Hacking the Wordpress Ecosystem

OWASP
The Open Web Application Security Project
Dan Catalin VASILE

• Information Security Consultant
• Researcher / Writer / Presenter
• OWASP Romania Board Member

• Online presence
  – http://www.pentest.ro
  – dan@pentest.ro / @DanCVASILE
Hacking the Wordpress Ecosystem

WHY?
More numbers

As of March 2012, WordPress is on 72.4M different websites around the globe, making WordPress the most widely used and popular CMS in existence.

By the end of 2011, it was estimated that around 50% of new websites published were built using the WordPress platform.

For existing websites, the rate is around 16%.

To date, there have been 98 version releases of WordPress.

In 2011, WordPress was responsible for 14.7% of the top 1,000,000 websites in the entire world.

Just a handful of examples of sites using WordPress include Handels, the NFL, the New York Times, Ford, CNN, Harvard Law School, NASA, BBC Top Gear, TechCrunch, National Geographic, Adobe Blogs, and numerous others.

48% of the top 100 blogs, as ranked by Technorati, currently use WordPress as their CMS.

Of the 48% that use WordPress:
- 59% are self-hosted.
- 41% are WordPress hosted.

Factoid
The top three self-hosted WordPress blogs on the Technorati top 100 list are:

- Mashable
- TMZ
- WordPress SEO by Yoast

All three of these hugely popular websites currently use Yoast's WordPress SEO plugin.
TO SCARE!!!!

Attacks on:

- The Worpress platform
- Plugins
- Themes
- Infrastructure
- Humans
and TO REPAIR.

Focus on:
- Infrastructure
- Installation process
- Protective server side measures
- Protective client side measures
- Reviewing source code
- Maintenance
Physical security
Common web server vulnerabilities

- Overflows
- DoS
- Remote command execution
- XSS in internal tools
- Security Misconfiguration

... just no name a few

http://httpd.apache.org/security/vulnerabilities_22.html
PHP vulnerabilities

- DoS
- Overflows
- Remote command execution
- SQL injection
- XSS
- Source code disclosure
- RFI
- CSRF

&more
Hacking the Wordpress platform

One example from the CVE Database

<table>
<thead>
<tr>
<th>CVE-1D</th>
<th>Learn more at National Vulnerability Database (NVD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2013-4338</td>
<td>Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings</td>
</tr>
</tbody>
</table>

Description

`wp-includes/functions.php` in WordPress before 3.6.1 does not properly determine whether data has been serialized, which allows remote attackers to execute arbitrary code by triggering erroneous PHP unserialize operations.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM: http://codex.wordpress.org/Version_3.6.1
- CONFIRM: http://core.trac.wordpress.org/changelog/29325
- CONFIRM: http://wordpress.org/news/2013/09/wordpress-3-6-1/
- DEBIAN: DSA-2757
- URL: http://www.debian.org/security/2013/dsa-2757
- FEDORA:FEDORA-2013-16855
- FEDORA:FEDORA-2013-16995
- FEDORA:FEDORA-2013-16925
How many plugins are there?
27,596 PLUGINS, 536,317,915 DOWNLOADS (as of October 2013)

How many of them are vulnerable? ☺☺☺☺
Not as many as you’ve expected. CVE lists ‘only’ 164 vulnerabilities (not all related to plugins)

Fear not! New plugins everyday & new disclosures on old plugins.
Hacking the themes

Themes can be vulnerable!

They sometimes come up with other plugins necessary to get the functionality needed

Think about TimThumb vulnerability!
What is TimThumb?
A small php script for cropping, zooming and resizing web images (jpg, png, gif). Perfect for use on blogs and other applications.

The problem!
“TimThumb” essentially, caches even remote files locally, without doing any proper sanitization.

The problem for hackers
The file “timthumb.php” does however, check if to see if the target file is actually an image or not. This timthumb file is also quite often renamed to something else and is used in many themes.
The easiest way to trick TimThumb into believing a remotely stored image (that also contains evil PHP code) is an actual image (with timthumbcraft).
Uploading the file

no image specified
Query String:
TimThumb version: 1.27
Additional problems with the TimThumb hack

- When uploading the image, the php script will be located in the cache directory with a ‘random’ name.
Last but not least, hacking the human element:

- Social engineering
- Phishing
- Exploiting bad habits
Let’s start fixing the Wordpress Ecosystem

Short recap:
- Infrastructure
- Wordpress base platform
- Wordpress plugins
- Wordpress themes
- Users
INFRASTRUCTURE

- Choose a decent data-center
- Use encryption for physical disks
- Use secure communication channels with the server (SSH, SFTP); do you still use FTP? You should be banned from the world.
- Keep the Web Server, PHP and Database updated to the latest version
- Secure configurations (disable directory listing, secure php.ini configuration, etc.)
- Log and analyze
WORDPRESS PLATFORM - INSTALLATION

- Always download the platform from a trusted source; use https://wordpress.org/download/
- Change the default ‘admin’ username
- Set a strong password
- Change the default ‘wp_’ table prefix
- Set an insane database password
- Move wp-config.php outside /public_html
WORDPRESS PLATFORM - MAINTENANCE

- BACKUP!!! ([BackWPup](https://backwpup.com) plugin)
- Update!
- Use SSL for authentication
- Use CAPTCHA for logging in ([Captcha on Login](https://captchaonlogin.com) plugin)
- Limit the access to /wp-admin (form .htaccess)
- Source code audit
THEMES

- Update
- Review the code
PLUGINS

- Delete unused plugins
- Update
- Review ratings and user comments
- Source code audit
Fixing the users

OWASP
The Open Web Application Security Project

USERS

- Awareness
- Set user roles and give only the privileges they need
- Log & audit user actions ([ARYO Activity Log](https://www.aryo.com/products/aryo-activity-log-plugin))
- Personal computer security
- Enforce the use of strong passwords ([Minimum Password Strength](https://www.aryo.com/products/password-strength-plugin)) plugin
Install one or more security plugins

- Login Security Solution
- AntiVirus
- WP Security Scan
- WordPress File Monitor Plus
- OSE Firewall Security
- Block Bad Queries
- Wordfence
Monitor the website from an external party

- **Website Defender**
- **Pingdom**
- **Change Detection**
Source code audit

Every line of code audited

September 10, 2012 in Development, WooThemes News

Over the past few months we’ve been working very closely with the Sucuri Security team who we commissioned to do a full audit of our core products’ codebase. We’ve already released WooSlider and WooDojo with Sucuri Security’s stamp of approval, and today we are happy to announce that the WooFramework — the engine that powers each and every one of our WordPress themes — is now also Sucuri safe.
If you know what you’re doing, do the whole ecosystem yourself.

Otherwise go with a managed solution:
• Wordpress.org
• Wpengine.com
• Godaddy.com
Etc.
Wordpress Security Checklist project on OWASP

My part:
- Establish the structure
- Contribute with content

I need help for:
- Content
- Plugin suggestions and reviews
- Source code audits
Thank you!