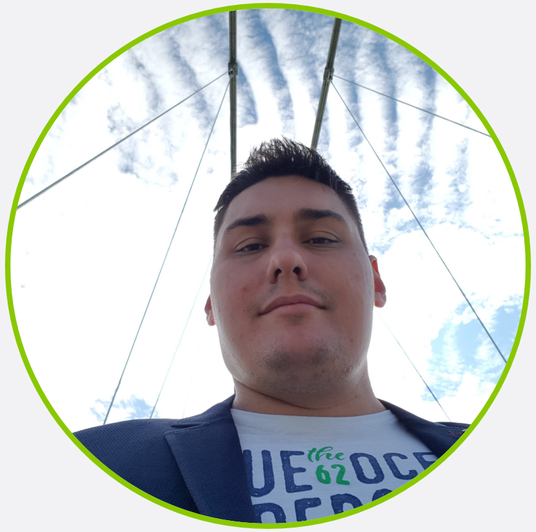
Moderni Web Security standardi



Igor Hrček, CTO

Započeo sam svoje preduzetničko putovanje sa 24 godina i osnovao hosting kompaniju Mint Services. Otkako znam za sebe bavim se programiranjem i stvaranjem visokokvalitetnih bagova. Zaljubljenik u rokenrol i kafu. Bogatu karijeru sam započeo kao 8bit Padawan, sad sam 64bit Jedi :)

o
nama

web hosting

Nudimo različite tipove hosting usluga, od Shared do Managed Cloud VPS hostinga

web dev

Već 10 godina razvijamo namenske web aplikacije prema potrebama trećih lica

business consulting

Planiranje projekata, roadmapping, budžetiranje, damage control, IT management

mint blog

https://mint.rs/blog

- WordPress terminologija za početnike
- WordPress razvoj za početnike – prvi koraci (uskoro)
- Kako popraviti hakovan WordPress (uskoro)

Prijavite se na naš newsletter

agenda
prezentacije

moderni web security standardi

Web Security standardi kao bitan deo bezbednosti

WordPress bezbednost

Kako da učinite svoj WordPress bezbednijim?

HTTPS

HTTP/2

~~Sprajtovi~~
~~Konkatenacija JS I CSS fajlova~~
~~Sharding na nivou domena zarad bržeg učitavanja~~

Nove mogućnosti

Geolocation API
AppCache

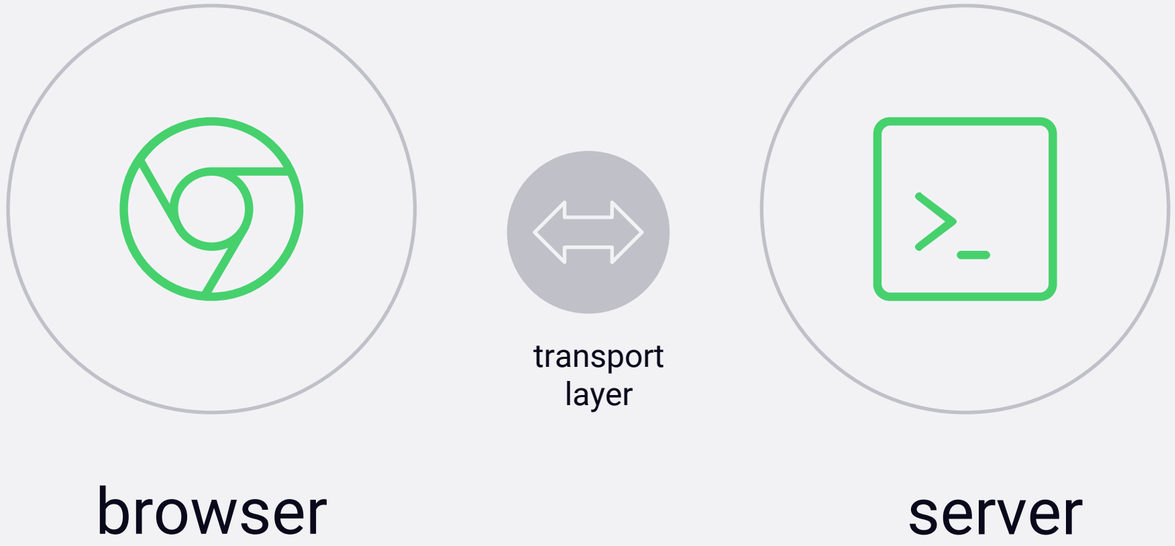
Brotli kompresija

Značajno napredniji algoritam za kompresiju koji će uskoro zameniti GZip

SEO ++

Google bolje rangira one sajtove koji koriste HTTPS protokol

evolucija
bezbednosti



security
headers

Content Security Policy (CSP)

Detekcija i mitigacija odgovarajućih tipova napada kao što su XSS i ubacivanje koda.

