CMS audit, ask more than the release number

A. Cervoise
antoine.cervoise@devoteam.com

July 8, 2013
Summary

1. **Introduction**

2. **World most used CMS**

3. **Why and how audit a CMS?**

4. **Tools for blackbox auditing most used CMS**

5. **Conclusion**
Who am I?

IT Security Consultant
- Vulnerability watching
- Incident response
- Security compliance

CMS knowledge
- As an administrator
- As an incident response engineer
- As a vulnerability researcher
Why am I doing this talk?

CMS are often forgotten

- security recommendations
- patch management
- pentest planning

Give some basic security knowledge to secure CMS

Tools

- Present you some tools
  - I am not a (main) developer from WPScan, joomscan, etc.
- Give some truth about some tools you may have heard about
Sumary

1. Introduction

2. World most used CMS

3. Why and how audit a CMS?
   - Why?
   - How to? Make it fast or make it clean

4. Tools for blackbox auditing most used CMS
   - Some oversold products
   - Joomscan
   - WPScan

5. Conclusion
Be careful!

Tools used in the following screenshots could be run with:

- `./toolname.ext` or `script_language toolname.ext`
- `toolname`

Since Kali Linux, all tools are included in the PATH!
Summary

1. Introduction
2. World most used CMS
3. Why and how audit a CMS?
4. Tools for blackbox auditing most used CMS
5. Conclusion
World most used CMS

What is a CMS?

- Content Management System

Why use a CMS?

- You don't need
  - Development knowledge
  - Graphical skills
- You get
  - Something quickly functional
  - Modularity with plugins
World most used CMS

- Some CMS:
  - Joomla!
  - Spip
  - WordPress
  - Blogger
  - Typo3
  - Drupal
  - DotNetNuke
  - PHPNuke
  - Etc.
## World most used CMS

### Top in Content Management System

The most popular CMS technologies on the internet.

<table>
<thead>
<tr>
<th>Name</th>
<th>Websites</th>
<th>Usage 10k %</th>
</tr>
</thead>
<tbody>
<tr>
<td>WordPress</td>
<td>7,547,067</td>
<td>8.78</td>
</tr>
<tr>
<td>Joomla!</td>
<td>1,869,060</td>
<td>0.36</td>
</tr>
<tr>
<td>Drupal</td>
<td>519,234</td>
<td>3.26</td>
</tr>
<tr>
<td>Blogger</td>
<td>271,019</td>
<td>0.2</td>
</tr>
</tbody>
</table>

**Figure:** [http://trends.builtwith.com/cms](http://trends.builtwith.com/cms) (04/17/2013)
# World most used CMS

![W3Techs](http://w3techs.com/technologies/overview/content_management/all)

<table>
<thead>
<tr>
<th>None</th>
<th>67.9%</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WordPress</strong></td>
<td>54.7%</td>
</tr>
<tr>
<td><strong>Joomla</strong></td>
<td>8.4%</td>
</tr>
<tr>
<td><strong>Drupal</strong></td>
<td>7.1%</td>
</tr>
<tr>
<td><strong>Blogger</strong></td>
<td>3.9%</td>
</tr>
<tr>
<td><strong>vBulletin</strong></td>
<td>3.5%</td>
</tr>
</tbody>
</table>

**Figure:**
http://w3techs.com/technologies/overview/content_management/all (04/17/2013)
World most used CMS

Figure: https://twitter.com/WordPress, https://twitter.com/drupal and https://twitter.com/joomla
World most used CMS

WordPress Users
The New York Times
People
... and hundreds more

Figure: http://wordpress.org/ and http://wordpress.org/showcase/tag/celebrities/ (04/17/2013)
World most used CMS

Figure: (04/17/2013) http://www.joomla.org/
World most used CMS

Sites Made with Drupal

Figure: http://drupal.org/ and http://drupal.org/case-studies/featured/25214 (04/17/2013)
Summary

1. Introduction
2. World most used CMS
3. Why and how audit a CMS?
   - Why?
   - How to? Make it fast or make it clean
4. Tools for blackbox auditing most used CMS
5. Conclusion
Why audit CMS?

