iSEC
information security inc.

WPScan

Information Security Inc.

Contents

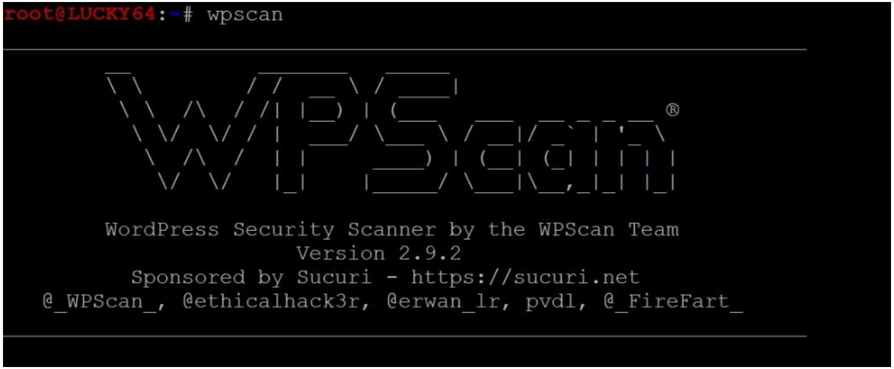
- About WPScan
- WPScan features
- Demo
- References

About WPScan

- WPScan is a black box vulnerability scanner for WordPress written in PHP mainly focus on different types of vulnerability in WordPress, WordPress themes, and plugins

- WPScan tool is already installed by default in Kali Linux, SamuraiWTF, Pentoo, BlackArch, and BackBox Linux

- WPScan uses the database of all the available plugins and themes (approximately over 18000 plugins and 2600 themes) during testing against the target to find outdated versions and vulnerabilities.



```
root@LUCKY64:~# wpscan
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.2
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________
```

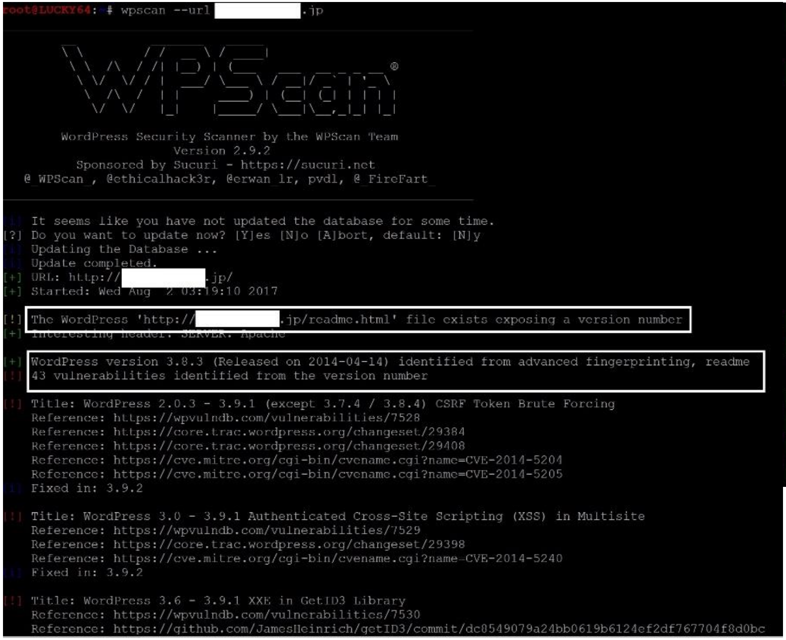
WPScan features

◎ WPScan main features

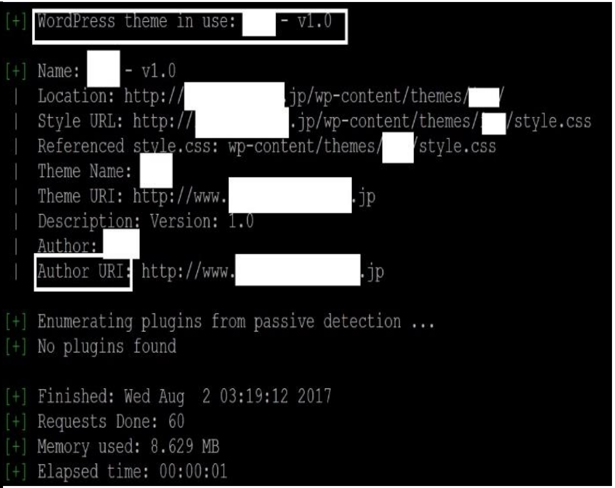
- Detect a version of currently installed WordPress
- Can detect sensitive files like readme, robots.txt, database replacing files, etc
- Detect enabled features on currently installed WordPress
- Enumerate theme version and name
- Detect installed plugins and can tell you if it is outdated or not.
- Enumerate user names

