

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).

```
▼ Response Headers
alt-svc: quic=":443"; ma=2592000; v="46,44,43,39"
cache-control: private, max-age=0
content-encoding: br
content-type: text/html; charset=UTF-8
date: Fri, 10 May 2019 15:32:07 GMT
expires: -1
server: gws
set-cookie: 1P_JAR=2019-05-10-15; expires=Sun, 09-Jun-2019 15:32:07 GMT; path=/; domain=.google.com
set-cookie: SIDCC=AN0-TYsWrvq1W9iEKwe0NQHV1Ec0BjWkuhbzvh-JvR0zbd1c4-3zf5Upo_gFE3pjRNEivKwNAqAR; expires=Thu, 08-Aug-2019 15:32:07 GMT; path=/; domain=.google.com; priority=high
status: 200
strict-transport-security: max-age=31536000
x-frame-options: SAMEORIGIN
x-xss-protection: 0
```

C S P

Content Security Policy
Polisa Sigurnosti Sadržaja

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

Pomaže u smanjivanju 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 zaglavljenjima

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

Pomaže u smanjivanju 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 zaglavljenjima

Svi moderni browseri podržavaju CSP, uključujući i mobilne browsere

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

Pomaže u smanjivanju 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 zaglavljenjima

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

Zaštítite 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, nginx...) 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, nginx...) 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, nginx...) 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, nginx...) 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

Jednostavnije 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/>

Overview

GD Security Headers



Settings
Tools
About

Security Headers

.HTACCESS	Available	Added
Content Security Policy	Recommended	Report Mode Active
XSS Protection	Recommended	Active
Referrer Policy	Recommended	Disabled
Content Type	Recommended	Active
Strict Transport Security	SSL Recommended	Disabled
Frame Options		Disabled

HTTP Headers Security Recommendation

Here are few recommendations to improve your website and your website users security.

- Check out the list of available HTTP headers and enable and configure all the headers that are recommended.
- Content Security Policy is currently configured as 'Report Only'. Make sure to switch it to 'Live Mode' once you set it up.
- You should use HTTPS everywhere on your website. For that, you need to configure valid and trusted SSL certificate on your server.
- Make sure to keep your website updated so that all core security updates are applied.

Plugin Settings

GD Security Headers

CSS and XXP reports logged in the past 7 days

CSP 233 reports	XXP 0 reports
Content Security Policy - Reports for URL's	
http://lite.local/wp-admin/admin.php?page=gd-security-headers-front	76 reports
http://lite.local/test-post-one/	40 reports
http://lite.local/members/	29 reports
http://lite.local/	22 reports
http://lite.local/2018/07/	20 reports
http://lite.local/wp-admin/admin.php?page=gd-security-headers-about	18 reports
http://lite.local/wp-admin/admin.php?page=gd-security-headers-tools	12 reports
http://lite.local/wp-admin/admin.php?page=gd-security-headers-settings	8 reports
http://lite.local/wp-admin/plugins.php?plugin_status=all&paged=1&s	4 reports
http://lite.local/wp-admin/admin.php?page=gd-security-headers-csp-reports	4 reports

X XSS Protection - Reports for URL's

No reports logged in the past 7 days.

All CSP reports All XXP reports

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

Add: X-Content-Type-Options	
Information	Prevents some browsers from MIME sniffing a response away from declared content type. Reduces exposure to some types of attacks.
Add Header	<input checked="" type="checkbox"/> Enabled

Add: Strict-Transport-Security	
Information	This header should strengthen secure connection implementation by forcing user agent to use HTTPS. Use only if you use HTTPS on your website!
Add Header	<input type="checkbox"/> Enabled
Max Age	<input type="text" value="31536000"/>
Extras	<input type="text" value="Include Subdomains"/>

Add: Referrer-Policy	
Information	This header allows website to control how much information browser includes when it navigates away from your website.
Add Header	<input checked="" type="checkbox"/> Enabled
Policy	<input type="text" value="No referrer when downgrade"/>

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

The image shows a configuration interface for Content Security Policy (CSP) rules, organized into four sections: Script, Style, Image, and Font. Each section has a 'Basic' dropdown menu and a 'Custom' input field with an 'Add new rule' button.

