Je website (nog beter) beveiligen met HTTP-Security Headers

Wat is HTTP?

- Het HTTP (Hypertext Transfer Protocol) protocol is een vrij eenvoudig, tekst gebaseerd, protocol. Dit HTTP protocol regelt de communicatie tussen de browser en de webserver.
- Er wordt gestart met een HTTP Request. Deze bevat de details van wat de browser wil en wat de browser van de webserver zal accepteren. Ook bevat dit request een header waarin het type, de versie en de mogelijkheden van de browser die de aanvraag doet wordt meegegeven.
- Als antwoord ontvangt de browser een HTTP Response. Een HTTP-response bestaat uit een resultaatcode, headervelden en een body (de boodschap).

Wat zijn headers?

Aanvraagheaders (538 B)

- Accept: text/html,application/xhtml+xm...plication/xml;q=0.9,*/*;q=0.8
- Accept-Encoding: gzip, deflate, br
- Accept-Language: nl,en-US;q=0.7,en;q=0.3
- Cache-Control: max-age=0
- Connection: keep-alive
- Cookie: 3a47b7d0932fd4658690796016dd35...546955304.; _pk_ses.15.db20=*
- DNT: 1
- Host: beernink.eu
- Upgrade-Insecure-Requests: 1
- User-Agent: Mozilla/5.0 (Windows NT 10.0; ...) Gecko/20100101 Firefox/64.0

Antwoordheaders (530 B)

- Cache-Control: no-store, no-cache, must-reval...te, post-check=0, pre-check=0
- Connection: Keep-Alive
- Content-Encoding: gzip
- Content-Type: text/html; charset=utf-8
- Date: Tue, 08 Jan 2019 13:51:01 GMT
- Expires: Wed, 17 Aug 2005 00:00:00 GMT
- Keep-Alive: timeout=15, max=100
- Last-Modified: Tue, 08 Jan 2019 13:51:02 GMT
- Pragma: no-cache
- Server: Apache
- Set-Cookie: rl_modals=3; expires=Wed, 08-J...GMT; Max-Age=31536000; path=/
- Transfer-Encoding: chunked
- X-Powered-By: PHP/7.2.13
- X-Powered-By: PleskLin

Wat zijn (security) headers?

- Wanneer een browser een pagina opvraagt van een webserver, reageert de server met HTTP Response Headers en de inhoud (HTML). Sommige van deze Response Headers bevatten metagegevens, zoals de inhoudcodering, cachebesturing, statusfoutcodes, enzovoort.
- HTTP Security headers controleren verkeer op je website en kunnen bepaald verkeer van de website weren. Hoewel niet geheel waterdicht, is het goed instellen van de security headers een goed **EXTRA** middel om het hackers moeilijker te maken.

Wat kun je met (security) headers?

- Onnodige info verbergen zoals de scripttaal en versie
- Aangeven dat een pagina niet in een (i)frame geladen mag worden (belangrijk voor webshops)
- Afslaan van aanvallen met een verkeerd MIME type (bijv. PHP bestand met extensie .jpg uploaden
- Verminderen van de kans op een Man in the Middle aanval
- Verminderen van de kans op Cross-Site Request Forgery (CSRF) / Cross-Site Scripting (XSS)

Content Security Policy

- Content Security Policy (CSP) is een nieuwe standaard die webdevelopers in staat stelt om beperkingen te definiëren op het gedrag van de website of -applicatie. Bijvoorbeeld: vanaf welke externe locaties worden scripts, stylesheets of images ingeladen? Mag de browser de site in een frame van een andere site inladen?
- Webservers kunnen in antwoord op elk verzoek een speciale header meesturen met de naam Content-Security-Policy.

