SYSTEM FAILURE

error 235553261...pending.....
fatal ER # 5444167QW32Z__WS @%$$

Securing

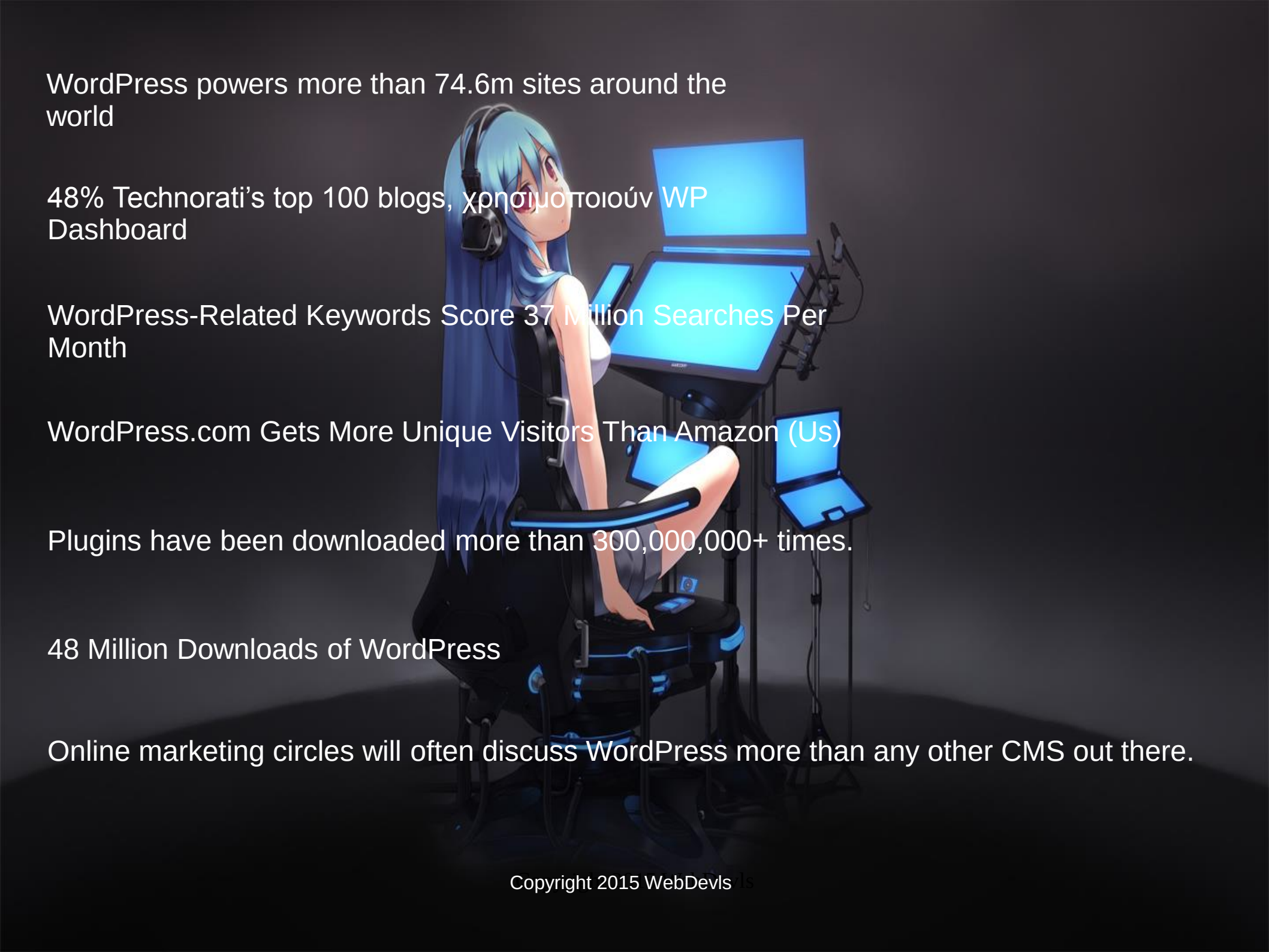
WordPress installations

Greek Community

Cyber Security and Wordpress Attacks

By

Grammenos Stefanos
Panagiotis Macromanolis



WordPress powers more than 74.6m sites around the world

48% Technorati’s top 100 blogs, χρησιμοποιούν WP Dashboard

WordPress-Related Keywords Score 37 Million Searches Per Month

WordPress.com Gets More Unique Visitors Than Amazon (Us)