Public-Key-Pin (HPKP)

Smanjuje rizik od MITM (Man in the middle) napada vezivanjem javnog ključa za odgovarajući web server.

Strict-Transport-Security (HSTS)

Striktno deklasiranje protokola koji Web browser mora da koristi.

Ima toga još...

SRI
X-Content-Type-Options
X-Frame-Options
X-XSS-Protection
X-Download-Options
Cross Domain Policies

CSP
content injections

Jednostavan primer

```
<body>
<textarea>
    </textarea><script src="//nsa.gov.us/i-am-not-evil-
script.js"></script><textarea>
</textarea>
</body>
```

šta je
CSP

HTTP odgovor

```
content-encoding: br
content-security-policy: [CSP direktive]
date: Fri, 13 Apr 2018 17:25:36 GMT
server: nginx
status: 200
strict-transport-security: max-age=15768000
```

CSP direktive

child-src, connect-src, default-src, **font-src**, frame-src
img-src, media-src, object-src, **script-src**, **style-src**

CSP
implementacija

```
add_header Content-Security-Policy default-src 'self';

script-src 'self' 'unsafe-inline' https://ssl.google-
analytics.com https://assets.zendesk.com
https://connect.facebook.net;

img-src 'self' https://ssl.google-analytics.com https://s-
static.ak.facebook.com https://assets.zendesk.com;

style-src 'self' 'unsafe-inline'
https://fonts.googleapis.com https://assets.zendesk.com;
```

CSP
mixed content

MINT

CSP
mixed content

```
<img src=http://nekiurl.rs/slika.jpg>
```

block-all-mixed-content

```
<img src=https://nekiurl.rs/slika.jpg>
```

upgrade-insecure-requests

CSP
testiranje

```
Refused to load the script
'https://www.google.com/recaptcha/api.js' because it
violates the following Content Security Policy directive:
"script-src 'self' 'unsafe-inline' 'unsafe-eval'
https://*.tynt.com https://de.tynt.com
https://ajax.cloudflare.com https://www.google-
analytics.com https://ssl.google-analytics.com
https://assets.zendesk.com https://connect.facebook.net".
```

```
Content-Security-Policy-Report-Only: [CSP direktive];
report-uri https://mint.rs/report
```

Strict-Transport-Security
HSTS OFF

Strict-Transport-Security
HSTS

šta je
HSTS

HTTP odgovor

```
content-encoding: br
date: Fri, 13 Apr 2018 17:25:36 GMT
server: nginx
status: 200
strict-transport-security: max-age=15768000
```

Podešavanje

```
max-age
includeSubDomains
preload
```

Strict-Transport-Security
HSTS ON

Public Key Pinning

Pravi sertifikat

Kompromitovani sertifikat

šta je
HPKP

HTTP odgovor

```
content-encoding: br
date: Fri, 13 Apr 2018 17:25:36 GMT
server: nginx
status: 200
public-key-pins: [polisa]

pin-sha256="cUPcTAZWKaASuYWhhneDttWpY3oBAkE3h2+soZS7sWs=";
max-age=5184000;
includeSubDomains;
report-uri="https://mint.rs/hpkp-report"
```

Generisanje hash-a

```
openssl rsa -in my-rsa-key-file.key -outform der -pubout |
openssl dgst -sha256 -binary | openssl enc -base64
```

integritet
spoljnih resursa

SRI – Sub-resource Integrity

- Rešava problem poverenja u fajlove koje distribuiraju CDN servisi
- Jednostavna implementacija u vidu base64 kriptografskog hash-a

Primer

```
<script src="https://jquery.com/jquery.3.10.min.js"
integrity="sha384-
oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC"
crossorigin="anonymous"></script>
```

Forsiranje kroz CSP

```
Content-Security-Policy: require-sri-for script;
```

Ručno generisanje

```
cat FILENAME.js | openssl dgst -sha384 -binary | openssl enc -
base64 -A
```

pauza za kafu

pitanja & odgovori

WordPress bezbednost

burek
diskusija

Sasa Kasapic
Yesterday at 9:47am

Visoko Intelektualno Pitanje ...
Koji plugin za secure ...