Content Security Policy

- Content Security Policy (CSP) is een nieuwe standaard die webdevelopers in staat stelt om beperkingen te definiëren op het gedrag van de website of -applicatie. Bijvoorbeeld: vanaf welke externe locaties worden scripts, stylesheets of images ingeladen? Mag de browser de site in een frame van een andere site inladen?
- https://hackdefense.nl/blog/csp-het-hoe-en-waarom-van-een-content-security-policy/
- https://content-security-policy.com/

Content Security Policy

Attributen die je kunt gebruiken

- **default-src**: hierop wordt teruggevallen wanneer er door de andere attributen niets gedefinieerd is. De waarde van dit attribuut is vaak 'self' om aan te geven dat resources alleen vanaf de eigen site worden ingeladen.
- **script-src**: beperkt de locaties van waar een extern script mag worden ingeladen. Gebruikt de site geen *client side* scripts dan kan dat met de waarde 'none' worden aangegeven.
- **img-src**: beperkt de locaties van waar afbeeldingen mogen worden ingeladen.
- **media-src**: beperkt de locaties van waar media, bijvoorbeeld video's, mogen worden ingeladen.
- **object-src**: beperkt de locaties van waar plugins mogen worden ingeladen.
- **frame-ancestors**: dit attribuut beperkt de locaties die de webpagina mogen inladen middels frame-, iframe-, object-, embed- of applet-elementen. frame-ancestors moet op den duur de HTTP response header X-Frame-Options gaan vervangen.
- **form-action**: beperkt de URL's die gebruikt mogen worden als actie van <form>-elementen. Met andere woorden, hiermee wordt gelimiteerd waar de browser ingevulde formulierdata heen kan sturen. *Let op dat dit attribuut niet wordt gedekt met default-src, dus dat dit apart moet worden gespecificeerd als uw site of applicatie form-elementen bevat.*

Feature-Policy

- De header HTTP Feature-Policy biedt een mechanisme om het gebruik van browserfuncties in zijn eigen frame toe te staan en te weigeren en in iframes die zijn ingesloten.
- Je hoeft alleen maar de beperkingen te bepalen bijvoorbeeld:

  Feature-Policy: camera 'self'; usermedia *; sync-xhr 'self' https://example.com
- https://www.smashingmagazine.com/2018/12/feature-policy/

X-Frame-Options

- Met deze header kun je aangeven of de website in een (i)frame geladen mag worden. Hiermee kun je clickjacking voorkomen (Je website wordt in een iframe geplaatst op een malafide site en functies van knoppen worden dan bijv. aangepast).
- De meestgebruikte optie is SAMEORIGIN (zelfde host, zelfde protocol, zelfde poort), deze optie verteld de browser om alleen inhoud van dezelfde webserver in een iframe te laden.
- Beste optie is DENY tenzij er een specifieke behoefte is voor framing.
- Kan ook met Admin Tools worden ingesteld (Protect against clickjacking) maar wordt dan op SAMEORIGIN gezet

X-XSS-Protection

- Deze header geldt voor Internet Explorer, Chrome en Safari en voorkomt XSS.
- Hiermee wordt XSS filtering aangezet in de browser.
- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