Plugins have been downloaded more than 300,000,000+ times.

48 Million Downloads of WordPress

Online marketing circles will often discuss WordPress more than any other CMS out there.

Securing

WordPress installations

Greek Community

Ασφάλεια Υπολογιστικών Συστημάτων

Sasser – Bagle – Zafi – MyDoom – Lovsan/Blaster – Klez - BugBeaR

Όταν είμαστε οπλισμένοι με τεχνικές συμβουλές και κοινή λογική. Μπορούμε
Να αποφύγουμε αρκετές από τις γνωστές επιθέσεις. Όσο περισσότερο δυσκολέψουμε
Το έργο ενός επιτιθέμενου στην ιστοσελίδα μας, τόσο πιο πιθανό είναι να μας αφήσει
Ήσυχο και να περάσει σε έναν πιο εύκολο στόχο.

Securing

WordPress installations

Greek Community

Οι κύριες WordPress Based επιθέσεις

Το WordPress παραμένει ο κύριος στόχος επιθέσεων C.M.S

- Brute-force password-guessing attacks
- XSS -(css)
- SQL Injection
- Directory Indexing
  Honorable Mentions
- Image HotLinking

Securing

WordPress installations

Greek Community

Brute Force Attack

Or Dictionary attack

Brute Force Attack is an automated process and can be done by using a program That will try to decrypt your password by using a list of words, symbols and numbers (wordlists).

The Attacker will try to compromize your website by brute force attacking to your wp-login.php

Securing

WordPress installations

Greek Community

Cross Site Scripting Attack

Hack-Attack that exploits web applications
A security exploit in which attacker inserts
Malicious code into a link that appears to be
From a trustworthy source.