- They are used by companies as intranet or internet websites or applications
- They are the first step to get in your system
Why?

Attack scenarios

Scenario 1

CMS on a DMZ server:

- CMS allows file upload
- Server allows privilege escalation (PHP vulnerability)

Attack 1

- CMS allows file upload $\rightarrow$ Code execution
- PHP allows privilege escalation $\rightarrow$ Root privilege on a server in your DMZ
Why?

Attack scenarios

Scenario 2
CMS on an external server, uses for your mailing campaign.
- CMS allows XSS

Attack 2
- CMS allows XSS → Stealing admin credential
- Use your CMS for spam or stealing your customer DB
Why?

Attack scenarios

Other cases

CMS vulnerable with ...

- Apache running as root
- CMS got a root account in MySQL
- etc.
Auditing CMS

Quick and dirty audit

- Which CMS?
- Which version?
- Is it vulnerable to known vulnerabilities?
Auditing CMS

Which CMS?
- Each CMS got its own spec (headers, files, admin dirs)

Which version?
- Headers can change between versions
- Look for new files
- Look for specific file hashes
Auditing CMS

Is it vulnerable to known vulnerabilities?

- CVE bulletins
- Editor bulletins
- Exploit-db, securityfocus
- etc.
Auditing CMS - Tools

- Your browser
  - Look into the HTML code, lazy guys

<meta name="Generator" content="Drupal 7 (http://drupal.org)" />

<meta name="generator" content="WordPress 3.5.1" />
Auditing CMS - Tools

- Wappalyzer (Firefox plugin)
Auditing CMS - Tools

- whatweb

```bash
root@kali:~# whatweb 192.168.56.101/Drupal/drupal7
/usr/lib/ruby/1.9.1/rubygems/custom_require.rb:36:in `require': iconv will be deprecated in the future, use String#encode instead.
http://192.168.56.101/Drupal/drupal7/ [301] Apache[2.2.22], Country[RESERVED][ZZ], HTTPServer[Windows (32 bit)][Apache/2.2.22 (Win32) PHP/5.2.2], IP[192.168.56.101], PHP[5.2.2], RedirectLocation[http://192.168.56.101/Drupal/drupal7/], Title[301 Moved Permanently]
http://192.168.56.101/Drupal/drupal7/ [200] Apache[2.2.22], Country[RESERVED][ZZ], Drupal, HTTPServer[Windows (32 bit)][Apache/2.2.22 (Win32) PHP/5.2.2], IP[192.168.56.101], Jquery, MetaGenerator[Drupal 7 (http://drupal.org)], PHP[5.2.2], PasswordField[pass], Script[text/javascript], Title[Welcome to localhost | localhost], UncommonHeaders[x-generator], X-Powered-By[PHP/5.2.2]
```
Audition CMS - Tools

- **BlindElephant.py**

BlindElephant.py 192.168.56.101/Drupal/drupal7 drupal

Loaded /usr/lib/python2.7/dist-packages/blindelephant/dbs/drupal.pkl with 145 versions, 478 differentiating paths, and 434 version groups.

Starting BlindElephant fingerprint for version of drupal at http://192.168.56.101/Drupal/drupal7

Hit http://192.168.56.101/Drupal/drupal7/CHANGELOG.txt

[...]

Hit http://192.168.56.101/Drupal/drupal7/misc/drupal.css

File produced no match. Error: Failed to reach a server: Not Found

Fingerprinting resulted in: 7.14

**Best Guess: 7.14**
Audition CMS - Tools

- BlindElephant.py

BlindElephant.py 192.168.56.101/WordPress/wordpress-3.5.1/wordpress

Loaded /usr/lib/python2.7/dist-packages/blindelephant/dbs/wordpress.pkl with 293 versions, 5389 differentiating paths, and 480 version groups.

Starting BlindElephant fingerprint for version of wordpress at http://192.168.56.101/WordPress/wordpress-3.5.1

[...]


File produced no match. Error: Retrieved file doesn’t match known fingerprint. fde5de4cc6965fed45dc224cf43a27ed

[...]