X-XSS-Protection

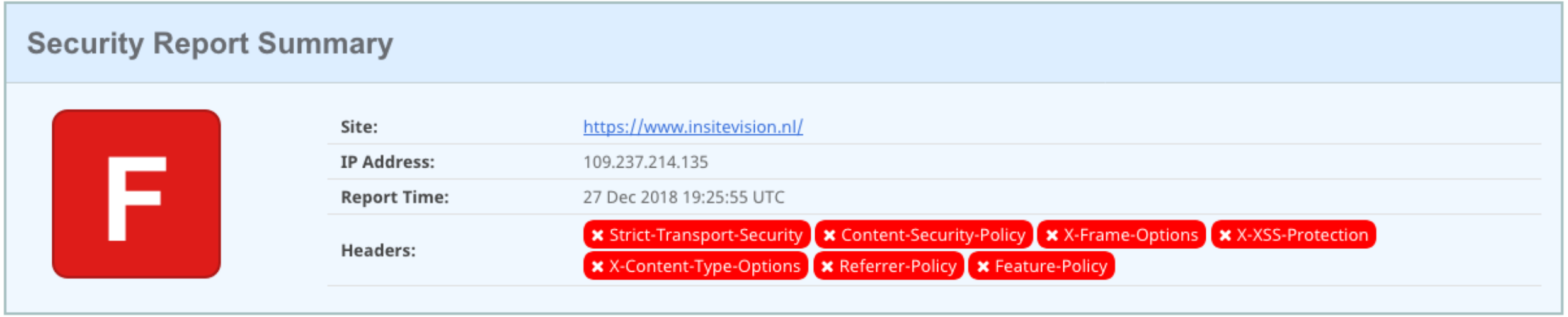
- **X-XSS-Protection:**
  Cross site scripting (XSS) is een veel gebruikte aanvalsvorm om websites mee te hacken. Met XSS injecteert een aanvaller kwaadaardige code in een website die bezoekers van deze website kan besmetten. Denk hierbij aan een formulier waarvan de input niet goed wordt gevalideerd en er bijv. PHP-, SQL- of javascriptcode ingevuld wordt die dan wordt uitgevoerd.

X-Content-Type-Options

- Deze header helpt voorkomen dat browsers het MIME-type proberen te raden wat gevolgen kan hebben voor de veiligheid.
- Een gebruiker kan een afbeelding uploaden met de .jpg-bestandsextensie, maar de inhoud ervan is eigenlijk HTML. Bij het bezoeken van die afbeelding kan de browser de HTML-pagina "uitvoeren", die mogelijk kwaadaardig JavaScript bevat.
- https://helmetjs.github.io/docs/dont-sniff-mimetype/

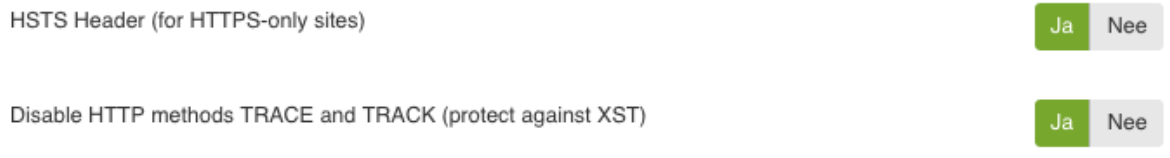
Hoe controleer je de security headers?

