Hacking the *Wordpress* Ecosystem

OWASP

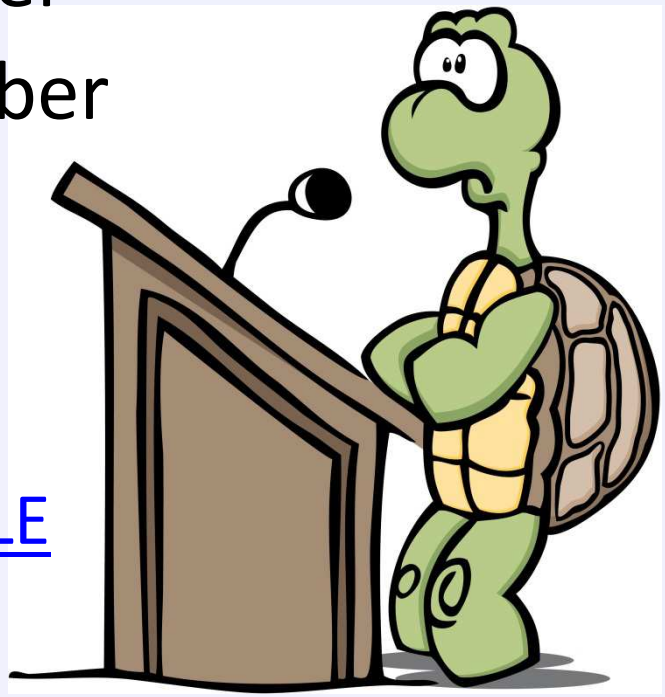
The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