Best Guess: 3.4.2
Auditing CMS

How to secure a CMS? (non-exhaustive)

- Keep up to date
  - the CMS
  - plugins/themes (themes are also vulnerable!)
- Don’t use some exotical plugins/themes
- Uninstall unused functionnalities (plugins/themes)
- Disable natives unused functionnalities
- Remove unused files (readme, install dir, etc.)
- Use strong password
- Configure your chmod
Auditing CMS

Complete audit

- Which
  - CMS
  - plugins/themes (themes are also vulnerable!)
  - versions
- Are they vulnerable to some known vulnerabilities (or to easy 0day)?
- What configuration?
- Usernames (and passwords)
Auditing CMS

Automatisation or partial automatisation

- Detect CMS/plugins/themes used, their versions and their configurations
- Look if versions are vulnerable
- Bruteforce authentication

What tools on the internet?

- WordPress Version Checker
- DPScan
- Joomscan
- WPScan
Auditing CMS

Simple scripts
- WordPress Version Checker
- DPScan

(Real) software
- Joomscan
- An OWASP project
- WPScan
Summary

1. Introduction

2. World most used CMS

3. Why and how audit a CMS?

4. Tools for blackbox auditing most used CMS
   - Some oversold products
   - Joomscan
   - WPScan

5. Conclusion
Some oversold products

- Simple Scripts
  - WordPress Version Checker
  - DPScan
- What is said on the internet?
- What do they really do?
- Another badass script from hell
Some oversold products

Some oversold products - WordPress Version Checker

- WordPress Version Checker
- What is said on the internet?

**Sécurité WordPress : Détecter la version du CMS via un hash MD5 c’est possible !**

2 octobre 2012 - 1 commentaire

Publié par UnderNews Actu

Les pirates informatiques sont très malins et exploitent la moindre astuce découverte afin de toucher un maximum de sites Web via leurs exploits développés exprès. Aujourd’hui, c’est une nouvelle technique de détection de la version du CMS WordPress qui fait son apparition.

*Figure:* http://www.undernews.fr/reseau-securite/securite-wordpress-detecter... (06/30/2013)
Some oversold products

Some oversold products - WordPress Version Checker

- WordPress Version Checker
- What does it do?
Some oversold products

Some oversold products - WordPress Version Checker

- WordPress Version Checker
- What does it do?
  - Just get MD5 sum of `/wp-includes/js/tinymce/tiny_mce.js`
  - Is given with a MD5 sum list
Some oversold products - WordPress Version Checker

- WordPress Version Checker
  - Method is not new (BlindElephant.py, WPScan)
  - Limitations
    - Do not work with WordPress older than 2.0
    - Do not give a specific version
    - Do not compare MD5 with the one in list
    - Code on pastebin
    - Original MD5 list is false
Some oversold products

Some oversold products - DPScan

- **DPScan**
- **What is said on the internet?**

**DPScan Drupal Security Scanner Tutorial**

There are different CMS (content management system) are available like wordpress, Joomla, light CMS and Drupal. Security of each CMS is very important and as a penetration tester we need to make a website secure by doing a penetration testing on it. There are different tools available to enumerate into wordpress and joomla and to find the known vulnerabilities in wordpress and joomla but there is no tool for other common content management system like drupal.

All Eloualiq has released a wonderful tool to enumerate into drupal based CMS, this is the simple python script and anyone can easily use it. This tutorial will show you how DPScan enumerate the modules used by the drupal CMS.

First of all go and download DPScan, I am using backtrack 5 R1 machine for this tutorial that has python by default but if you are using some other operating system like Windows and other Linux distribution then install python first.

Open your terminal and then locate the directory where you have download the python script of DPScan, remember you can copy the script and then paste in your word editor than save it to whatever.py

**Figure:** [http://www.ehacking.net/2012/02/dpscan-drupal-security-scanner-tutorial.html](http://www.ehacking.net/2012/02/dpscan-drupal-security-scanner-tutorial.html) (04/18/2013)
Some oversold products

Some oversold products - DPScan

- DPScan
- What is said on the internet?