Securing

WordPress installations

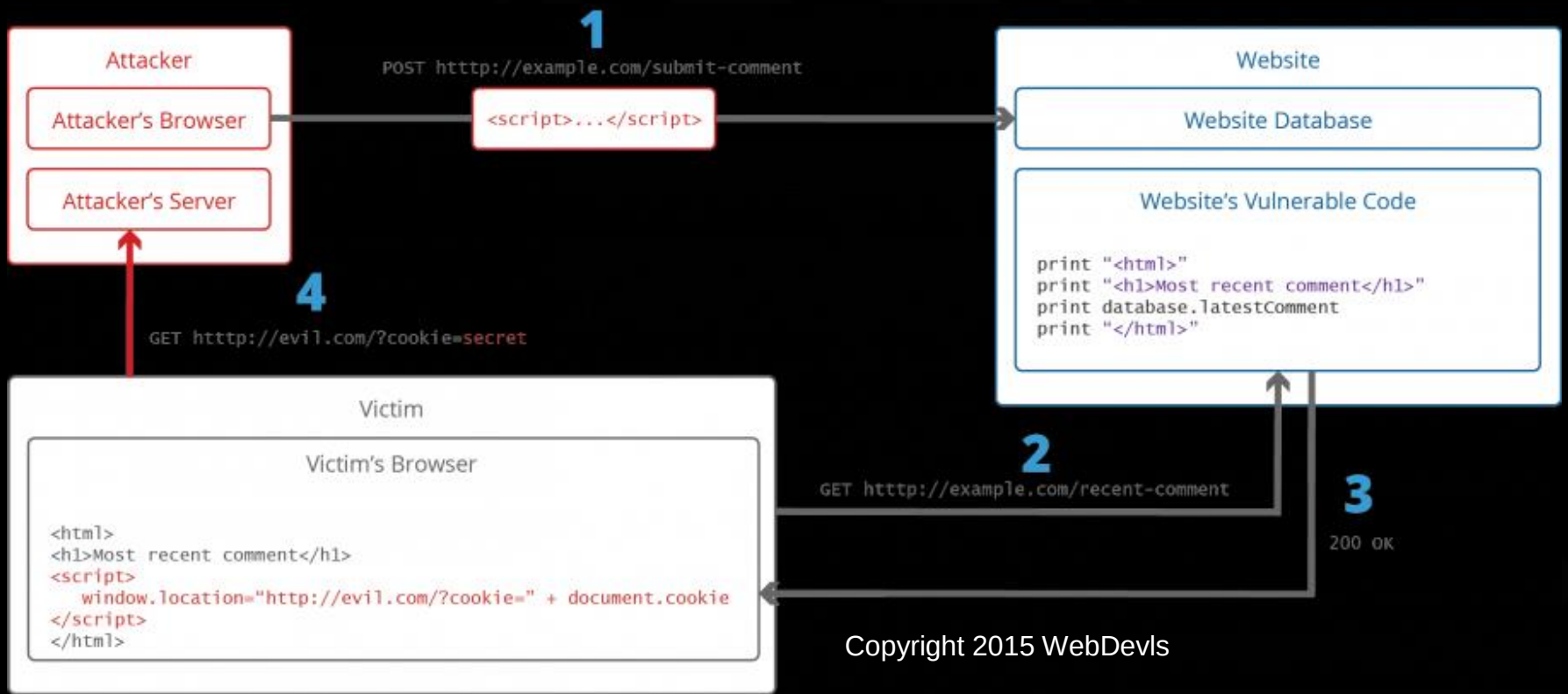
Greek Community

The attacker injects a payload in the website's database by submitting a vulnerable form with some malicious JavaScript

1. victim requests the web page from the website

2. The website serves the victim's browser the page with the attacker's payload as part of the HTML body.

3. The victim's browser will execute the malicious script inside the HTML body.
In this case it would send the victim's cookie to the attacker's server.
The attacker now simply needs to extract the victim's cookie when the HTTP request arrives to the server
after which the attacker can use the victim's stolen cookie for impersonation.



Securing

WordPress installations

Greek Community

SQL Injection

Query Database Attack.

Attacker tries to find vulnerable queries in the code.

Access, to the Whole Database Tables and Schema.

Securing

WordPress installations

Greek Community

Directory Indexing

Is a way for an attacker, to find out our servers' folder structure.

Can find our server user name in the process.

Securing

WordPress installations

Greek Community

Image HotLinking

The ability for another website to use our own bandwidth

Securing

WordPress installations

Greek Community

DDoS

A DDoS or a **Distributed Denial of Service** Attack is used to target a single (or multiple) Systems by sending a very large amount of traffic packets in to the system and finally overwhelming it and make it unavailable.

Distributed via botnets (infected systems)

Securing

WordPress installations

Greek Community

Ways to Secure your Installation

Securing

WordPress installations

Greek Community

Brute Force Algorithm

The brute-force method is to simply generate all possible routes and compare the distances. For a very small N, it works well, but it rapidly becomes absurdly inefficient when N increases.

Don't use the 'admin' username

Good Passwords

Security Plugins

Two Step Verification
/plugins/google-authenticator/

Security Plugins

Securing

WordPress installations

Greek Community

Brute Force Algorithm

The brute-force method is to simply generate all possible routes and compare the distances. For a very small N, it works well, but it rapidly becomes absurdly inefficient when N increases.

Block access to wp-admin by IP.

