WordPress & CSP

Polisa Sigurnosti Sadržaja
za **WordPress**

Milan Petrović
18.5.2019.
WordCamp Niš

dev4press
www.dev4press.com

Predavanje, Google Docs:

https://d4p.me/wordcampnis

HTTP Zaglavlja

Svaki HTTP odgovor počinje zaglavljima

Zaglavlja opisuju stranu, sliku ili drugi tip resursa koje server šalje korisniku i sadrži tip sadržaja, veličinu, datum nastanka i modifikacije i druge informacije

Zaglavlja mogu da sadrže i veliki broj drugih informacija, uključujući i informacije vezane za sigurnost kao što je Polisa Sigurnosti Sadržaja (CSP).

C S P

Content Security Policy
Polisa Sigurnosti Sadržaja

Set direktiva koje određuju koji sadržaj browser može da učita i izvrši

Set direktiva koje određuju koji sadržaj browser može da učita i izvrši

Pomaže u smanivanju rizika od **XSS** (Cross Site Scripting) vrsta napada

Set direktiva koje određuju koji sadržaj browser može da učita i izvrši

Pomaže u smanivanju rizika od **XSS** (Cross Site Scripting) vrsta napada

CSP specifikacija uključuje i slanje izveštaja o prekršajima polise

Set direktiva koje određuju koji sadržaj browser može da učita i izvrši

Pomaže u smanivanju rizika od **XSS** (Cross Site Scripting) vrsta napada

CSP specifikacija uključuje i slanje izveštaja o prekršajima polise

Može da se kombinuje sa drugim sigurnosnim HTTP zaglavljima

Set direktiva koje određuju koji sadržaj browser može da učita i izvrši

Pomaže u smanivanju rizika od **XSS** (Cross Site Scripting) vrsta napada

CSP specifikacija uključuje i slanje izveštaja o prekršajima polise

Može da se kombinuje sa drugim sigurnosnim HTTP zaglavljima

Svi moderni browseri podržavaju CSP, uključujući i mobilne browsere

Set direktiva koje određuju koji sadržaj browser može da učita i izvrši

Pomaže u smanivanju rizika od **XSS** (Cross Site Scripting) vrsta napada

CSP specifikacija uključuje i slanje izveštaja o prekršajima polise

Može da se kombinuje sa drugim sigurnosnim HTTP zaglavljima

Svi moderni browseri podržavaju CSP, uključujući i mobilne browsere

Trenutno su upotrebi dve specifikacije: Level 1 i Level 2

Set direktiva koje određuju koji sadržaj browser može da učita i izvrši

Pomaže u smanivanju rizika od **XSS** (Cross Site Scripting) vrsta napada

CSP specifikacija uključuje i slanje izveštaja o prekršajima polise

Može da se kombinuje sa drugim sigurnosnim HTTP zaglavljima

Svi moderni browseri podržavaju CSP, uključujući i mobilne browsere

Trenutno su upotrebi dve specifikacije: Level 1 i Level 2

Može da radi u report modu i samo da obaveštava o prekršajima

Spisak CSP Direktiva

Šta sve može da se limitira korišćenjem CSP-a?

- Standardna: **default-src**
- JavaScript: **script-src**
- CSS: **style-src**
- Slike: **img-src**
- Fontovi: **font-src**
- Audio/Video: **media-src**
- Forme: **form-src**
- Frejmovi: **frame-src**, **child-src** i **frame-ancestors**
- Konekcije: **connect-src**
- Objekti: **object-src**
- MIME: **plugin-types**

Dodatne CSP direktive

Šta još CSP može da uradi?

- **upgrade-insecure-requests**
  svi zahtevi koji idu na http:// se automatski menjaju na https://
- **block-all-mixed-content**
  zabrani sve http:// zahteve ako se strana izvršava na https://
- **report-uri**
  adresa na koju browser šalje izveštaje o prekršajima

Dozvoljene vrednosti direktiva

Svaka direktiva može imati jednu ili više vrednosti.

- *
- ‘none’
- ‘self’
- data:
- blob:
- filesystem:
- https:
- subdomain.example.com
- *.example.com
- https://www.example.com
- ‘nonce-{value}’
- ‘sha256-{value}’
- ‘unsafe-inline’
- ‘unsafe-eval’

Primer direktive **script-src**

script-src

```
'self'
'unsafe-inline'
cdn.ampproject.org
www.google-analytics.com
ajax.googleapis.com
fsd3dasddfgdsr3.cloudfront.net
```

Primer restriktivne početne polise

```
Content-Security-Policy
    "default-src 'none';
     script-src 'self' 'unsafe-inline';
     connect-src 'self';
     img-src 'self';
     style-src 'self';
     font-src 'self';
     Report-uri https://mywebsite.com/report-csp;"
```

WordPress

Zaštitite sajt CSP-om
i drugim sigurnosnim zaglavljima

Preporuka je da sajt koristi SSL sertifikat i **https://** adresu.