Demo

- Testing environment: Kali Linux x64
- From terminal run #wpscan --url

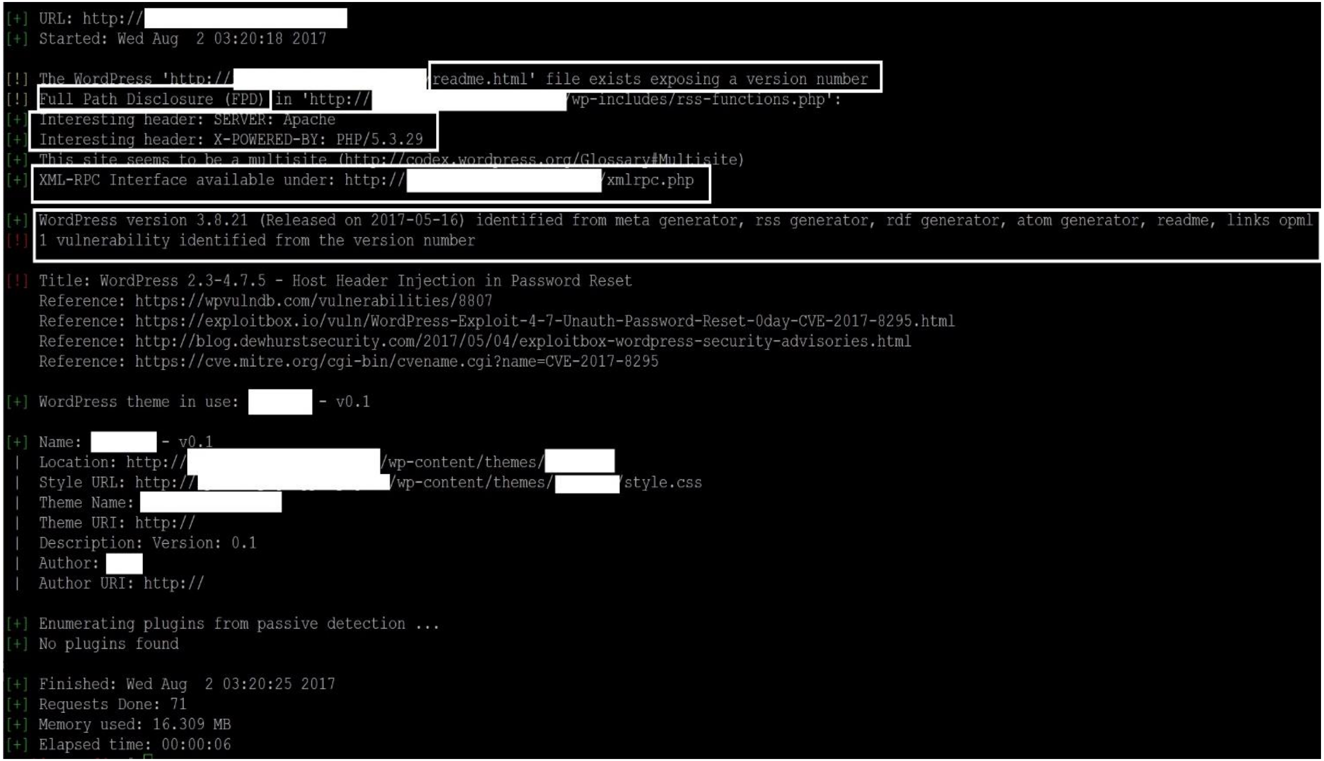


```
root@LUCKY64:~# wpscan --url [redacted].jp
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.2
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o [A]bort, default: [N]y
[i] Updating the Database ...
[i] Update completed.
[+] URL: http://[redacted].jp/
[+] Started: Wed Aug  2 03:19:10 2017

[!] The WordPress 'http://[redacted].jp/readme.html' file exists exposing a version number
[+] Interesting header: SERVER: Apache

[+] WordPress version 3.8.3 (Released on 2014-04-14) identified from advanced fingerprinting, readme
[!] 43 vulnerabilities identified from the version number

[!] Title: WordPress 2.0.3 - 3.9.1 (except 3.7.4 / 3.8.4) CSRF Token Brute Forcing
    Reference: https://wpvulndb.com/vulnerabilities/7528
    Reference: https://core.trac.wordpress.org/changeset/29384
    Reference: https://core.trac.wordpress.org/changeset/29408
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5204
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5205
[i] Fixed in: 3.9.2

[!] Title: WordPress 3.0 - 3.9.1 Authenticated Cross-Site Scripting (XSS) in Multisite
    Reference: https://wpvulndb.com/vulnerabilities/7529
    Reference: https://core.trac.wordpress.org/changeset/29398
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5240
[i] Fixed in: 3.9.2

[!] Title: WordPress 3.6 - 3.9.1 XXE in GetID3 Library
    Reference: https://wpvulndb.com/vulnerabilities/7530
    Reference: https://github.com/JamesHeinrich/getID3/commit/dc8549079a24bb0619b6124ef2df767704f8d0bc
```



```
[+] WordPress theme in use: [redacted] - v1.0

[+] Name: [redacted] - v1.0
 |  Location: http://[redacted].jp/wp-content/themes/[redacted]/
 |  Style URL: http://[redacted].jp/wp-content/themes/[redacted]/style.css
 |  Referenced style.css: wp-content/themes/[redacted]/style.css
 |  Theme Name: [redacted]
 |  Theme URI: http://www.[redacted].jp
 |  Description: Version: 1.0
 |  Author: [redacted]
 |  Author URI: http://www.[redacted].jp

[+] Enumerating plugins from passive detection ...
[+] No plugins found

[+] Finished: Wed Aug  2 03:19:12 2017
[+] Requests Done: 60
[+] Memory used: 8.629 MB
[+] Elapsed time: 00:00:01
```

