```
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.3
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[+] URL: http://10.250.200.5/
[+] Started: Wed Nov  8 15:14:56 2017

[+] robots.txt available under: 'http://10.250.200.5/robots.txt'
[+] Interesting entry from robots.txt: http://10.250.200.5/wp-admin/admin-ajax.php
[!] The WordPress 'http://10.250.200.5/readme.html' file exists exposing a version
number
[!] Full Path Disclosure (FPD) in
'http://10.250.200.5/wp-includes/rss-functions.php':
[+] Interesting header: LINK: <http://10.250.200.5/wp-json/>;
rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.10 (Debian)
[+] Interesting header: X-POWERED-BY: PHP/5.6.25
[+] XML-RPC Interface available under: http://10.250.200.5/xmlrpc.php

[+] WordPress version 4.6 (Released on 2016-08-16) identified from advanced
fingerprinting, meta generator, readme, links opml, stylesheets numbers
[!] 29 vulnerabilities identified from the version number

[!] Title: WordPress 2.5-4.6 - Authenticated Stored Cross-Site Scripting via Image
Filename
    Reference: https://wpvulndb.com/vulnerabilities/8615
    Reference:
https://wordpress.org/news/2016/09/wordpress-4-6-1-security-and-maintenance-release
/
    Reference:
https://github.com/WordPress/WordPress/commit/c9e60dab176635d4bfaaf431c0ea891e4726d
6e0
    Reference:
https://sumofpwn.nl/advisory/2016/persistent_cross_site_scripting_vulnerability_in_
wordpress_due_to_unsafe_processing_of_file_names.html
    Reference: http://seclists.org/fulldisclosure/2016/Sep/6
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7168
[i] Fixed in: 4.6.1
```

[!] Title: WordPress 2.8-4.6 - Path Traversal in Upgrade Package Uploader
    Reference: https://wpvulndb.com/vulnerabilities/8616
    Reference:
https://wordpress.org/news/2016/09/wordpress-4-6-1-security-and-maintenance-release
/
    Reference:
https://github.com/WordPress/WordPress/commit/54720a14d85bc1197ded7cb09bd3ea790caa0
b6e
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7169
[i] Fixed in: 4.6.1

[!] Title: WordPress 4.3-4.7 - Remote Code Execution (RCE) in PHPMailer
    Reference: https://wpvulndb.com/vulnerabilities/8714
    Reference: https://www.wordfence.com/blog/2016/12/phpmailer-vulnerability/
    Reference:
https://github.com/PHPMailer/PHPMailer/wiki/About-the-CVE-2016-10033-and-CVE-2016-1
0045-vulnerabilities
    Reference:
https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release
/
    Reference:
https://github.com/WordPress/WordPress/commit/24767c76d359231642b0ab48437b64e8c6c7f
491
    Reference:
http://legalhackers.com/advisories/PHPMailer-Exploit-Remote-Code-Exec-CVE-2016-1003
3-Vuln.html
    Reference:
https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_phpmailer_host_header
[i] Fixed in: 4.7.1

[!] Title: WordPress 2.9-4.7 - Authenticated Cross-Site scripting (XSS) in
update-core.php
    Reference: https://wpvulndb.com/vulnerabilities/8716
    Reference:
https://github.com/WordPress/WordPress/blob/c9ea1de1441bb3bda133bf72d513ca9de66566c
2/wp-admin/update-core.php
    Reference:
https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release
/
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5488
[i] Fixed in: 4.6.2

[!] Title: WordPress 3.4-4.7 - Stored Cross-Site Scripting (XSS) via Theme Name
fallback
    Reference: https://wpvulndb.com/vulnerabilities/8718
    Reference: https://www.mehmetince.net/low-severity-wordpress/
    Reference:

https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/
    Reference: https://github.com/WordPress/WordPress/commit/ce7fb2934dd111e6353784852de8aea2a938b359
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5490
[i] Fixed in: 4.6.2

[!] Title: WordPress <= 4.7 - Post via Email Checks mail.example.com by Default
    Reference: https://wpvulndb.com/vulnerabilities/8719
    Reference: https://github.com/WordPress/WordPress/commit/061e8788814ac87706d8b95688df276fe3c8596a
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5491
[i] Fixed in: 4.6.2

[!] Title: WordPress 2.8-4.7 - Accessibility Mode Cross-Site Request Forgery (CSRF)
    Reference: https://wpvulndb.com/vulnerabilities/8720
    Reference: https://github.com/WordPress/WordPress/commit/03e5c0314aeffe6b27f4b98fef842bf0fb00c733
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5492
[i] Fixed in: 4.6.2

[!] Title: WordPress 3.0-4.7 - Cryptographically Weak Pseudo-Random Number Generator (PRNG)
    Reference: https://wpvulndb.com/vulnerabilities/8721
    Reference: https://github.com/WordPress/WordPress/commit/cea9e2dc62abf777e06b12ec4ad9d1aaa49b29f4
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5493
[i] Fixed in: 4.6.2