Preporuka je da sajt koristi SSL sertifikat i **https://** adresu.

CSP treba da se doda na server strani (konfiguracija za Apache, ngnix...) da bi se primenjivao na sve strane ali i fajlove koje server šalje korisniku.

Preporuka je da sajt koristi SSL sertifikat i **https://** adresu.

CSP treba da se doda na server strani (konfiguracija za Apache, ngnix...) da bi se primenjivao na sve strane ali i fajlove koje server šalje korisniku.

Za Apache, može u **.htaccess** fajl na nivou WordPress instalacije.

Preporuka je da sajt koristi SSL sertifikat i **https://** adresu.

CSP treba da se doda na server strani (konfiguracija za Apache, ngnix...) da bi se primenjivao na sve strane ali i fajlove koje server šalje korisniku.

Za Apache, može u **.htaccess** fajl na nivou WordPress instalacije.

Mnogo CSS stilova i JavaScript koda se dodaje direktno u HTML,

Zbog toga se mora koristiti **‘unsafe-inline’** vrednost za neke direktive.

Preporuka je da sajt koristi SSL sertifikat i **https://** adresu.

CSP treba da se doda na server strani (konfiguracija za Apache, ngnix...) da bi se primenjivao na sve strane ali i fajlove koje server šalje korisniku.

Za Apache, može u **.htaccess** fajl na nivou WordPress instalacije.

Mnogo CSS stilova i JavaScript koda se dodaje direktno u HTML,

Zbog toga se mora koristiti **‘unsafe-inline’** vrednost za neke direktive.

WordPress-u treba centralizovani metod za dodavanje koda u HTML kako bi mogli da se generišu signurni blokovi koji sadrže ‘nonce’ ili ‘sha256’ bazirane vrednosti za identifikaciju dodatog koda.

Da li je CSP neophodan?

Ukratko: **Da**

CSP pomaže u zaštiti sajta i korisnika sajta.

CSP pomaže u zaštiti sajta i korisnika sajta.

Korisnikov kompjuter može biti kompromitovan.

CSP pomaže u zaštiti sajta i korisnika sajta.

Korisnikov kompjuter može biti kompromitovan.

Ekstenzije za Chrome i Firefox mogu biti kompromitovane.

CSP pomaže u zaštiti sajta i korisnika sajta.

Korisnikov kompjuter može biti kompromitovan.

Ekstenzije za Chrome i Firefox mogu biti kompromitovane.

Sajt može biti kompromitovan.

CSP pomaže u zaštiti sajta i korisnika sajta.

Korisnikov kompjuter može biti kompromitovan.

Ekstenzije za Chrome i Firefox mogu biti kompromitovane.

Sajt može biti kompromitovan.

Hosting kompanije mogu biti zlonamerne modifikovanjem vašeg sadržaja.

CSP pomaže u zaštiti sajta i korisnika sajta.

Korisnikov kompjuter može biti kompromitovan.

Ekstenzije za Chrome i Firefox mogu biti kompromitovane.

Sajt može biti kompromitovan.

Hosting kompanije mogu biti zlonamerne modifikovanjem vašeg sadržaja.

Ekstenzije mogu biti zlonamerne i mogu da ubacuju svoj sadržaj.

Kako dodati **CSP** u **WordPress** sajt?

Manuelno

Pomoću plugin-a

Kako dodati **CSP** u **WordPress** sajt?

Manuelno

Više za iskusne server administratore
Zahteva direktan pristup podešavanjima servera
Češće modifikovanje konfiguracije servera

Pomoću plugin-a

Kako dodati **CSP** u **WordPress** sajt?

Manuelno

Više za iskusne server administratore
Zahteva direktan pristup podešavanjima servera
Češće modifikovanje konfiguracije servera

Pomoću plugin-a

Jednostvanije za većinu WP korisnika
Preglednija lista pravila u samom WP
Lakše i brže testiranje

Kako dodati **CSP** u **WordPress** sajt?

