Scan Rapport

Algemene Informatie
Klant: wp-example
Bedrijf: console
Email: webapplicatietest@gmail.com

Scan Informatie
URL: http://cms.local
Server: Apache
Scan type: Full Scan
Start tijd: 2017-09-30 00:42:01
Eind tijd: 2017-09-30 00:42:40
Scan tijd: 39 secondes

Scan Resultaten

Dreigingsniveau (Kleur code)	Niveau	Omschrijving
	4	Er zijn één of meer zeer zorgwekkende kwetsbaarheden op de website gevonden. De kans op exploitatie door hackers is zeer hoog. Hackers kunnen toegang krijgen tot het backend systeem en daarop de databases muteren.

Totale dreigementen gevonden
Hoog: 18
gemiddeld: 168
Laag: 168

Categorie dreigementen	Dreigingsniveau	Aantal	Omschrijving
XSS	hoog	18	Cross-site scripting is een type kwetsbaarheid dat vooral gevonden wordt in webapplicaties. XSS maakt het mogelijk voor hackers om client-side scripting talen te injecteren op webpagina's.
Security Headers Gemiddeld	gemiddeld	168	De http security headers van dit niveau voorzien een website met een extra laag van beveiliging om aanvallen af te weren en kwetsbaarheidlekken te dichten, kwetsbaarheden met betrekking tot XSS. Het missen van security headers maakt uw website kwetsbaar voor aanvallen.
Security Headers Laag	laag	168	De http security headers van dit niveau hebben vooral betrekking op misconfiguraties aan de server kant. Dit kan leiden tot het lekken van informatie.

Advies: XSS

Cross-site scripting is een veel voorkomende client-side kwetsbaarheid waarbij
de aanvaller client-site code injecteert op webpagina.
Er zijn twee basis regels waar een website aan moet
voldoen om dit probleem te verkomen:

Regels

- Voer nooit onvertrouwde data in, behalve op toegestaande locaties
- Voordat de data wordt ingevoerd moet de HTML Escaped worden

Advies: Security Headers

Secuirty Headers zorgen voor een veilig verkeer tussen de server en de client.
Wanneer hier niet gebruik van gemaakt wordt kan het zijn dat hackers het als een kans
zien om uw website te exploiteren. Om dit te voorkomen kunt u gebruik maken van de volgende headers:

- X-Content-Type-Options
- X-Frame-Options
- X-XSS-Protection
- Content-Secuirty-Policy
- Public-Key-Pins (SLL)
- HttpOnly

Detials van gevonden kwetsbaarheden

ID: 19299

Module: Public-Key-Pins

Risico: low

Target URL: http://cms.local/?C=S;O=D

Parameter: n/a

Aanval: n/a

Error: Public Key is missing (Only for SLL)

WASC ID: 14

Methode: GET

Datum: 2017-09-30 00:42:31