3/27/14

Emanuel Zelić

- linux system administrator
- korisnička podrška
- iskustvo sa WordPress-om

plus HOSTING

Ranjivost WordPress-a

- WordPress je jedan od najčešće korištenih CMS-ova na svijetu
- U kolovozu 2013. je imao udio od 18.9% od 10 milijuna top web stranica
- U srpnju 2013. je otkriveno da je 50 najčešće skidanih pluginova ranjihova na SQL Injection napade
- Odvojena inspekcija top deset e-commerce pluginova je pokazala da je sedam od njih ranjivo
- Od WordPress-a verzije 3.7 je uvedena automatska nadogradna u pozadini.

Kako dolazi do napada

- 41% zbog malwarea
- 29% zbog propusta u temama
- 22% kroz pluginove
- 8% zbog slabih lozinki

Što hakeri/crackeri žele

- Ugled
- Zabava
- Da bi došli do podataka
- Da postave linkove na stranici
- Da naprave štetu vlasniku stranice

Maliciozni napadi koštaju!

- vremena
- energije
- novca
- ugleda

Nadogradnja aplikacije

- WordPress, pluginove i teme treba redovno nadograđivati
- Popis propusta WordPressa koji su otkriveni i otklonjeni kroz patcheve su vidljivi na stranici:

  http://di.si/ru9az
- Izbjegavajte besplatne teme i pluginove koje se ne nalaze u WordPress repozitoriju

Zaštita računala i lozinke

- Računala na kojima radite moraju biti čista od malware-a i virusa
- **Koristite jake lozinke**
  - Loša lozinka: admin123
  - Dobra lozinka: bmjB1XjhvfTMf
- **Koristite password managere**
  - KeePass (Win/Mac/Linux)

Koristite SSH I SFTP

- Nemojte koristiti FTP klijent, koristite SFTP ili SSH protokole za prijenos podataka
- Redoviti backupi svih podataka
- Koristite ugledne web hosting firme

Zaštita wp-admin direktorija

- Password protected directories:

Create User:

Username:

New Password:

Password (Again):

Strength (why?): Very Weak (0/100) Password Generator

Add/modify authorized user

Zaštita wp-admin direktorija

U “.htaccess” datoteku potom ubaciti:

AuthType Basic

AuthName “Login required”

AuthUserFile “/home/<CPANEL USERNAME>/.htpasswds/public_html/passwd”

ErrorDocument 401 default

Autentikacija za wp-login i wp-admin

<Files “wp-login.php”>

require valid-user

</Files>

Zaštita wp-includes direktorija

U “.htaccess” datoteku ubaciti:

```
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
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]
</IfModule>
```

Dodatna zaštita datoteka

- Onemogućavanje editiranja datoteka kroz dashboard umetanjem sljedeće linije u wp-config.php datoteku:

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

- Pomaknite wp-config.php datoteku nivo iznad web direktorija WordPress instalacije

Koristite sigurnosne pluginove

- WordPress Firewall
- All in One WordPress Firewall
- Better WP Security
- Wordfence security
- Simple Login Lockdown

Security through obscurity

- Ne koristiti admin username za admin korisnika

```
UPDATE wp_users SET user_login = 'newuser' WHERE user_login = 'admin';
```

- Promjena defaultnog WordPress table prefixa wp_
  - WordPress Table Prefix Rename Plugin

Optimizacija

- **Svrha Cache mehanizma:**
  - Brža isporuka web sadržaja
  - Smanjeno opterećenje web servera
- 90% slučajeva sporog učitavanja uzrokovano temom i konfiguracijom WordPress-a

Quick Cache

- Mali plugin, page cache bez kompresije
- Jednostavan za konfiguraciju

WP Super Cache

- Relativno lagan za podesiti i ne zahtijeva puno tehničkog znanja
- Kreira cache na tri načina:
  - mod_rewrite
  - Php
  - Legacy cache mode