Dan Catalin VASILE

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

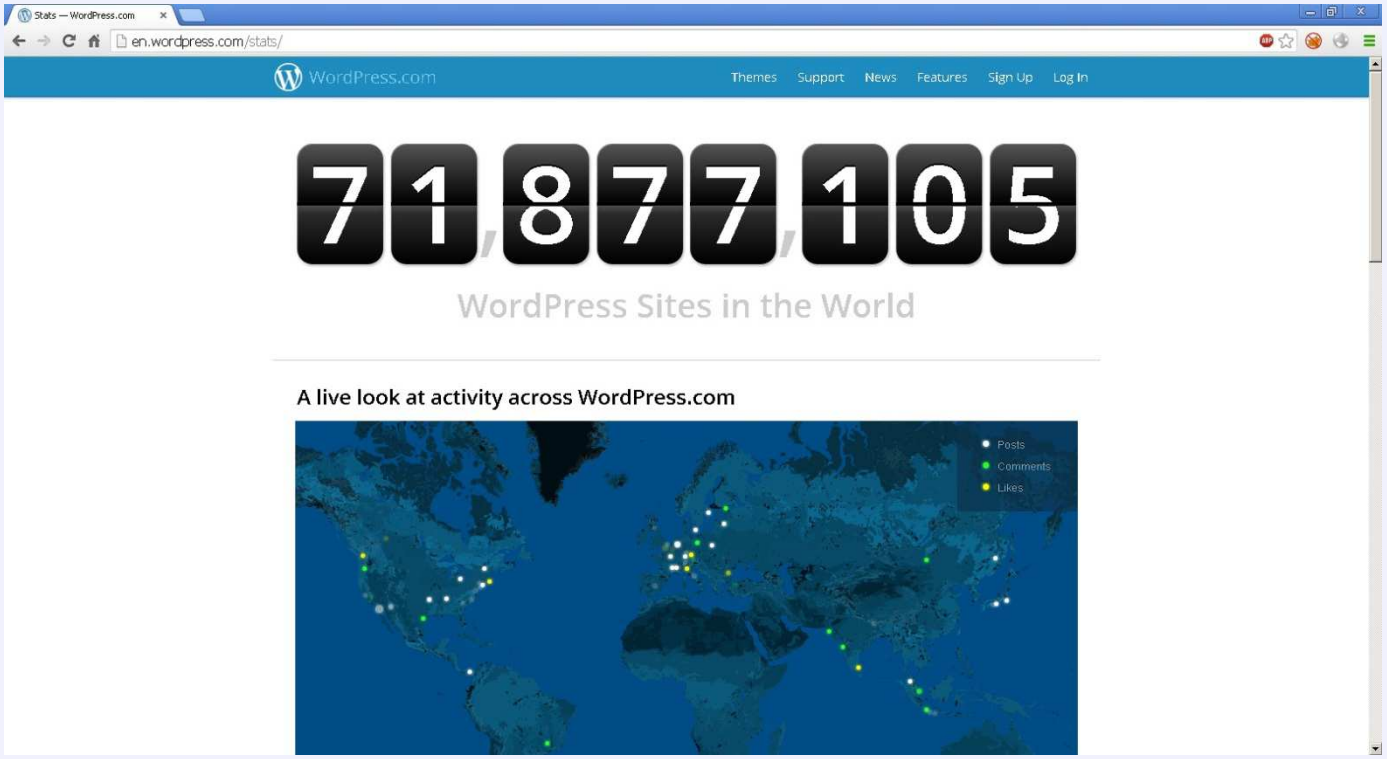


- Online presence
  - http://www.pentest.ro
  - dan@pentest.ro / @DanCVASILE

OWASP
The Open Web Application Security Project

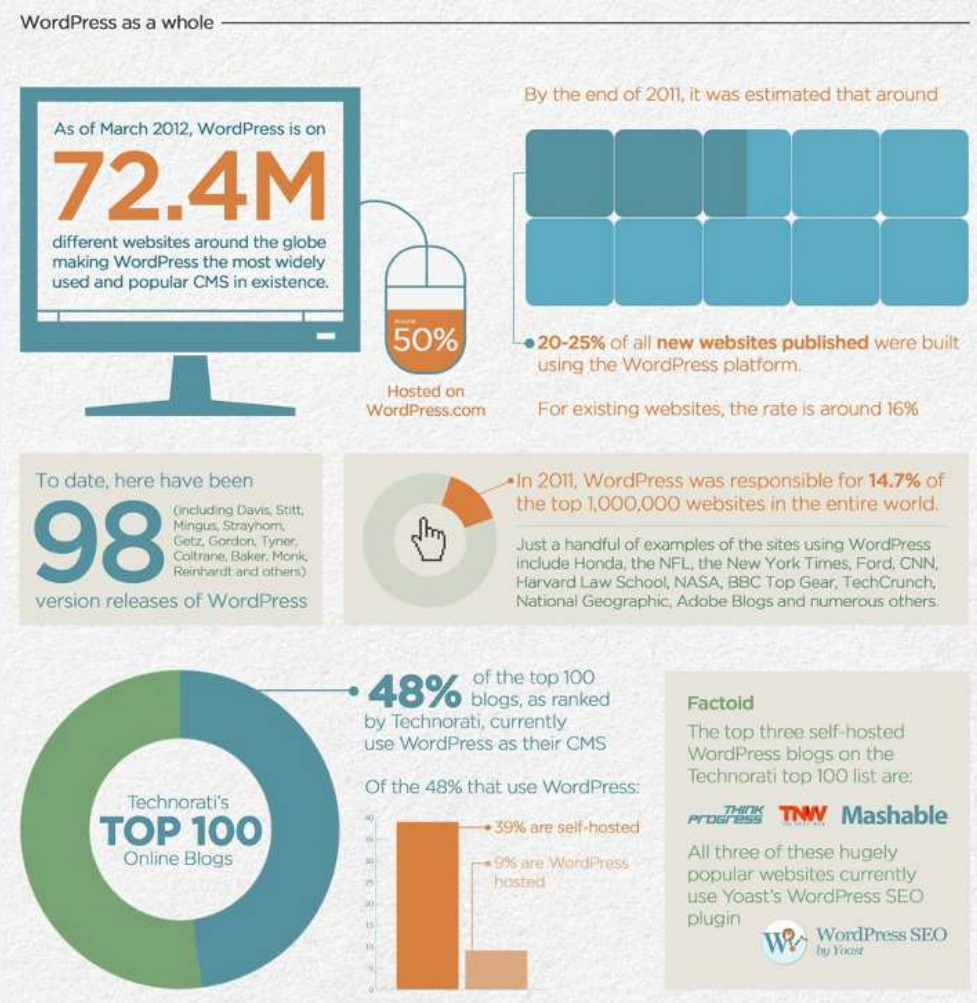
Hacking the Wordpress Ecosystem

WHY?