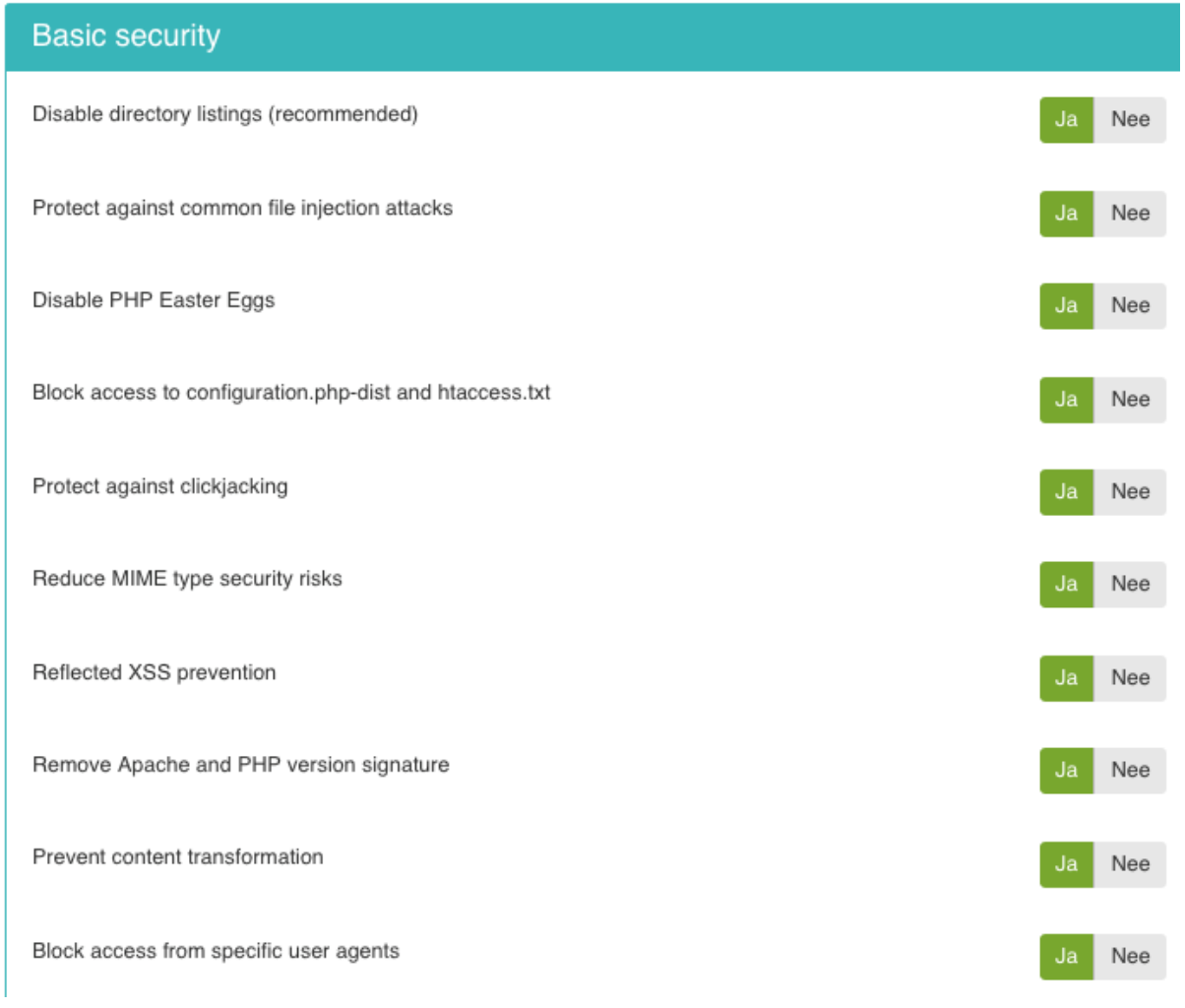
- Op https://securityheaders.com
- Standaard Joomla installatie scoort slecht



Hoe scoor je beter?

- Installeer Admin Tools
- Configureer Basic security
- HSTS Header (for HTTPS-only sites)
- Referer Policy header





Hoe scoor je beter?

Security Report Summary

Site:	https://beernink.eu/
IP Address:	109.237.214.134
Report Time:	05 Jan 2019 14:21:59 UTC
Headers:	✔ X-Frame-Options ✔ Strict-Transport-Security ✔ Referrer-Policy ✔ X-Content-Type-Options ✔ X-XSS-Protection ✖ Content-Security-Policy ✖ Feature-Policy

De headers toevoegen aan je .htaccess

```
## Extra Security Headers
#
<ifModule mod_headers.c>
Header set X-XSS-Protection "1; mode=block"
Header always append X-Frame-Options DENY
Header set X-Content-Type-Options nosniff
Header set Content-Security-Policy "connect-src 'self';"
Header always set Feature-Policy "geolocation none;midi none;notifications
none;push none;sync-xhr none;microphone none;camera none;magnetometer
none;gyroscope none;speaker self;vibrate none;fullscreen self;payment none;"
Header always unset X-Powered-By
ServerSignature Off
</ifModule>
#
## Einde extra security headers
```

Eindresultaat

Security Report Summary

A+

Site:	https://www.insitevision.nl/
IP Address:	109.237.214.135
Report Time:	27 Dec 2018 20:29:42 UTC
Headers:	✔ X-Frame-Options ✔ Feature-Policy ✔ Strict-Transport-Security ✔ Referrer-Policy ✔ X-XSS-Protection ✔ X-Content-Type-Options ✔ Content-Security-Policy