Like Share

Marko Pavisic Wordfence. Mada sam čuo da real time skeniranje hoće da uspori prilično server, te bi bilo dobro to isključiti.
Like · 1d · 2

Branislav Bokun Wordfense, ithemes, all in one wp, succuri, pa biraj...
Like · 1d · 1

Sasa Kasapic hvala · 1
Like · 1d

Luka Petrovic Nijedan. Svaki usporava sajt. Hosting sa mod_sec i dovoljno.
Like · 7h · 4

Sasa Kasapic hvala svima ...
Like · 4h

An admin turned off commenting for this post.

priča o bezbednosti

- Ma ko će mene da dira?
- Jedna mera nije adekvatna za sve
- Kako proceniti efektivnu snagu bezbednosnih mera?
- Bezbednost je lanac sastavljen od pojedinačnih karika
- **OWASP 10**

✓ A1 Injection / 42%
✓ A2 Broken Authentication and Session Management
✓ A3 Cross-Site Scripting (XSS) / 37%
✓ A4 Insecure Direct Object References
✓ A5 Security Misconfiguration
✓ A6 Sensitive Data Exposure / 3%
✓ A7 Missing Function Level Access Control
✓ A8 Cross-Site Request Forgery (CSRF) / 4%
✓ A9 Using Components with Known Vulnerabilities
✓ A10 Unvalidated Redirects and Forwards

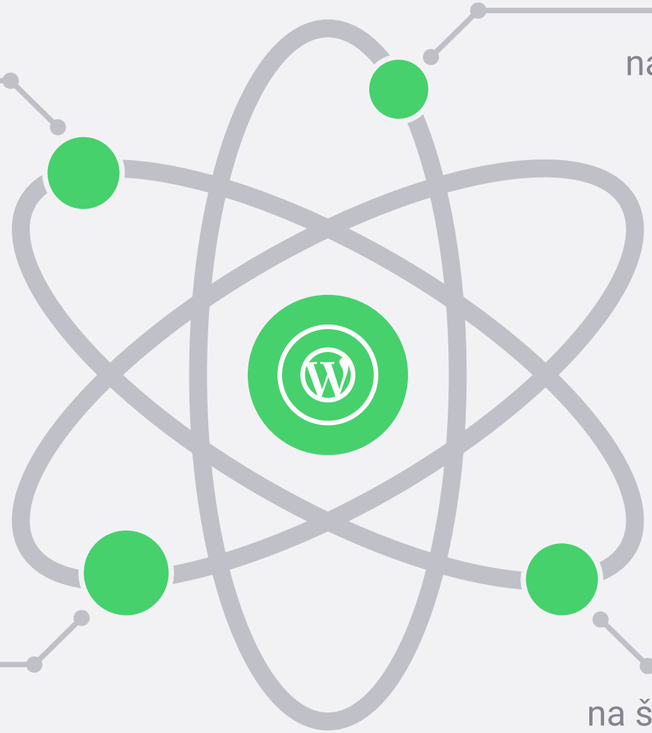
wordpress
lanac bezbednosti

web hosting

kako odabrati dobar hosting?

dodaci

na šta obratiti pažnju kod dodataka?



kako se odnositi prema WordPress osnovi

wordpress core

teme

na šta obratiit pažnju kod tema?

Na šta obratiti pažnju?

- Birajte uslugu u skladu sa potrebama sajta
- Saznajte više o sigurnosnim praksama provajdera
- Raspitajte se o istorijatu provajdera
- Nemojte biti sam svoj majstor

WordPress
core

- WordPress je frejmvork zasnovan na mikrokernel arhitekturi
- WordPress je javno dostupan svima na uvid
- Izbegavajte version lock
- **Redovno ažurirajte WordPress Core**

WordPress
dodaci

Na šta obratiti pažnju?