OWASP
The Open Web Application Security Project

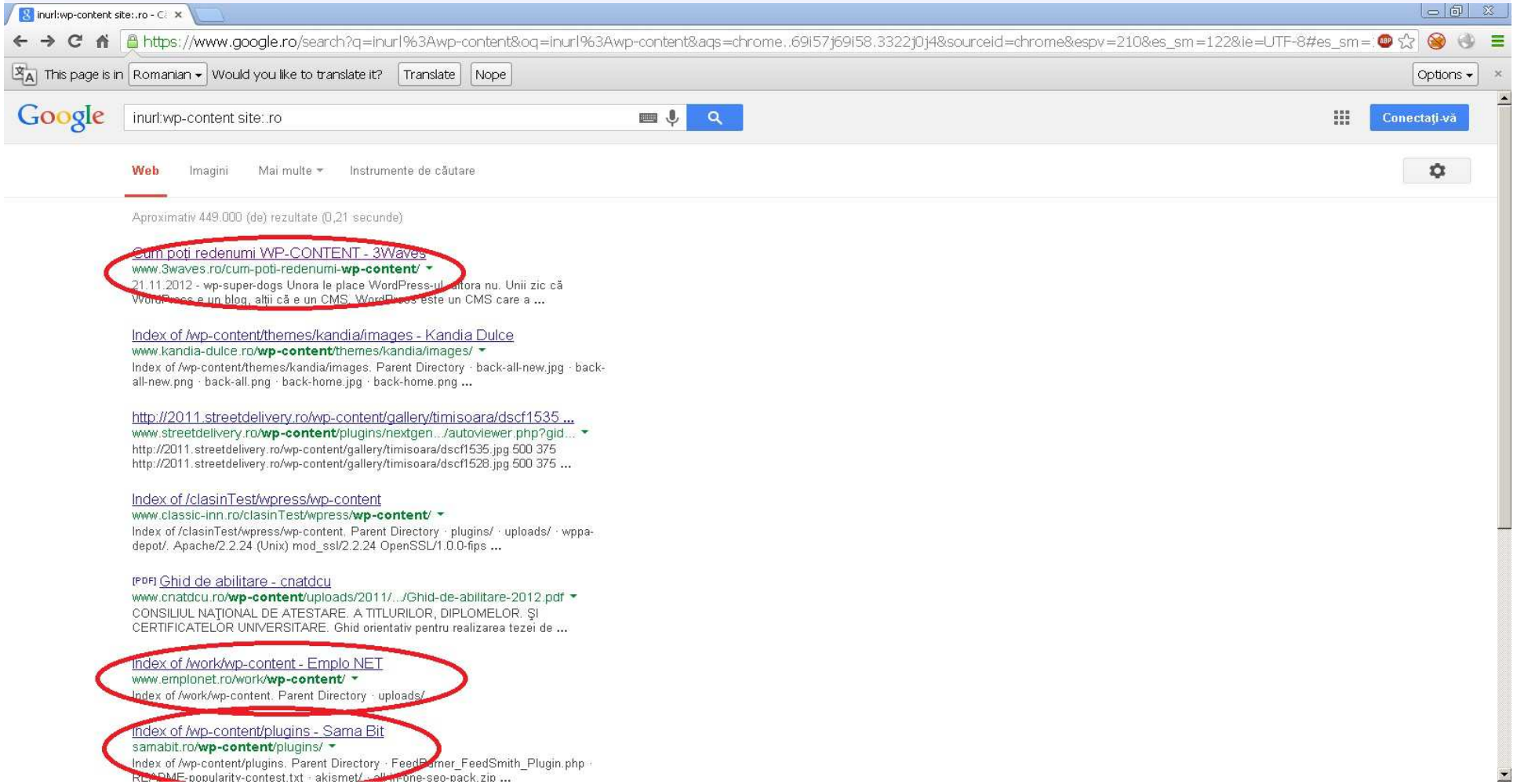
More numbers



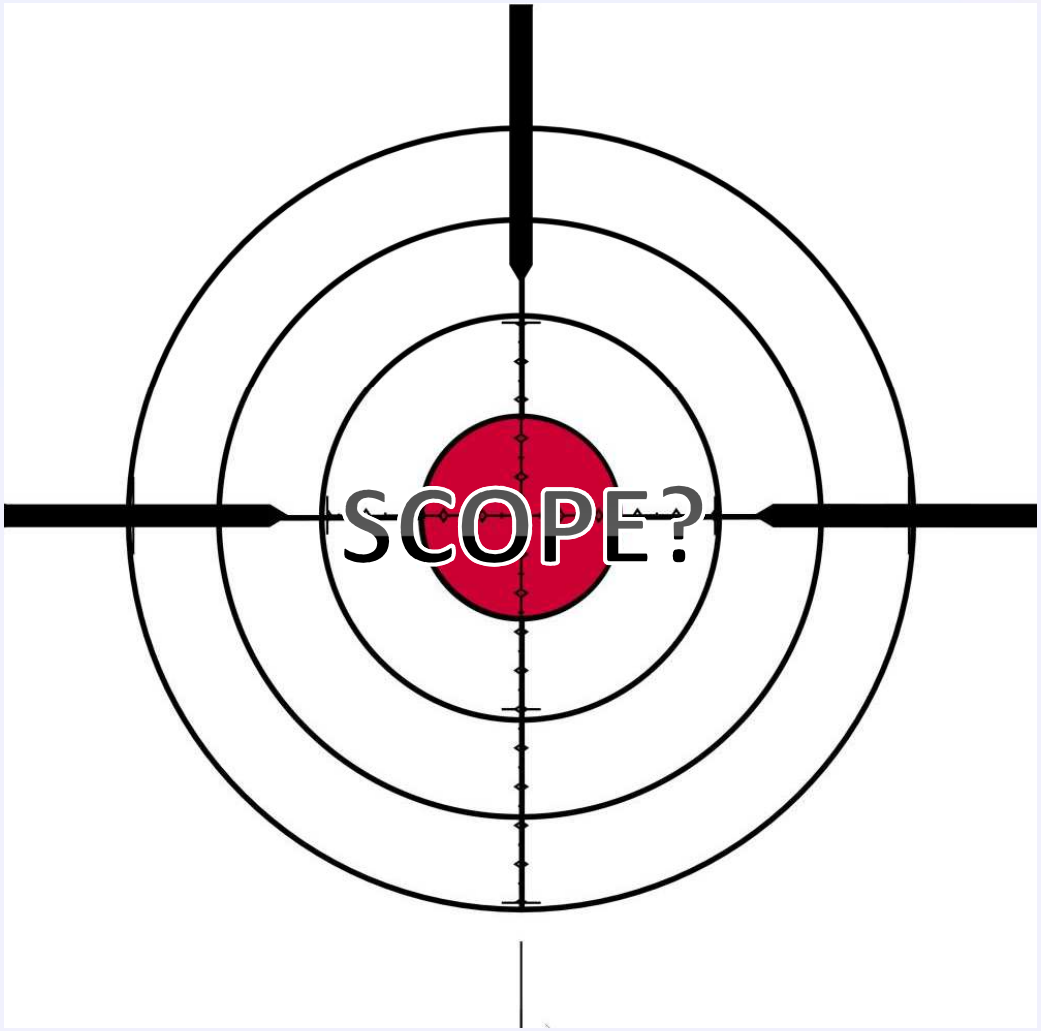
About the talk

OWASP
The Open Web Application Security Project

Finding Wordpress!



Scope



Scope

TO SCARE!!!!

Attacks on:

- The Worpress platform
- Plugins
- Themes
- Infrastructure
- Humans

OWASP
The Open Web Application Security Project

and TO REPAIR.

Focus on:

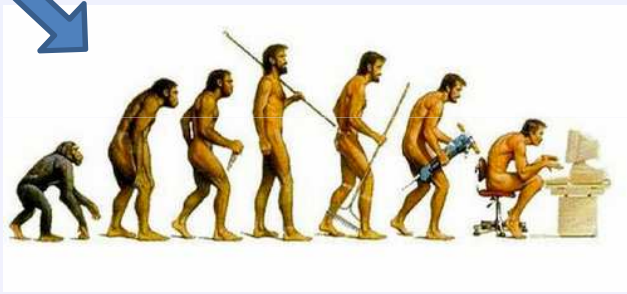
- Infrastructure
- Installation process
- Protective server side measures
- Protective client side measures
