Abertay University

# Evaluation of WordPress Scanners: WPScan and Vane

Rory Leanord

CMP320: Mini Project
BSc Ethical Hacking Year 3
2020/21

*Note that Information contained in this document is for educational purposes.*

.

# Abstract

WordPress, the content management system, is utilized extensively across the intent, to provide a method for users to create a website without the technical knowledge of web development. This provides the unique opportunity for any user to create a website, increasing the accessibility of the internet.

However, due to the widespread use of WordPress, exploits and vulnerabilities are constantly being discovered for the system. To combat this, security tools were developed to scan WordPress instances for known vulnerabilities. Within this paper, two WordPress scanners will be evaluated for their accuracy and speed. This will be done through scanning 10 separate instances of WordPress, five instances built for testing and 5 remote hosted instances.

These results were then evaluated to make an informed evaluation of the scanners. The evaluation will take into consideration the speed at which the scans were completed, as well as the accuracy of the scans.

.

# Contents

.

.

# Table of Tables

.

# Table of Figures

.

# 1 INTRODUCTION

## 1.1 BACKGROUND

As the amount of content available on the internet grows, so too do the associated security risks. Within a website, the Content Management System (CMS) is an essential part of the webserver functionality. The CMS is a tool used to create, modify, and manage content without technical knowledge. CMS' holds an essential role in website development as it allows for people lacking in technical knowledge to develop sites. The most popular CMS is WordPress, being utilized by 64% of websites where the CMS is known (Kinsta, 2019). Since WordPress has such a high market share, the security of the system is paramount. The often comes down to the choice of "Plugins" used within the website.

WordPress as a system initially lacks functionality, and as such requires "Plugins" to be installed. These Plugins are written in PHP, a universal web development language. However, the level of security depends on the development of the plugin, and this can vary between plugins. This poses a massive threat to the security of WordPress as attackers only need one insecure plugin to get access to the site. To combat this risk specialty security tools, targeted for WordPress have been developed.

These tools including scanners and scrapers specifically made for WordPress sites, and the plugins being used within the sites. This allows developers to know if the sites, as well as plugins, being developed, are secure from known flaws and exploits. As mentioned previously WordPress plugins are developed in PHP, allowing for functionality to be added. However, due to the prevalence of PHP across the internet exploits and flaws are constantly being discovered. These vulnerabilities range from denial of service crashes to reverse shell delivery and remote code execution.

Between WordPress and PHP, there are just under one thousand Common Vulnerabilities and Exposures (CVEs). These are common exploits and vulnerabilities that are publicly known and uniquely referenced. In 2020/21 there have been 23 vulnerabilities for WordPress released, ranging from denial of service vulnerabilities to code execution, possibly leading to machine compromise (CVE, 2021). Alongside this there have been multiple Cross-site scripting (XSS) vulnerabilities discovered, possibly allowing for user compromise. For PHP, a similar situation exists, in the same timeframe 2020/21 19 CVEs were released, including DoS and code execution exploits (CVE, 2021).

Due to the widespread use of WordPress, a lot of security tools exist, within this paper various WordPress scanners are going to be evaluated for their effectiveness. This includes the degree of accuracy which the scanners can detect plugins, the speed of the scanners and the overall ease of use that each scanner presents.

## 1.2 AIM

There are several goals which this project aims to complete. These are.

- The creation of a WordPress environment for testing – This is so that the testing is completed in an ethically responsible way and so there is a baseline knowledge of the plugins present.
- Create multiple WordPress instances – To ensure the results of testing are as accurate as possible, multiple WordPress instances will be created with 15-20 random plugins, as well as utilizing instances hosted on TryHackMe.
- The evaluation of the various scanners being tested across accuracy and speed
    - Accuracy – Due to preexisting knowledge of the plugins and the version numbers present on the WordPress instance, the accuracy can be measured for each respective scanner.
    - Speed – When the scanners being evaluated are used, the speed at which they can produce results is important.

# 2 PROCEDURE

## 2.1 OVERVIEW OF PROCEDURE

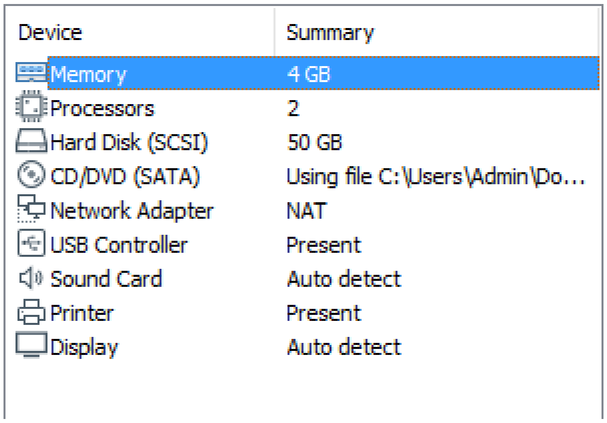
The first stage of the evaluation is to build the environment where the WordPress site will be hosted. To do this a LAMP (Linux, Apache, MySQL, PHP) server was built, within an Ubuntu virtual environment. Within the server, a WordPress instance was installed, along with all the required supporting modules. At this point the server was snapshotted, so multiple deployments could take place on the one VM.

Alongside built WordPress instances, the Capture The Flag (CTF) service, certain TryHackMe boxes were also tested, these are boxes that contain a WordPress instance. These are WordPress instances that were designed to contain security flaws and misconfigurations. These are hosted within the THM network, designed for a safe space when individuals can practice their security skills.

A VM install of Kali Linux will also be created, to conduct testing. The testing can be done from the Ubuntu server, however, to imitate real-world use, a separate VM was used. The Kali VM and the Ubuntu server were added onto a virtual network for testing. Whereas the THM boxes were tested with the same Kali VM but on the THM network, accessed through OpenVPN.

## 2.2 CREATION OF THE LAMP SERVER

To host a WordPress server, a LAMP server was created. This server was made using Ubuntu 21.04 Desktop. The first stage was to create the VM, to do this VMware was used, with the default settings being used, the settings can be seen in Figure A. After the VM was created, Ubuntu was installed using the 21.04 ISO, which can be found on the Ubuntu website.



| Device | Summary |
|---|---|
| Memory | 4 GB |
| Processors | 2 |
| Hard Disk (SCSI) | 50 GB |
| CD/DVD (SATA) | Using file C:\Users\Admin\Do... |
| Network Adapter | NAT |
| USB Controller | Present |
| Sound Card | Auto detect |
| Printer | Present |
| Display | Auto detect |

*Figure A - Server VM settings*

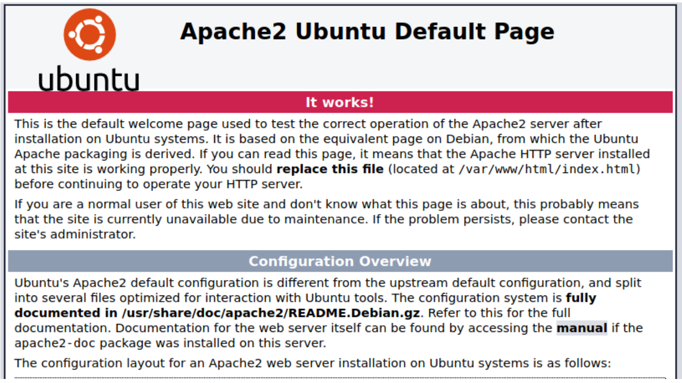
After the VM and Ubuntu were configured and installed, the LAMP stack was created.

### 2.2.1 Installing Apache2

To start this process apache2 was installed, this is done through the command:

```
apt install apache2
```

This will be the webserver for the project and the foundation for the site. To ensure apache2 is installed correctly, localhost was navigated to within a web browser and can be seen in Figure B.



**Apache2 Ubuntu Default Page**

**It works!**

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

**Configuration Overview**

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

*Figure B - Verifying Apache Install*

### 2.2.2 Installing and Configuring MariaDB

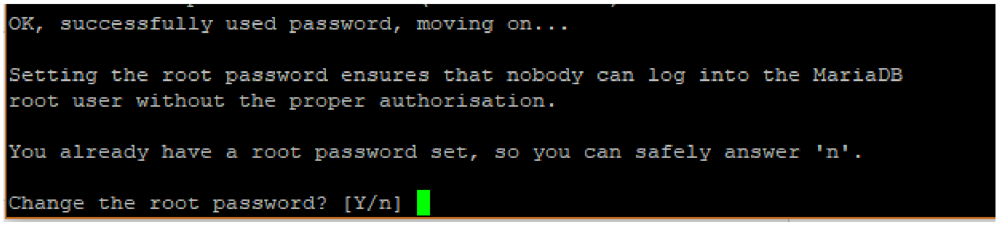
The next stage in the creation of the LAMP server was to install MySQL. The MySQL client chosen is MariaDB, an open-source fork of MySQL. The command;

```
apt install mariadb-server mariadb-client
```

was inputted to install the database client. Following the installation of the MariaDB client, it was subsequently configured. To configure the database the command

```
mysql_secure_installation
```

was inputted, the output can be seen in figure C. This allows for the database to be configured. This configuration was to keep the root password the same, disallow remote logins and disallow remote logins.



```
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

You already have a root password set, so you can safely answer 'n'.

Change the root password? [Y/n]
```

*Figure C - MariaDM install*

### 2.2.3 Installing PHP

To install PHP onto the server, this was done through the command.

```
apt install php php-mysql
```

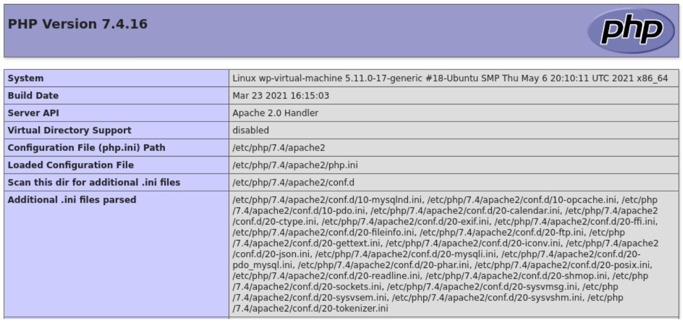
to verify if PHP has been installed correctly, a testing page will be created. The following command was inputted

```
nano /var/www/html/info.php
```

This creates a PHP document within the browsable file structure on the server. Within the file, the lines seen below were inputted.

```
<?php
phpinfo();
?>
```

Once saved and navigated to on a web browser, by entering “localhost/info.php”, it was verified that PHP was installed correctly, this can be seen in Figure D.



**PHP Version 7.4.16**

| | |
|---|---|
| **System** | Linux wp-virtual-machine 5.11.0-17-generic #18-Ubuntu SMP Thu May 6 20:10:11 UTC 2021 x86_64 |
| **Build Date** | Mar 23 2021 16:15:03 |
| **Server API** | Apache 2.0 Handler |
| **Virtual Directory Support** | disabled |
| **Configuration File (php.ini) Path** | /etc/php/7.4/apache2 |
| **Loaded Configuration File** | /etc/php/7.4/apache2/php.ini |
| **Scan this dir for additional .ini files** | /etc/php/7.4/apache2/conf.d |
| **Additional .ini files parsed** | /etc/php/7.4/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-ffi.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-json.ini, /etc/php/7.4/apache2/conf.d/20-mysqli.ini, /etc/php/7.4/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini, /etc/php/7.4/apache2/conf.d/20-shmop.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.4/apache2/conf.d/20-sysvsem.ini, /etc/php/7.4/apache2/conf.d/20-sysvshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini |

*Figure D - Verifying PHP install*

### 2.2.4 Creating the Database

After verifying that PHP was installed correctly, the database backend for the WordPress site was created. To do this the SQL client was logged in as root, through the command

```
$ mysql -u root -p
```

After this point, the commands issued can be found in Appendix A. After the database was created, a user was created, with the privileges to access the database.

### 2.2.5 Installing WordPress CMS

The first stage in the installation of WordPress was to download the CMS files. To download the files, the command

```
cd /tmp && wget https://wordpress.org/latest.tar.gz
```

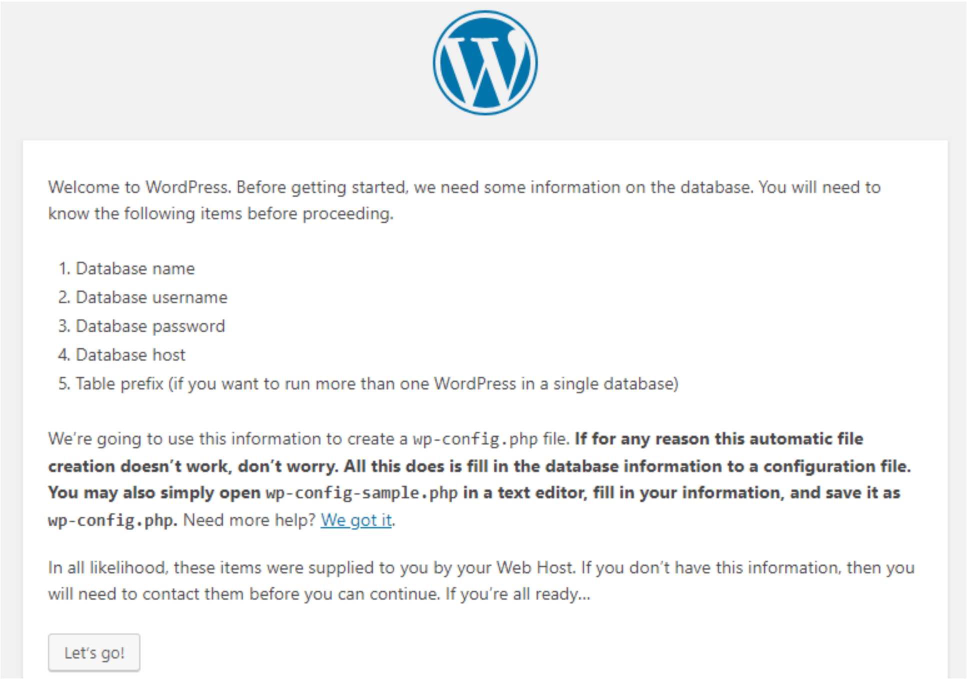
This command enters the temp file, as well as downloads the WordPress tar file. This tar file had to be uncompressed for the install to continue, so the command

```
tar -xvf latest.tar.gz
```

This extracts the downloaded file and allows it to be usable. Following the extraction, the file had to be moved to the web-accessible directory, in this case, that was “`/var/www/html/`”. To move the extracted file the command seen below was inputted.

```
cp -R wordpress /var/www/html/
```

This placed the WordPress directory into the accessible directory of the server. To verify the installation of WordPress, the URL “Localhost/WordPress” was navigated to, this can be seen in Figure E.



Welcome to WordPress. Before getting started, we need some information on the database. You will need to know the following items before proceeding.

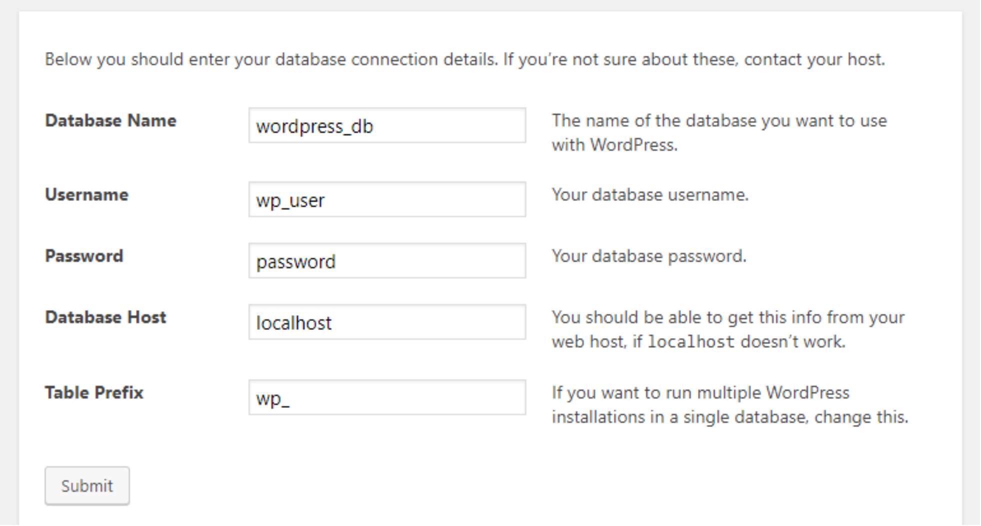
1. Database name
2. Database username
3. Database password
4. Database host
5. Table prefix (if you want to run more than one WordPress in a single database)

We're going to use this information to create a `wp-config.php` file. **If for any reason this automatic file creation doesn't work, don't worry. All this does is fill in the database information to a configuration file. You may also simply open `wp-config-sample.php` in a text editor, fill in your information, and save it as `wp-config.php`.** Need more help? We got it.

In all likelihood, these items were supplied to you by your Web Host. If you don't have this information, then you will need to contact them before you can continue. If you're all ready…

*Figure E - Default automatic configuration page*

The next stage is the configuration, which was to populate the fields as seen in Figure F.



Below you should enter your database connection details. If you're not sure about these, contact your host.

| | | |
|---|---|---|
| **Database Name** | wordpress_db | The name of the database you want to use with WordPress. |
| **Username** | wp_user | Your database username. |
| **Password** | password | Your database password. |
| **Database Host** | localhost | You should be able to get this info from your web host, if `localhost` doesn't work. |
| **Table Prefix** | wp_ | If you want to run multiple WordPress installations in a single database, change this. |

*Figure F - Configuration Populated*

Once the setup wizard has been completed, the WordPress management dashboard will be available. From here all the settings of the website can be accessed and modified. Alongside this, the dashboards allow access to add plugins and themes to the site.

## 2.3 CREATING THE WORDPRESS INSTANCES

As mentioned within the aims section, 5 instances of WordPress will be created. These were created with 15-20 random plugins. This was done to ensure reliability in the results of the testing. The selection of plugins was done through a random number generator. First, a number was generated to get the page of the plugin, and secondly to select the plugin itself. This method allowed for a vast array of plugins to be selected. All the instances of WordPress can be found in appendix B. This includes the plugins installed as well as the version numbers. Alongside adding the plugins to the sites, all the plugins were also activated to emulate use in the wild.

To create the instances firstly a base install snapshot was created. This is to allow multiple "forks" of the server to exist. The plugins were then selected through random number generation, and once all plugins were installed, a new snapshot was created. After the new snapshot was created, the VM was then restored to the base install snapshot. These snapshots will be used to test the scanners.