- Izbegavajte ”**There is a plugin for that”** pristup
- Obratite pažnju na performanse i bezbednost, a ne samo na funkcionalnost
- Proverite reputaciju developera koji je razvio dodatak
- Proverite koliko često se ažurira i kada je zadnji put bio ažuriran
- Proverite kakvu podršku developer pruža i koliko je zaista dostupan
- Proverite da li je dodatak ranije imao sigurnosnih propusta
- Pratite Security izveštaje
- Premium dodatak ne znači kvalitet
- Izbegavajte Nulled dodatke
- **Obrišite dodatke koje ne koristite**
- **Redovno ažurirajte instalirane dodatke**

WordPress
teme

Na šta obratiti pažnju?

- Teme nisu prezentacija već kompleksne aplikacije
- Obratite pažnju na performanse i bezbednost, a ne samo na funkcionalnost
- Proverite reputaciju developera koji je razvio temu
- Proverite koliko često se ažurira i kakva je bila podrška za prethodne verzije WordPress-a
- Proverite kakvu podršku developer pruža i koliko je zaista dostupan
- Proverite da li je tema ranije imala sigurnosnih propusta
- Pratite Security izveštaje
- Premium tema gotovo uvek znači loš kvalitet
- U tok urazvoja svoje teme, obratite pažnju na bezbednosni aspekt
- Ako ne koristite, obrišite podrazumevane WordPress teme
- **Redovno ažurirajte instalirane teme**

security dodaci
su loše rešenje

- Kao bezbednosni mehanizam, nalaze se na pogrešnom mestu
- Unose nove potencijalne bezbednosne probleme u već kompleksan lanac
- Ne pomažu oko mitigacije većine napada sa OWASP 10 liste
- Negativno utiču na performanse sajta
- Sve što nude predstavlja set alata koji je već dostupan

security dodaci
su loše rešenje

iThemes
security primer

Sakrivanje wp-login

```
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteRule ^skrivenilogin/?$ /wp-login.php?[vas-tajni-salt] [R,L]
RewriteCond %{HTTP_COOKIE} !^.*wordpress_logged_in_.*$
RewriteRule ^skriveniwpadmin/?$ /wp-login.php?[vas-tajni-salt]&redirect_to=/wp-admin/ [R,L]
RewriteRule ^skriveniwpadmin/?$ /wp-admin/?[vas-tajni-salt] [R,L]
RewriteRule ^registracija/?$ /wp-login.php?[vas-tajni-salt]&action=register [R,L]
RewriteCond %{SCRIPT_FILENAME} !^(.*)admin-ajax\.php
RewriteCond %{HTTP_REFERER} !^(.*)nekisajt.rs/wp-admin
RewriteCond %{HTTP_REFERER} !^(.*)nekisajt.rs/wp-login\.php
RewriteCond %{HTTP_REFERER} !^(.*)nekisajt.rs/skrivenilogin
RewriteCond %{HTTP_REFERER} !^(.*)nekisajt.rs/skriveniwpadmin
RewriteCond %{HTTP_REFERER} !^(.*)nekisajt.rs/registracija
RewriteCond %{QUERY_STRING} !^[vas-tajni-salt]
RewriteCond %{QUERY_STRING} !^action=logout
RewriteCond %{QUERY_STRING} !^action=rp
RewriteCond %{QUERY_STRING} !^action=registracija
RewriteCond %{QUERY_STRING} !^action=postpass
RewriteCond %{HTTP_COOKIE} !^.*wordpress_logged_in_.*$
RewriteRule ^.*wp-admin/?|^.*wp-login\.php /not_found [R,L]
RewriteCond %{QUERY_STRING} ^loggedout=true
RewriteRule ^.*$ /wp-login.php?[vas-tajni-salt] [R,L]
</IfModule>
```

Protect System Files

```
find /path/to/your/wordpress/install/ -type d -exec chmod 755 {} \;
find /path/to/your/wordpress/install/ -type f -exec chmod 644 {} \;
```

iThemes
security primer

Disable PHP in uploads

```
<Files ~ "\.ph(?:p[345]?|t|tml)$">
    deny from all
</Files>
```

iThemes
security primer

Disable File Editing

```
define('DISALLOW_FILE_EDIT', true);
```

iThemes
security primer

404 detection

```
function uradi_nesto_sa_404(){
    if( is_404() ){
        // uradi nesto?
    }
} 7
add_action( 'template_redirect’, ‘uradi_nesto_sa_404' );
```