Στο .htaccess file μας.

```
# Block access to wp-admin.
order deny,allow
allow from x.x.x.x
deny from all
```

Securing

WordPress installations

Greek Community

Protect your WP Installation from XSS by:

1. Keep your systems secured and updated.
2. Always download Themes and Plugins from trusted sources.
3. **Ninja Firewall** (WP Plugin)
4. **Bullet Proof Security** (WP Plugin)

Securing

WordPress installations

Greek Community

Preventing SQL Injection

By Using Plugins.

By Using .htaccess *

By Changing the Default Database Prefix.

Securing

WordPress installations

Greek Community

Prevent Directory Indexing

By configuring your .htaccess file
Drop the code:

Options -Indexes

By creating a blank index.php in all your subfolders:

Securing

WordPress installations

Greek Community

Prevent Image HotLinking

```
RewriteEngine on
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http(s)?://(www\.)?your-site.com [NC]
RewriteCond %{HTTP_REFERER} !^http(s)?://(www\.)?your-other-domain.com [NC]
RewriteRule \.(jpg|jpeg|png|gif)$ “http://ieikonamou.png” [NC,R,L]
```

Appendix

1.

```
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteCond %{REQUEST_METHOD} ^(HEAD|TRACE|DELETE|TRACK) [NC]
RewriteRule ^(.*)$ - [F,L]
RewriteCond %{QUERY_STRING} \.\.\/ [NC,OR]
RewriteCond %{QUERY_STRING} boot\.ini [NC,OR]
RewriteCond %{QUERY_STRING} tag\= [NC,OR]
RewriteCond %{QUERY_STRING} ftp\:  [NC,OR]
RewriteCond %{QUERY_STRING} http\:  [NC,OR]
RewriteCond %{QUERY_STRING} https\:  [NC,OR]
RewriteCond %{QUERY_STRING} (\<|%3C).*script.*(\>|%3E) [NC,OR]
RewriteCond %{QUERY_STRING} mosConfig_[a-zA-Z_]{1,21}(=|%3D) [NC,OR]
RewriteCond %{QUERY_STRING} base64_encode.*\(.*\) [NC,OR]
RewriteCond %{QUERY_STRING} ^.*(\[|\]|\(|\)|<|>|ê|"|;|\?|\*|=$).* [NC,OR]
RewriteCond %{QUERY_STRING} ^.*(&#x22;|&#x27;|&#x3C;|&#x3E;|&#x5C;|&#x7B;|&#x7C;).* [NC,OR]
RewriteCond %{QUERY_STRING} ^.*(%24&x).* [NC,OR]
RewriteCond %{QUERY_STRING} ^.*(%0|%A|%B|%C|%D|%E|%F|127\.0).* [NC,OR]
RewriteCond %{QUERY_STRING} ^.*(globals|encode|localhost|loopback).* [NC,OR]
RewriteCond %{QUERY_STRING} ^.*(request|select|insert|union|declare).* [NC]
RewriteCond %{HTTP_COOKIE} !^.*wordpress_logged_in_.*$
RewriteRule ^(.*)$ - [F,L]
</IfModule>
```

Securing

WordPress installations

Greek Community

Recommended WordPress Security Plugins

-Brute Forcing (etc)

1.Block Bad Queries (BBQ)
2. WordFence
3. WordPress Simple Firewall

-IDS

1.Acunetix WP Security
2.Sucuri
3.Ithemes Sec Pro

- Firewall +Scanners

1.Sucuri
2.Ithemes Sec Pro

Securing

WordPress installations

Greek Community

General Guide Lines

1. Maintain strong passwords.
2. Always Update Everything.
3. Protect your WordPress Admin.
4. Guard against brute Force Attacks.
5. Monitor for malware.
6. ...Then do something about malware.
7. Choose the right Web Host.
8. Always have your site cleaned.
9. Control sensitive information
10. Use any CDN Service

Securing

WordPress installations

Greek Community

11. Stay Vigilant !!!

Securing

WordPress installations

Greek Community

THANK YOU!!!