## 2.4 TRYHACKME WORDPRESS INSTANCES

To widen the scope of testing, instances of WordPress hosted within THM CTF boxes were used. These instances are designed to be vulnerable to hackers and allow for prospective penetration testers to improve their skills within a safe environment. In total 5 boxes will be utilized for testing the WordPress scanners, these boxes are as follows;

- Cyber Week2021 (TryHackMe, 2021)
- Jack (TryHackMe, 2021)
- Blog (TryHackMe, 2021)
- Mr Robot (TryHackMe, 2020)
- Internal (TryHackMe, 2021)

To connect to the boxes within the THM network, a THM account is needed to be created, to get an OpenVPN configuration file. This file was used within the Kali Linux VM to connect to the THM boxes.

## 2.5 TESTING THE SCANNERS

Previously, the instances of WordPress have been created, along with the hosting server. The scanners that will be tested are;

- WPScan – WPScan is the current leading scanner in the WordPress security space. It offers access to a vulnerability API. The API will be evaluated within this paper. WPScan has long term support with more vulnerabilities being added each day. (WPScan, 2021)
- Vane – Vane is a more competing WordPress scanner. It doesn't utilize an API for vulnerabilities but instead checks against osvDB and several other vulnerability sites. Vane merges WPScan and features from another scanner, WPSeku. (Vane, 2019)

The scanners are going to be run from an external Kali Linux VM to imitate a real-world use as closely as possible. Each scanner will be run 5 times against each WordPress instance to improve the reliability of the results. The scanners will be evaluated on 2 different points, these are as follows.

- Speed – The speed across the 5 scans will be accumulated with the mode, median and mean calculated.
- Accuracy – The results of the scanners will be processed to ensure there are no discrepancies within the results of the output of the scanner.

The scans used for testing can be seen below;

WPScan - `wpscan --url=`**`Host IP`**` -e ap,u,vt,tt,cb,dbe`

This scan enumerates all the plugins present on the server, users IDs, Vulnerable themes on the instance, Timthumbs, a security flaw present within an image resizing script(TimThumb with WordPress | WP Engine®, 2021), Config backups and database exports

For Vane, as there are fewer overall flags for enumeration the command was.

```
ruby vane.rb --url Host --enumerate p -v
```

This scan enumerates the plugins present on the machine and a verbose output, to ensure the maximum amount of data is enumerated.

# 3 RESULTS

The results of each scan will be broken down between the self-hosted VMs and the THM WordPress instances. Alongside this, the results will be broken down to compare the two scanners on each respective instance.

## 3.1 SELF-HOSTED VM 1

The list of addons and configuration present on VM1 can be found in appendix B. The full list of scans can be found in Appendix C.

*Table 1 - VM1 Results*

| Scanner | Speed | Plugins Identified |
|---|---|---|
| **WPScan** | All WPScans ran in 4 seconds | 3/17 |
| **Vane** | All Vane Scans ran in 4 seconds | 16/17 |

As can be seen from the table above, both scanners performed at the same speed, with the outputs stating all scans ran in 4 seconds. However, where the scans differ is the number of plugins identified. WPScan only identified 3 out of the 17 present on the machine, whereas Vane identified 16, missing only XML sitemaps. On the flipside, WPScan enumerated more general information about the server, an instance, such as the users on the system. WPScan also checked for backups and exports of the database whereas Vane didn’t check for such information.

## 3.2 SELF-HOSTED VM 2

The list of addons and configuration present on VM2 can be found in appendix B. The full list of scans can be found in Appendix D.

*Table 2 - VM2 Results*

| Scanner | Speed | | Plugins Identified |
|---|---|---|---|
| **WPScan** | All WPScans ran in 4 seconds | | 0/17 |
| **Vane** | Mean | 3.6 | 1/17 |
| | Median | 3 | |
| | Mode | 3 | |

Within this WordPress instance, there were 17 plugins present on the machines, with both scanners performing poorly. The only plugin identified by Vane was WooCommerce. However, this may be due to the nature of the plugins present within the instance, as both scanners initially crashed siting 403 – permission denied errors. To work around this, the scan commands were altered to add a random user-agent, in the case of WPscan the ignore redirect flag was also added, these can be seen in the table below.

*Table 3 - VM2 Workaround*

| | Workaround Command | Original Command |
|---|---|---|
| **WPScan** | wpscan --url=HOST -e ap,u,vt,tt,cb,dbe --ignore-main-redirect --random-user-agent | wpscan --url=HOST -e ap,u,vt,tt,cb,dbe |
| **Vane** | ruby vane.rb --url 10.10.172.31 --enumerate p -v –random-user-agent | ruby vane.rb --url 10.10.172.31 --enumerate p -v |

Due to the necessity of having to change the command, the scans were run with, it no longer had a control variable and as such the instance is disregarded from the final evaluation.

## 3.3 Self-Hosted VM 3

The list of addons and configuration present on VM3 can be found in appendix B. The full list of scans can be found in appendix E.

*Table 4 - VM3 Results*

| Scanner | Speed | | Plugins Identified |
|---|---|---|---|
| **WPScan** | Mean | 4.4 | 1/17 |
| | Median | 4 | |
| | Mode | 4 | |
| **Vane** | N/A | | N/A |

Within this instance of WordPress and testing, only WPScan was able to get through to the site. Vane responded with a 403 error, stating that a plugin was blocking it from scanning. The plugin responsible for this block is most likely iThemes Security. Like with the previous WordPress instances scanned, WP scan enumerated the user account on the site. Unlike with VM2, both scanners were executed using a changed command, and as such this instance will be used towards the final accuracy evaluation of the scanners, but not speed.

## 3.4 Self-Hosted VM 4

The list of addons and configuration present on VM4 can be found in appendix B. The full list of scans can be found in Appendix F.

*Table 5 - VM4 Results*

| Scanner | Speed | | Plugins Identified |
|---|---|---|---|
| **WPScan** | All WPScans ran in 7 seconds | | 0/19 |
| **Vane** | Mean | 4.8 | 1/19 |
| | Median | 4 | |
| | Mode | 4 | |

The only plugin either scanner found was “Akismet Anti-Spam”, which was is pre-installed within WordPress insistence, the plugin is activated however it was not configured in any way. Like previous scans, WPScan enumerated more about the server the instance was running on, such as user accounts and service versions.

## 3.5 SELF-HOSTED VM 5

The list of addons and configuration present on VM5 can be found in appendix B. The full list of scans can be found in Appendix G.

*Table 6 - VM5 Results*

| Scanner | Speed(Seconds) | | Plugins Identified |
|---|---|---|---|
| **WPScan** | Mean | 5.2 | 1/24 |
| | Median | 5 | |
| | Mode | 5 | |
| **Vane** | Mean | 3.6 | 1/24 |
| | Median | 3 | |
| | Mode | 3 | |

Both scanners identified 1 plugin apiece, however, they were 2 separate plugins. In the case of WPscan, the plugin identified was “images-lazyload-and-slideshow”. The plugin Vane identified was “Akismet Anti-Spam”. WPScan also enumerated users on the instance as well as overall more server information.

## 3.6 THM: BLOG

Due to these instances of WordPress running on an external service, the list of installed plugins isn’t available. However, the scans can be found in Appendix H.

*Table 7 - THM: Blog Results*

| Scanner | Speed(Minutes) | | Plugins Identified |
|---|---|---|---|
| **WPScan** | Mean | 4.526(4:32) | 0 |
| | Median | 4.72(4:43) | |
| | Mode | 4.17, 4.95, 4.72, 4.97, 3.82 | |
| **Vane** | Mean | 5.398(5:24) | 1 |
| | Median | 5.87(5:52) | |
| | Mode | 5.98, 4.52, 5.87, 5.9, 4.72 | |

Both scanners took much longer on the THM WordPress instances. Vane only detected 1 plugin, called “feed”, however could not determine the version number of the service. On the flipside, WPScan detected 0 plugins, however, did enumerate users, as well as server information.

## 3.7 THM: CyberWeek 2021

Due to these instances of WordPress running on an external service, the list of installed plugins isn’t available. However, the scans can be found in Appendix I.

*Table 8 - THM: CyberWeek Results*

| Scanner | Speed(Minutes) | | Plugins Identified |
|---|---|---|---|
| **WPScan** | Mean | 0.478 (0: 28.68) | 0 |
| | Median | 0.48 (0:28) | |
| | Mode | 0.48 | |
| **Vane** | Mean | 0.266 (0:16) | 1 |
| | Median | 0.29 (0:17) | |
| | Mode | 0.28, 0.13, 0.33, 0.29, 0.3 | |

Vane detected 1 plugin; in this case, it was “Akismet Anti-Spam”. Vane also detected the theme running on the site, along with the theme author. WPScan detected 0 plugins, however, did enumerate users, as well as server information.

## 3.8 THM: Internal

Due to these instances of WordPress running on an external service, the list of installed plugins isn’t available. However, the scans can be found in Appendix J.

*Table 9 - THM: Internal Results*

| Scanner | Speed(Minutes) | | Plugins Identified |
|---|---|---|---|
| **WPScan** | Mean | 0.446 (0: 27) | 0 |
| | Median | 0.45 (0:27) | |
| | Mode | 0.45 | |

| | | | |
|---|---|---|---|
| **Vane** | Mean | 0.306 (0:18) | 0 |
| | Median | 0.28 (0:17) | |
| | Mode | 0.25, 0.3, 0.27, 0.28, 0.43 | |

Both scanners found no plugins for the site, however, Vane was significantly faster than WPScan. The same pattern for enumerating further information was continued with this WordPress instance.

## 3.9 THM: Jack

Due to these instances of WordPress running on an external service, the list of installed plugins isn't available. However, the scans can be found in Appendix K.

*Table 10 - THM: Jack Results*

| Scanner | Speed(Minutes) | | Plugins Identified |
|---|---|---|---|
| **WPScan** | Mean | 5.212 (5:13) | 0 |
| | Median | 5.03 (5:02) | |
| | Mode | 1.1, 9.9, 5.03, 5.55, 4.48 | |
| **Vane** | Mean | 4.31 (4:19) | 2 |
| | Median | 4.67 (4:40) | |
| | Mode | 2.55, 4.93, 4.98, 4.67, 4.42 | |

Vane identified 2 plugins where as WPscan didn't return any. Both detected the theme, including the version number. However, Vane retrieved the theme URL. WPscan identified that the version of WordPress running on the site was out of date and insecure.

## 3.10 THM: MR ROBOT

Due to these instances of WordPress running on an external service, the list of installed plugins isn't available. However, the scans can be found in Appendix L.

*Table 11 - THM: Mr Robot Results*

| Scanner | Speed(Minutes) | | Plugins Identified |
|---|---|---|---|
| **WPScan** | Mean | 6.314 (6:19) | 0 |
| | Median | 6.1 (6:06) | |
| | Mode | 7.47 | |
| **Vane** | Mean | 5.14 (5:08) | 11 |
| | Median | 4.7 (4:42) | |
| | Mode | 4.1, 4.27, 4.7, 4.8, 7.83 | |

As can be seen, Vane identified multiple different plugins along with the respective version numbers, comparatively, WPScan revealed none. However, this data set is unique. Within the scans, Vane enumerated over 50 vulnerabilities within the core WordPress system. These were vulnerabilities such as XSS, redirect bypasses, security bypasses, information disclosure. Vane also identified over 100 CVEs that may be exploitable within the site. This information is essential knowledge in building a secure website.

# 4 Discussion

## 4.1 General Discussion

After performing all scans, a clear trend in the results and testing emerged. This trend was, although the self-hosted VMs had installed and activated plugins, the times they scanned in relative to the THM WordPress instances, was vastly shorter. This was most likely due to the lack of configuration of the plugins within the WordPress instance. These configurations would in turn make the instance more complex leading to the scanners taking longer. However, within the THM WordPress instances, there was vastly more configuration, but fewer plugins. Suggesting that the speed of the scanners isn't altered severely by the number of plugins present within the instance, but more the configuration of the plugins present.

For the Accuracy of the scanners, both scanners enumerated a surprisingly low number of plugins. Each self-hosted instance had a minimum of 17 plugins installed and the scanners picked up a maximum of 16, with the majority being in single digits. However, when the scanners did pick up the plugins, the version they identified was correct. The THM WordPress instances were in the similar situation, where the majority of the scans found single-digit plugins. This will be discussed in more detail in section 4.3.

## 4.2 Speed

To compare the speed of the scanners, the Mean time of each WordPress instance will be taken and averaged out. This can be seen in the below table.

*Table 12 - WordPress Instance Speed*

| | WPScan | Vane | Percentage Difference |
|---|---|---|---|
| **VM1** | **0.09** | **0.09** | 0% |
| **VM2** | N/A | N/A | N/A |
| **VM3** | 0.09 | N/A | N/A |
| **VM4** | 0.11 | **0.08** | 37.5% |
| **VM5** | **0.05** | **0.05** | 0% |
| **Blog** | **4.526** | 5.398 | 19.3% |
| **CyberWeek 2021** | 0.478 | **0.226** | 111.5% |
| **Internal** | 0.446 | **0.306** | 45.7% |
| **Jack** | 5.212 | **4.31** | 20.9% |
| **Mr Robot** | 6.314 | **5.14** | 22.8 |
| **Average Time** | **1.924** | 1.945 | 1.1% |

Bold indicates faster the scanner within that instance. The percentage difference is relative to the faster scanner.

As can be seen from the above table, WPScan runs slightly faster than Vane on the same instance. The largest differences between the scanners were during the THM instance blog, and Mr Robot, the percentages can be seen below.

As can be seen above WP scan had a lower average scan time, but also had the highest percentage difference at 111.5% slower than Vane within the THM CyberWeek 2021 instance.

The overall average speed of the 2 scanners differed by 1.1% across 100 scans. This difference in performance is marginal and using the calculated average, accounts for 2 seconds. Within CyberWeek 2021, the largest percentage difference, the speed difference resulted in a change of 15 seconds.

## 4.3 Accuracy

As mentioned within the general discussion, the overall pickup rate of plugins was low. However, the accuracy of the scanners was high for the plugins and themes identified by the scanners.

All of the self-hosted VMs ran the theme, “Twenty Twenty-One”, V 1.3. All of the Vane scans identified this theme correctly. Vanes output also stated the themes URI link within WordPress, along with the description and tags. This wasn’t the case for WPScan which stated the main theme cannot be discovered.

WPScan however consistently enumerated more of the overall infrastructure configuration. This included the server and user accounts within the instance. WPScan also checked for database backups and exports, due to the nature of the machines tested there were no backups or exports.

Both scanners detected a surprisingly low number of plugins present on the machines, however, when the plugins were detected, both scanners had 100% accuracy. Vane detected more plugins on average, however, WPScan detected more information on the infrastructure of the server,

## 4.4 Conclusions

In conclusion, both scanners were found to have equally advantages and disadvantages. The speed differences between the two scanners are negligible, with the meantime of all the scans being separated by 1.1% (2 seconds). Both scanners are also easy to configure and use.

The accuracy of the scanners is also very similar, with Vane detecting more of the plugins present on the site, and WPScan detecting more of the infrastructure the site is running on.

When both scanners detected plugins, there were several instances that the plugins detected were different. However, those detected plugins were always the correct version number. This is interesting, as Vane is based on WPScan with some improvements. However, the last commit on GitHub was 3 years ago, whereas WPScan has been constantly being developed and improved.

Overall, both scanners are evenly matched in the testing conducted and each scanner possesses its benefits. Both can be recommended for an organization dependent on the use case and scenario within the organization. In some instances, both scanners detected different plugins. The success of a pen test usually relies on the amount of enumeration done on the target, and as such both scanners can be utilized to enumerate site and instances.

## 4.5 FUTURE WORK

There are several aspects of this investigation that could be expanded upon. These aspects of further investigation are the extra variables, such as the addition of more scanners, testing different commands, testing against real-world WordPress Instances.

### 4.5.1 Extra Scanners

Initially, an evaluation of four different scanners was planned, these scanners being, WPScan, WPSeku, Vane and WordPress Exploit Framework (WPXF). However, when WPSeku and WPXF were attempted to be installed, the installs failed, and the scanners were unable to be used for this investigation. With more time and experience, these issues could be overcome and lead to a more thorough comparison of the scanners.

### 4.5.2 Different Flags

The testing of different flags would allow for a more thorough evaluation of the WordPress scanners, as each scanner comes with an array of options and settings to be utilized in scanning. This evaluation was completed, except for VM2, where the command had to be altered to access the WordPress Instance, with a basic scan enumerating the plugins and other basic server information. Some examples of the functionality which can be tested are.

- Brute forcing accounts with wordlists
- The difference in speed using single threads
- Different detection modes

With more time these functionalities can be tested and evaluated for a deeper evaluation on the overall scanners.

Alongside the different flags, WPScan can utilize WPScans vulnerability API. The API could be utilized in further testing to evaluate the scanners. This feature wasn’t utilized throughout testing.

### 4.5.3 Real-world uses

All the instances of WordPress used in this evaluation were built for testing. The self-hosted VMs were built exclusively for this evaluation. The THM WordPress instances were purpose-built to be vulnerable, to allow for people to practice cyber security within a safe space. This inherently doesn’t match with real-world usages, where vulnerabilities aren’t built into the system. However, they do emulate a configured WordPress implementation.

For future work, real-world examples of WordPress instances could be utilized within testing. Including both hardware and cloud-hosted instances. This would allow for an increased practical understanding of the scanners.

# REFERENCES

CVE, 2021. *CVE Details.* [Online]
Available at: https://www.cvedetails.com/vendor/74/PHP.html
[Accessed 10 May 2021].

CVE, 2021. *CVE Details.* [Online]
Available at: https://www.cvedetails.com/vendor/2337/Wordpress.html
[Accessed 10 May 2021].

Kinsta, 2019. *WordPress market share.* [Online]
Available at: https://kinsta.com/wordpress-market-share/
[Accessed 10 May 2021].

TryHackMe, 2020. *Mr Robot.* [Online]
Available at: https://tryhackme.com/room/mrrobot
[Accessed 16 May 2021].

TryHackMe, 2021. *Blog.* [Online]
Available at: https://tryhackme.com/room/blog
[Accessed 15 May 2021].

TryHackMe, 2021. *Cyber Scotland 2021.* [Online]
Available at: https://tryhackme.com/room/cyberweek2021
[Accessed 10 May 2021].

TryHackMe, 2021. *Internal.* [Online]
Available at: https://tryhackme.com/room/internal
[Accessed 16 May 2021].

TryHackMe, 2021. *Jack.* [Online]
Available at: https://tryhackme.com/room/jack
[Accessed 16 May 2021].

Vane, 2019. *Vane.* [Online]
Available at: https://github.com/delvelabs/vane
[Accessed 16 May 2021].

WPScan, 2021. *WPScan.* [Online]
Available at: https://github.com/wpscanteam/wpscan
[Accessed 16 May 2021].