Manuelno

Više za iskusne server administratore
Zahteva direktan pristup podešavanjima servera
Češće modifikovanje konfiguracije servera

Pomoću plugin-a

Jednostvanije za većinu WP korisnika
Preglednija lista pravila u samom WP
Lakše i brže testiranje

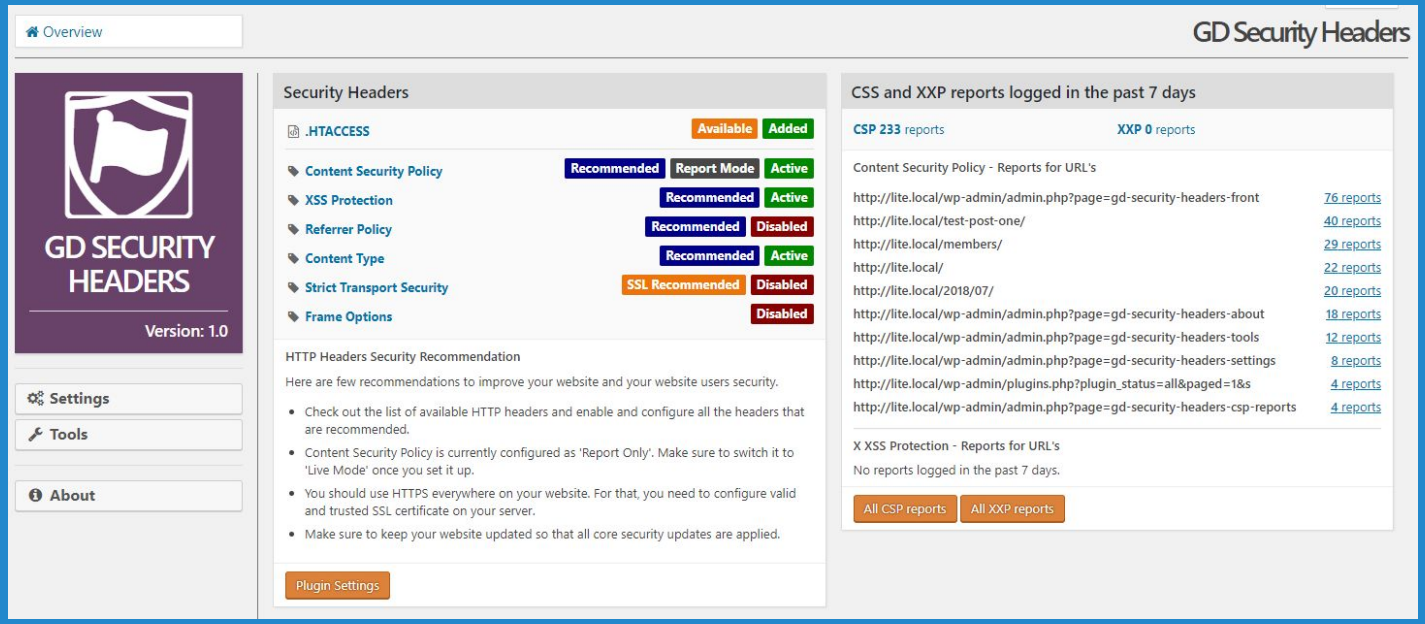
Neophodna je analiza sadržaja kako bi se definisale vrednosti za direktive.

No postoji pouzdan automatski metod generisanja potrebnih vrednosti.

Kombinacija oba pristupa neophodna u slučaju korišćenja NGINX i IIS servera.