- Reviewing source code
- Maintenance

Wordpress Ecosystem

OWASP
The Open Web Application Security Project

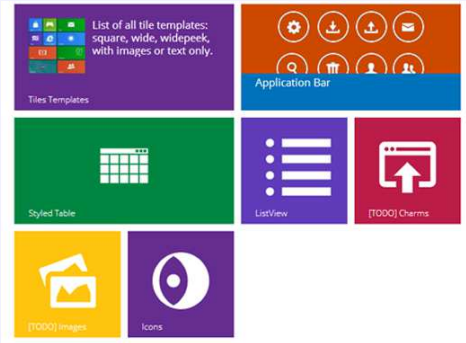
Infrastructure

Base platform



Users

Themes



Plugins

OWASP
The Open Web Application Security Project

Physical security

OWASP
The Open Web Application Security Project

Common web server vulnerabilities

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

… just no name a few

& more

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

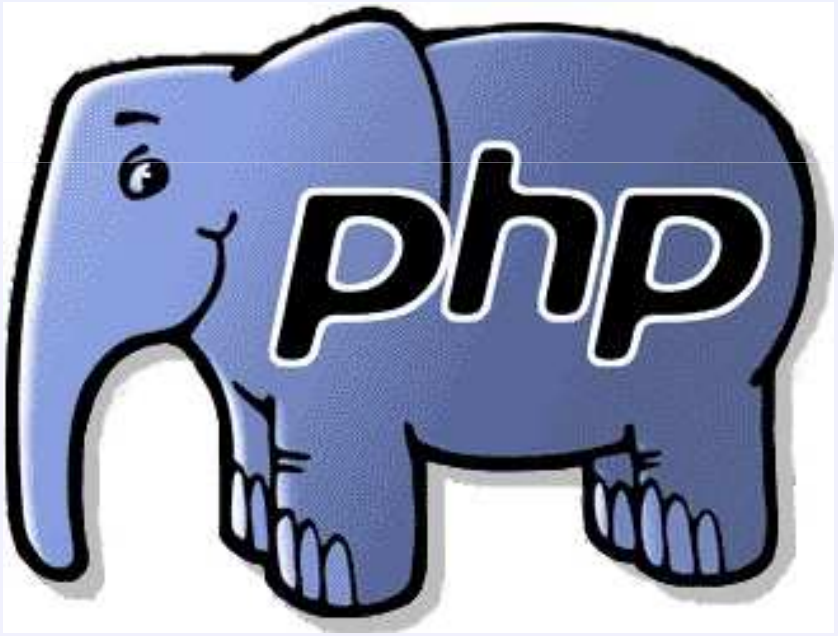
OWASP
The Open Web Application Security Project