# APPENDICES

## APPENDIX A – DATABASE CONFIGURATION

```
CREATE DATABASE wordpress_db;

CREATE USER 'wp_user'@'localhost' IDENTIFIED BY 'password';

GRANT ALL ON wordpress_db.* TO 'wp_user'@'localhost' IDENTIFIED BY
'password';

FLUSH PRIVILEGES;

Exit;
```

## APPENDIX B – WORDPRESS CONFIGURATIONS

VM Addons 1 - Most popular
-----------------
Contact Form 7 - 5.4.1
Yoast SEO - 16.2
Classic Editor - 1.6
Elementor Website Builder - 3.2.3
Akismet Spam Protection - 4.1.9
WooCommerce - 5.3.0
Jetpack - 9.7
Really Simple SSL - 4.0.15
WP forms - 1.6.7
Wordfence Security - 7.5.3
WordPress Importer - 0.7
Yoast Duplicate Post - 4.1.2
All-in-One WP Migration - 7.42
UpdraftPlus WordPress Backup Plugin - 1.16.56
MonsterInsights - 7.17.0
XML Sitemaps - 4.1.1
Redirection - 5.1.1
Advanced Custom Fields - 5.9.5
Regenerate Thumbnails - 3.1.5
Cookie Notice & Compliance for GDPR - 2.0.4
-------------------------------------------------------------

VM Addons 2 - Least popular

------------------------

woocommerce - 5.3.0
My Custom Ads Management - 1.0.0
Warehouse.Space - 20.2.1
Birthday mails bp - 1.0
Wijntransport - 1.4.1
RP Recreate Slugs - 1.1
Activity Link Preview For BuddyPress - 1.0
Mt8 Post Share - 1.0.1
Woo Aus EZi Freight - 1.1.3
Whitelist - 3.5
Embed JavaScript File Content - 1.0
The Buffer Button - 1.0
Free Guest Post - 1.3.1
Smart Popup - 1.0.2
GoalieTron - 1.3
Change Links - 1.1
Starcross MLB Standings Widget - 1.4.1

-----------------------

VM Addons 3 - Second most popular

----------------------

Smash Balloon Instagram Feed - 2.9.1
Coming Soon Page - 6.2.1
Better Search Replace - 1.3.4
Elementor - 1.5.9
One Click Demo Import - 3.0.2
Page Builder by SiteOrigin - 2.12.1
Gutenberg Template Library - 4.1.26
CookieYes - 2.0.1
Marketing Toolkit by OptinMonster - 2.3.3
iThemes Security - 7.9.1
Ninja Forms - 3.5.4
Custom Post Type UI - 1.9.1
Limit Login Attempts - 1.7.1
Hello Dolly - 1.7.2
TablePress - 1.13
WP Maintenance Mode - 2.4.0

VM Addons 4 - page 1000

---------------------------------

Bizuno Skins - 1.0

ClickSports Map - 1.2
Color Keywords - 1.0
Disc Golf Metrix - 2.0
Disc Space Usage - 1.1
Get YouTube Subs - 1.0
hAtom Missing Fields - 1.1.2
Hello Dolly - 1.7.2
Mujib Borsho Countdown - 2.0.3
plus twit like  - 0.01
Password Vault - 1.8.3
Surbma | GDPR Proof Gravity Forms - 3.0
SVT-Simple - 1.0.1
Swoop: Password-Free Authentication With 2FA - 1.2.1
Web Rank Get - 1.0
Widget Github Profile Card - 1.0.0
WordPress Document Automation - 1.0.0

VM Addons 5
---------------------------------
WP TXT Sitemap - 1.3
Custom 404 pages -  1.2
Background with Particle.js - 1.0.1
Random File - 1.8.10
WP-DuoShuo-Gravatar - 1.0
Checkout Styling for WooCommerce and Elementor - 1.0.0
Responsive Image Gallery - 4.0
AffiliateImporterAl - 2.0.5
Статистика сайта по счетчику LiveInternet.ru - 0.1
Simple Stopwatch - 1.0.0
Custom New User Notification - 1.1.4
WP Clear RSS Cache - 1.1
Sermon Manager Import - 0.2.5
Hybrid Hook Widgets - 0.1
RA Widgets Bundle - 1.0.3
Images Lazyload and Slideshow - 3.4
Share Line - 1.1
Passagens Promo - 1.6.1
weather press - 4.7
Admin Bar Login - 1.0.2
Simple Database Export+Import+Migration - 4.7.21
Yet Another Smooth Scroll - 4.4.25

## APPENDIX C – VM1 - VANE

```
Vane - a Free WordPress vulnerability scanner
[+] URL: http://192.168.78.129/wordpress/
[+] Started: Mon May 17 13:43:43 2021

[!] The WordPress 'http://192.168.78.129/wordpress/readme.html' file exists exposing a version number
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.46 (Ubuntu)
[+] XML-RPC Interface available under: http://192.168.78.129/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled: http://192.168.78.129/wordpress/wp-content/uploads/

[+] WordPress version 5.7.2 identified from links opml

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

[+] Name: twentytwentyone - v1.3
 |  Location: http://192.168.78.129/wordpress/wp-content/themes/twentytwentyone/
 |  Readme: http://192.168.78.129/wordpress/wp-content/themes/twentytwentyone/readme.txt
 |  Style URL: http://192.168.78.129/wordpress/wp-content/themes/twentytwentyone/style.css
 |  Referenced style.css: http://localhost/wordpress/wp-content/themes/twentytwentyone/style.css
 |  Theme Name: Twenty Twenty-One
 |  Theme URI: https://wordpress.org/themes/twentytwentyone/
 |  Description: Twenty Twenty-One is a blank canvas for your ideas and it makes the block editor your best brush. With new block patterns, which allow you to create a beautiful layout in a matter of seconds, this theme's soft colors and eye-catching — yet timeless — design will let your work shine. Take it for a spin! See how Twenty Twenty-One elevates your portfolio, business website, or personal blog.
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: one-column, accessibility-ready, custom-colors, custom-menu, custom-logo, editor-style, featured-images, footer-widgets, block-patterns, rtl-language-support, sticky-post, threaded-comments, translation-ready
 |  Text Domain: twentytwentyone

[+] Enumerating installed plugins  ...

   Time: 00:00:01
<=================================================================================================>
(1829 / 1829) 100.00% Time: 00:00:01
```

```
[+] We found 16 plugins:

[+] Name: advanced-custom-fields - v5.9.5
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/advanced-custom-fields/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/advanced-custom-fields/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/advanced-custom-fields/

[+] Name: akismet - v4.1.9
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/akismet/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/akismet/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-content/plugins/akismet/changelog.txt

[+] Name: contact-form-7 - v5.4.1
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/contact-form-7/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/contact-form-7/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/contact-form-7/

[+] Name: cookie-notice - v2.0.4
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/cookie-notice/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/cookie-notice/readme.txt

[+] Name: duplicate-post - v4.1.2
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/duplicate-post/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/duplicate-post/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/duplicate-post/

[+] Name: google-analytics-for-wordpress - v7.17.0
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/google-analytics-for-wordpress/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/google-analytics-for-wordpress/readme.txt

[+] Name: google-sitemap-generator - v4.1.1
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/google-sitemap-generator/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/google-sitemap-generator/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/google-sitemap-generator/

[+] Name: jetpack - v9.7
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/jetpack/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/jetpack/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/jetpack/
[!] Title: ** DISPUTED ** SQL injection vulnerability in modules/sharedaddy.php in the Jetpack plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter
    Reference: http://xforce.iss.net/xforce/xfdb/71404
    Reference: http://www.securityfocus.com/bid/50730
    Reference: http://www.exploit-db.com/exploits/18126
    Reference: https://exchange.xforce.ibmcloud.com/vulnerabilities/71404
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4673
[i] CVSS: 7.5

[+] Name: really-simple-ssl - v4.0.15
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/really-simple-ssl/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/really-simple-ssl/readme.txt

[+] Name: redirection - v5.1.1
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/redirection/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/redirection/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/redirection/

[+] Name: regenerate-thumbnails - v3.1.5
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/regenerate-thumbnails/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/regenerate-thumbnails/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/regenerate-thumbnails/

[+] Name: updraftplus - v1.16.56
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/updraftplus/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/updraftplus/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-content/plugins/updraftplus/changelog.txt

[+] Name: woocommerce - v5.3.0
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/

[!] Title: WooCommerce 2.0.17 - hide-wc-extensions-message Parameter Reflected XSS
    Reference: http://packetstormsecurity.com/files/123684/
    Reference: http://www.securityfocus.com/bid/63228
    Reference: http://osvdb.org/98754
    Reference: https://wpvulndb.com/vulnerabilities/6673

[+] Name: wordpress-importer - v0.7
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-importer/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-importer/readme.txt
```

```
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-
importer/

[+] Name: wordpress-seo - v16.2
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/readme.txt

[+] Name: wpforms-lite - v1.6.7
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/wpforms-lite/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/wpforms-lite/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-content/plugins/wpforms-lite/changelog.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/wpforms-lite/

[+] Finished: Mon May 17 13:43:50 2021
[+] Memory used: 217.34 MB
[+] Elapsed time: 00:00:04
Vane - a Free WordPress vulnerability scanner
[+] URL: http://192.168.78.129/wordpress/
[+] Started: Mon May 17 13:43:50 2021

[!] The WordPress 'http://192.168.78.129/wordpress/readme.html' file exists exposing a
version number
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-json/>;
rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.46 (Ubuntu)
[+] XML-RPC Interface available under: http://192.168.78.129/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled: http://192.168.78.129/wordpress/wp-
content/uploads/

[+] WordPress version 5.7.2 identified from links opml

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

[+] Name: twentytwentyone - v1.3
 |  Location: http://192.168.78.129/wordpress/wp-content/themes/twentytwentyone/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/readme.txt
 |  Style URL: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Referenced style.css: http://localhost/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Theme Name: Twenty Twenty-One
 |  Theme URI: https://wordpress.org/themes/twentytwentyone/
 |  Description: Twenty Twenty-One is a blank canvas for your ideas and it makes the block
editor your best brush. With new block patterns, which allow you to create a beautiful layout
in a matter of seconds, this theme’s soft colors and eye-catching — yet timeless — design will
let your work shine. Take it for a spin! See how Twenty Twenty-One elevates your portfolio,
business website, or personal blog.
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: one-column, accessibility-ready, custom-colors, custom-menu, custom-logo, editor-
style, featured-images, footer-widgets, block-patterns, rtl-language-support, sticky-post,
threaded-comments, translation-ready
 |  Text Domain: twentytwentyone

[+] Enumerating installed plugins  ...

  Time: 00:00:01
<============================================================================
===> (1829 / 1829) 100.00% Time: 00:00:01

[+] We found 16 plugins:

[+] Name: advanced-custom-fields - v5.9.5
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/advanced-custom-fields/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/advanced-custom-
fields/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/advanced-custom-fields/

[+] Name: akismet - v4.1.9
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/akismet/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/akismet/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-content/plugins/akismet/changelog.txt

[+] Name: contact-form-7 - v5.4.1
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/contact-form-7/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/contact-form-
7/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/contact-
form-7/

[+] Name: cookie-notice - v2.0.4
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/cookie-notice/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/cookie-notice/readme.txt
```

```
[+] Name: duplicate-post - v4.1.2
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/duplicate-post/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/duplicate-post/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/duplicate-post/

[+] Name: google-analytics-for-wordpress - v7.17.0
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/google-analytics-for-
wordpress/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/google-analytics-for-
wordpress/readme.txt

[+] Name: google-sitemap-generator - v4.1.1
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/google-sitemap-
generator/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/google-sitemap-
generator/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/google-
sitemap-generator/

[+] Name: jetpack - v9.7
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/jetpack/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/jetpack/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/jetpack/

[!] Title: ** DISPUTED ** SQL injection vulnerability in modules/sharedaddy.php in the Jetpack
plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the id
parameter
    Reference: http://xforce.iss.net/xforce/xfdb/71404
    Reference: http://www.securityfocus.com/bid/50730
    Reference: http://www.exploit-db.com/exploits/18126
    Reference: https://exchange.xforce.ibmcloud.com/vulnerabilities/71404
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4673
[i] CVSS: 7.5

[+] Name: really-simple-ssl - v4.0.15
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/really-simple-ssl/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/really-simple-
ssl/readme.txt

[+] Name: redirection - v5.1.1
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/redirection/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/redirection/readme.txt
```

```
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/redirection/

[+] Name: regenerate-thumbnails - v3.1.5
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/regenerate-thumbnails/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/regenerate-thumbnails/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/regenerate-thumbnails/

[+] Name: updraftplus - v1.16.56
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/updraftplus/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/updraftplus/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-content/plugins/updraftplus/changelog.txt

[+] Name: woocommerce - v5.3.0
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/

[!] Title: WooCommerce 2.0.17 - hide-wc-extensions-message Parameter Reflected XSS
    Reference: http://packetstormsecurity.com/files/123684/
    Reference: http://www.securityfocus.com/bid/63228
    Reference: http://osvdb.org/98754
    Reference: https://wpvulndb.com/vulnerabilities/6673

[+] Name: wordpress-importer - v0.7
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-importer/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-importer/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-importer/

[+] Name: wordpress-seo - v16.2
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/readme.txt

[+] Name: wpforms-lite - v1.6.7
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/wpforms-lite/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/wpforms-lite/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-content/plugins/wpforms-
lite/changelog.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/wpforms-lite/

[+] Finished: Mon May 17 13:43:54 2021
[+] Memory used: 223.566 MB
[+] Elapsed time: 00:00:04
Vane - a Free WordPress vulnerability scanner
[+] URL: http://192.168.78.129/wordpress/
[+] Started: Mon May 17 13:43:50 2021

[!] The WordPress 'http://192.168.78.129/wordpress/readme.html' file exists exposing a
version number
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-json/>;
rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.46 (Ubuntu)
[+] XML-RPC Interface available under: http://192.168.78.129/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled: http://192.168.78.129/wordpress/wp-
content/uploads/

[+] WordPress version 5.7.2 identified from links opml

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

[+] Name: twentytwentyone - v1.3
 |  Location: http://192.168.78.129/wordpress/wp-content/themes/twentytwentyone/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/readme.txt
 |  Style URL: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Referenced style.css: http://localhost/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Theme Name: Twenty Twenty-One
 |  Theme URI: https://wordpress.org/themes/twentytwentyone/
 |  Description: Twenty Twenty-One is a blank canvas for your ideas and it makes the block
editor your best brush. With new block patterns, which allow you to create a beautiful layout
in a matter of seconds, this theme’s soft colors and eye-catching — yet timeless — design will
let your work shine. Take it for a spin! See how Twenty Twenty-One elevates your portfolio,
business website, or personal blog.
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: one-column, accessibility-ready, custom-colors, custom-menu, custom-logo, editor-
style, featured-images, footer-widgets, block-patterns, rtl-language-support, sticky-post,
threaded-comments, translation-ready
 |  Text Domain: twentytwentyone

[+] Enumerating installed plugins  ...

   Time: 00:00:01
<==========================================================================
===> (1829 / 1829) 100.00% Time: 00:00:01

[+] We found 16 plugins:

[+] Name: advanced-custom-fields - v5.9.5
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/advanced-custom-fields/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/advanced-custom-
fields/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/advanced-custom-fields/

[+] Name: akismet - v4.1.9
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/akismet/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/akismet/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-content/plugins/akismet/changelog.txt

[+] Name: contact-form-7 - v5.4.1
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/contact-form-7/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/contact-form-
7/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/contact-
form-7/

[+] Name: cookie-notice - v2.0.4
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/cookie-notice/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/cookie-notice/readme.txt

[+] Name: duplicate-post - v4.1.2
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/duplicate-post/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/duplicate-post/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/duplicate-post/

[+] Name: google-analytics-for-wordpress - v7.17.0
```

```
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/google-analytics-for-wordpress/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/google-analytics-for-wordpress/readme.txt

[+] Name: google-sitemap-generator - v4.1.1
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/google-sitemap-generator/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/google-sitemap-generator/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/google-sitemap-generator/

[+] Name: jetpack - v9.7
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/jetpack/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/jetpack/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/jetpack/

[!] Title: ** DISPUTED ** SQL injection vulnerability in modules/sharedaddy.php in the Jetpack plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter
    Reference: http://xforce.iss.net/xforce/xfdb/71404
    Reference: http://www.securityfocus.com/bid/50730
    Reference: http://www.exploit-db.com/exploits/18126
    Reference: https://exchange.xforce.ibmcloud.com/vulnerabilities/71404
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4673
[i] CVSS: 7.5

[+] Name: really-simple-ssl - v4.0.15
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/really-simple-ssl/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/really-simple-ssl/readme.txt

[+] Name: redirection - v5.1.1
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/redirection/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/redirection/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/redirection/

[+] Name: regenerate-thumbnails - v3.1.5
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/regenerate-thumbnails/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/regenerate-thumbnails/readme.txt
```

```
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/regenerate-thumbnails/

[+] Name: updraftplus - v1.16.56
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/updraftplus/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/updraftplus/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-
content/plugins/updraftplus/changelog.txt

[+] Name: woocommerce - v5.3.0
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/plugins/woocommerce/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/woocommerce/

[!] Title: WooCommerce 2.0.17 - hide-wc-extensions-message Parameter Reflected XSS
    Reference: http://packetstormsecurity.com/files/123684/
    Reference: http://www.securityfocus.com/bid/63228
    Reference: http://osvdb.org/98754
    Reference: https://wpvulndb.com/vulnerabilities/6673

[+] Name: wordpress-importer - v0.7
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-importer/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-
importer/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/wordpress-importer/

[+] Name: wordpress-seo - v16.2
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-
seo/readme.txt

[+] Name: wpforms-lite - v1.6.7
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/wpforms-lite/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/wpforms-lite/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-content/plugins/wpforms-
lite/changelog.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/wpforms-lite/

[+] Finished: Mon May 17 13:43:54 2021
[+] Memory used: 223.566 MB
[+] Elapsed time: 00:00:04
Vane - a Free WordPress vulnerability scanner
[+] URL: http://192.168.78.129/wordpress/
[+] Started: Mon May 17 13:43:59 2021

[!] The WordPress 'http://192.168.78.129/wordpress/readme.html' file exists exposing a
version number
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-json/>;
rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.46 (Ubuntu)
[+] XML-RPC Interface available under: http://192.168.78.129/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled: http://192.168.78.129/wordpress/wp-
content/uploads/

[+] WordPress version 5.7.2 identified from links opml

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

[+] Name: twentytwentyone - v1.3
 |  Location: http://192.168.78.129/wordpress/wp-content/themes/twentytwentyone/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/readme.txt
 |  Style URL: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Referenced style.css: http://localhost/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Theme Name: Twenty Twenty-One
 |  Theme URI: https://wordpress.org/themes/twentytwentyone/
 |  Description: Twenty Twenty-One is a blank canvas for your ideas and it makes the block
editor your best brush. With new block patterns, which allow you to create a beautiful layout
in a matter of seconds, this theme’s soft colors and eye-catching — yet timeless — design will
let your work shine. Take it for a spin! See how Twenty Twenty-One elevates your portfolio,
business website, or personal blog.
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: one-column, accessibility-ready, custom-colors, custom-menu, custom-logo, editor-
style, featured-images, footer-widgets, block-patterns, rtl-language-support, sticky-post,
threaded-comments, translation-ready
 |  Text Domain: twentytwentyone

[+] Enumerating installed plugins  ...
```

```
  Time: 00:00:01
<==========================================================================
===> (1829 / 1829) 100.00% Time: 00:00:01

[+] We found 16 plugins:

[+] Name: advanced-custom-fields - v5.9.5
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/advanced-custom-fields/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/advanced-custom-
fields/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/advanced-custom-fields/

[+] Name: akismet - v4.1.9
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/akismet/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/akismet/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-content/plugins/akismet/changelog.txt

[+] Name: contact-form-7 - v5.4.1
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/contact-form-7/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/contact-form-
7/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/contact-
form-7/

[+] Name: cookie-notice - v2.0.4
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/cookie-notice/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/cookie-notice/readme.txt

[+] Name: duplicate-post - v4.1.2
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/duplicate-post/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/duplicate-post/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/duplicate-post/

[+] Name: google-analytics-for-wordpress - v7.17.0
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/google-analytics-for-
wordpress/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/google-analytics-for-
wordpress/readme.txt

[+] Name: google-sitemap-generator - v4.1.1
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/google-sitemap-
generator/
```

```
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/google-sitemap-
generator/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/google-
sitemap-generator/

[+] Name: jetpack - v9.7
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/jetpack/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/jetpack/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/jetpack/

[!] Title: ** DISPUTED ** SQL injection vulnerability in modules/sharedaddy.php in the Jetpack
plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the id
parameter
    Reference: http://xforce.iss.net/xforce/xfdb/71404
    Reference: http://www.securityfocus.com/bid/50730
    Reference: http://www.exploit-db.com/exploits/18126
    Reference: https://exchange.xforce.ibmcloud.com/vulnerabilities/71404
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4673
[i] CVSS: 7.5

[+] Name: really-simple-ssl - v4.0.15
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/really-simple-ssl/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/really-simple-
ssl/readme.txt

[+] Name: redirection - v5.1.1
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/redirection/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/redirection/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/redirection/

[+] Name: regenerate-thumbnails - v3.1.5
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/regenerate-thumbnails/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/regenerate-
thumbnails/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/regenerate-thumbnails/

[+] Name: updraftplus - v1.16.56
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/updraftplus/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/updraftplus/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-
content/plugins/updraftplus/changelog.txt
```

```
[+] Name: woocommerce - v5.3.0
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/plugins/woocommerce/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/woocommerce/

[!] Title: WooCommerce 2.0.17 - hide-wc-extensions-message Parameter Reflected XSS
    Reference: http://packetstormsecurity.com/files/123684/
    Reference: http://www.securityfocus.com/bid/63228
    Reference: http://osvdb.org/98754
    Reference: https://wpvulndb.com/vulnerabilities/6673

[+] Name: wordpress-importer - v0.7
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-importer/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-
importer/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/wordpress-importer/

[+] Name: wordpress-seo - v16.2
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-
seo/readme.txt

[+] Name: wpforms-lite - v1.6.7
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/wpforms-lite/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/wpforms-lite/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-content/plugins/wpforms-
lite/changelog.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/wpforms-lite/

[+] Finished: Mon May 17 13:44:03 2021
[+] Memory used: 220.395 MB
[+] Elapsed time: 00:00:04
Vane - a Free WordPress vulnerability scanner
[+] URL: http://192.168.78.129/wordpress/
[+] Started: Mon May 17 13:44:04 2021

[!] The WordPress 'http://192.168.78.129/wordpress/readme.html' file exists exposing a
version number
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-json/>;
rel="https://api.w.org/"
```

```
[+] Interesting header: SERVER: Apache/2.4.46 (Ubuntu)
[+] XML-RPC Interface available under: http://192.168.78.129/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled: http://192.168.78.129/wordpress/wp-
content/uploads/

[+] WordPress version 5.7.2 identified from links opml

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

[+] Name: twentytwentyone - v1.3
 |  Location: http://192.168.78.129/wordpress/wp-content/themes/twentytwentyone/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/readme.txt
 |  Style URL: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Referenced style.css: http://localhost/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Theme Name: Twenty Twenty-One
 |  Theme URI: https://wordpress.org/themes/twentytwentyone/
 |  Description: Twenty Twenty-One is a blank canvas for your ideas and it makes the block
editor your best brush. With new block patterns, which allow you to create a beautiful layout
in a matter of seconds, this theme’s soft colors and eye-catching — yet timeless — design will
let your work shine. Take it for a spin! See how Twenty Twenty-One elevates your portfolio,
business website, or personal blog.
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: one-column, accessibility-ready, custom-colors, custom-menu, custom-logo, editor-
style, featured-images, footer-widgets, block-patterns, rtl-language-support, sticky-post,
threaded-comments, translation-ready
 |  Text Domain: twentytwentyone

[+] Enumerating installed plugins  ...

   Time: 00:00:01
<=============================================================================
===> (1829 / 1829) 100.00% Time: 00:00:01

[+] We found 16 plugins:

[+] Name: advanced-custom-fields - v5.9.5
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/advanced-custom-fields/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/advanced-custom-fields/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/advanced-custom-fields/

[+] Name: akismet - v4.1.9
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/akismet/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/akismet/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-content/plugins/akismet/changelog.txt

[+] Name: contact-form-7 - v5.4.1
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/contact-form-7/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/contact-form-7/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/contact-form-7/

[+] Name: cookie-notice - v2.0.4
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/cookie-notice/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/cookie-notice/readme.txt

[+] Name: duplicate-post - v4.1.2
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/duplicate-post/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/duplicate-post/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/duplicate-post/

[+] Name: google-analytics-for-wordpress - v7.17.0
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/google-analytics-for-wordpress/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/google-analytics-for-wordpress/readme.txt

[+] Name: google-sitemap-generator - v4.1.1
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/google-sitemap-generator/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/google-sitemap-generator/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/google-sitemap-generator/

[+] Name: jetpack - v9.7
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/jetpack/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/jetpack/readme.txt
```

```
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/jetpack/

[!] Title: ** DISPUTED ** SQL injection vulnerability in modules/sharedaddy.php in the Jetpack plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter
    Reference: http://xforce.iss.net/xforce/xfdb/71404
    Reference: http://www.securityfocus.com/bid/50730
    Reference: http://www.exploit-db.com/exploits/18126
    Reference: https://exchange.xforce.ibmcloud.com/vulnerabilities/71404
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4673
[i] CVSS: 7.5

[+] Name: really-simple-ssl - v4.0.15
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/really-simple-ssl/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/really-simple-ssl/readme.txt

[+] Name: redirection - v5.1.1
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/redirection/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/redirection/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/redirection/

[+] Name: regenerate-thumbnails - v3.1.5
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/regenerate-thumbnails/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/regenerate-thumbnails/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/regenerate-thumbnails/

[+] Name: updraftplus - v1.16.56
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/updraftplus/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/updraftplus/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-content/plugins/updraftplus/changelog.txt

[+] Name: woocommerce - v5.3.0
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/

[!] Title: WooCommerce 2.0.17 - hide-wc-extensions-message Parameter Reflected XSS
```

```
 Reference: http://packetstormsecurity.com/files/123684/
 Reference: http://www.securityfocus.com/bid/63228
 Reference: http://osvdb.org/98754
 Reference: https://wpvulndb.com/vulnerabilities/6673

[+] Name: wordpress-importer - v0.7
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-importer/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-
importer/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/wordpress-importer/

[+] Name: wordpress-seo - v16.2
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-
seo/readme.txt

[+] Name: wpforms-lite - v1.6.7
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/wpforms-lite/
 |  Readme: http://192.168.78.129/wordpress/wp-content/plugins/wpforms-lite/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-content/plugins/wpforms-
lite/changelog.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/wpforms-lite/

[+] Finished: Mon May 17 13:44:08 2021
[+] Memory used: 221.172 MB
[+] Elapsed time: 00:00:04
```

