:41 PM	75/100	B
December 16, 2017 3:30 PM	105/100	A+
December 15, 2017 10:41 PM	75/100	B
December 15, 2017 10:35 PM	20/100	F
December 15, 2017 10:18 PM	105/100	A+
November 5, 2017 3:33 PM	75/100	B
November 5, 2017 3:00 PM	40/100	D+
November 2, 2017 10:20 AM	20/100	F

Certificaat

by mozilla

HTTP Observatory | TLS Observatory | SSH Observatory (Beta) | **Third-party Tests**

ssllabs.com

Host:	wjid.nl
Complete Results:	https://www.ssllabs.com/ssltest/analyze?d=wjid.nl

QUALYS SSL LABS

Configuration

Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

For TLS 1.3 tests, we currently support draft version 18.

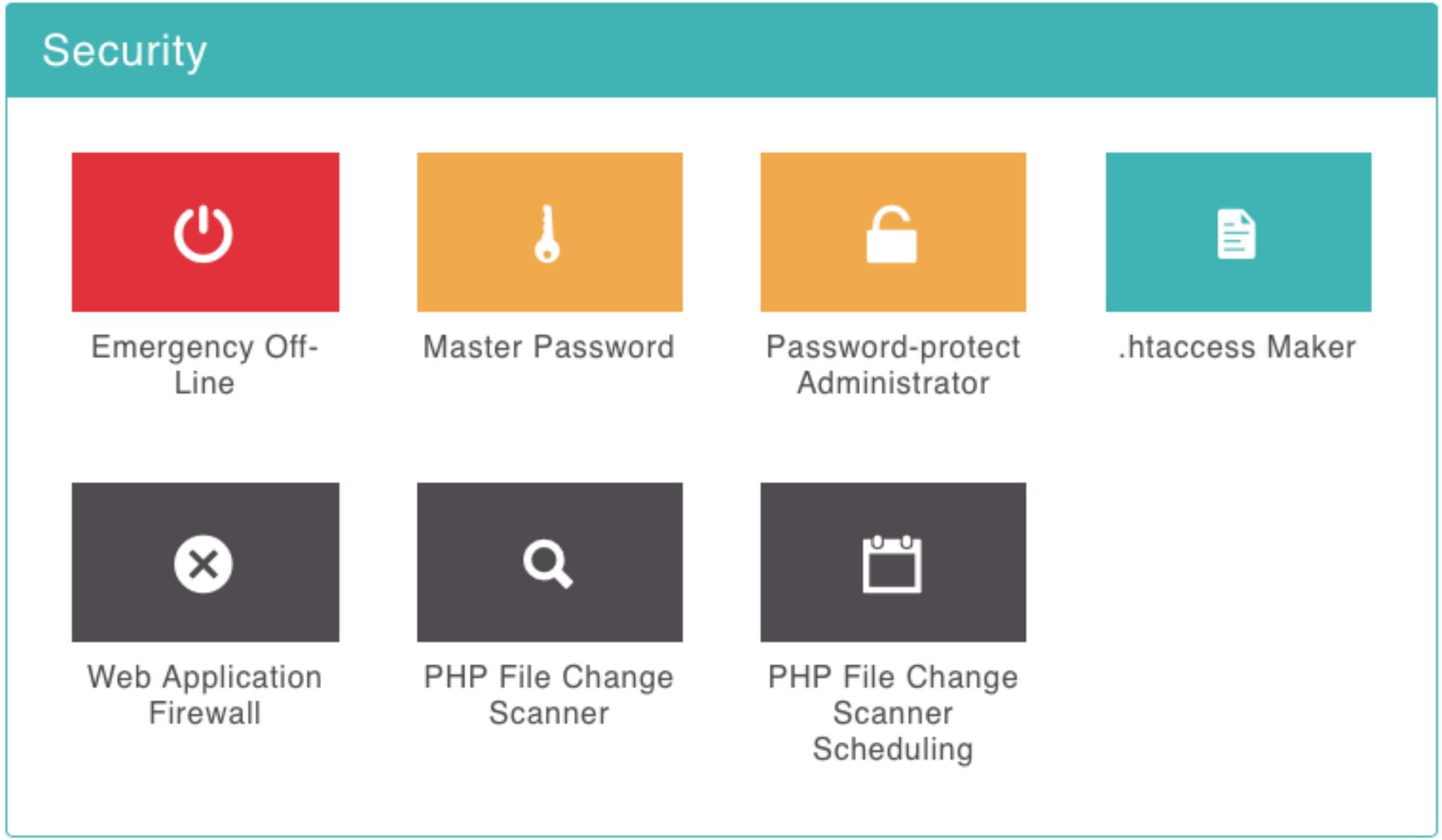
Formulieren

- Pas op met formulieren!
  Ga niet zelf een maken……

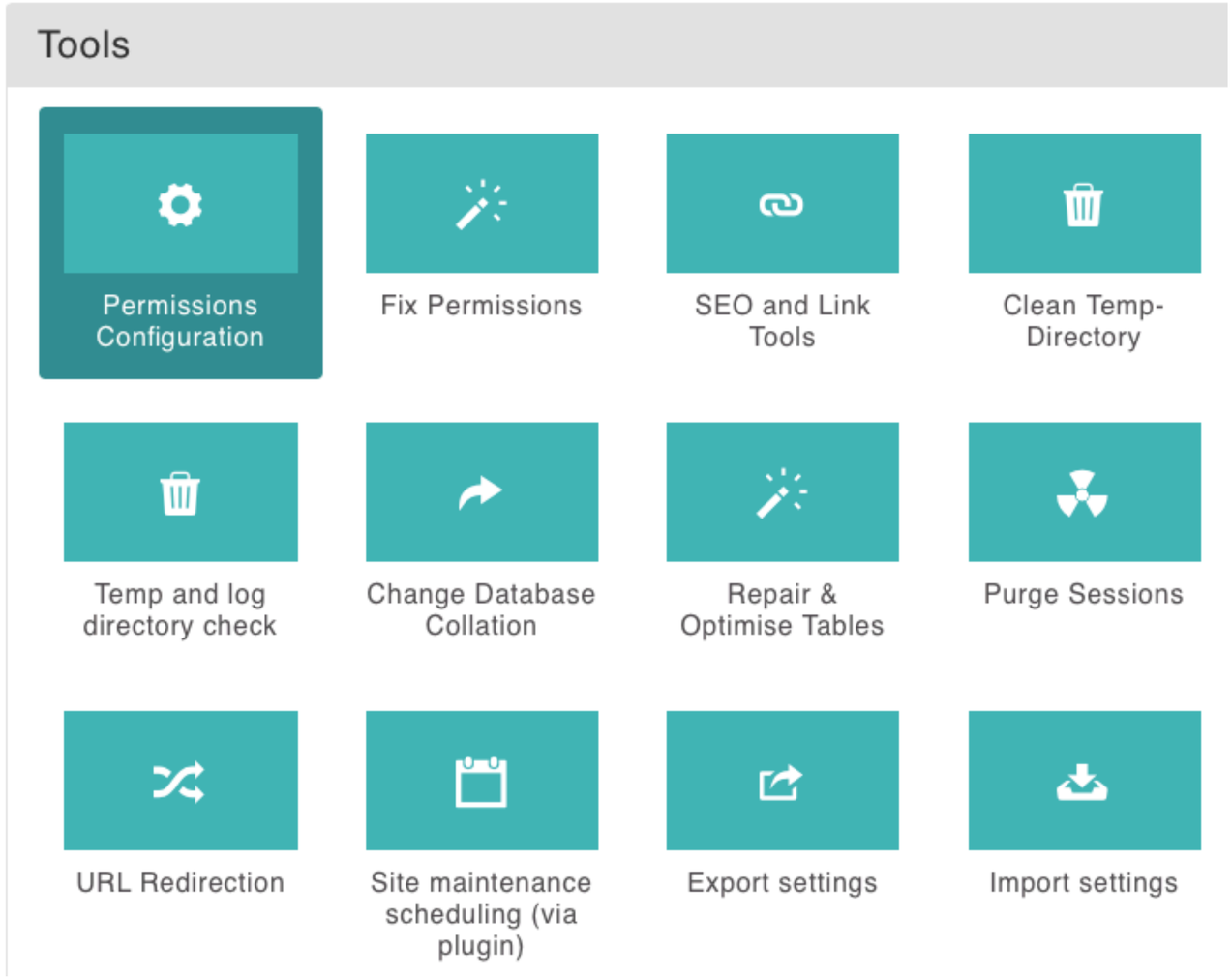
- Gebruik een uit de Joomla extentions directory:

- Gebruik eventueel een formulier buiten de site zoals Google forms

Admin tools van Akeeba



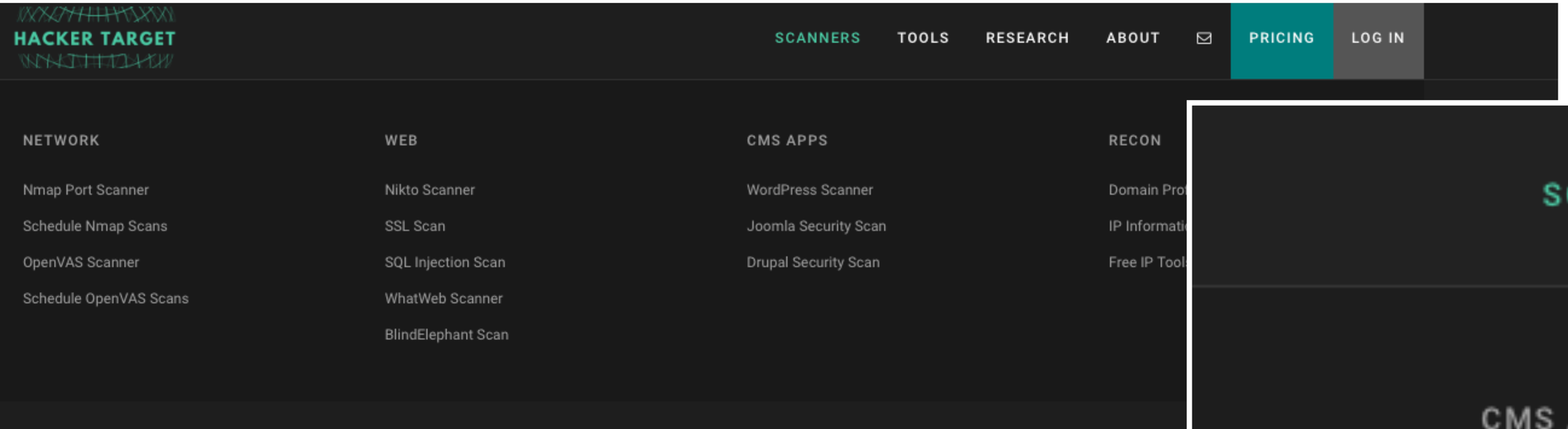
Admin tools van Akeeba

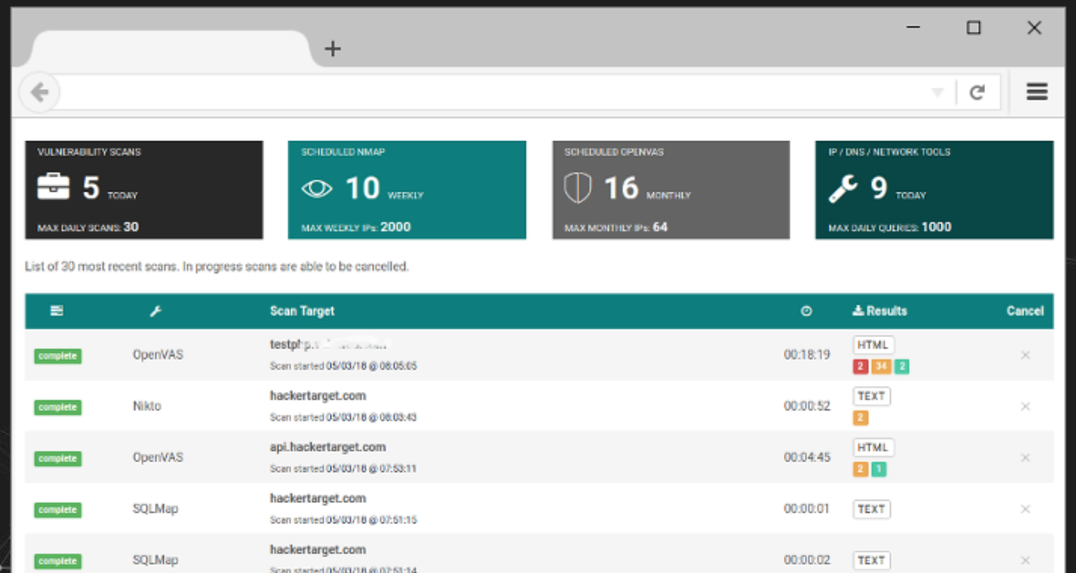


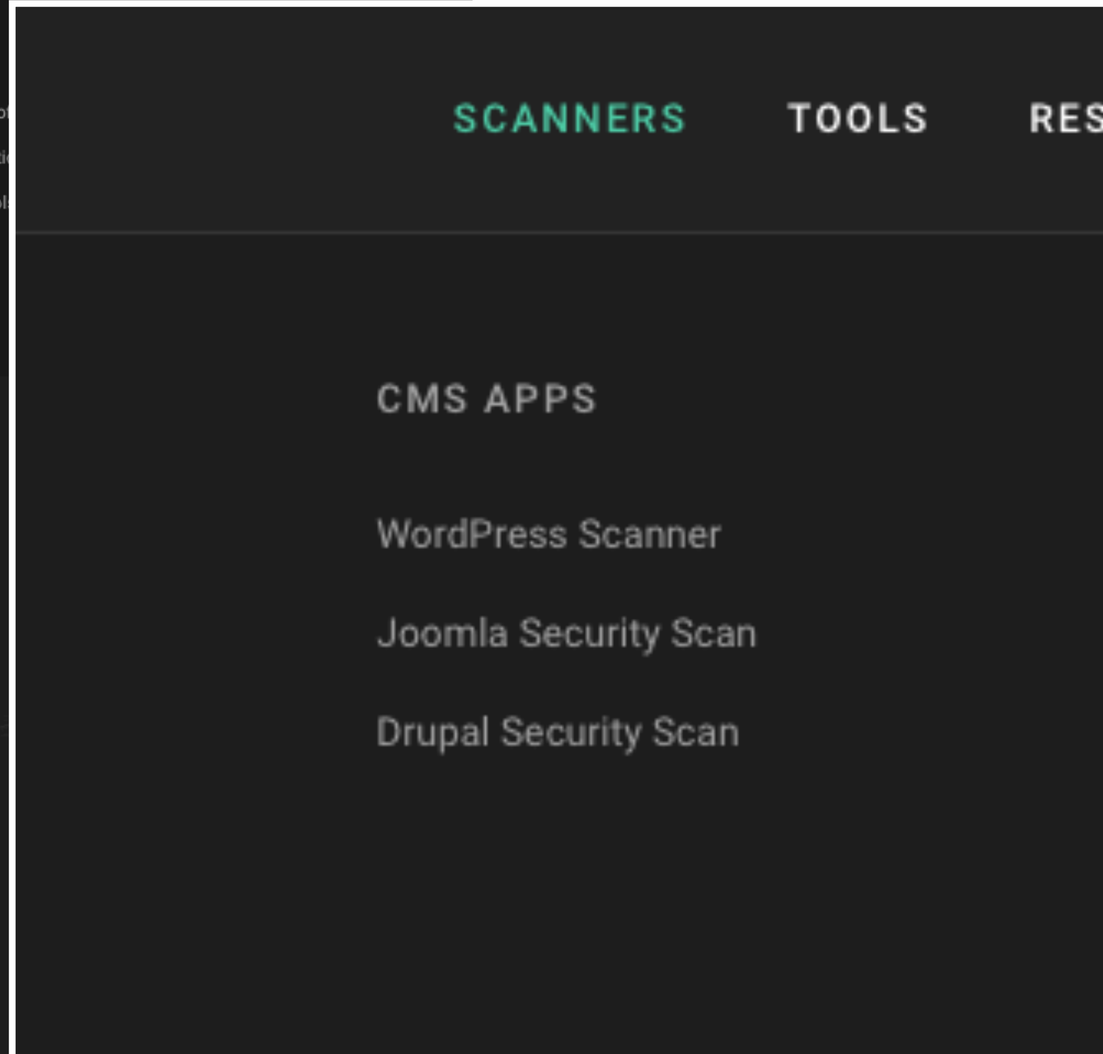
Watchful


Dashboard
Download Center
Knowledge Base
Support
wj@wjid.nl
More
1 - 20 of 20
Updates
CMS
Site name
Tags
Go to website
Core
PHP
Last backup
Anthonisgilde
Front - Back
3.8.3
7.0.7
11/12/2017
Anthonisgilde TEST
16/05/2017
Eenhart.nl
7.0.25
16/05/2016
fam. ten Wolde
BCK
01/01/2018
Harpe Davids
10/01/2018
Historisch Museum Schiedam
Jemeverproefkring
09/01/2018
Jenevergilde
Jeneverie 't Spul
Jeneverie 't Spul - Nieuw
Jeneverie 't Spul - OUD
marjannahelpt.nl
Stichting Hobby-Expo Dongen
5.6.33
Tablet Services Rijnmond
4.9.1
Teksterlei
08/01/2018
Terra Mirabili
Terra Mitabili TEST
Wjid
OTP
05/01/2018
Wjid
Wjid test
1 - 20 of 20