PHP vulnerabilities

- DoS
- Overflows
- Remote command execution

- SQL injection
- XSS
- Source code disclosure
- RFI
- CSRF

&more



OWASP
The Open Web Application Security Project

One example from the CVE Database

CVE-ID
CVE-2013-4338 Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
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/changeset/25325
- 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
- URL:http://lists.fedoraproject.org/pipermail/package-announce/2013-September/116828.html
- FEDORA:FEDORA-2013-16895
- URL:http://lists.fedoraproject.org/pipermail/package-announce/2013-September/117118.html
- FEDORA:FEDORA-2013-16925
- URL:http://lists.fedoraproject.org/pipermail/package-announce/2013-September/116832.html

OWASP
The Open Web Application Security Project

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

OWASP
The Open Web Application Security Project

Themes can be vulnerable!

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

Think about TimThumb vulnerability!

OWASP
The Open Web Application Security Project

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.

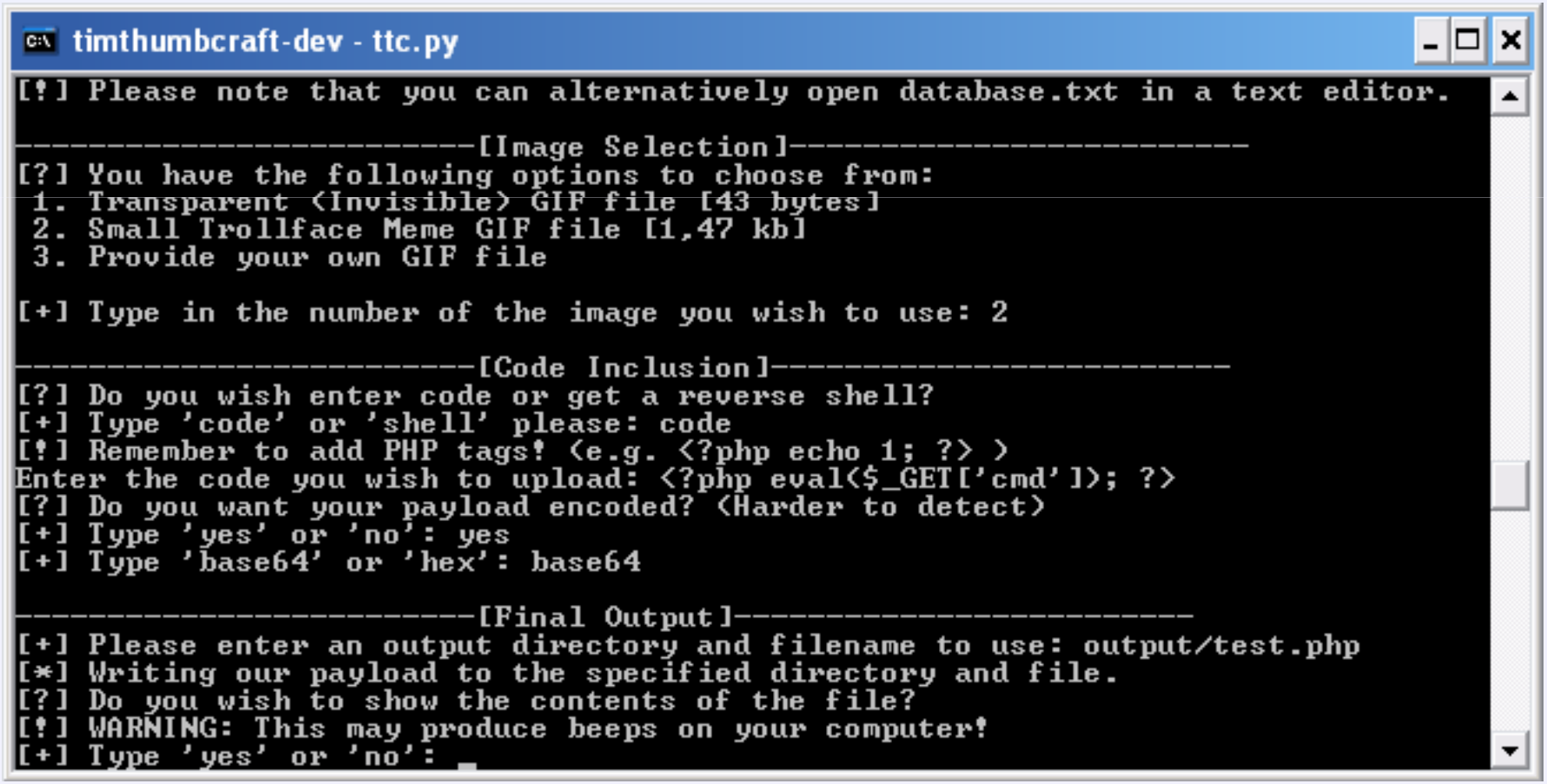
The problem for hackers

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.