## APPENDIX C – VM1 - WPSCAN

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

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

```
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 13:17:45 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.46 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.
```

```
[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] google-analytics-for-wordpress
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/google-analytics-for-wordpress/
 | Latest Version: 7.17.0 (up to date)
 | Last Updated: 2021-04-28T04:17:00.000Z
 |
 | Found By: Monster Insights Comment (Passive Detection)
 |
 | Version: 7.17.0 (100% confidence)
 | Found By: Monster Insights Comment (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'Google Analytics by MonsterInsights plugin v7.17.0 -'
 | Confirmed By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.78.129/wordpress/wp-content/plugins/google-analytics-for-wordpress/readme.txt

[+] woocommerce
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/
 | Latest Version: 5.3.0 (up to date)
 | Last Updated: 2021-05-11T17:11:00.000Z
 |
 | Found By: Meta Generator (Passive Detection)
 |
 | Version: 5.3.0 (100% confidence)
 | Found By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WooCommerce 5.3.0'
 | Confirmed By:
 |  Readme - Stable Tag (Aggressive Detection)
 |   - http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/readme.txt
 |  Readme - ChangeLog Section (Aggressive Detection)
 |   - http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/readme.txt

[+] wordpress-seo
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/
 | Latest Version: 16.2 (up to date)
 | Last Updated: 2021-04-28T09:37:00.000Z
 |
 | Found By: Comment (Passive Detection)
 |
 | Version: 16.2 (100% confidence)
 | Found By: Comment (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'optimized with the Yoast SEO plugin v16.2 -'
 | Confirmed By:
 |  Readme - Stable Tag (Aggressive Detection)
 |   - http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/readme.txt
 |  Readme - ChangeLog Section (Aggressive Detection)
 |   - http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/readme.txt

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<========================================================> (348 / 348) 100.00% Time:
00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<======================================================> (2568 / 2568) 100.00% Time:
00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00
<=========================================================> (137 / 137) 100.00% Time:
00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<===============================================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<==========================================================> (10 / 10) 100.00% Time:
00:00:00

[i] User(s) Identified:

[+] rory
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpscan.com/register

[+] Finished: Mon May 17 13:17:49 2021
[+] Requests Done: 3138
[+] Cached Requests: 43
[+] Data Sent: 868.902 KB
[+] Data Received: 439.818 KB
[+] Memory used: 208.379 MB
[+] Elapsed time: 00:00:04
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 13:17:51 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.46 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] google-analytics-for-wordpress
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/google-analytics-for-wordpress/
 | Latest Version: 7.17.0 (up to date)
 | Last Updated: 2021-04-28T04:17:00.000Z
 |
 | Found By: Monster Insights Comment (Passive Detection)
 |
 | Version: 7.17.0 (100% confidence)
 | Found By: Monster Insights Comment (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'Google Analytics by MonsterInsights plugin v7.17.0 -'
 | Confirmed By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.78.129/wordpress/wp-content/plugins/google-analytics-for-wordpress/readme.txt

[+] woocommerce
```

```
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/
 | Latest Version: 5.3.0 (up to date)
 | Last Updated: 2021-05-11T17:11:00.000Z
 |
 | Found By: Meta Generator (Passive Detection)
 |
 | Version: 5.3.0 (100% confidence)
 | Found By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WooCommerce 5.3.0'
 | Confirmed By:
 |  Readme - Stable Tag (Aggressive Detection)
 |   - http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/readme.txt
 |  Readme - ChangeLog Section (Aggressive Detection)
 |   - http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/readme.txt

[+] wordpress-seo
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/
 | Latest Version: 16.2 (up to date)
 | Last Updated: 2021-04-28T09:37:00.000Z
 |
 | Found By: Comment (Passive Detection)
 |
 | Version: 16.2 (100% confidence)
 | Found By: Comment (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'optimized with the Yoast SEO plugin v16.2 -'
 | Confirmed By:
 |  Readme - Stable Tag (Aggressive Detection)
 |   - http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/readme.txt
 |  Readme - ChangeLog Section (Aggressive Detection)
 |   - http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/readme.txt

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<===============================================================> (348 / 348) 100.00% Time:
00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<=============================================================> (2568 / 2568) 100.00% Time:
00:00:01

[i] No Timthumbs Found.
```

```
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00
<============================================================> (137 / 137) 100.00% Time:
00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<==================================================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<=============================================================> (10 / 10) 100.00% Time:
00:00:00

[i] User(s) Identified:

[+] rory
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpscan.com/register

[+] Finished: Mon May 17 13:17:56 2021
[+] Requests Done: 3138
[+] Cached Requests: 43
[+] Data Sent: 868.902 KB
[+] Data Received: 439.818 KB
[+] Memory used: 208.418 MB
[+] Elapsed time: 00:00:04
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|
         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 13:17:57 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.46 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] google-analytics-for-wordpress
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/google-analytics-for-wordpress/
 | Latest Version: 7.17.0 (up to date)
 | Last Updated: 2021-04-28T04:17:00.000Z
 |
 | Found By: Monster Insights Comment (Passive Detection)
 |
 | Version: 7.17.0 (100% confidence)
 | Found By: Monster Insights Comment (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'Google Analytics by MonsterInsights plugin v7.17.0 -'
 | Confirmed By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.78.129/wordpress/wp-content/plugins/google-analytics-for-wordpress/readme.txt

[+] woocommerce
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/
 | Latest Version: 5.3.0 (up to date)
 | Last Updated: 2021-05-11T17:11:00.000Z
 |
 | Found By: Meta Generator (Passive Detection)
 |
 | Version: 5.3.0 (100% confidence)
 | Found By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WooCommerce 5.3.0'
 | Confirmed By:
 |  Readme - Stable Tag (Aggressive Detection)
 |   - http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/readme.txt
 |  Readme - ChangeLog Section (Aggressive Detection)
 |   - http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/readme.txt

[+] wordpress-seo
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/
 | Latest Version: 16.2 (up to date)
 | Last Updated: 2021-04-28T09:37:00.000Z
 |
 | Found By: Comment (Passive Detection)
 |
 | Version: 16.2 (100% confidence)
 | Found By: Comment (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'optimized with the Yoast SEO plugin v16.2 -'
 | Confirmed By:
 |  Readme - Stable Tag (Aggressive Detection)
 |   - http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/readme.txt
 |  Readme - ChangeLog Section (Aggressive Detection)
 |   - http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/readme.txt

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<========================================================> (348 / 348) 100.00% Time:
00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<======================================================> (2568 / 2568) 100.00% Time:
00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00
<=========================================================> (137 / 137) 100.00% Time:
00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<===============================================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<==========================================================> (10 / 10) 100.00% Time:
00:00:00
```

```
[i] User(s) Identified:

[+] rory
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpscan.com/register

[+] Finished: Mon May 17 13:18:02 2021
[+] Requests Done: 3138
[+] Cached Requests: 43
[+] Data Sent: 868.902 KB
[+] Data Received: 439.855 KB
[+] Memory used: 208.516 MB
[+] Elapsed time: 00:00:04
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 13:18:04 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.46 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
```

```
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] google-analytics-for-wordpress
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/google-analytics-for-wordpress/
 | Latest Version: 7.17.0 (up to date)
 | Last Updated: 2021-04-28T04:17:00.000Z
 |
 | Found By: Monster Insights Comment (Passive Detection)
 |
 | Version: 7.17.0 (100% confidence)
 | Found By: Monster Insights Comment (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'Google Analytics by MonsterInsights plugin v7.17.0 -'
 | Confirmed By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.78.129/wordpress/wp-content/plugins/google-analytics-for-wordpress/readme.txt

[+] woocommerce
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/
 | Latest Version: 5.3.0 (up to date)
 | Last Updated: 2021-05-11T17:11:00.000Z
 |
 | Found By: Meta Generator (Passive Detection)
 |
 | Version: 5.3.0 (100% confidence)
 | Found By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WooCommerce 5.3.0'
 | Confirmed By:
 |  Readme - Stable Tag (Aggressive Detection)
 |   - http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/readme.txt
 |  Readme - ChangeLog Section (Aggressive Detection)
 |   - http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/readme.txt

[+] wordpress-seo
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/
 | Latest Version: 16.2 (up to date)
 | Last Updated: 2021-04-28T09:37:00.000Z
 |
 | Found By: Comment (Passive Detection)
 |
 | Version: 16.2 (100% confidence)
 | Found By: Comment (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'optimized with the Yoast SEO plugin v16.2 -'
 | Confirmed By:
 |  Readme - Stable Tag (Aggressive Detection)
 |   - http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/readme.txt
 |  Readme - ChangeLog Section (Aggressive Detection)
 |   - http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/readme.txt

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<========================================================> (348 / 348) 100.00% Time:
00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
```

```
 Checking Known Locations - Time: 00:00:01
<==========================================================> (2568 / 2568) 100.00% Time:
00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00
<=============================================================> (137 / 137) 100.00% Time:
00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<===================================================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<==============================================================> (10 / 10) 100.00% Time:
00:00:00

[i] User(s) Identified:

[+] rory
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpscan.com/register

[+] Finished: Mon May 17 13:18:08 2021
[+] Requests Done: 3138
[+] Cached Requests: 43
[+] Data Sent: 868.902 KB
[+] Data Received: 439.837 KB
[+] Memory used: 208.578 MB
[+] Elapsed time: 00:00:04 _____________________________________________________________
    __          _______   _____
    \ \        / /  __ \ / ____|
     \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
```

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

     WordPress Security Scanner by the WPScan Team
                     Version 3.8.10
   Sponsored by Automattic - https://automattic.com/
   @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 13:18:10 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.46 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299
```

```
[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] google-analytics-for-wordpress
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/google-analytics-for-wordpress/
 | Latest Version: 7.17.0 (up to date)
 | Last Updated: 2021-04-28T04:17:00.000Z
 |
 | Found By: Monster Insights Comment (Passive Detection)
 |
 | Version: 7.17.0 (100% confidence)
 | Found By: Monster Insights Comment (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'Google Analytics by MonsterInsights plugin v7.17.0 -'
 | Confirmed By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.78.129/wordpress/wp-content/plugins/google-analytics-for-wordpress/readme.txt

[+] woocommerce
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/
 | Latest Version: 5.3.0 (up to date)
 | Last Updated: 2021-05-11T17:11:00.000Z
 |
 | Found By: Meta Generator (Passive Detection)
 |
 | Version: 5.3.0 (100% confidence)
 | Found By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WooCommerce 5.3.0'
 | Confirmed By:
 |  Readme - Stable Tag (Aggressive Detection)
 |   - http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/readme.txt
 |  Readme - ChangeLog Section (Aggressive Detection)
 |   - http://192.168.78.129/wordpress/wp-content/plugins/woocommerce/readme.txt

[+] wordpress-seo
```

```
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/
 | Latest Version: 16.2 (up to date)
 | Last Updated: 2021-04-28T09:37:00.000Z
 |
 | Found By: Comment (Passive Detection)
 |
 | Version: 16.2 (100% confidence)
 | Found By: Comment (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'optimized with the Yoast SEO plugin v16.2 -'
 | Confirmed By:
 |  Readme - Stable Tag (Aggressive Detection)
 |   - http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/readme.txt
 |  Readme - ChangeLog Section (Aggressive Detection)
 |   - http://192.168.78.129/wordpress/wp-content/plugins/wordpress-seo/readme.txt

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<========================================================> (348 / 348) 100.00% Time:
00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<======================================================> (2568 / 2568) 100.00% Time:
00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00
<=========================================================> (137 / 137) 100.00% Time:
00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<===============================================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
```

```
 Brute Forcing Author IDs - Time: 00:00:00
<=========================================================> (10 / 10) 100.00% Time:
00:00:00

[i] User(s) Identified:

[+] rory
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpscan.com/register

[+] Finished: Mon May 17 13:18:14 2021
[+] Requests Done: 3138
[+] Cached Requests: 43
[+] Data Sent: 868.902 KB
[+] Data Received: 439.818 KB
[+] Memory used: 207.992 MB
[+] Elapsed time: 00:00:04
```

## APPENDIX D - VM2 – VANE

```
Vane - a Free WordPress vulnerability scanner
[i] The remote host tried to redirect to:
http://localhost/wordpress/?FSEG-Roadblock
[?] Do you want follow the redirection ? [Y]es [N]o [A]bort, default: [N]n
[+] URL: http://192.168.78.129/wordpress/
[+] Started: Mon May 17 14:07:19 2021

[!] The WordPress 'http://192.168.78.129/wordpress/readme.html' file
exists exposing a version number
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-
json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.46 (Ubuntu)
[+] Interesting header: X-REDIRECT-BY: WordPress
[+] XML-RPC Interface available under:
http://192.168.78.129/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/

[+] WordPress version 5.7.2 identified from links opml

[+] Enumerating installed plugins  ...