W3 Total Cache

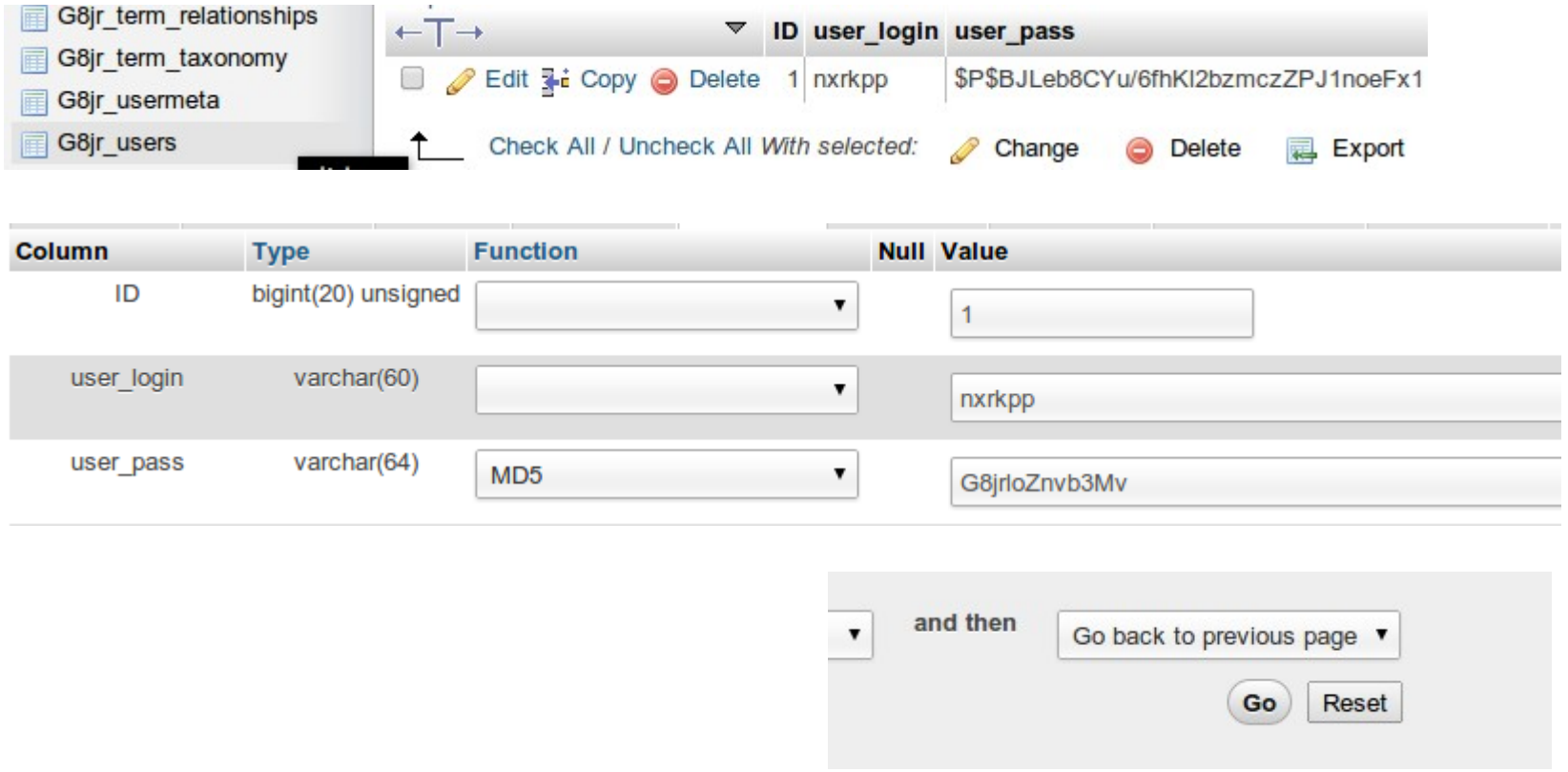
- Najcjenjeniji i najkompletniji WordPress performance plugin
- Mogućnosti:
  - Html cache,
  - Minification,
  - Object cache,
  - Database cache,
  - CDN,
  - Etc…