Hackertarget.com





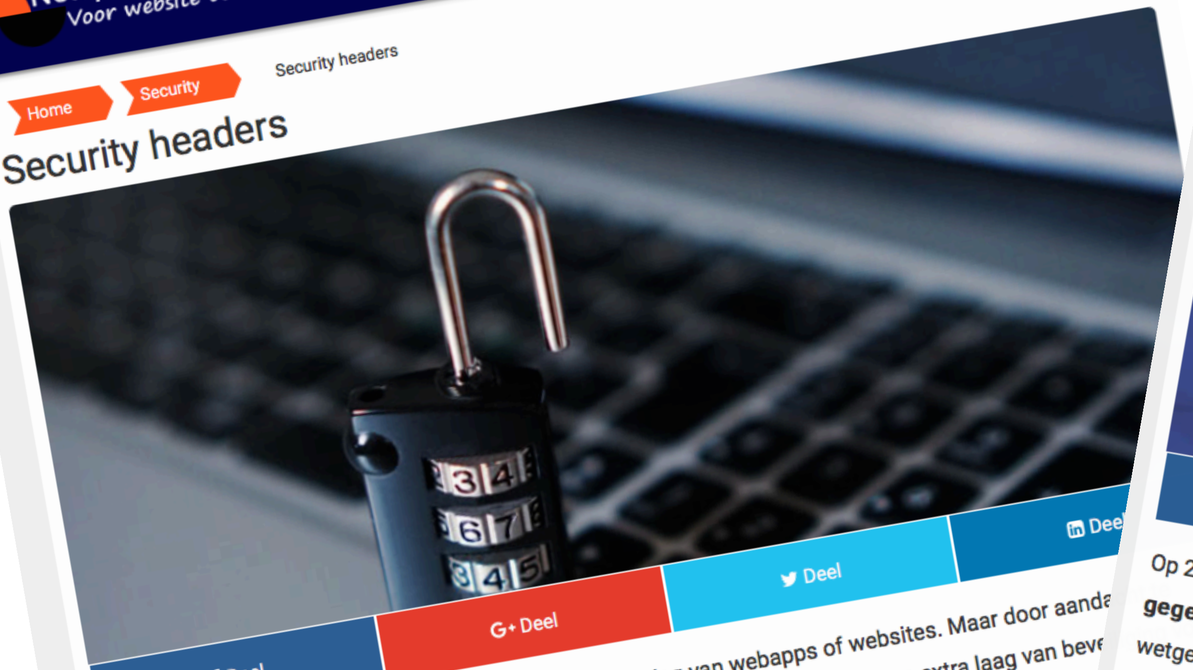


Netspecialist.NL
Voor website bouwers !

Home Blog Ebooks

Home Security Security headers

Security headers



Deel G+ Deel Deel Deel

Security headers worden vaak vergeten bij de beveiliging van webapps of websites. Maar door aanda
besteden aan de security headers en door deze goed in te stellen, zorg je voor een extra laag van beve
website.

Wat zijn security headers?

Wanneer iemand met zijn of haar browser je website opent, dan zal de webserver waarop jouw
reageren door de inhoud van je website af te leveren vergezeld met een aantal HTTP headers
vertellen de browser onder andere welke meta data er is, of er gebruik wordt gemaakt van c
GZIP), informatie over de server, cache contol etc.

Netspecialist.NL
Voor website bouwers !

Home Blog Ebooks

Home Netspecialist Algemeen AVG Wetgeving (GDPR)

AVG Wetgeving (GDPR)

Deel G+ Deel Deel Deel

Op 25 mei 2018 zal de nieuwe Europese privacy wetgeving van kracht worden, de **Algemene verordening gegevensbescherming (AVG)**. De internationale benaming is GDPR (General Data Protection Regulation). Deze wetgeving zal behoorlijk wat consequenties hebben voor website eigenaren en (internet)ondernemers.

De AVG is al in mei 2016 in werking getreden, maar er is toen een periode van 2 jaar ingesteld tot het daadwerkelijk van toepassing worden van deze wetgeving. Vanaf 25 mei wordt de wetgeving dus daadwerkelijk van kracht in de gehele EU en zal er op gehandhaafd worden.

Handige links

- Testen website
  https://observatory.mozilla.org
  https://hackertarget.com/scan-membership/

- 10 Handige Security tips
  https://geekflare.com/joomla-security/

- Netspecialist
  https://netspecialist.nl/security/516-security-headers
  https://netspecialist.nl/netspecialist-algemeen/522-avg-wetgeving-gdpr

- PEN test info
  https://www.owasp.org/

- https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/in_10_stappen_voorbereid_op_de_avg.pdf

- http://map.norsecorp.com/#/explore

Vragen ?

Dank voor de aandacht!

[Applaus] …… [buigen]