Demo



```
[+] URL: http://[redacted]
[+] Started: Wed Aug  2 03:20:18 2017

[!] The WordPress 'http://[redacted]/readme.html' file exists exposing a version number
[!] Full Path Disclosure (FPD) in 'http://[redacted]/wp-includes/rss-functions.php':
[+] Interesting header: SERVER: Apache
[+] Interesting header: X-POWERED-BY: PHP/5.3.29
[+] This site seems to be a multisite (http://codex.wordpress.org/Glossary#Multisite)
[+] XML-RPC Interface available under: http://[redacted]/xmlrpc.php

[+] WordPress version 3.8.21 (Released on 2017-05-16) identified from meta generator, rss generator, rdf generator, atom generator, readme, links opml
[!] 1 vulnerability identified from the version number

[!] Title: WordPress 2.3-4.7.5 - Host Header Injection in Password Reset
    Reference: https://wpvulndb.com/vulnerabilities/8807
    Reference: https://exploitbox.io/vuln/WordPress-Exploit-4-7-Unauth-Password-Reset-0day-CVE-2017-8295.html
    Reference: http://blog.dewhurstsecurity.com/2017/05/04/exploitbox-wordpress-security-advisories.html
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8295

[+] WordPress theme in use: [redacted] - v0.1

[+] Name: [redacted] - v0.1
 |  Location: http://[redacted]/wp-content/themes/[redacted]
 |  Style URL: http://[redacted]/wp-content/themes/[redacted]/style.css
 |  Theme Name: [redacted]
 |  Theme URI: http://
 |  Description: Version: 0.1
 |  Author: [redacted]
 |  Author URI: http://

[+] Enumerating plugins from passive detection ...
[+] No plugins found

[+] Finished: Wed Aug  2 03:20:25 2017
[+] Requests Done: 71
[+] Memory used: 16.309 MB
[+] Elapsed time: 00:00:06
```

References

- WPScan
https://wpscan.org/

- GitHub
https://github.com/wpscanteam/wpscan