[!] Title: WordPress 4.2.0-4.7.1 - Press This UI Available to Unauthorised Users
    Reference: https://wpvulndb.com/vulnerabilities/8729
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-2-security-release/
    Reference: https://github.com/WordPress/WordPress/commit/21264a31e0849e6ff793a06a17de877dd88ea454

    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5610
[i] Fixed in: 4.6.3

[!] Title: WordPress 3.5-4.7.1 - WP_Query SQL Injection
    Reference: https://wpvulndb.com/vulnerabilities/8730
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-2-security-release/
    Reference:
https://github.com/WordPress/WordPress/commit/85384297a60900004e27e417eac56d24267054cb
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5611
[i] Fixed in: 4.6.3

[!] Title: WordPress 4.3.0-4.7.1 - Cross-Site Scripting (XSS) in posts list table
    Reference: https://wpvulndb.com/vulnerabilities/8731
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-2-security-release/
    Reference:
https://github.com/WordPress/WordPress/commit/4482f9207027de8f36630737ae085110896ea849
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5612
[i] Fixed in: 4.6.3

[!] Title: WordPress 3.6.0-4.7.2 - Authenticated Cross-Site Scripting (XSS) via Media File Metadata
    Reference: https://wpvulndb.com/vulnerabilities/8765
    Reference:
https://wordpress.org/news/2017/03/wordpress-4-7-3-security-and-maintenance-release/
    Reference:
https://github.com/WordPress/WordPress/commit/28f838ca3ee205b6f39cd2bf23eb4e5f52796bd7
    Reference:
https://sumofpwn.nl/advisory/2016/wordpress_audio_playlist_functionality_is_affected_by_cross_site_scripting.html
    Reference: http://seclists.org/oss-sec/2017/q1/563
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6814
[i] Fixed in: 4.6.4

[!] Title: WordPress 2.8.1-4.7.2 - Control Characters in Redirect URL Validation
    Reference: https://wpvulndb.com/vulnerabilities/8766
    Reference:
https://wordpress.org/news/2017/03/wordpress-4-7-3-security-and-maintenance-release/
    Reference:
https://github.com/WordPress/WordPress/commit/288cd469396cfe7055972b457eb589cea51ce40e
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6815
[i] Fixed in: 4.6.4

[!] Title: WordPress 4.0-4.7.2 - Authenticated Stored Cross-Site Scripting (XSS) in YouTube URL Embeds
    Reference: https://wpvulndb.com/vulnerabilities/8768
    Reference: https://wordpress.org/news/2017/03/wordpress-4-7-3-security-and-maintenance-release/
    Reference: https://github.com/WordPress/WordPress/commit/419c8d97ce8df7d5004ee0b566bc5e095f0a6ca8
    Reference: https://blog.sucuri.net/2017/03/stored-xss-in-wordpress-core.html
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6817
[i] Fixed in: 4.6.4

[!] Title: WordPress 4.2-4.7.2 - Press This CSRF DoS
    Reference: https://wpvulndb.com/vulnerabilities/8770
    Reference: https://wordpress.org/news/2017/03/wordpress-4-7-3-security-and-maintenance-release/
    Reference: https://github.com/WordPress/WordPress/commit/263831a72d08556bc2f3a328673d95301a152829
    Reference: https://sumofpwn.nl/advisory/2016/cross_site_request_forgery_in_wordpress_press_this_function_allows_dos.html
    Reference: http://seclists.org/oss-sec/2017/q1/562
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6819
[i] Fixed in: 4.6.4

[!] Title: WordPress 2.3-4.8.3 - 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://core.trac.wordpress.org/ticket/25239
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8295

[!] Title: WordPress 2.7.0-4.7.4 - Insufficient Redirect Validation
    Reference: https://wpvulndb.com/vulnerabilities/8815
    Reference: https://github.com/WordPress/WordPress/commit/76d77e927bb4d0f87c7262a50e28d84e01fd2b11
    Reference: https://wordpress.org/news/2017/05/wordpress-4-7-5/
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9066
[i] Fixed in: 4.6.6

[!] Title: WordPress 2.5.0-4.7.4 - Post Meta Data Values Improper Handling in XML-RPC
    Reference: https://wpvulndb.com/vulnerabilities/8816
    Reference: https://wordpress.org/news/2017/05/wordpress-4-7-5/
    Reference: https://github.com/WordPress/WordPress/commit/3d95e3ae816f4d7c638f40d3e936a4be19724381
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9062
[i] Fixed in: 4.6.6

[!] Title: WordPress 3.4.0-4.7.4 - XML-RPC Post Meta Data Lack of Capability Checks

    Reference: https://wpvulndb.com/vulnerabilities/8817
    Reference: https://wordpress.org/news/2017/05/wordpress-4-7-5/
    Reference: https://github.com/WordPress/WordPress/commit/e88a48a066ab2200ce3091b131d43e2fab2460a4
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9065
[i] Fixed in: 4.6.6

[!] Title: WordPress 2.5.0-4.7.4 - Filesystem Credentials Dialog CSRF
    Reference: https://wpvulndb.com/vulnerabilities/8818
    Reference: https://wordpress.org/news/2017/05/wordpress-4-7-5/
    Reference: https://github.com/WordPress/WordPress/commit/38347d7c580be4cdd8476e4bbc653d5c79ed9b67
    Reference: https://sumofpwn.nl/advisory/2016/cross_site_request_forgery_in_wordpress_connection_information.html
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9064
[i] Fixed in: 4.6.6