The First Security scanner for Drupal CMS has been released by Ali Elouafiq, on his Blog. His team develop a tool that will enumerate at least the modules used by Drupal so we can simulate a White Box audit on our private machines.

This small tool is public and accessible to you for use however you please. It may help other auditors or penetration testers do their job faster. Here is a little demonstration. After downloading the script (in python), you simply type:

> python DPScan.py [website url]

**Figure:** [http://www.thehackinguniverse.com/2012/06/dpscan-drupal-security-scanner.html](http://www.thehackinguniverse.com/2012/06/dpscan-drupal-security-scanner.html) (04/18/2013)
Some oversold products - DPScan

- **DPScan**
  - Real name: DRUPAL Modules Enumerator
  - What does it do?
    - Analyze a HTML page (a file or with wget)
    - Looks for pattern `modules/module_name`
    - Return the list of modules

DRUPAL Modules Enumerator v0.1beta-- written by Ali Elouafiq 2012

```
<ScriptName> [filename.txt]
<ScriptName> [URL]
<ScriptName> [URL] user password // FOR HTTP AUTHORIZATION
```
Some oversold products

Some oversold products - DPScan

- **DPScan**
  - Limitations
    - Limit the investigation to what is shown
    - Lots of bugs
    - Original code is unavailable at original URL
  - Version 0.3beta which corrected theses points here: https://github.com/cervoise/DPScan
Some oversold products

**Some oversold products - CMTE**

- Detect plugins/themes from any CMS
  - Method: BruteForce
  - Bases: CMS with plugins/themes path and plugins and themes list
Some oversold products - CMTE

Usage

- `python cmte.py url`
- Choose your CMS

```
python cmte.py 192.168.56.101/Drupal/drupal_commerce
```

Choose your CMS:
[1]: wordpress
[2]: wordpress_themes
[3]: drupal
[4]: drupal_theme
[...]
[13]: mediawiki
[14]: guppy
```
### Usage

- **Brute-force from lists**

After scan, try to go `192.168.56.101/Drupal/drupal_commerce/modules`, you could get more info.

41 modules or themes to check
41 modules or themes already checked
40 module(s) or theme(s) found:
aggregator
[...]
user
Some oversold products

Some oversold products - CMTE

Project architecture

- `cms-list.txt` → list of CMS and path
- `databases/` → dir with modules/themes lists
- `get-mt-list/` → scripts for get some lists from the net
- `readme.txt`
- `todo.txt`
Some oversold products

Some oversold products - CMTE

How to add CMS

- Get module dir
  - For example, in Drupal modules are in /modules
- Add it in CMS base:
  - drupal:modules
- Add a list of modules
  - in /databases/drupal.txt
Some oversold products

Some oversold products - CMTE

Automatic modules list

- WordPress
  - Use WPScan databases
- TYPO3 and SPIP
  - Plugins dir names are on official websites
  - Crawl official websites for getting all of them
Some oversold products

Some oversold products - CMTE

SPIP

CFG
Gestion de configurations.

PORTE PLUME
Une barre d'outil pour bien écrire

IMAGES
Filtres de transformation d'images et de couleurs

SAFEHTML
Protection des forums contre le cross-site scripting

SUPPORT VIEUX NAVIGATEURS
PNG et sélecteurs CSS pour les vieux navigateurs

TYPO3

5010 extensions found

TD Calendar
by Thomas Dutzak
A Calendar Script based on functionality of JMY Calendar
Version 0.2.10
Last Updated April 18, 2013
Downloads 1,038
Manual Not yet rendered

myComments
by Armin Riediger-Vieweg
Simple and powerful extension for providing comments.
Version 1.2.0 Stable
Last Updated April 18, 2013
Downloads 472
Manual Not yet rendered

PageType Creator
by David Jötschke
creates new types of pages (doctypes) for various uses
Version 1.1.1 Beta
Last Updated April 18, 2013
Downloads 419
Manual Not yet rendered

Orphan Files
by Den Ursulya
This backend extension finds any file uploaded by an editor which is not used anymore in the CMS
Version 0.1.0
Last Updated April 18, 2013
Downloads 2
Manual Read online

Automatic base url
by Matthieu Tocanne
Add automatically base url based on current domain
Version 1.2.0 Stable
Last Updated April 18, 2013
Downloads 0
Manual Not available
Some oversold products

Some oversold products - CMTE
Some oversold products

Some oversold products - CMTE

<table>
<thead>
<tr>
<th>TD Calendar</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>by Thomas Dudzak</td>
<td></td>
</tr>
<tr>
<td>A Calendar Script based on functionality of JW Calendar</td>
<td></td>
</tr>
<tr>
<td>Version</td>
<td>0.2.10</td>
</tr>
<tr>
<td>Last Updated</td>
<td>April 18, 2013</td>
</tr>
<tr>
<td>Downloads</td>
<td>1,038</td>
</tr>
<tr>
<td>Manual</td>
<td>Not yet rendered</td>
</tr>
</tbody>
</table>
Some oversold products

Some oversold products - CMTE

**Evolution**

- Add an update function using the scripts for automatic modules lists
- Add a CMS detection at the beginning of the script

**GitHub**

https://github.com/cervoise/CMTE
Some oversold products

Some oversold products - CMTE

Alternative
- Use pattern and plugins lists in DirBuster
Some oversold products - CMTE