iThemes
security primer

Change WordPress Salts

https://api.wordpress.org/secret-key/1.1/salt/

```
define('AUTH_KEY', '?DApUB/Z=-| H<s=|i&-e2|j8iJlg?v66kmYTK&*>[AF?^;m3CjW<>Y]_5SzD3Va');
define('SECURE_AUTH_KEY', 'C[+#I:?kz&-UYD2=2,qlr.lH80U/V9)5tqW<x2-<^kTieUNQ=<rPd.bnH; }qGrM');
define('LOGGED_IN_KEY', ' 2mh!qdrlWST~GN}bl1A-K:|.5Yh^iN`-d~xJJ|Du%`#GPGaC4T:W9q$?dM[:Ki+');
define('NONCE_KEY', 'c`P.W0M1+!dXV Jynz+:=vf{fF8kq>ldJ/M) #Uq6jl}r+h(8:7:Z92TQ J$f!]j');
define('AUTH_SALT', '01 t?:M|vSXtp<]FmZol58.^!1IoyIfM4+a,C>I8*9<Q&>$@d|Kj|nE(;j3OsOAp');
define('SECURE_AUTH_SALT', '9r?tgD< wxR$(vm8e<{3yS)6Oy2^?%U1XS)TDl$#eqGqb25sW;]-;;QaW4Na ,)(');
define('LOGGED_IN_SALT', 'lG<KrZ:-1SsxS C- `.iE#sMy@Z|K+(}Vk/S.=}AWJ+#+4JH0gX._i+zzX3vd|*p');
define('NONCE_SALT', 'GKW/|fL2[Y_J+EseXnrM]i*V+(]>|b/*gMdI.6}/>ZBVe(5mO2c+U_+dfD#[?IZ(');
```

iThemes
security primer

Disable XML-RPC

```
# Block WordPress xmlrpc.php requests
<Files xmlrpc.php>
order deny,allow
deny from all
allow from 123.123.123.123
</Files>

add_filter('xmlrpc_enabled', '__return_false');
```

iThemes
security primer

Monitor File Change

```
function hashDirectory($directory)
{
    if (! is_dir($directory)) return false;

    $files = array();
    $dir = dir($directory);

    while (false !== ($file = $dir->read())) {
        if ($file != '.' and $file != '..') {
            if (is_dir($directory . '/' . $file)) {
                $files[] = hashDirectory($directory . '/' . $file);
            }
            else {
                $files[] = md5_file($directory . '/' . $file);
            }
        }
    }
    $dir->close();
    return md5(implode('', $files));
}
```

predlozi za
bolju bezbednost

Tips & tricks

- Bolji Access Control
- 2FA autentifikacija
- Koristite jake lozinke
- Radite redovan bekap na nivou servera
- Setujte ispravne dozvole nad fajlovima i direktorijumima – **izbegavajte 777**
- Dodajte Basic Auth u wp-admin
- Odobrite pristup WP administraciji samo sa malog broja IP adresa
- Zabranite direktan pristup fajlovima i direktorijumima koji nisu od direktnog značaja

```
RewriteRule ^wp-admin/includes/ - [F,L]
RewriteRule !^wp-includes/ - [S=3]
RewriteRule ^wp-includes/[^/]+\.php$ - [F,L]
RewriteRule ^wp-includes/js/tinymce/langs/.+\.php - [F,L]
RewriteRule ^wp-includes/theme-compat/ - [F,L]
<files wp-config.php>
order allow,deny
deny from all
</files>
```

predlozi za
bolju bezbednost

Tips & tricks

- Isključite File Editor u administraciji
- Prilikom odabira hosting provajdera, saznajte više o sigurnosnim praksama i istorijatu
- Odaberite hosting uslugu u skladu sa potrebama sajta
- Osigurajte se da na serveru postoji Application Firewall poput ModSecurity
- Vršite konstantan monitoring vašeg sajta
- Nemojte instalirati sve i svašta od dodataka
- Uvek pazite na reputaciju, poslednje ažuriranje, kompatibilnost i istorijat propusta dodatka
- Uvek pazite na reputaciju, poslednje ažuriranje, kompatibilnost i istorijat propusta teme

- Prilikom razvoja obratite pažnju na OWASP 10 listu propusta i unapred planirajte metode za mitigaciju

https://www.owasp.org/index.php/PHP_Security_Cheat_Sheet

to je to, nema više

pitanja & odgovori

kutija

igor.hrcek

mint.rs

hvala ☺