[!] Title: WordPress 3.3-4.7.4 - Large File Upload Error XSS
    Reference: https://wpvulndb.com/vulnerabilities/8819
    Reference: https://wordpress.org/news/2017/05/wordpress-4-7-5/
    Reference: https://github.com/WordPress/WordPress/commit/8c7ea71edbbffca5d9766b7bea7c7f3722ffafa6
    Reference: https://hackerone.com/reports/203515
    Reference: https://hackerone.com/reports/203515
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9061
[i] Fixed in: 4.6.6

[!] Title: WordPress 3.4.0-4.7.4 - Customizer XSS & CSRF
    Reference: https://wpvulndb.com/vulnerabilities/8820
    Reference: https://wordpress.org/news/2017/05/wordpress-4-7-5/
    Reference: https://github.com/WordPress/WordPress/commit/3d10fef22d788f29aed745b0f5ff6f6baea69

af3
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9063
[i] Fixed in: 4.6.6

[!] Title: WordPress 2.3.0-4.8.1 - $wpdb->prepare() potential SQL Injection
    Reference: https://wpvulndb.com/vulnerabilities/8905
    Reference:
https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release
/
    Reference:
https://github.com/WordPress/WordPress/commit/70b21279098fc973eae803693c0705a548128
e48
    Reference:
https://github.com/WordPress/WordPress/commit/fc930d3daed1c3acef010d04acc2c5de93cd1
8ec
[i] Fixed in: 4.8.2

[!] Title: WordPress 2.3.0-4.7.4 - Authenticated SQL injection
    Reference: https://wpvulndb.com/vulnerabilities/8906
    Reference: https://medium.com/websec/wordpress-sqli-bbb2afcc8e94
    Reference:
https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release
/
    Reference:
https://github.com/WordPress/WordPress/commit/70b21279098fc973eae803693c0705a548128
e48
    Reference: https://wpvulndb.com/vulnerabilities/8905
[i] Fixed in: 4.7.5

[!] Title: WordPress 2.9.2-4.8.1 - Open Redirect
    Reference: https://wpvulndb.com/vulnerabilities/8910
    Reference:
https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release
/
    Reference: https://core.trac.wordpress.org/changeset/41398
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14725
[i] Fixed in: 4.6.7

[!] Title: WordPress 3.0-4.8.1 - Path Traversal in Unzipping
    Reference: https://wpvulndb.com/vulnerabilities/8911
    Reference:
https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release
/
    Reference: https://core.trac.wordpress.org/changeset/41457
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14719
[i] Fixed in: 4.6.7

[!] Title: WordPress 4.4-4.8.1 - Cross-Site Scripting (XSS) in oEmbed

```
    Reference: https://wpvulndb.com/vulnerabilities/8913
    Reference:
https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release
/
    Reference: https://core.trac.wordpress.org/changeset/41448
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14724
[i] Fixed in: 4.6.7

[!] Title: WordPress 4.2.3-4.8.1 - Authenticated Cross-Site Scripting (XSS) in
Visual Editor
    Reference: https://wpvulndb.com/vulnerabilities/8914
    Reference:
https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release
/
    Reference: https://core.trac.wordpress.org/changeset/41395
    Reference:
https://blog.sucuri.net/2017/09/stored-cross-site-scripting-vulnerability-in-wordpr
ess-4-8-1.html
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14726
[i] Fixed in: 4.6.7

[!] Title: WordPress <= 4.8.2 - $wpdb->prepare() Weakness
    Reference: https://wpvulndb.com/vulnerabilities/8941
    Reference: https://wordpress.org/news/2017/10/wordpress-4-8-3-security-release/
    Reference:
https://github.com/WordPress/WordPress/commit/a2693fd8602e3263b5925b9d799ddd5772021
67d
    Reference: https://twitter.com/ircmaxell/status/923662170092638208
    Reference:
https://blog.ircmaxell.com/2017/10/disclosure-wordpress-wpdb-sql-injection-technica
l.html
[i] Fixed in: 4.6.8

[+] WordPress theme in use: twentysixteen - v1.3

[+] Name: twentysixteen - v1.3
 |  Latest version: 1.3 (up to date)
 |  Last updated: 2016-12-06T00:00:00.000Z
 |  Location: http://10.250.200.5/wp-content/themes/twentysixteen/
 |  Readme: http://10.250.200.5/wp-content/themes/twentysixteen/readme.txt
 |  Style URL: http://10.250.200.5/wp-content/themes/twentysixteen/style.css
 |  Theme Name: Twenty Sixteen
 |  Theme URI: https://wordpress.org/themes/twentysixteen/
 |  Description: Twenty Sixteen is a modernized take on an ever-popular WordPress
layout — the horizontal masthe...
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
```

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

[+] Finished: Wed Nov  8 15:15:00 2017
[+] Requests Done: 44
[+] Memory used: 17.238 MB
[+] Elapsed time: 00:00:04
```