TIPS and TRICKS

- Zaboravljena lozinka
- Preseljenje WordPress aplikacije
- wp-cron.php

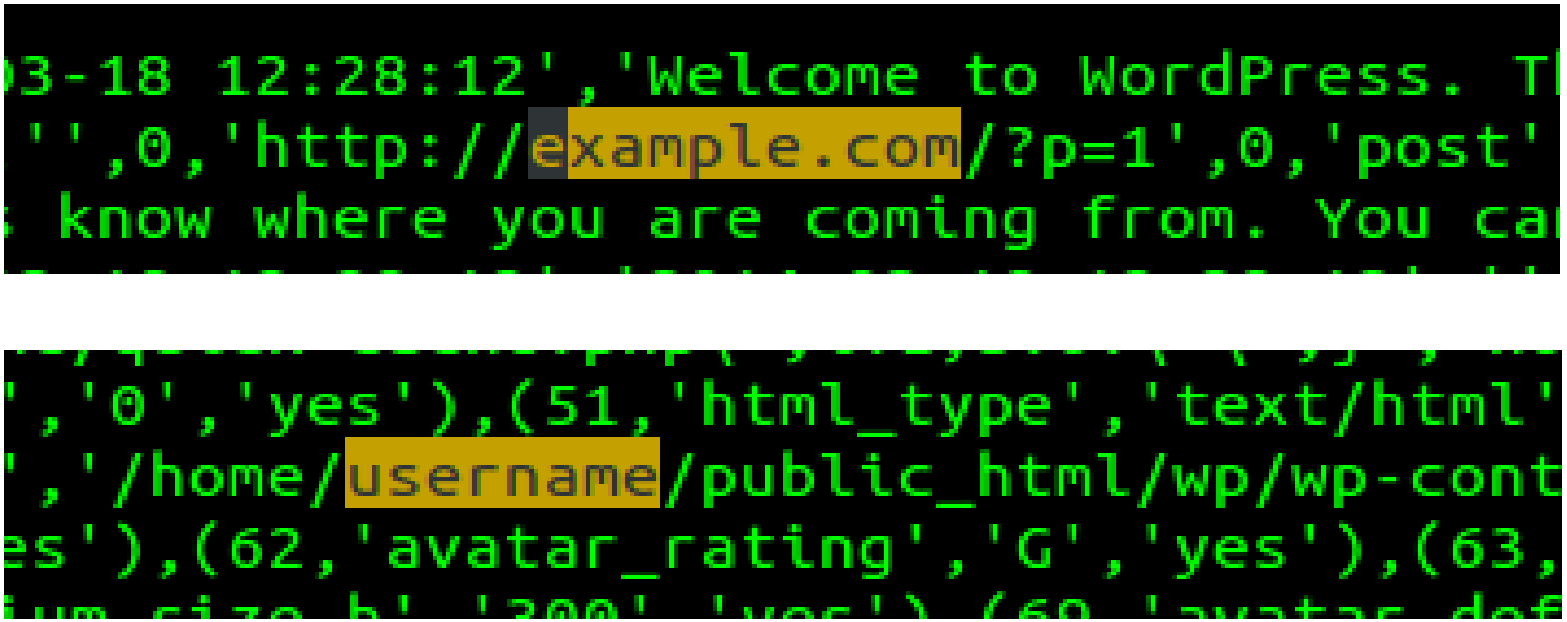
Zaboravljena lozinka

- Promjena lozinke kroz phpMyAdmin:



Preseljenje aplikacije

- Domenski nazivi i putanje direktorija su definirani unutar WordPress baze:



wp-cron.php

- wp-cron.php: virtualni cronjob
- **Namjena:**
  - Automatizacija objave postova
  - Provjera pluginova
  - Nadogradnja tema
  - Slanje mail notifikacija ...
- **Problem:**
  - Izvršavanje kod svakog otvaranja stranice

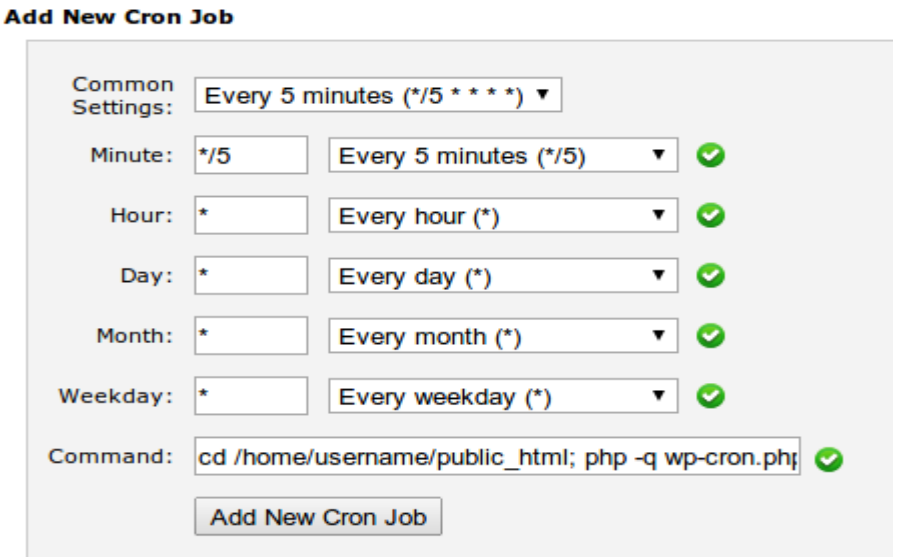
wp-cron.php - rješenje

- Onemogućiti njeno izvršavanje prilikom svakog otvaranja kroz wp-config.php:

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

- Definirati izvršenje skript preko sistemskog cronjoba:

```
cd /home/username/public_html; php -q wp-cron.php
```



Pitanja?