TimThumb hack

OWASP
The Open Web Application Security Project

The easiest way to trick TimThumb into believing a remotely stored image (that also contains evil PHP code) is an actual image (with timthumbcraft)



TimThumb hack

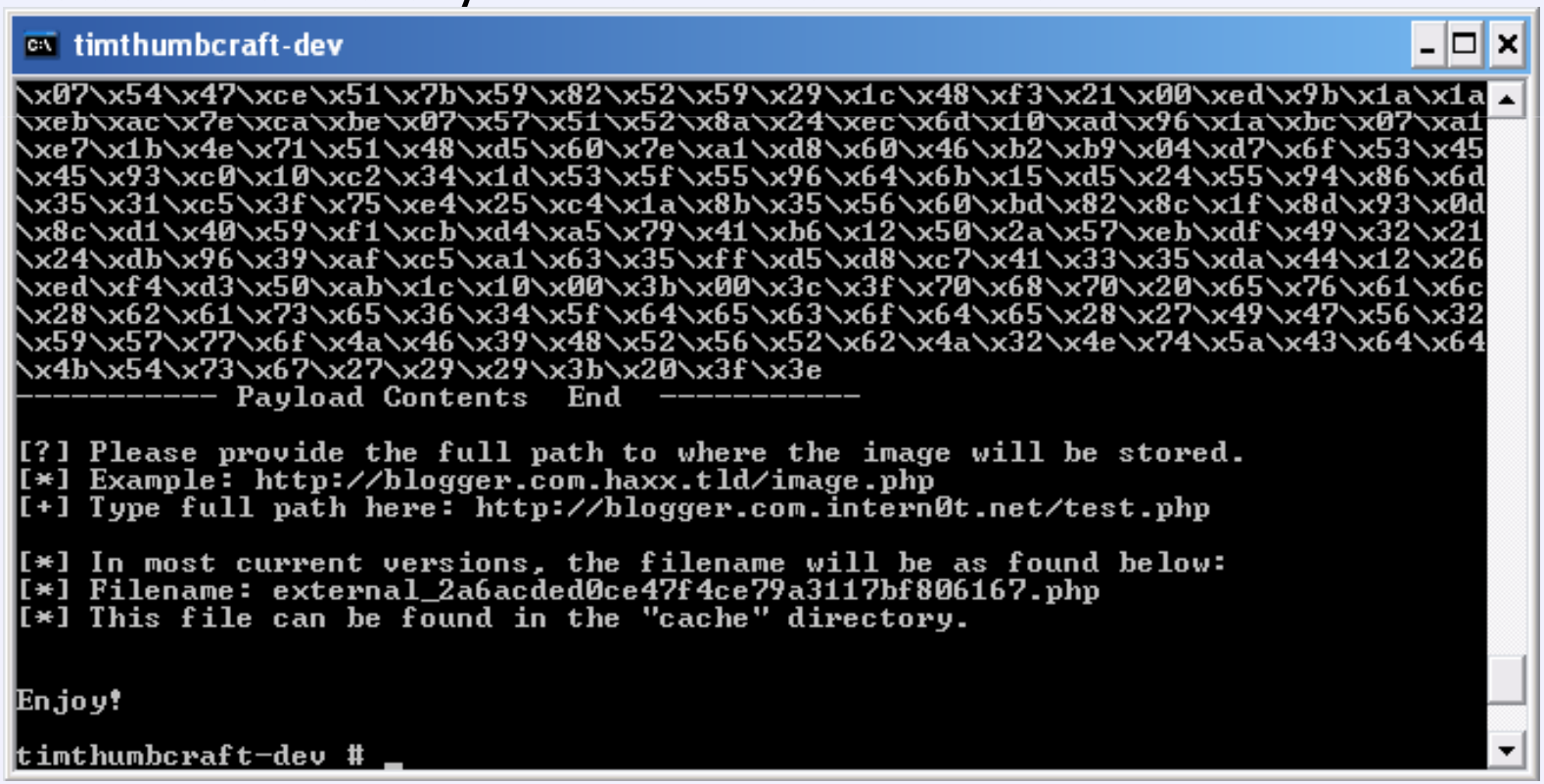
OWASP
The Open Web Application Security Project