```
<table>
<thead>
<tr>
<th>OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File</strong></td>
</tr>
<tr>
<td><strong>Target URL (eg <a href="http://example.com:80/">http://example.com:80/</a>)</strong></td>
</tr>
<tr>
<td><a href="http://192.168.56.101">http://192.168.56.101</a></td>
</tr>
<tr>
<td><strong>Work Method</strong></td>
</tr>
<tr>
<td>○ Use GET requests only</td>
</tr>
<tr>
<td><strong>Number Of Threads</strong></td>
</tr>
<tr>
<td>10 Threads</td>
</tr>
<tr>
<td>○ Go Faster</td>
</tr>
<tr>
<td><strong>Select scanning type:</strong></td>
</tr>
<tr>
<td>○ List based brute force</td>
</tr>
<tr>
<td><strong>File with list of dirs/files</strong></td>
</tr>
<tr>
<td>/root/Desktop/CMTE/databases/drupal.txt</td>
</tr>
<tr>
<td><strong>Char set</strong></td>
</tr>
<tr>
<td>a-zA-Z-0-9%20_</td>
</tr>
<tr>
<td><strong>Select starting options:</strong></td>
</tr>
<tr>
<td>○ Standard start point</td>
</tr>
<tr>
<td>□ Be Recursive</td>
</tr>
<tr>
<td>□ Brute Force Files</td>
</tr>
<tr>
<td>File extension: php</td>
</tr>
<tr>
<td>URL to fuzz: /test.html?url={dir}.asp</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>□ Exit</td>
</tr>
<tr>
<td>DirBuster Stopped</td>
</tr>
</tbody>
</table>
```

Tools for blackbox auditing most used CMS

Conclusion
Some oversold products

Some oversold products - CMTE

![OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing](image)

- Type: Dir
- Found: /Drupal/drupal7/modules/
- Response: 403
- Size: 401

Current speed: 0 requests/sec
Average speed: (T) 4, (C) 4 requests/sec
Parse Queue Size: 0
Total Requests: 42/42
Time To Finish: 00:00:00

Current number of running threads: 10
Joomscan

History
- First release in December 2008
- Donated to OWASP in May 2009
- More info: `./joomscan.pl history`

Compatibility
- Win XP/Vista/Seven
- BackTrack 2/3/4/5 - Kali Linux
- Gentoo

Support
- Proxy
- Cookie
Joomscan

How it works?

- Try to connect to website
- Look for admin directory
- Look for anti scanner measure
- Look for Joomla Firewall
- Fingerprint
  - Meta generator tag and specific files content
- Look for component on the index page
  - As in DPScan
- Look for vulnerabilities
Joomscan

Pattern hardcoded in the script
- Look for admin directory
- Look for anti scanner measure
- Look for Joomla Firewall
- Fingerprint
- Look for component on the index page

External .txt DB
- Look for vulnerabilities
Joomscan

Target: http://192.168.56.101/Joomla/Joomla-1.5
Server: Apache/2.2.22 (Win32) PHP/5.2.2
X-Powered-By: PHP/5.2.2

## Checking if the target has deployed an Anti-Scanner measure
[!]: Scanning Passed ..... OK

## Detecting Joomla! based Firewall ...
[!]: No known firewall detected!

## Fingerprinting in progress ...
~1.5.x revealed [1.5.16 - 1.5.26]
~Generic version family ....... [1.5.x]