GD Security Headers

`https://wordpress.org/plugins/gd-security-headers/`

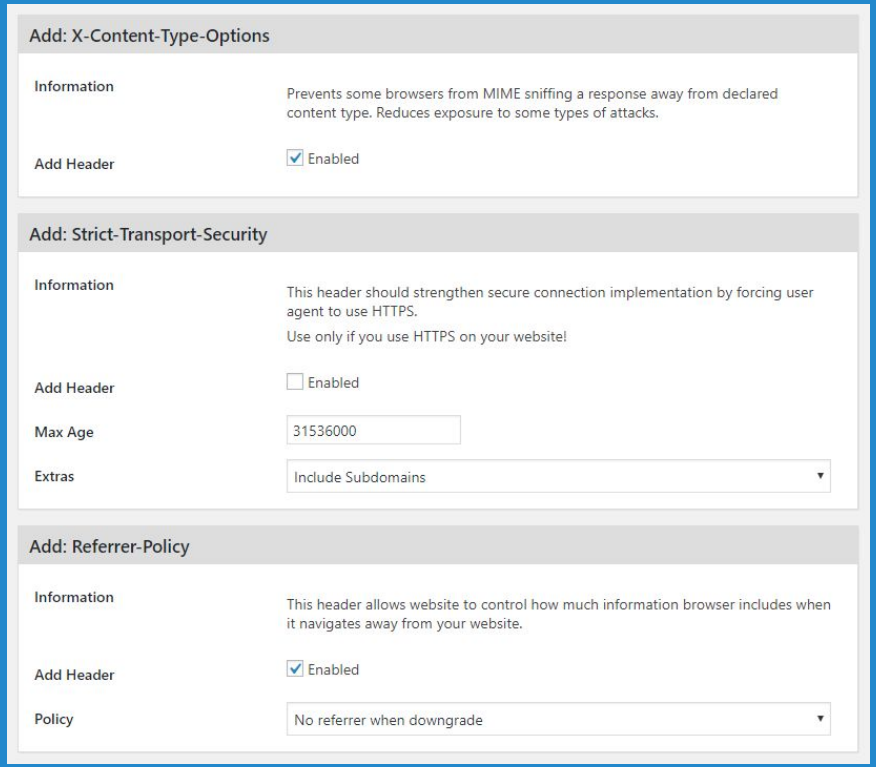


Podržana HTTP zaglavlja

Content Security Policy
X-XSS Protection
X-Content-Type-Options
Strict-Transport-Security
Referrer-Policy
X-Frame-Options

Ostale Funkcije

CSP i X-XSS-Protection Izveštaji o prekršajima
Dodaje zaglavlja u HTACCESS
Generiše zaglavlja za Apache, NGINX i IIS