Uploading the file

OWASP
The Open Web Application Security Project

Additional problems with the TimThumb hack

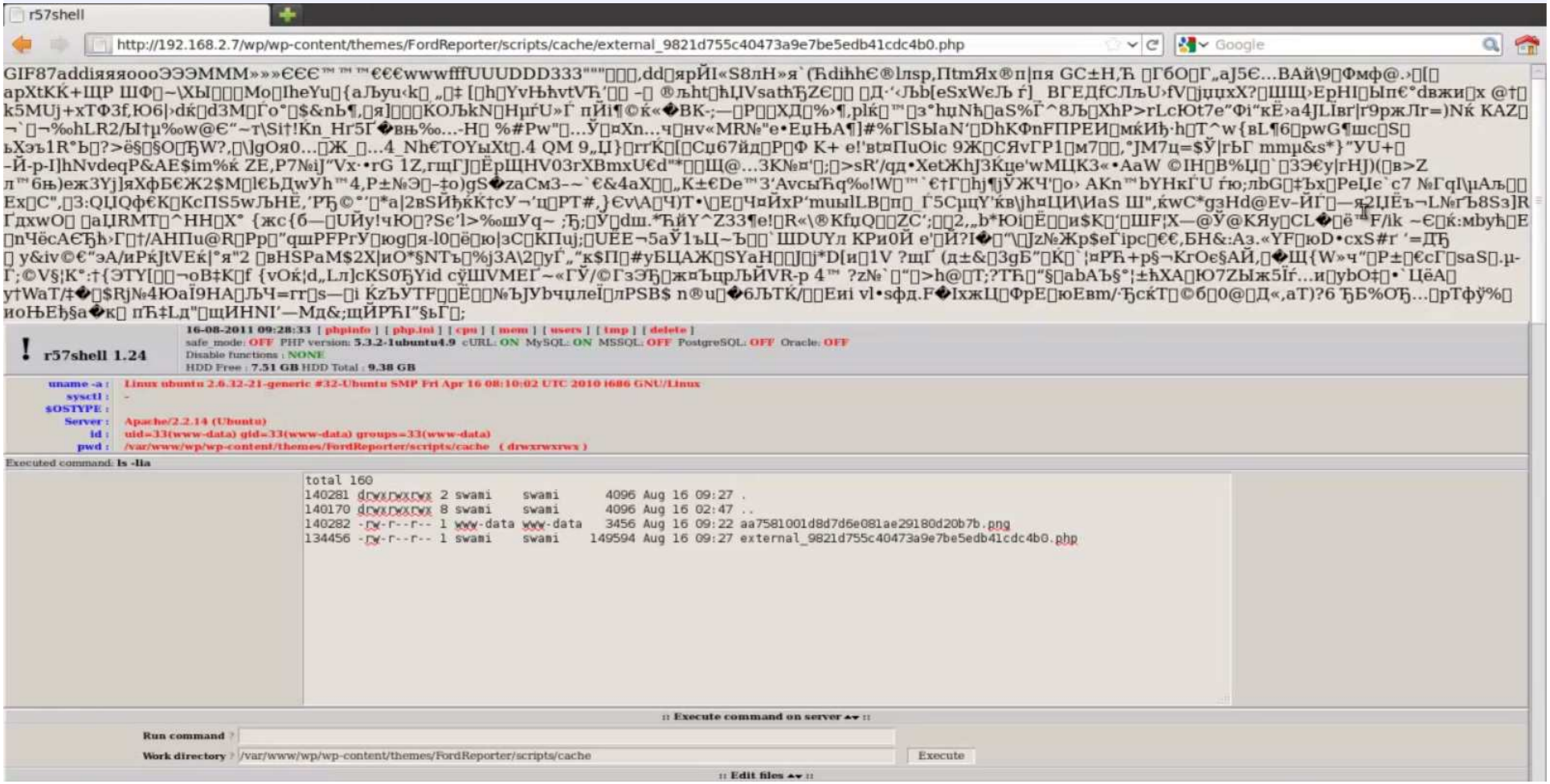
- When uploading the image, the php script will be located in the cache directory with a ‘random’ name



TimThumb hack

OWASP
The Open Web Application Security Project

We're IN!