   Time: 00:00:01
<=========================================================================
======> (1829 / 1829) 100.00% Time: 00:00:01
```

```
[+] We found 1 plugins:

[+] Name: woocommerce - v5.3.0
 |  Location: http://192.168.78.129/wordpress/wp-
content/plugins/woocommerce/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/plugins/woocommerce/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/woocommerce/

[!] Title: WooCommerce 2.0.17 - hide-wc-extensions-message Parameter
Reflected XSS
    Reference: http://packetstormsecurity.com/files/123684/
    Reference: http://www.securityfocus.com/bid/63228
    Reference: http://osvdb.org/98754
    Reference: https://wpvulndb.com/vulnerabilities/6673

[+] Finished: Mon May 17 14:07:26 2021
[+] Memory used: 230.367 MB
[+] Elapsed time: 00:00:06
Vane - a Free WordPress vulnerability scanner
[i] The remote host tried to redirect to:
http://localhost/wordpress/?FSEG-Roadblock
[?] Do you want follow the redirection ? [Y]es [N]o [A]bort, default: [N]n
[+] URL: http://192.168.78.129/wordpress/
[+] Started: Mon May 17 14:07:29 2021

[!] The WordPress 'http://192.168.78.129/wordpress/readme.html' file
exists exposing a version number
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-
json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.46 (Ubuntu)
[+] Interesting header: X-REDIRECT-BY: WordPress
[+] XML-RPC Interface available under:
http://192.168.78.129/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/

[+] WordPress version 5.7.2 identified from links opml

[+] Enumerating installed plugins  ...

   Time: 00:00:01
<=========================================================================
======> (1829 / 1829) 100.00% Time: 00:00:01

[+] We found 1 plugins:

[+] Name: woocommerce - v5.3.0
 |  Location: http://192.168.78.129/wordpress/wp-
content/plugins/woocommerce/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/plugins/woocommerce/readme.txt
```

```
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/woocommerce/

[!] Title: WooCommerce 2.0.17 - hide-wc-extensions-message Parameter
Reflected XSS
    Reference: http://packetstormsecurity.com/files/123684/
    Reference: http://www.securityfocus.com/bid/63228
    Reference: http://osvdb.org/98754
    Reference: https://wpvulndb.com/vulnerabilities/6673

[+] Finished: Mon May 17 14:07:33 2021
[+] Memory used: 231.039 MB
[+] Elapsed time: 00:00:03
Vane - a Free WordPress vulnerability scanner
[i] The remote host tried to redirect to:
http://localhost/wordpress/?FSEG-Roadblock
[?] Do you want follow the redirection ? [Y]es [N]o [A]bort, default: [N]n
[+] URL: http://192.168.78.129/wordpress/
[+] Started: Mon May 17 14:07:35 2021

[!] The WordPress 'http://192.168.78.129/wordpress/readme.html' file
exists exposing a version number
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-
json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.46 (Ubuntu)
[+] Interesting header: X-REDIRECT-BY: WordPress
[+] XML-RPC Interface available under:
http://192.168.78.129/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/

[+] WordPress version 5.7.2 identified from links opml

[+] Enumerating installed plugins  ...

   Time: 00:00:01
<==========================================================================
======> (1829 / 1829) 100.00% Time: 00:00:01

[+] We found 1 plugins:

[+] Name: woocommerce - v5.3.0
 |  Location: http://192.168.78.129/wordpress/wp-
content/plugins/woocommerce/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/plugins/woocommerce/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/woocommerce/

[!] Title: WooCommerce 2.0.17 - hide-wc-extensions-message Parameter
Reflected XSS
    Reference: http://packetstormsecurity.com/files/123684/
    Reference: http://www.securityfocus.com/bid/63228
    Reference: http://osvdb.org/98754
    Reference: https://wpvulndb.com/vulnerabilities/6673

[+] Finished: Mon May 17 14:07:38 2021
[+] Memory used: 231.375 MB
[+] Elapsed time: 00:00:03
Vane - a Free WordPress vulnerability scanner
[i] The remote host tried to redirect to:
http://localhost/wordpress/?FSEG-Roadblock
[?] Do you want follow the redirection ? [Y]es [N]o [A]bort, default: [N]n
[+] URL: http://192.168.78.129/wordpress/
[+] Started: Mon May 17 14:07:40 2021

[!] The WordPress 'http://192.168.78.129/wordpress/readme.html' file
exists exposing a version number
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-
json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.46 (Ubuntu)
[+] Interesting header: X-REDIRECT-BY: WordPress
[+] XML-RPC Interface available under:
http://192.168.78.129/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/

[+] WordPress version 5.7.2 identified from links opml

[+] Enumerating installed plugins  ...

   Time: 00:00:01
<===========================================================================
======> (1829 / 1829) 100.00% Time: 00:00:01

[+] We found 1 plugins:

[+] Name: woocommerce - v5.3.0
 |  Location: http://192.168.78.129/wordpress/wp-
content/plugins/woocommerce/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/plugins/woocommerce/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/woocommerce/

[!] Title: WooCommerce 2.0.17 - hide-wc-extensions-message Parameter
Reflected XSS
    Reference: http://packetstormsecurity.com/files/123684/
    Reference: http://www.securityfocus.com/bid/63228
    Reference: http://osvdb.org/98754
    Reference: https://wpvulndb.com/vulnerabilities/6673

[+] Finished: Mon May 17 14:07:44 2021
[+] Memory used: 230.148 MB
[+] Elapsed time: 00:00:03
Vane - a Free WordPress vulnerability scanner
[i] The remote host tried to redirect to:
http://localhost/wordpress/?FSEG-Roadblock
```

```
[?] Do you want follow the redirection ? [Y]es [N]o [A]bort, default: [N]n
[+] URL: http://192.168.78.129/wordpress/
[+] Started: Mon May 17 14:07:45 2021

[!] The WordPress 'http://192.168.78.129/wordpress/readme.html' file
exists exposing a version number
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-
json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.46 (Ubuntu)
[+] Interesting header: X-REDIRECT-BY: WordPress
[+] XML-RPC Interface available under:
http://192.168.78.129/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/

[+] WordPress version 5.7.2 identified from links opml

[+] Enumerating installed plugins  ...

   Time: 00:00:01
<==========================================================================
======> (1829 / 1829) 100.00% Time: 00:00:01

[+] We found 1 plugins:

[+] Name: woocommerce - v5.3.0
 |  Location: http://192.168.78.129/wordpress/wp-
content/plugins/woocommerce/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/plugins/woocommerce/readme.txt
[!] Directory listing is enabled: http://192.168.78.129/wordpress/wp-
content/plugins/woocommerce/

[!] Title: WooCommerce 2.0.17 - hide-wc-extensions-message Parameter
Reflected XSS
    Reference: http://packetstormsecurity.com/files/123684/
    Reference: http://www.securityfocus.com/bid/63228
    Reference: http://osvdb.org/98754
    Reference: https://wpvulndb.com/vulnerabilities/6673

[+] Finished: Mon May 17 14:07:49 2021
[+] Memory used: 229.824 MB
[+] Elapsed time: 00:00:03
```

## APPENDIX D - VM2 – WPSCAN

```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|
         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 14:03:59 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.46 (Ubuntu)
 |  - X-Redirect-By: WordPress
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled:
http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299
```

```
[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<========================================================> (348 / 348)
100.00% Time: 00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<======================================================> (2568 / 2568)
100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00
<=========================================================> (137 / 137)
100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<===============================================================> (71 /
71) 100.00% Time: 00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<==========================================================> (10 / 10)
100.00% Time: 00:00:00

[i] No Users Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 14:04:04 2021
[+] Requests Done: 3137
[+] Cached Requests: 45
[+] Data Sent: 868.568 KB
[+] Data Received: 432.558 KB
[+] Memory used: 208.527 MB
[+] Elapsed time: 00:00:04
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 14:04:06 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.46 (Ubuntu)
 |  - X-Redirect-By: WordPress
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled:
http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
```

```
[+] Upload directory has listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<========================================================> (348 / 348)
100.00% Time: 00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<======================================================> (2568 / 2568)
100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00
<=========================================================> (137 / 137)
100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<===============================================================> (71 /
71) 100.00% Time: 00:00:00

[i] No DB Exports Found.
```

```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<=============================================================> (10 / 10)
100.00% Time: 00:00:00

[i] No Users Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 14:04:10 2021
[+] Requests Done: 3137
[+] Cached Requests: 45
[+] Data Sent: 868.568 KB
[+] Data Received: 432.558 KB
[+] Memory used: 207.293 MB
[+] Elapsed time: 00:00:04
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 14:04:12 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.46 (Ubuntu)
 |  - X-Redirect-By: WordPress
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled:
http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
```

```
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<=======================================================> (348 / 348)
100.00% Time: 00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<=====================================================> (2568 / 2568)
100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
```

```
 Checking Config Backups - Time: 00:00:00
<=========================================================> (137 / 137)
100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<===============================================================> (71 /
71) 100.00% Time: 00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<==========================================================> (10 / 10)
100.00% Time: 00:00:00

[i] No Users Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 14:04:17 2021
[+] Requests Done: 3137
[+] Cached Requests: 45
[+] Data Sent: 868.568 KB
[+] Data Received: 432.539 KB
[+] Memory used: 226.93 MB
[+] Elapsed time: 00:00:04
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 14:04:18 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.46 (Ubuntu)
 |  - X-Redirect-By: WordPress
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled:
http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
```

```
 Checking Known Locations - Time: 00:00:00
<=======================================================> (348 / 348)
100.00% Time: 00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<=====================================================> (2568 / 2568)
100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00
<=========================================================> (137 / 137)
100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<===============================================================> (71 /
71) 100.00% Time: 00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<==========================================================> (10 / 10)
100.00% Time: 00:00:00

[i] No Users Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 14:04:23 2021
[+] Requests Done: 3137
[+] Cached Requests: 45
[+] Data Sent: 868.568 KB
[+] Data Received: 432.558 KB
[+] Memory used: 207.348 MB
[+] Elapsed time: 00:00:04
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|
         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 14:04:25 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.46 (Ubuntu)
 |  - X-Redirect-By: WordPress
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled:
http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
```

```
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<========================================================> (348 / 348)
100.00% Time: 00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<======================================================> (2568 / 2568)
100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00
<=========================================================> (137 / 137)
100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<===============================================================> (71 /
71) 100.00% Time: 00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<==========================================================> (10 / 10)
100.00% Time: 00:00:00

[i] No Users Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 14:04:29 2021
[+] Requests Done: 3137
[+] Cached Requests: 45
[+] Data Sent: 868.568 KB
[+] Data Received: 432.539 KB
[+] Memory used: 207.215 MB
[+] Elapsed time: 00:00:04
```

## Appendix E – VM3 - Vane

```
Vane - a Free WordPress vulnerability scanner

The target is responding with a 403, this might be due to a WAF or a
plugin.
You should try to supply a valid user-agent via the --user-agent option or
use the --random-agent option
Vane - a Free WordPress vulnerability scanner

The target is responding with a 403, this might be due to a WAF or a
plugin.
You should try to supply a valid user-agent via the --user-agent option or
use the --random-agent option
Vane - a Free WordPress vulnerability scanner

The target is responding with a 403, this might be due to a WAF or a
plugin.
You should try to supply a valid user-agent via the --user-agent option or
use the --random-agent option
Vane - a Free WordPress vulnerability scanner

The target is responding with a 403, this might be due to a WAF or a
plugin.
You should try to supply a valid user-agent via the --user-agent option or
use the --random-agent option
Vane - a Free WordPress vulnerability scanner

The target is responding with a 403, this might be due to a WAF or a
plugin.
You should try to supply a valid user-agent via the --user-agent option or
use the --random-agent option
```

## Appendix E – VM3 – WPScan

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

         WordPress Security Scanner by the WPScan Team
```

```
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 14:59:35 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.46 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled:
http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.7.2'
```

```
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] instagram-feed
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/instagram-
feed/
 | Latest Version: 2.9.1 (up to date)
 | Last Updated: 2021-05-07T18:48:00.000Z
 |
 | Found By: Javascript Var (Passive Detection)
 |
 | Version: 2.9.1 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.78.129/wordpress/wp-content/plugins/instagram-
feed/README.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://192.168.78.129/wordpress/wp-content/plugins/instagram-
feed/README.txt

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.
```

```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] rory
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 14:59:40 2021
[+] Requests Done: 3173
[+] Cached Requests: 4
[+] Data Sent: 1.157 MB
[+] Data Received: 671.487 KB
[+] Memory used: 208.348 MB
[+] Elapsed time: 00:00:05
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 14:44:04 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.46 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled:
http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - 
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  - 
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - 
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  - 
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: 
http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: 
http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] instagram-feed
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/instagram-
feed/
 | Latest Version: 2.9.1 (up to date)
 | Last Updated: 2021-05-07T18:48:00.000Z
 |
 | Found By: Javascript Var (Passive Detection)
 |
 | Version: 2.9.1 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.78.129/wordpress/wp-content/plugins/instagram-
feed/README.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://192.168.78.129/wordpress/wp-content/plugins/instagram-
feed/README.txt

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<========================================================> (348 / 348)
100.00% Time: 00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<======================================================> (2568 / 2568)
100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00
<=========================================================> (137 / 137)
100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<===============================================================> (71 /
71) 100.00% Time: 00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<==========================================================> (10 / 10)
100.00% Time: 00:00:00

[i] User(s) Identified:

[+] rory
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 14:44:09 2021
[+] Requests Done: 3138
[+] Cached Requests: 39
[+] Data Sent: 868.902 KB
[+] Data Received: 439.679 KB
[+] Memory used: 208.355 MB
[+] Elapsed time: 00:00:04
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 14:44:10 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.46 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled:
http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
```

```
[+] The external WP-Cron seems to be enabled:
http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] instagram-feed
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/instagram-
feed/
 | Latest Version: 2.9.1 (up to date)
 | Last Updated: 2021-05-07T18:48:00.000Z
 |
 | Found By: Javascript Var (Passive Detection)
 |
 | Version: 2.9.1 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.78.129/wordpress/wp-content/plugins/instagram-
feed/README.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://192.168.78.129/wordpress/wp-content/plugins/instagram-
feed/README.txt

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<========================================================> (348 / 348)
100.00% Time: 00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<======================================================> (2568 / 2568)
100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
```

```
 Checking Config Backups - Time: 00:00:00
<==========================================================> (137 / 137)
100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<================================================================> (71 /
71) 100.00% Time: 00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<===========================================================> (10 / 10)
100.00% Time: 00:00:00

[i] User(s) Identified:

[+] rory
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 14:44:15 2021
[+] Requests Done: 3138
[+] Cached Requests: 39
[+] Data Sent: 868.902 KB
[+] Data Received: 439.678 KB
[+] Memory used: 207.148 MB
[+] Elapsed time: 00:00:04
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 14:44:17 2021

Interesting Finding(s):
```

```
[+] Headers
 | Interesting Entry: Server: Apache/2.4.46 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled:
http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:
```

```
[+] instagram-feed
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/instagram-
feed/
 | Latest Version: 2.9.1 (up to date)
 | Last Updated: 2021-05-07T18:48:00.000Z
 |
 | Found By: Javascript Var (Passive Detection)
 |
 | Version: 2.9.1 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.78.129/wordpress/wp-content/plugins/instagram-
feed/README.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://192.168.78.129/wordpress/wp-content/plugins/instagram-
feed/README.txt

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<========================================================> (348 / 348)
100.00% Time: 00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<=======================================================> (2568 / 2568)
100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00
<=========================================================> (137 / 137)
100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<===============================================================> (71 /
71) 100.00% Time: 00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<==========================================================> (10 / 10)
100.00% Time: 00:00:00

[i] User(s) Identified:

[+] rory
```

```
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 14:44:22 2021
[+] Requests Done: 3138
[+] Cached Requests: 39
[+] Data Sent: 868.902 KB
[+] Data Received: 439.745 KB
[+] Memory used: 207.699 MB
[+] Elapsed time: 00:00:04
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 14:44:23 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.46 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled:
http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
```

```
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] instagram-feed
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/instagram-
feed/
 | Latest Version: 2.9.1 (up to date)
 | Last Updated: 2021-05-07T18:48:00.000Z
 |
 | Found By: Javascript Var (Passive Detection)
 |
 | Version: 2.9.1 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.78.129/wordpress/wp-content/plugins/instagram-
feed/README.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://192.168.78.129/wordpress/wp-content/plugins/instagram-
feed/README.txt

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
```

```
 Checking Known Locations - Time: 00:00:00
<========================================================> (348 / 348)
100.00% Time: 00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<======================================================> (2568 / 2568)
100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00
<=========================================================> (137 / 137)
100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<===============================================================> (71 /
71) 100.00% Time: 00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<==========================================================> (10 / 10)
100.00% Time: 00:00:00

[i] User(s) Identified:

[+] rory
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 14:44:28 2021
[+] Requests Done: 3138
[+] Cached Requests: 39
[+] Data Sent: 868.902 KB
[+] Data Received: 463.465 KB
[+] Memory used: 207.938 MB
[+] Elapsed time: 00:00:05
```