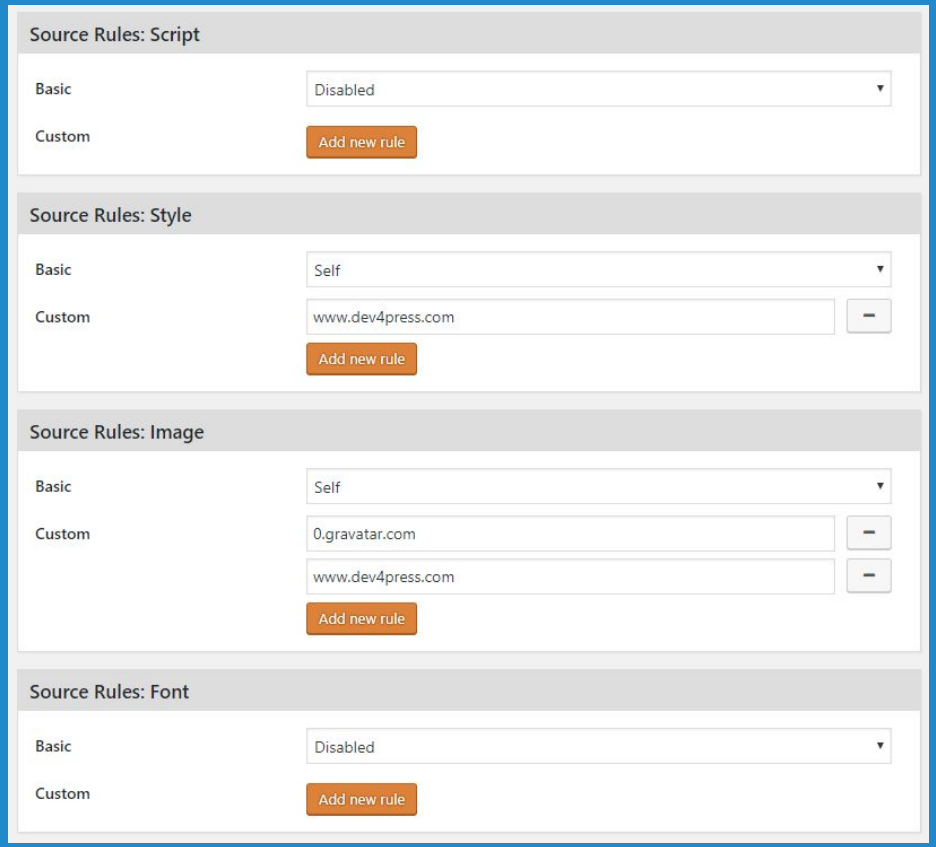


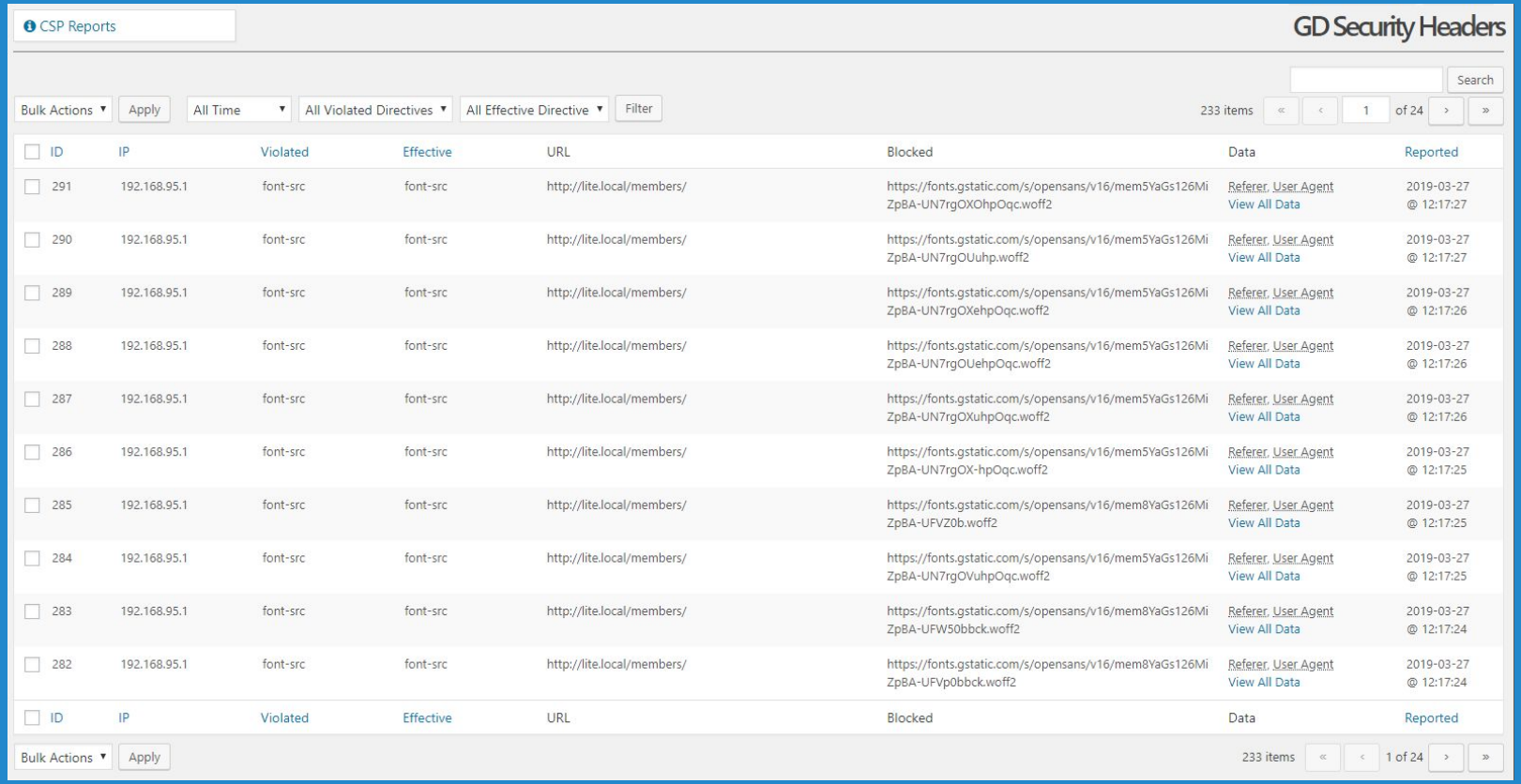
CSP Podešavanja

CSP Live ili Report mod
Automatska pravila
Dodatne direktive
Eskperimentalne direktive

Pravila za popularne servise

Google Adsense, Google Fonts, Google Analytics, Google Maps, Google Translate





CSP Izveštaji i prekršajima koje browser-i šalju sajtu

Nginx Server

If you use NGINX server, you can copy rules from here to add to the server 'conf' file.

```
# content-security-policy
add_header Content-Security-Policy-Report-Only "default-src 'self' 'unsafe-inline' 'unsafe-eval' data: ; r

# x-xss-protection
add_header X-XSS-Protection "1; mode=block; report=http://bbpress.local?gdsih-xxp-report;";

# x-content-type-options
add_header X-Content-Type-Options "nosniff";

# x-frame-options
add_header X-Frame-Options "SAMEORIGIN";

# referrer-policy
add_header Referrer-Policy "no-referrer-when-downgrade";
```

HTTP zaglavlja za NGINX server. Plugin generiše zaglavlja za Apache i IIS.

Milan Petrović

Dev4Press:
www.dev4press.com

Twitter:
twitter.com/milangd

WordPress.org:
profiles.wordpress.org/gdragon/

www.dev4press.com

part of **WordPress** community since **2008**

premium plugins for your
WordPress powered website

professional development,
consulting and training for
WordPress & **bbPress**