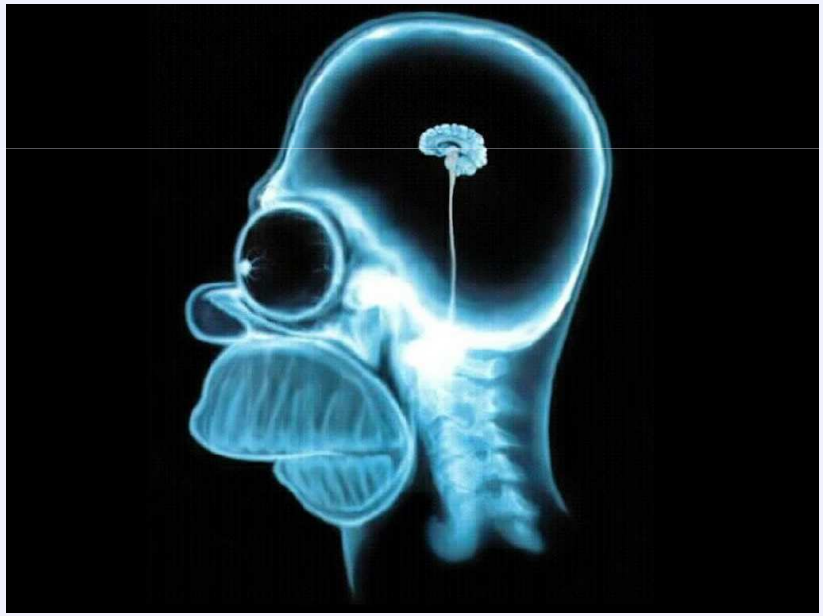


Hacking the users

OWASP
The Open Web Application Security Project

Last but not least, hacking the human element:

- Social engineering
- Phishing
- Exploiting bad habits



Let’s fix it

OWASP
The Open Web Application Security Project

Let’s start fixing the Wordpress Ecosystem

Short recap:

- Infrastructure
- Wordpress base platform
- Wordpress plugins
- Wordpress themes
- Users

OWASP
The Open Web Application Security Project

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

OWASP
The Open Web Application Security Project

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

OWASP
The Open Web Application Security Project

WORDPRESS PLATFORM - MAINTENANCE

- BACKUP!!! (BackWPup plugin)
- Update!
- Use SSL for authentication
- Use CAPTCHA for logging in (Captcha on Login plugin)
- Limit the access to /wp-admin (form .htaccess)
- Source code audit

Fixing the themes

OWASP
The Open Web Application Security Project

THEMES

- Update
- Review the code

OWASP
The Open Web Application Security Project

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 plugin)
- Personal computer security
- Enforce the use of strong passwords (Minimum Password Strength plugin)

Further actions

OWASP
The Open Web Application Security Project

Install one or more security plugins

- Login Security Solution
- AntiVirus
- WP Security Scan
- WordPress File Monitor Plus
- OSE Firewall Security
- Block Bad Queries
- Wordfence

Further actions

Monitor the website from an external party

- WebsiteDefender
- Pingdom
- Change Detection

OWASP
The Open Web Application Security Project

Source code audit

Mark Forrester

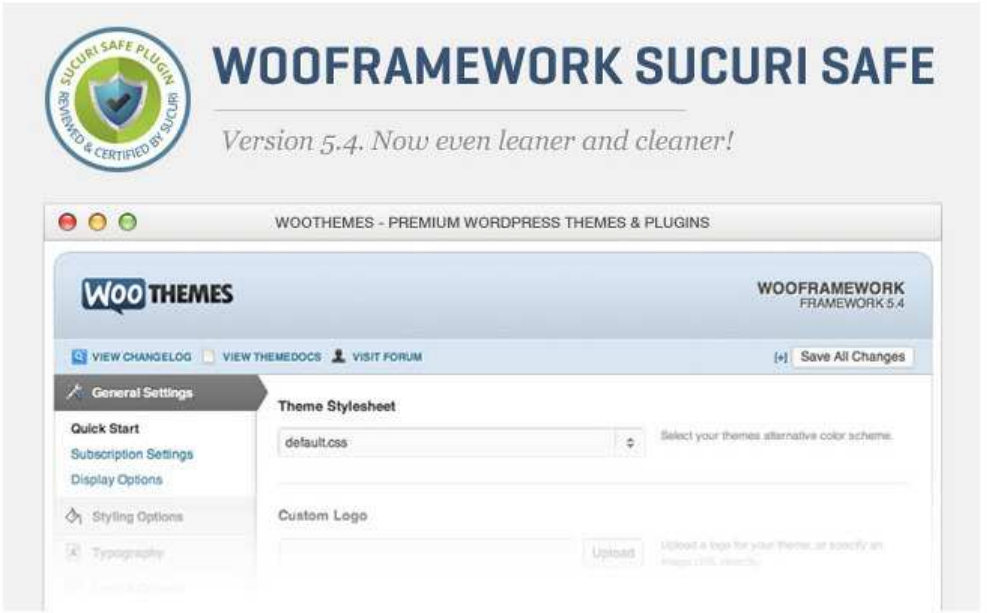
126

91

19

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.

What to do

OWASP
The Open Web Application Security Project

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.

Goal

OWASP
The Open Web Application Security Project

Wordpress Security Checklist project on OWASP
https://www.owasp.org/index.php/OWASP_Wordpress_Security_Checklist_Project

My part:
- Establish the structure
- Contribute with content

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

OWASP
The Open Web Application Security Project

Thank you!