## APPENDIX F – VM4 – VANE

```
Vane - a Free WordPress vulnerability scanner
[+] URL: http://192.168.78.129/wordpress/
[+] Started: Mon May 17 15:10:59 2021

[!] The WordPress 'http://192.168.78.129/wordpress/readme.html' file
exists exposing a version number
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-
json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.46 (Ubuntu)
[+] XML-RPC Interface available under:
http://192.168.78.129/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/

[+] WordPress version 5.7.2 identified from links opml

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

[+] Name: twentytwentyone - v1.3
 |  Location: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/readme.txt
 |  Style URL: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Referenced style.css: http://localhost/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Theme Name: Twenty Twenty-One
 |  Theme URI: https://wordpress.org/themes/twentytwentyone/
 |  Description: Twenty Twenty-One is a blank canvas for your ideas and it
makes the block editor your best brush....
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/

[+] Enumerating installed plugins  ...

   Time: 00:00:02
<==========================================================================
======> (1829 / 1829) 100.00% Time: 00:00:02

[+] We found 1 plugins:

[+] Name: akismet - v4.1.9
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/akismet/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/plugins/akismet/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-
content/plugins/akismet/changelog.txt

[+] Finished: Mon May 17 15:11:06 2021
[+] Memory used: 232.863 MB
[+] Elapsed time: 00:00:07
Vane - a Free WordPress vulnerability scanner
[+] URL: http://192.168.78.129/wordpress/
[+] Started: Mon May 17 15:11:09 2021

[!] The WordPress 'http://192.168.78.129/wordpress/readme.html' file
exists exposing a version number
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-
json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.46 (Ubuntu)
[+] XML-RPC Interface available under:
http://192.168.78.129/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/

[+] WordPress version 5.7.2 identified from links opml

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

[+] Name: twentytwentyone - v1.3
 |  Location: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/readme.txt
 |  Style URL: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Referenced style.css: http://localhost/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Theme Name: Twenty Twenty-One
 |  Theme URI: https://wordpress.org/themes/twentytwentyone/
 |  Description: Twenty Twenty-One is a blank canvas for your ideas and it
makes the block editor your best brush....
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/

[+] Enumerating installed plugins  ...

   Time: 00:00:02
<==========================================================================
======> (1829 / 1829) 100.00% Time: 00:00:02

[+] We found 1 plugins:

[+] Name: akismet - v4.1.9
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/akismet/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/plugins/akismet/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-
content/plugins/akismet/changelog.txt

[+] Finished: Mon May 17 15:11:14 2021
[+] Memory used: 237.633 MB
[+] Elapsed time: 00:00:04
Vane - a Free WordPress vulnerability scanner
```

```
[+] URL: http://192.168.78.129/wordpress/
[+] Started: Mon May 17 15:11:17 2021

[!] The WordPress 'http://192.168.78.129/wordpress/readme.html' file
exists exposing a version number
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-
json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.46 (Ubuntu)
[+] XML-RPC Interface available under:
http://192.168.78.129/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/

[+] WordPress version 5.7.2 identified from links opml

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

[+] Name: twentytwentyone - v1.3
 |  Location: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/readme.txt
 |  Style URL: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Referenced style.css: http://localhost/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Theme Name: Twenty Twenty-One
 |  Theme URI: https://wordpress.org/themes/twentytwentyone/
 |  Description: Twenty Twenty-One is a blank canvas for your ideas and it
makes the block editor your best brush....
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/

[+] Enumerating installed plugins  ...

   Time: 00:00:02
<==========================================================================
======> (1829 / 1829) 100.00% Time: 00:00:02

[+] We found 1 plugins:

[+] Name: akismet - v4.1.9
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/akismet/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/plugins/akismet/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-
content/plugins/akismet/changelog.txt

[+] Finished: Mon May 17 15:11:22 2021
[+] Memory used: 233.219 MB
[+] Elapsed time: 00:00:04
Vane - a Free WordPress vulnerability scanner
[+] URL: http://192.168.78.129/wordpress/
[+] Started: Mon May 17 15:11:25 2021
```

```
[!] The WordPress 'http://192.168.78.129/wordpress/readme.html' file
exists exposing a version number
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-
json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.46 (Ubuntu)
[+] XML-RPC Interface available under:
http://192.168.78.129/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/

[+] WordPress version 5.7.2 identified from links opml

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

[+] Name: twentytwentyone - v1.3
 |  Location: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/readme.txt
 |  Style URL: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Referenced style.css: http://localhost/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Theme Name: Twenty Twenty-One
 |  Theme URI: https://wordpress.org/themes/twentytwentyone/
 |  Description: Twenty Twenty-One is a blank canvas for your ideas and it
makes the block editor your best brush....
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/

[+] Enumerating installed plugins  ...

   Time: 00:00:02
<==========================================================================
======> (1829 / 1829) 100.00% Time: 00:00:02

[+] We found 1 plugins:

[+] Name: akismet - v4.1.9
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/akismet/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/plugins/akismet/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-
content/plugins/akismet/changelog.txt

[+] Finished: Mon May 17 15:11:30 2021
[+] Memory used: 231.672 MB
[+] Elapsed time: 00:00:04
Vane - a Free WordPress vulnerability scanner
[+] URL: http://192.168.78.129/wordpress/
[+] Started: Mon May 17 15:11:33 2021
```

```
[!] The WordPress 'http://192.168.78.129/wordpress/readme.html' file
exists exposing a version number
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-
json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.46 (Ubuntu)
[+] XML-RPC Interface available under:
http://192.168.78.129/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/

[+] WordPress version 5.7.2 identified from links opml

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

[+] Name: twentytwentyone - v1.3
 |  Location: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/readme.txt
 |  Style URL: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Referenced style.css: http://localhost/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Theme Name: Twenty Twenty-One
 |  Theme URI: https://wordpress.org/themes/twentytwentyone/
 |  Description: Twenty Twenty-One is a blank canvas for your ideas and it
makes the block editor your best brush....
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/

[+] Enumerating installed plugins  ...

   Time: 00:00:02
<==========================================================================
======> (1829 / 1829) 100.00% Time: 00:00:02

[+] We found 1 plugins:

[+] Name: akismet - v4.1.9
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/akismet/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/plugins/akismet/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-
content/plugins/akismet/changelog.txt

[+] Finished: Mon May 17 15:11:38 2021
[+] Memory used: 231.312 MB
[+] Elapsed time: 00:00:05
```

## APPENDIX E – VM4 - WPSCAN

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

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 15:11:08 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.46 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled:
http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
```

```
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:01
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:01

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] rory
```

```
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 15:11:16 2021
[+] Requests Done: 3171
[+] Cached Requests: 4
[+] Data Sent: 1.068 MB
[+] Data Received: 518.58 KB
[+] Memory used: 208.043 MB
[+] Elapsed time: 00:00:07
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 15:11:20 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.46 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled:
http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
```

```
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:01
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:01

[i] No Config Backups Found.
```

```
[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] rory
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 15:11:27 2021
[+] Requests Done: 3171
[+] Cached Requests: 4
[+] Data Sent: 1.105 MB
[+] Data Received: 518.58 KB
[+] Memory used: 207.961 MB
[+] Elapsed time: 00:00:07
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 15:11:32 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.46 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled:
http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
```

```
 Checking Known Locations - Time: 00:00:00
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:01
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:01

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] rory
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 15:11:39 2021
[+] Requests Done: 3171
[+] Cached Requests: 4
[+] Data Sent: 1.105 MB
[+] Data Received: 518.562 KB
[+] Memory used: 207.801 MB
[+] Elapsed time: 00:00:07
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 15:11:44 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.46 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled:
http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
```

```
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:01
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:01

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] rory
```

```
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 15:11:52 2021
[+] Requests Done: 3171
[+] Cached Requests: 4
[+] Data Sent: 1.156 MB
[+] Data Received: 518.58 KB
[+] Memory used: 207.449 MB
[+] Elapsed time: 00:00:07
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 15:11:56 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.46 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled:
http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
```

```
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:01
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:01

[i] No Config Backups Found.
```

```
[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] rory
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 15:12:03 2021
[+] Requests Done: 3171
[+] Cached Requests: 4
[+] Data Sent: 1.011 MB
[+] Data Received: 518.58 KB
[+] Memory used: 208.441 MB
[+] Elapsed time: 00:00:07
```

## APPENDIX G – VM5 - VANE

```
Vane - a Free WordPress vulnerability scanner
[+] URL: http://192.168.78.129/wordpress/
[+] Started: Mon May 17 15:23:46 2021

[!] The WordPress 'http://192.168.78.129/wordpress/readme.html' file
exists exposing a version number
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-
json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.46 (Ubuntu)
[+] XML-RPC Interface available under:
http://192.168.78.129/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/

[+] WordPress version 5.7.2 identified from links opml
[+] WordPress theme in use: twentytwentyone - v1.3

[+] Name: twentytwentyone - v1.3
 |  Location: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/readme.txt
 |  Style URL: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Referenced style.css: http://localhost/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Theme Name: Twenty Twenty-One
 |  Theme URI: https://wordpress.org/themes/twentytwentyone/
 |  Description: Twenty Twenty-One is a blank canvas for your ideas and it
makes the block editor your best brush. With new block patterns, which
allow you to create a beautiful layout in a matter of seconds, this
theme’s soft colors and eye-catching — yet timeless — design will let your
work shine. Take it for a spin! See how Twenty Twenty-One elevates your
portfolio, business website, or personal blog.
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: one-column, accessibility-ready, custom-colors, custom-menu,
custom-logo, editor-style, featured-images, footer-widgets, block-
patterns, rtl-language-support, sticky-post, threaded-comments,
translation-ready
 |  Text Domain: twentytwentyone

[+] Enumerating installed plugins  ...

   Time: 00:00:01
<==========================================================================
======> (1829 / 1829) 100.00% Time: 00:00:01

[+] We found 1 plugins:

[+] Name: akismet - v4.1.9
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/akismet/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/plugins/akismet/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-
content/plugins/akismet/changelog.txt

[+] Finished: Mon May 17 15:23:53 2021
[+] Memory used: 203.375 MB
[+] Elapsed time: 00:00:06
Vane - a Free WordPress vulnerability scanner
[+] URL: http://192.168.78.129/wordpress/
[+] Started: Mon May 17 15:23:53 2021

[!] The WordPress 'http://192.168.78.129/wordpress/readme.html' file
exists exposing a version number
```

```
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-
json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.46 (Ubuntu)
[+] XML-RPC Interface available under:
http://192.168.78.129/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/

[+] WordPress version 5.7.2 identified from links opml

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

[+] Name: twentytwentyone - v1.3
 |  Location: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/readme.txt
 |  Style URL: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Referenced style.css: http://localhost/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Theme Name: Twenty Twenty-One
 |  Theme URI: https://wordpress.org/themes/twentytwentyone/
 |  Description: Twenty Twenty-One is a blank canvas for your ideas and it
makes the block editor your best brush. With new block patterns, which
allow you to create a beautiful layout in a matter of seconds, this
theme’s soft colors and eye-catching — yet timeless — design will let your
work shine. Take it for a spin! See how Twenty Twenty-One elevates your
portfolio, business website, or personal blog.
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: one-column, accessibility-ready, custom-colors, custom-menu,
custom-logo, editor-style, featured-images, footer-widgets, block-
patterns, rtl-language-support, sticky-post, threaded-comments,
translation-ready
 |  Text Domain: twentytwentyone

[+] Enumerating installed plugins  ...

   Time: 00:00:01
<==========================================================================
======> (1829 / 1829) 100.00% Time: 00:00:01

[+] We found 1 plugins:

[+] Name: akismet - v4.1.9
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/akismet/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/plugins/akismet/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-
content/plugins/akismet/changelog.txt
```

```
[+] Finished: Mon May 17 15:23:57 2021
[+] Memory used: 232.098 MB
[+] Elapsed time: 00:00:03
Vane - a Free WordPress vulnerability scanner
[+] URL: http://192.168.78.129/wordpress/
[+] Started: Mon May 17 15:23:57 2021

[!] The WordPress 'http://192.168.78.129/wordpress/readme.html' file
exists exposing a version number
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-
json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.46 (Ubuntu)
[+] XML-RPC Interface available under:
http://192.168.78.129/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/

[+] WordPress version 5.7.2 identified from links opml

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

[+] Name: twentytwentyone - v1.3
 |  Location: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/readme.txt
 |  Style URL: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Referenced style.css: http://localhost/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Theme Name: Twenty Twenty-One
 |  Theme URI: https://wordpress.org/themes/twentytwentyone/
 |  Description: Twenty Twenty-One is a blank canvas for your ideas and it
makes the block editor your best brush. With new block patterns, which
allow you to create a beautiful layout in a matter of seconds, this
theme’s soft colors and eye-catching — yet timeless — design will let your
work shine. Take it for a spin! See how Twenty Twenty-One elevates your
portfolio, business website, or personal blog.
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: one-column, accessibility-ready, custom-colors, custom-menu,
custom-logo, editor-style, featured-images, footer-widgets, block-
patterns, rtl-language-support, sticky-post, threaded-comments,
translation-ready
 |  Text Domain: twentytwentyone

[+] Enumerating installed plugins  ...

   Time: 00:00:01
<=========================================================================
======> (1829 / 1829) 100.00% Time: 00:00:01
```

```
[+] We found 1 plugins:

[+] Name: akismet - v4.1.9
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/akismet/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/plugins/akismet/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-
content/plugins/akismet/changelog.txt

[+] Finished: Mon May 17 15:24:01 2021
[+] Memory used: 232.805 MB
[+] Elapsed time: 00:00:03
ane - a Free WordPress vulnerability scanner
[+] URL: http://192.168.78.129/wordpress/
[+] Started: Mon May 17 15:24:01 2021

[!] The WordPress 'http://192.168.78.129/wordpress/readme.html' file
exists exposing a version number
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-
json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.46 (Ubuntu)
[+] XML-RPC Interface available under:
http://192.168.78.129/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/

[+] WordPress version 5.7.2 identified from links opml

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

[+] Name: twentytwentyone - v1.3
 |  Location: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/readme.txt
 |  Style URL: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Referenced style.css: http://localhost/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Theme Name: Twenty Twenty-One
 |  Theme URI: https://wordpress.org/themes/twentytwentyone/
 |  Description: Twenty Twenty-One is a blank canvas for your ideas and it
makes the block editor your best brush. With new block patterns, which
allow you to create a beautiful layout in a matter of seconds, this
theme’s soft colors and eye-catching — yet timeless — design will let your
work shine. Take it for a spin! See how Twenty Twenty-One elevates your
portfolio, business website, or personal blog.
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: one-column, accessibility-ready, custom-colors, custom-menu,
custom-logo, editor-style, featured-images, footer-widgets, block-
```

```
patterns, rtl-language-support, sticky-post, threaded-comments,
translation-ready
 |  Text Domain: twentytwentyone

[+] Enumerating installed plugins  ...

   Time: 00:00:01
<==========================================================================
======> (1829 / 1829) 100.00% Time: 00:00:01

[+] We found 1 plugins:

[+] Name: akismet - v4.1.9
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/akismet/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/plugins/akismet/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-
content/plugins/akismet/changelog.txt

[+] Finished: Mon May 17 15:24:05 2021
[+] Memory used: 232.191 MB
[+] Elapsed time: 00:00:03
Vane - a Free WordPress vulnerability scanner
[+] URL: http://192.168.78.129/wordpress/
[+] Started: Mon May 17 15:24:06 2021

[!] The WordPress 'http://192.168.78.129/wordpress/readme.html' file
exists exposing a version number
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-
json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.46 (Ubuntu)
[+] XML-RPC Interface available under:
http://192.168.78.129/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/

[+] WordPress version 5.7.2 identified from links opml

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

[+] Name: twentytwentyone - v1.3
 |  Location: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/readme.txt
 |  Style URL: http://192.168.78.129/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Referenced style.css: http://localhost/wordpress/wp-
content/themes/twentytwentyone/style.css
 |  Theme Name: Twenty Twenty-One
 |  Theme URI: https://wordpress.org/themes/twentytwentyone/
 |  Description: Twenty Twenty-One is a blank canvas for your ideas and it
makes the block editor your best brush. With new block patterns, which
allow you to create a beautiful layout in a matter of seconds, this
```

```
theme’s soft colors and eye-catching — yet timeless — design will let your
work shine. Take it for a spin! See how Twenty Twenty-One elevates your
portfolio, business website, or personal blog.
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: one-column, accessibility-ready, custom-colors, custom-menu,
custom-logo, editor-style, featured-images, footer-widgets, block-
patterns, rtl-language-support, sticky-post, threaded-comments,
translation-ready
 |  Text Domain: twentytwentyone

[+] Enumerating installed plugins  ...