* Deduced version range is : [1.5.16 - 1.5.26]

## Fingerprinting done.
Joomscan

## 9 Components Found in front page ##
com_content  com_newsfeeds
com_weblinks  com_search  com_contact
com_user  com_wrapper  com_mailto
com_poll
# 7
Info -> Core: Missing JEXEC Check - Path Disclosure Vulnerability
Versions effected: 1.5.11 <=
Check: /libraries/phpxmlrpc/xmlrpcs.php
Exploit: /libraries/phpxmlrpc/xmlrpcs.php
Vulnerable? No

Core:  Missing JEXEC Check - Path Disclosure Vulnerability
Versions effected: 1.5.11 <= |/libraries/phpxmlrpc/xmlrpcs.php|/libraries/phpxmlrpc/xmlrpcs.php
# 59
Info -> Core: Password change vulnerability & Information disclosure
Version effected: 1.5.25 <=
Check: /?1.5.25
Vulnerable? Yes

Core: Password change vulnerability & Information disclosure
WPSan

History
- Started in 2011
- Sponsored by the RandomStorm Open Source Initiative

Compatibility
- Windows not supported
- Ruby $\geq$ 1.9
- RubyGems
- Git
- Works on: Fedora, Debian, Ubuntu, Kali Linux, BackTrack, ArchLinux, MacOSX, etc.
WPScan

Support

- Multithread
  - For login bruteforce
  - For plugins/themes enumeration
- Proxy and proxy auth
- HTTP auth
WPScan

How it works?
By default make a non intrusive scan:

ruby wpscan.rb --url www.example.com
WPScan

Default scan, look for

- searchreplacedb2.php
  - An administration tool which allow to load info from wp-config.php
- Multisites
- Enable registration
- Enable XML RPC
  - XML-RPC functionality is turned on by default since v3.5
Default scan, look for

- robots.txt
- readme.html
- Full Path Disclosure
  - wp-includes/rss-functions.php
  - Wordpress allows a FPD, the only correction is to disable the display_error in .htaccess or php.ini file.
- wp-config.php backup
  - List of wp-config.bak/.old/.txt etc.
  - From feross.org/cmsploit
WPScan

Default scan, look for
- Malwares
  - Known infection patterns
  - Load from data/malwares.txt
- Plugins and themes (passive detection)

Default scan, make fingerprinting
- HTML headers
- Specific files hashes
  - From wp_version.xml
**WPScan**

URL: http://192.168.56.101/WordPress/wordpress-3.5.1/

Started on Sat Jul 6 11:15:53 2013

- Full Path Disclosure (FPD) in 'http://192.168.56.101/WordPress/wordpress-3.5.1/wp-includes/rss-functions.php'
- WordPress version 3.5.1 identified from meta generator

- We have identified 7 vulnerabilities from the version number:
- [...]

---

70/ 85 - A. Cervoise - Devoteam - RMLL/LSM 2013
[-] The WordPress theme in use is twentytwelve v1.1

| Name: twentytwelve v1.1 |
| Location: http://192.168.56.101/WordPress/wordpress-3.5.1/wp-content/themes/twentytwelve/

[-] Enumerating plugins from passive detection ...
No plugins found :(

[-] Finished at Sat Jul 6 11:15:53 2013
[-] Elapsed time: 00:00:00
WPScan

Differents enumeration options