- Source Rules: Script**
 - Basic: Disabled
 - Custom: Add new rule
- Source Rules: Style**
 - Basic: Self
 - Custom: www.dev4press.com
 - Add new rule
- Source Rules: Image**
 - Basic: Self
 - Custom: 0.gravatar.com
 - www.dev4press.com
 - Add new rule
- Source Rules: Font**
 - Basic: Disabled
 - Custom: Add new rule

Bulk Actions ▾

Apply

All Time ▾

All Violated Directives ▾

All Effective Directive ▾

Filter

233 items

<<

<

1

of 24

>

>>

Search

<input type="checkbox"/>	ID	IP	Violated	Effective	URL	Blocked	Data	Reported
<input type="checkbox"/>	291	192.168.95.1	font-src	font-src	http://lite.local/members/	https://fonts.gstatic.com/s/opensans/v16/mem5YaGs126MiZpBA-UN7rgOXhPQqc.woff2	Referer, User Agent View All Data	2019-03-27 @ 12:17:27
<input type="checkbox"/>	290	192.168.95.1	font-src	font-src	http://lite.local/members/	https://fonts.gstatic.com/s/opensans/v16/mem5YaGs126MiZpBA-UN7rgOUuHP.woff2	Referer, User Agent View All Data	2019-03-27 @ 12:17:27
<input type="checkbox"/>	289	192.168.95.1	font-src	font-src	http://lite.local/members/	https://fonts.gstatic.com/s/opensans/v16/mem5YaGs126MiZpBA-UN7rgOXehPQqc.woff2	Referer, User Agent View All Data	2019-03-27 @ 12:17:26
<input type="checkbox"/>	288	192.168.95.1	font-src	font-src	http://lite.local/members/	https://fonts.gstatic.com/s/opensans/v16/mem5YaGs126MiZpBA-UN7rgOUehPQqc.woff2	Referer, User Agent View All Data	2019-03-27 @ 12:17:26
<input type="checkbox"/>	287	192.168.95.1	font-src	font-src	http://lite.local/members/	https://fonts.gstatic.com/s/opensans/v16/mem5YaGs126MiZpBA-UN7rgOXuHPQqc.woff2	Referer, User Agent View All Data	2019-03-27 @ 12:17:26
<input type="checkbox"/>	286	192.168.95.1	font-src	font-src	http://lite.local/members/	https://fonts.gstatic.com/s/opensans/v16/mem5YaGs126MiZpBA-UN7rgOX-hpQqc.woff2	Referer, User Agent View All Data	2019-03-27 @ 12:17:25
<input type="checkbox"/>	285	192.168.95.1	font-src	font-src	http://lite.local/members/	https://fonts.gstatic.com/s/opensans/v16/mem8YaGs126MiZpBA-UFVZ0b.woff2	Referer, User Agent View All Data	2019-03-27 @ 12:17:25
<input type="checkbox"/>	284	192.168.95.1	font-src	font-src	http://lite.local/members/	https://fonts.gstatic.com/s/opensans/v16/mem5YaGs126MiZpBA-UN7rgOUuHPQqc.woff2	Referer, User Agent View All Data	2019-03-27 @ 12:17:25
<input type="checkbox"/>	283	192.168.95.1	font-src	font-src	http://lite.local/members/	https://fonts.gstatic.com/s/opensans/v16/mem8YaGs126MiZpBA-UFW50bbck.woff2	Referer, User Agent View All Data	2019-03-27 @ 12:17:24
<input type="checkbox"/>	282	192.168.95.1	font-src	font-src	http://lite.local/members/	https://fonts.gstatic.com/s/opensans/v16/mem8YaGs126MiZpBA-UFVp0bbck.woff2	Referer, User Agent View All Data	2019-03-27 @ 12:17:24

Bulk Actions ▾

Apply

233 items

<<

<

1 of 24

>

>>

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/

dev4press

www.dev4press.com

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

premium plugins for your
WordPress powered website

professional development,
consulting and training for
WordPress & bbPress