   Time: 00:00:01
<=========================================================================
======> (1829 / 1829) 100.00% Time: 00:00:01

[+] We found 1 plugins:

[+] Name: akismet - v4.1.9
 |  Location: http://192.168.78.129/wordpress/wp-content/plugins/akismet/
 |  Readme: http://192.168.78.129/wordpress/wp-
content/plugins/akismet/readme.txt
 |  Changelog: http://192.168.78.129/wordpress/wp-
content/plugins/akismet/changelog.txt

[+] Finished: Mon May 17 15:24:10 2021
[+] Memory used: 238.629 MB
[+] Elapsed time: 00:00:03
```

## Appendix G – VM5 – WPScan

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

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 15:18:09 2021

Interesting Finding(s):
```

```
[+] Headers
 | Interesting Entry: Server: Apache/2.4.46 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled:
http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:
```

```
[+] images-lazyload-and-slideshow
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/images-
lazyload-and-slideshow/
 | Latest Version: 3.4 (up to date)
 | Last Updated: 2016-06-17T18:11:00.000Z
 |
 | Found By: Comment (Passive Detection)
 |
 | Version: 3.4 (100% confidence)
 | Found By: Comment (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'Images Lazyload and
Slideshow 3.4'
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://192.168.78.129/wordpress/wp-content/plugins/images-lazyload-
and-slideshow/readme.txt

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] rory
```

```
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 15:18:15 2021
[+] Requests Done: 3182
[+] Cached Requests: 4
[+] Data Sent: 1.047 MB
[+] Data Received: 789.942 KB
[+] Memory used: 208.195 MB
[+] Elapsed time: 00:00:05
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 15:18:16 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.46 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled:
http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
```

```
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] images-lazyload-and-slideshow
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/images-
lazyload-and-slideshow/
 | Latest Version: 3.4 (up to date)
 | Last Updated: 2016-06-17T18:11:00.000Z
 |
 | Found By: Comment (Passive Detection)
 |
 | Version: 3.4 (100% confidence)
 | Found By: Comment (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'Images Lazyload and
Slideshow 3.4'
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://192.168.78.129/wordpress/wp-content/plugins/images-lazyload-
and-slideshow/readme.txt

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
```

```
 Checking Known Locations - Time: 00:00:00
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] rory
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 15:18:22 2021
[+] Requests Done: 3182
[+] Cached Requests: 4
[+] Data Sent: 1.011 MB
[+] Data Received: 789.961 KB
[+] Memory used: 206.844 MB
[+] Elapsed time: 00:00:05
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 15:18:31 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.46 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled:
http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
```

```
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<==========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<==========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00
<==========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<==========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<==========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] rory
```

```
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 15:18:36 2021
[+] Requests Done: 3147
[+] Cached Requests: 37
[+] Data Sent: 1.004 MB
[+] Data Received: 684.191 KB
[+] Memory used: 207.645 MB
[+] Elapsed time: 00:00:04
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 15:11:44 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.46 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled:
http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
```

```
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<==========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<==========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:01
<==========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:01

[i] No Config Backups Found.
```

```
[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] rory
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 15:11:52 2021
[+] Requests Done: 3171
[+] Cached Requests: 4
[+] Data Sent: 1.156 MB
[+] Data Received: 518.58 KB
[+] Memory used: 207.449 MB
[+] Elapsed time: 00:00:07
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.78.129/wordpress/ [192.168.78.129]
[+] Started: Mon May 17 15:18:37 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.46 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled:
http://192.168.78.129/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://192.168.78.129/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled:
http://192.168.78.129/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://192.168.78.129/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.7.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'WordPress 5.7.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] images-lazyload-and-slideshow
```

```
 | Location: http://192.168.78.129/wordpress/wp-content/plugins/images-
lazyload-and-slideshow/
 | Latest Version: 3.4 (up to date)
 | Last Updated: 2016-06-17T18:11:00.000Z
 |
 | Found By: Comment (Passive Detection)
 |
 | Version: 3.4 (100% confidence)
 | Found By: Comment (Passive Detection)
 |  - http://192.168.78.129/wordpress/, Match: 'Images Lazyload and
Slideshow 3.4'
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://192.168.78.129/wordpress/wp-content/plugins/images-lazyload-
and-slideshow/readme.txt

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:00

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:01
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] rory
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
```

```
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 15:18:43 2021
[+] Requests Done: 3182
[+] Cached Requests: 4
[+] Data Sent: 963.824 KB
[+] Data Received: 790.025 KB
[+] Memory used: 206.961 MB
[+] Elapsed time: 00:00:05
```

## Appendix H – Blog - Vane

```
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.0.134/
[+] Started: Mon May 17 17:16:13 2021

[+] robots.txt available under: 'http://10.10.0.134/robots.txt'
[+] Interesting entry from robots.txt: http://10.10.0.134/wp-admin/admin-
ajax.php
[!] The WordPress 'http://10.10.0.134/readme.html' file exists exposing a
version number
[+] Interesting header: LINK: <http://blog.thm/wp-json/>;
rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.29 (Ubuntu)
[+] XML-RPC Interface available under: http://10.10.0.134/xmlrpc.php
[!] Upload directory has directory listing enabled: http://10.10.0.134/wp-
content/uploads/

[+] WordPress version 5.0 identified from links opml

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

[+] Name: twentytwenty - v1.3
 |  Location: http://10.10.0.134/wp-content/themes/twentytwenty/
 |  Readme: http://10.10.0.134/wp-content/themes/twentytwenty/readme.txt
 |  Style URL: http://10.10.0.134/wp-content/themes/twentytwenty/style.css
 |  Referenced style.css: http://blog.thm/wp-
content/themes/twentytwenty/style.css
 |  Theme Name: Twenty Twenty
 |  Theme URI: https://wordpress.org/themes/twentytwenty/
 |  Description: Our default theme for 2020 is designed to take full
advantage of the flexibility of the block editor. Organizations and
businesses have the ability to create dynamic landing pages with endless
layouts using the group and column blocks. The centered content column and
fine-tuned typography also makes it perfect for traditional blogs.
Complete editor styles give you a good idea of what your content will look
like, even before you publish. You can give your site a personal touch by
```

```
changing the background colors and the accent color in the Customizer. The
colors of all elements on your site are automatically calculated based on
the colors you pick, ensuring a high, accessible color contrast for your
visitors.
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: blog, one-column, custom-background, custom-colors, custom-logo,
custom-menu, editor-style, featured-images, footer-widgets, full-width-
template, rtl-language-support, sticky-post, theme-options, threaded-
comments, translation-ready, block-styles, wide-blocks, accessibility-
ready
 |  Text Domain: twentytwenty

[+] Enumerating installed plugins  ...

   Time: 00:05:47
<==========================================================================
===========================================================> (1829 / 1829)
100.00% Time: 00:05:47

[+] We found 1 plugins:

[+] Name: feed
 |  Location: http://10.10.0.134/wp-content/plugins/feed/

[+] We could not determine a version so all vulnerabilities are printed
out

[!] Title: Feed - news_dt.php nid Parameter SQL Injection
    Reference: http://packetstormsecurity.com/files/122260/
    Reference: http://osvdb.org/94804
    Reference: https://wpvulndb.com/vulnerabilities/6965

[+] Finished: Mon May 17 17:22:12 2021
[+] Memory used: 208.023 MB
[+] Elapsed time: 00:05:59
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.0.134/
[+] Started: Mon May 17 17:22:13 2021

[+] robots.txt available under: 'http://10.10.0.134/robots.txt'
[+] Interesting entry from robots.txt: http://10.10.0.134/wp-admin/admin-
ajax.php
[!] The WordPress 'http://10.10.0.134/readme.html' file exists exposing a
version number
[+] Interesting header: LINK: <http://blog.thm/wp-json/>;
rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.29 (Ubuntu)
[+] XML-RPC Interface available under: http://10.10.0.134/xmlrpc.php
[!] Upload directory has directory listing enabled: http://10.10.0.134/wp-
content/uploads/
```

```
[+] WordPress version 5.0 identified from links opml

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

[+] Name: twentytwenty - v1.3
 |  Location: http://10.10.0.134/wp-content/themes/twentytwenty/
 |  Readme: http://10.10.0.134/wp-content/themes/twentytwenty/readme.txt
 |  Style URL: http://10.10.0.134/wp-content/themes/twentytwenty/style.css
 |  Referenced style.css: http://blog.thm/wp-
content/themes/twentytwenty/style.css
 |  Theme Name: Twenty Twenty
 |  Theme URI: https://wordpress.org/themes/twentytwenty/
 |  Description: Our default theme for 2020 is designed to take full
advantage of the flexibility of the block editor. Organizations and
businesses have the ability to create dynamic landing pages with endless
layouts using the group and column blocks. The centered content column and
fine-tuned typography also makes it perfect for traditional blogs.
Complete editor styles give you a good idea of what your content will look
like, even before you publish. You can give your site a personal touch by
changing the background colors and the accent color in the Customizer. The
colors of all elements on your site are automatically calculated based on
the colors you pick, ensuring a high, accessible color contrast for your
visitors.
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: blog, one-column, custom-background, custom-colors, custom-logo,
custom-menu, editor-style, featured-images, footer-widgets, full-width-
template, rtl-language-support, sticky-post, theme-options, threaded-
comments, translation-ready, block-styles, wide-blocks, accessibility-
ready
 |  Text Domain: twentytwenty

[+] Enumerating installed plugins  ...

   Time: 00:04:22
<==========================================================================
=========================================================> (1829 / 1829)
100.00% Time: 00:04:22

[+] We found 1 plugins:

[+] Name: feed
 |  Location: http://10.10.0.134/wp-content/plugins/feed/

[+] We could not determine a version so all vulnerabilities are printed
out

[!] Title: Feed - news_dt.php nid Parameter SQL Injection
    Reference: http://packetstormsecurity.com/files/122260/
    Reference: http://osvdb.org/94804
    Reference: https://wpvulndb.com/vulnerabilities/6965
```

```
[+] Finished: Mon May 17 17:26:44 2021
[+] Memory used: 207.285 MB
[+] Elapsed time: 00:04:31
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.0.134/
[+] Started: Mon May 17 17:26:45 2021

[+] robots.txt available under: 'http://10.10.0.134/robots.txt'
[+] Interesting entry from robots.txt: http://10.10.0.134/wp-admin/admin-
ajax.php
[!] The WordPress 'http://10.10.0.134/readme.html' file exists exposing a
version number
[+] Interesting header: LINK: <http://blog.thm/wp-json/>;
rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.29 (Ubuntu)
[+] XML-RPC Interface available under: http://10.10.0.134/xmlrpc.php
[!] Upload directory has directory listing enabled: http://10.10.0.134/wp-
content/uploads/

[+] WordPress version 5.0 identified from links opml

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

[+] Name: twentytwenty - v1.3
 |  Location: http://10.10.0.134/wp-content/themes/twentytwenty/
 |  Readme: http://10.10.0.134/wp-content/themes/twentytwenty/readme.txt
 |  Style URL: http://10.10.0.134/wp-content/themes/twentytwenty/style.css
 |  Referenced style.css: http://blog.thm/wp-
content/themes/twentytwenty/style.css
 |  Theme Name: Twenty Twenty
 |  Theme URI: https://wordpress.org/themes/twentytwenty/
 |  Description: Our default theme for 2020 is designed to take full
advantage of the flexibility of the block editor. Organizations and
businesses have the ability to create dynamic landing pages with endless
layouts using the group and column blocks. The centered content column and
fine-tuned typography also makes it perfect for traditional blogs.
Complete editor styles give you a good idea of what your content will look
like, even before you publish. You can give your site a personal touch by
changing the background colors and the accent color in the Customizer. The
colors of all elements on your site are automatically calculated based on
the colors you pick, ensuring a high, accessible color contrast for your
visitors.
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: blog, one-column, custom-background, custom-colors, custom-logo,
custom-menu, editor-style, featured-images, footer-widgets, full-width-
template, rtl-language-support, sticky-post, theme-options, threaded-
comments, translation-ready, block-styles, wide-blocks, accessibility-
ready
 |  Text Domain: twentytwenty

[+] Enumerating installed plugins  ...
```

```
   Time: 00:05:45
<=========================================================================
==========================================================> (1829 / 1829)
100.00% Time: 00:05:45

[+] We found 1 plugins:

[+] Name: feed
 |  Location: http://10.10.0.134/wp-content/plugins/feed/

[+] We could not determine a version so all vulnerabilities are printed
out

[!] Title: Feed - news_dt.php nid Parameter SQL Injection
    Reference: http://packetstormsecurity.com/files/122260/
    Reference: http://osvdb.org/94804
    Reference: https://wpvulndb.com/vulnerabilities/6965

[+] Finished: Mon May 17 17:32:40 2021
[+] Memory used: 207.355 MB
[+] Elapsed time: 00:05:54
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.0.134/
[+] Started: Mon May 17 17:32:41 2021

[+] robots.txt available under: 'http://10.10.0.134/robots.txt'
[+] Interesting entry from robots.txt: http://10.10.0.134/wp-admin/admin-
ajax.php
[!] The WordPress 'http://10.10.0.134/readme.html' file exists exposing a
version number
[+] Interesting header: LINK: <http://blog.thm/wp-json/>;
rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.29 (Ubuntu)
[+] XML-RPC Interface available under: http://10.10.0.134/xmlrpc.php
[!] Upload directory has directory listing enabled: http://10.10.0.134/wp-
content/uploads/

[+] WordPress version 5.0 identified from links opml

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

[+] Name: twentytwenty - v1.3
 |  Location: http://10.10.0.134/wp-content/themes/twentytwenty/
 |  Readme: http://10.10.0.134/wp-content/themes/twentytwenty/readme.txt
 |  Style URL: http://10.10.0.134/wp-content/themes/twentytwenty/style.css
 |  Referenced style.css: http://blog.thm/wp-
content/themes/twentytwenty/style.css
 |  Theme Name: Twenty Twenty
 |  Theme URI: https://wordpress.org/themes/twentytwenty/
 |  Description: Our default theme for 2020 is designed to take full
advantage of the flexibility of the block editor. Organizations and
businesses have the ability to create dynamic landing pages with endless
layouts using the group and column blocks. The centered content column and
```

```
fine-tuned typography also makes it perfect for traditional blogs.
Complete editor styles give you a good idea of what your content will look
like, even before you publish. You can give your site a personal touch by
changing the background colors and the accent color in the Customizer. The
colors of all elements on your site are automatically calculated based on
the colors you pick, ensuring a high, accessible color contrast for your
visitors.
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: blog, one-column, custom-background, custom-colors, custom-logo,
custom-menu, editor-style, featured-images, footer-widgets, full-width-
template, rtl-language-support, sticky-post, theme-options, threaded-
comments, translation-ready, block-styles, wide-blocks, accessibility-
ready
 |  Text Domain: twentytwenty

[+] Enumerating installed plugins  ...

   Time: 00:05:44
<==========================================================================
==========================================================> (1829 / 1829)
100.00% Time: 00:05:44

[+] We found 1 plugins:

[+] Name: feed
 |  Location: http://10.10.0.134/wp-content/plugins/feed/

[+] We could not determine a version so all vulnerabilities are printed
out

[!] Title: Feed - news_dt.php nid Parameter SQL Injection
    Reference: http://packetstormsecurity.com/files/122260/
    Reference: http://osvdb.org/94804
    Reference: https://wpvulndb.com/vulnerabilities/6965

[+] Finished: Mon May 17 17:38:35 2021
[+] Memory used: 207.617 MB
[+] Elapsed time: 00:05:54
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.0.134/
[+] Started: Mon May 17 17:38:36 2021

[+] robots.txt available under: 'http://10.10.0.134/robots.txt'
[+] Interesting entry from robots.txt: http://10.10.0.134/wp-admin/admin-
ajax.php
[!] The WordPress 'http://10.10.0.134/readme.html' file exists exposing a
version number
[+] Interesting header: LINK: <http://blog.thm/wp-json/>;
rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.29 (Ubuntu)
[+] XML-RPC Interface available under: http://10.10.0.134/xmlrpc.php
```

```
[!] Upload directory has directory listing enabled: http://10.10.0.134/wp-
content/uploads/

[+] WordPress version 5.0 identified from links opml

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

[+] Name: twentytwenty - v1.3
 |  Location: http://10.10.0.134/wp-content/themes/twentytwenty/
 |  Readme: http://10.10.0.134/wp-content/themes/twentytwenty/readme.txt
 |  Style URL: http://10.10.0.134/wp-content/themes/twentytwenty/style.css
 |  Referenced style.css: http://blog.thm/wp-
content/themes/twentytwenty/style.css
 |  Theme Name: Twenty Twenty
 |  Theme URI: https://wordpress.org/themes/twentytwenty/
 |  Description: Our default theme for 2020 is designed to take full
advantage of the flexibility of the block editor. Organizations and
businesses have the ability to create dynamic landing pages with endless
layouts using the group and column blocks. The centered content column and
fine-tuned typography also makes it perfect for traditional blogs.
Complete editor styles give you a good idea of what your content will look
like, even before you publish. You can give your site a personal touch by
changing the background colors and the accent color in the Customizer. The
colors of all elements on your site are automatically calculated based on
the colors you pick, ensuring a high, accessible color contrast for your
visitors.
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: blog, one-column, custom-background, custom-colors, custom-logo,
custom-menu, editor-style, featured-images, footer-widgets, full-width-
template, rtl-language-support, sticky-post, theme-options, threaded-
comments, translation-ready, block-styles, wide-blocks, accessibility-
ready
 |  Text Domain: twentytwenty

[+] Enumerating installed plugins  ...

   Time: 00:04:33
<==========================================================================
============================================================> (1829 / 1829)
100.00% Time: 00:04:33

[+] We found 1 plugins:

[+] Name: feed
 |  Location: http://10.10.0.134/wp-content/plugins/feed/

[+] We could not determine a version so all vulnerabilities are printed
out

[!] Title: Feed - news_dt.php nid Parameter SQL Injection
    Reference: http://packetstormsecurity.com/files/122260/
    Reference: http://osvdb.org/94804
    Reference: https://wpvulndb.com/vulnerabilities/6965

[+] Finished: Mon May 17 17:43:19 2021
[+] Memory used: 213.492 MB
[+] Elapsed time: 00:04:43
```

## Appendix H – Blog – WPScan

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

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.0.134/ [10.10.0.134]
[+] Started: Mon May 17 16:53:12 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.10.0.134/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.0.134/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
```

```
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://10.10.0.134/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://10.10.0.134/wp-
content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.0.134/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.0 identified (Insecure, released on 2018-12-06).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.0.134/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.0'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.0.134/, Match: 'WordPress 5.0'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:39
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:39

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:03:04
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:03:04

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
```

```
 Checking Config Backups - Time: 00:00:12
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:12

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:06
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:06

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] bjoel
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.10.0.134/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] kwheel
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.10.0.134/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] Karen Wheeler
 | Found By: Rss Generator (Aggressive Detection)