```
--enumerate | -e [option(s)]  Enumeration.
    option :
        u  usernames from id 1 to 10
        u[10-20] usernames from id 10 to 20 (you must write
               [] chars)
        p  plugins
        vp only vulnerable plugins
        ap all plugins (can take a long time)
        tt timthumbs
        t  themes
        vt only vulnerable themes
        at all themes (can take a long time)

Multiple values are allowed : ’-e tt,p’ will enumerate
    timthumbs and plugins
If no option is supplied, the default is ’vt,tt,u,vp’
```
WPScan

Vulnerabilities

Checks vulnerabilities for your WordPress version (from `data/wp_vulns.xml`).

[!] We have identified 7 vulnerabilities from the version number:

| * Title: CVE-2013-2173: WordPress 3.4-3.5.1 DoS in `class-phpass.php`
| * Reference: http://seclists.org/fulldisclosure/2013/Jun/65
| * Reference: http://secunia.com/advisories/53676/
| * Reference: http://osvdb.org/94235

[...]

| * Title: WordPress HTTP API Unspecified Server Side Request Forgery (SSRF)
| * Reference: http://osvdb.org/94784
<wordpress version="3.5.1">
  <vulnerability>
    <title>CVE-2013-2173: WordPress 3.4-3.5.1 DoS in class-phpass.php</title>
    <reference>http://osvdb.org/94235</reference>
    <type>UNKNOWN</type>
  </vulnerability>
  [
  ...
  <vulnerability>
    <title>WordPress HTTP API Unspecified Server Side Request Forgery (SSRF)</title>
    <reference>http://osvdb.org/94784</reference>
    <type>SSRF</type>
  </vulnerability>
Vulnerabilities

- WPScan checks if there are known vulnerabilities in your plugins or themes (from `data/theme_vulns.xml` and `data/theme_vulns.xml`)
- But it don’t look if the versions you are using are vulnerable
  - You must do the comparaison by yourself!
WPScan

[+] Enumerating installed plugins ...

Time: 00:00:06 <=======> (2501 / 2501) 100.00% Time: 00:00:06

[+] We found 3 plugins:

  | Name: akismet
| Name: syntaxhighlighter |
| Directory listing enabled: Yes |

* Title: syntaxhighlighter clipboard.swf XSS
* Reference: https://secunia.com/advisories/53235/
<plugin name="syntaxhighlighter">
  <vulnerability>
    <title>syntaxhighlighter clipboard.swf XSS</title>
    <type>XSS</type>
    <fixed_in>3.1.6</fixed_in>
  </vulnerability>
</plugin>
Multithreaded authentication bruteforce

- Based on a wordlist
- Can bypass some bad captcha plugins
  - Like captcha
  - Due to a bad implementation
  - If you make a POST request to the authentication webpage without using captcha plugin specific post var, it works!
WPScan

- Do wordlist password brute force on enumerated users using 50 threads:

  ruby wpscan.rb --url www.example.com --wordlist darkc0de.lst --threads 50

- Do wordlist password brute force on the admin username only:

  ruby wpscan.rb --url www.example.com --wordlist darkc0de.lst --username admin
Summary

1. Introduction
2. World most used CMS
3. Why and how audit a CMS?
4. Tools for blackbox auditing most used CMS
5. Conclusion
How to secure a CMS? (non-exhaustive)

- Keep up to date
  - the CMS
  - plugins/themes (themes are also vulnerable!)
- Don’t use some exotical plugins/themes
- Uninstall unused functionnalities (plugins/themes)
- Disable natives unused functionnalities
- Remove unused files (readme, install dir, etc.)
- Use strong password
- Configure your chmod
## Tools comparaison

<table>
<thead>
<tr>
<th>Functionnalities</th>
<th>Joomscan</th>
<th>WPScan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security detection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Malware detection</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Service enumeration</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Plugin/theme enumeration (passive and BF)</td>
<td>Passive</td>
<td>Yes</td>
</tr>
<tr>
<td>Vulnerability scanner</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User enumeration</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Authentication bruteforce</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Conclusion

Create one CMS audit tool with

- Version detection,
- Vulnerability scanner,
- Service enumeration,
- Plugin/theme enumeration (passive and brute force),
- User enumeration,
- Authentication brute force.
Questions?