[+] Billy Joel
 | Found By: Rss Generator (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 16:57:23 2021
[+] Requests Done: 3182
[+] Cached Requests: 5
[+] Data Sent: 948.315 KB
[+] Data Received: 1.124 MB
[+] Memory used: 209.195 MB
[+] Elapsed time: 00:04:10
_______________________________________________________________
```

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

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.0.134/ [10.10.0.134]
[+] Started: Mon May 17 16:57:25 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.10.0.134/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.0.134/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://10.10.0.134/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://10.10.0.134/wp-
content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.0.134/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.0 identified (Insecure, released on 2018-12-06).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.0.134/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.0'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.0.134/, Match: 'WordPress 5.0'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:31
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:31

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:03:58
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:03:58

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:12
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:12

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:06
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:06

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
```

```
 Brute Forcing Author IDs - Time: 00:00:01
<============================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] bjoel
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.10.0.134/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] kwheel
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.10.0.134/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] Karen Wheeler
 | Found By: Rss Generator (Aggressive Detection)

[+] Billy Joel
 | Found By: Rss Generator (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 17:02:23 2021
[+] Requests Done: 3182
[+] Cached Requests: 5
[+] Data Sent: 930.602 KB
[+] Data Received: 1.124 MB
[+] Memory used: 237.953 MB
[+] Elapsed time: 00:04:57
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.0.134/ [10.10.0.134]
[+] Started: Mon May 17 17:02:25 2021
```

```
Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.10.0.134/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.0.134/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://10.10.0.134/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://10.10.0.134/wp-
content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.0.134/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.0 identified (Insecure, released on 2018-12-06).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.0.134/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.0'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.0.134/, Match: 'WordPress 5.0'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:32
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:32

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:03:44
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:03:44

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:12
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:12

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:06
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:06

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] bjoel
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.10.0.134/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] kwheel
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.10.0.134/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] Karen Wheeler
 | Found By: Rss Generator (Aggressive Detection)

[+] Billy Joel
 | Found By: Rss Generator (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 17:07:09 2021
[+] Requests Done: 3182
[+] Cached Requests: 5
[+] Data Sent: 944.506 KB
[+] Data Received: 1.124 MB
[+] Memory used: 208.578 MB
[+] Elapsed time: 00:04:43
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.0.134/ [10.10.0.134]
[+] Started: Mon May 17 17:07:11 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.10.0.134/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.0.134/xmlrpc.php
```

```
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://10.10.0.134/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://10.10.0.134/wp-
content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.0.134/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.0 identified (Insecure, released on 2018-12-06).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.0.134/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.0'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.0.134/, Match: 'WordPress 5.0'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:32
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:32

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
```

```
 Checking Known Locations - Time: 00:03:59
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:03:59

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:12
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:12

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:06
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:06

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<=========================================================================
====================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] bjoel
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.10.0.134/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] kwheel
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.10.0.134/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] Karen Wheeler
 | Found By: Rss Generator (Aggressive Detection)

[+] Billy Joel
 | Found By: Rss Generator (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 17:12:10 2021
[+] Requests Done: 3182
[+] Cached Requests: 5
[+] Data Sent: 874.844 KB
[+] Data Received: 1.124 MB
[+] Memory used: 208.867 MB
[+] Elapsed time: 00:04:58
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.0.134/ [10.10.0.134]
[+] Started: Mon May 17 17:12:12 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.10.0.134/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.0.134/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access
```

```
[+] WordPress readme found: http://10.10.0.134/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://10.10.0.134/wp-
content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.0.134/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.0 identified (Insecure, released on 2018-12-06).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.0.134/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.0'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.0.134/, Match: 'WordPress 5.0'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:32
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:32

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:02:51
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:02:51

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:12
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:12

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:06
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:06

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<==========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] bjoel
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.10.0.134/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] kwheel
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.10.0.134/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] Karen Wheeler
 | Found By: Rss Generator (Aggressive Detection)

[+] Billy Joel
 | Found By: Rss Generator (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 17:16:02 2021
[+] Requests Done: 3182
[+] Cached Requests: 5
[+] Data Sent: 908.918 KB
[+] Data Received: 1.124 MB
[+] Memory used: 209.926 MB
[+] Elapsed time: 00:03:49
```

## APPENDIX I – CYBER WEEK 2021 - VANE

```
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.232.46/
[+] Started: Mon May 17 15:45:40 2021
```

```
[!] The WordPress 'http://10.10.232.46/readme.html' file exists exposing a
version number
[+] Interesting header: LINK:
<http://repairshop.sbrc/index.php?rest_route=/>; rel="https://api.w.org/",
<http://repairshop.sbrc/index.php?rest_route=/wp/v2/pages/8>;
rel="alternate"; type="application/json", <http://repairshop.sbrc/>;
rel=shortlink
[+] Interesting header: SERVER: Apache/2.4.37 (centos)
[+] Interesting header: X-POWERED-BY: PHP/7.2.24
[+] XML-RPC Interface available under: http://10.10.232.46/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://10.10.232.46/wp-content/uploads/

[+] WordPress version 5.6.1 identified from links opml

[+] WordPress theme in use: computer - v1.1

[+] Name: computer - v1.1
 |  Location: http://10.10.232.46/wp-content/themes/computer/
 |  Readme: http://10.10.232.46/wp-content/themes/computer/readme.txt
 |  Style URL: http://10.10.232.46/wp-content/themes/computer/style.css
 |  Referenced style.css: http://repairshop.sbrc/wp-
content/themes/computer/style.css
 |  Theme Name: Computer
 |  Theme URI: https://flythemes.net/wordpress-themes/free-computer-
wordpress-theme/
 |  Description: Computer is a responsive WordPress theme crafted for any
computer, mobile phones, tablet, Mac or electronic repair business who
wants a professional online presence. Theme looks great on any device,
from mobile to desktop and beyond. Our responsive design fits to any
screen, and clean code means it loads fast too. Import demo content with
one click to get your theme up and running. This content will guide you
through creating your website, so you can easily add the right content in
the right places. This theme is fully responsive and well perform with all
the resolutions also it is compatible with the latest version of WordPress
and most popular plugins like contact form 7, woocommerce etc.
 |  Author: Flythemes
 |  Author URI: https://flythemes.net
 |  License: GNU General Public License
 |  License URI: license.txt
 |  Tags: one-column, two-columns, right-sidebar, custom-background,
custom-header, custom-menu, featured-images, full-width-template, theme-
options, threaded-comments, custom-logo, blog
 |  Text Domain: computer

[+] Enumerating installed plugins  ...

   Time: 00:00:14
<=========================================================================
==========================================================> (1829 / 1829)
100.00% Time: 00:00:14

[+] We found 1 plugins:
```

```
[+] Name: akismet - v4.1.8
 |  Location: http://10.10.232.46/wp-content/plugins/akismet/
 |  Readme: http://10.10.232.46/wp-content/plugins/akismet/readme.txt
 |  Changelog: http://10.10.232.46/wp-
content/plugins/akismet/changelog.txt

[+] Finished: Mon May 17 15:45:58 2021
[+] Memory used: 230.703 MB
[+] Elapsed time: 00:00:18
ane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.232.46/
[+] Started: Mon May 17 15:45:59 2021

[!] The WordPress 'http://10.10.232.46/readme.html' file exists exposing a
version number
[+] Interesting header: LINK:
<http://repairshop.sbrc/index.php?rest_route=/>; rel="https://api.w.org/",
<http://repairshop.sbrc/index.php?rest_route=/wp/v2/pages/8>;
rel="alternate"; type="application/json", <http://repairshop.sbrc/>;
rel=shortlink
[+] Interesting header: SERVER: Apache/2.4.37 (centos)
[+] Interesting header: X-POWERED-BY: PHP/7.2.24
[+] XML-RPC Interface available under: http://10.10.232.46/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://10.10.232.46/wp-content/uploads/

[+] WordPress version 5.6.1 identified from links opml

[+] WordPress theme in use: computer - v1.1

[+] Name: computer - v1.1
 |  Location: http://10.10.232.46/wp-content/themes/computer/
 |  Readme: http://10.10.232.46/wp-content/themes/computer/readme.txt
 |  Style URL: http://10.10.232.46/wp-content/themes/computer/style.css
 |  Referenced style.css: http://repairshop.sbrc/wp-
content/themes/computer/style.css
 |  Theme Name: Computer
 |  Theme URI: https://flythemes.net/wordpress-themes/free-computer-
wordpress-theme/
 |  Description: Computer is a responsive WordPress theme crafted for any
computer, mobile phones, tablet, Mac or electronic repair business who
wants a professional online presence. Theme looks great on any device,
from mobile to desktop and beyond. Our responsive design fits to any
screen, and clean code means it loads fast too. Import demo content with
one click to get your theme up and running. This content will guide you
through creating your website, so you can easily add the right content in
the right places. This theme is fully responsive and well perform with all
the resolutions also it is compatible with the latest version of WordPress
and most popular plugins like contact form 7, woocommerce etc.
 |  Author: Flythemes
 |  Author URI: https://flythemes.net
 |  License: GNU General Public License
 |  License URI: license.txt
 |  Tags: one-column, two-columns, right-sidebar, custom-background,
custom-header, custom-menu, featured-images, full-width-template, theme-
options, threaded-comments, custom-logo, blog
 |  Text Domain: computer

[+] Enumerating installed plugins  ...

   Time: 00:00:13
<=========================================================================
==========================================================> (1829 / 1829)
100.00% Time: 00:00:13

[+] We found 1 plugins:

[+] Name: akismet - v4.1.8
 |  Location: http://10.10.232.46/wp-content/plugins/akismet/
 |  Readme: http://10.10.232.46/wp-content/plugins/akismet/readme.txt
 |  Changelog: http://10.10.232.46/wp-
content/plugins/akismet/changelog.txt

[+] Finished: Mon May 17 15:46:16 2021
[+] Memory used: 233.07 MB
[+] Elapsed time: 00:00:17
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.232.46/
[+] Started: Mon May 17 15:46:17 2021

[!] The WordPress 'http://10.10.232.46/readme.html' file exists exposing a
version number
[+] Interesting header: LINK:
<http://repairshop.sbrc/index.php?rest_route=/>; rel="https://api.w.org/",
<http://repairshop.sbrc/index.php?rest_route=/wp/v2/pages/8>;
rel="alternate"; type="application/json", <http://repairshop.sbrc/>;
rel=shortlink
[+] Interesting header: SERVER: Apache/2.4.37 (centos)
[+] Interesting header: X-POWERED-BY: PHP/7.2.24
[+] XML-RPC Interface available under: http://10.10.232.46/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://10.10.232.46/wp-content/uploads/

[+] WordPress version 5.6.1 identified from links opml

[+] WordPress theme in use: computer - v1.1

[+] Name: computer - v1.1
 |  Location: http://10.10.232.46/wp-content/themes/computer/
 |  Readme: http://10.10.232.46/wp-content/themes/computer/readme.txt
 |  Style URL: http://10.10.232.46/wp-content/themes/computer/style.css
 |  Referenced style.css: http://repairshop.sbrc/wp-
content/themes/computer/style.css
 |  Theme Name: Computer
 |  Theme URI: https://flythemes.net/wordpress-themes/free-computer-
wordpress-theme/
```

```
 |  Description: Computer is a responsive WordPress theme crafted for any
computer, mobile phones, tablet, Mac or electronic repair business who
wants a professional online presence. Theme looks great on any device,
from mobile to desktop and beyond. Our responsive design fits to any
screen, and clean code means it loads fast too. Import demo content with
one click to get your theme up and running. This content will guide you
through creating your website, so you can easily add the right content in
the right places. This theme is fully responsive and well perform with all
the resolutions also it is compatible with the latest version of WordPress
and most popular plugins like contact form 7, woocommerce etc.
 |  Author: Flythemes
 |  Author URI: https://flythemes.net
 |  License: GNU General Public License
 |  License URI: license.txt
 |  Tags: one-column, two-columns, right-sidebar, custom-background,
custom-header, custom-menu, featured-images, full-width-template, theme-
options, threaded-comments, custom-logo, blog
 |  Text Domain: computer

[+] Enumerating installed plugins  ...

   Time: 00:00:16
<==========================================================================
============================================================> (1829 / 1829)
100.00% Time: 00:00:16

[+] We found 1 plugins:

[+] Name: akismet - v4.1.8
 |  Location: http://10.10.232.46/wp-content/plugins/akismet/
 |  Readme: http://10.10.232.46/wp-content/plugins/akismet/readme.txt
 |  Changelog: http://10.10.232.46/wp-
content/plugins/akismet/changelog.txt

[+] Finished: Mon May 17 15:46:38 2021
[+] Memory used: 231.352 MB
[+] Elapsed time: 00:00:20
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.232.46/
[+] Started: Mon May 17 15:46:38 2021

[!] The WordPress 'http://10.10.232.46/readme.html' file exists exposing a
version number
[+] Interesting header: LINK:
<http://repairshop.sbrc/index.php?rest_route=/>; rel="https://api.w.org/",
<http://repairshop.sbrc/index.php?rest_route=/wp/v2/pages/8>;
rel="alternate"; type="application/json", <http://repairshop.sbrc/>;
rel=shortlink
[+] Interesting header: SERVER: Apache/2.4.37 (centos)
[+] Interesting header: X-POWERED-BY: PHP/7.2.24
[+] XML-RPC Interface available under: http://10.10.232.46/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://10.10.232.46/wp-content/uploads/
```

```
[+] WordPress version 5.6.1 identified from links opml

[+] WordPress theme in use: computer - v1.1

[+] Name: computer - v1.1
 |  Location: http://10.10.232.46/wp-content/themes/computer/
 |  Readme: http://10.10.232.46/wp-content/themes/computer/readme.txt
 |  Style URL: http://10.10.232.46/wp-content/themes/computer/style.css
 |  Referenced style.css: http://repairshop.sbrc/wp-
content/themes/computer/style.css
 |  Theme Name: Computer
 |  Theme URI: https://flythemes.net/wordpress-themes/free-computer-
wordpress-theme/
 |  Description: Computer is a responsive WordPress theme crafted for any
computer, mobile phones, tablet, Mac or electronic repair business who
wants a professional online presence. Theme looks great on any device,
from mobile to desktop and beyond. Our responsive design fits to any
screen, and clean code means it loads fast too. Import demo content with
one click to get your theme up and running. This content will guide you
through creating your website, so you can easily add the right content in
the right places. This theme is fully responsive and well perform with all
the resolutions also it is compatible with the latest version of WordPress
and most popular plugins like contact form 7, woocommerce etc.
 |  Author: Flythemes
 |  Author URI: https://flythemes.net
 |  License: GNU General Public License
 |  License URI: license.txt
 |  Tags: one-column, two-columns, right-sidebar, custom-background,
custom-header, custom-menu, featured-images, full-width-template, theme-
options, threaded-comments, custom-logo, blog
 |  Text Domain: computer

[+] Enumerating installed plugins  ...

   Time: 00:00:12
<=========================================================================
==========================================================> (1829 / 1829)
100.00% Time: 00:00:12

[+] We found 1 plugins:

[+] Name: akismet - v4.1.8
 |  Location: http://10.10.232.46/wp-content/plugins/akismet/
 |  Readme: http://10.10.232.46/wp-content/plugins/akismet/readme.txt
 |  Changelog: http://10.10.232.46/wp-
content/plugins/akismet/changelog.txt

[+] Finished: Mon May 17 15:46:55 2021
[+] Memory used: 231.531 MB
[+] Elapsed time: 00:00:16
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.232.46/
[+] Started: Mon May 17 15:46:56 2021
```

```
[!] The WordPress 'http://10.10.232.46/readme.html' file exists exposing a
version number
[+] Interesting header: LINK:
<http://repairshop.sbrc/index.php?rest_route=/>; rel="https://api.w.org/",
<http://repairshop.sbrc/index.php?rest_route=/wp/v2/pages/8>;
rel="alternate"; type="application/json", <http://repairshop.sbrc/>;
rel=shortlink
[+] Interesting header: SERVER: Apache/2.4.37 (centos)
[+] Interesting header: X-POWERED-BY: PHP/7.2.24
[+] XML-RPC Interface available under: http://10.10.232.46/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://10.10.232.46/wp-content/uploads/

[+] WordPress version 5.6.1 identified from links opml

[+] WordPress theme in use: computer - v1.1

[+] Name: computer - v1.1
 |  Location: http://10.10.232.46/wp-content/themes/computer/
 |  Readme: http://10.10.232.46/wp-content/themes/computer/readme.txt
 |  Style URL: http://10.10.232.46/wp-content/themes/computer/style.css
 |  Referenced style.css: http://repairshop.sbrc/wp-
content/themes/computer/style.css
 |  Theme Name: Computer
 |  Theme URI: https://flythemes.net/wordpress-themes/free-computer-
wordpress-theme/
 |  Description: Computer is a responsive WordPress theme crafted for any
computer, mobile phones, tablet, Mac or electronic repair business who
wants a professional online presence. Theme looks great on any device,
from mobile to desktop and beyond. Our responsive design fits to any
screen, and clean code means it loads fast too. Import demo content with
one click to get your theme up and running. This content will guide you
through creating your website, so you can easily add the right content in
the right places. This theme is fully responsive and well perform with all
the resolutions also it is compatible with the latest version of WordPress
and most popular plugins like contact form 7, woocommerce etc.
 |  Author: Flythemes
 |  Author URI: https://flythemes.net
 |  License: GNU General Public License
 |  License URI: license.txt
 |  Tags: one-column, two-columns, right-sidebar, custom-background,
custom-header, custom-menu, featured-images, full-width-template, theme-
options, threaded-comments, custom-logo, blog
 |  Text Domain: computer

[+] Enumerating installed plugins  ...

   Time: 00:00:13
<==========================================================================
=============================================================> (1829 / 1829)
100.00% Time: 00:00:13

[+] We found 1 plugins:
```

```
[+] Name: akismet - v4.1.8
 |  Location: http://10.10.232.46/wp-content/plugins/akismet/
 |  Readme: http://10.10.232.46/wp-content/plugins/akismet/readme.txt
 |  Changelog: http://10.10.232.46/wp-
content/plugins/akismet/changelog.txt

[+] Finished: Mon May 17 15:47:14 2021
[+] Memory used: 231.398 MB
[+] Elapsed time: 00:00:17
```

## APPENDIX I – CYBER WEEK 2021 – WPSCAN

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

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.232.46/ [10.10.232.46]
[+] Started: Mon May 17 15:43:18 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.37 (centos)
 |  - X-Powered-By: PHP/7.2.24
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.232.46/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
```

```
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://10.10.232.46/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://10.10.232.46/wp-
content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.232.46/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.6.1 identified (Insecure, released on 2021-02-03).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.232.46/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.6.1'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.232.46/, Match: 'WordPress 5.6.1'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:02
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:02

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:18
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:00:18

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:01
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:01

[i] No Config Backups Found.
```

```
[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] theo
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 15:43:47 2021
[+] Requests Done: 3170
[+] Cached Requests: 4
[+] Data Sent: 944.463 KB
[+] Data Received: 513.176 KB
[+] Memory used: 208.852 MB
[+] Elapsed time: 00:00:29
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.232.46/ [10.10.232.46]
[+] Started: Mon May 17 15:43:50 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
```

```
 |  - Server: Apache/2.4.37 (centos)
 |  - X-Powered-By: PHP/7.2.24
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.232.46/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://10.10.232.46/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://10.10.232.46/wp-
content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.232.46/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.6.1 identified (Insecure, released on 2021-02-03).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.232.46/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.6.1'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.232.46/, Match: 'WordPress 5.6.1'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
```

```
 Checking Known Locations - Time: 00:00:02
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:02

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:18
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:00:18

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:01
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:01

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] theo
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 15:44:19 2021
[+] Requests Done: 3170
[+] Cached Requests: 4
[+] Data Sent: 991.725 KB
[+] Data Received: 513.176 KB
[+] Memory used: 208.945 MB
[+] Elapsed time: 00:00:28
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.232.46/ [10.10.232.46]
[+] Started: Mon May 17 15:45:22 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.37 (centos)
 |  - X-Powered-By: PHP/7.2.24
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.232.46/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://10.10.232.46/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://10.10.232.46/wp-
content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.232.46/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.6.1 identified (Insecure, released on 2021-02-03).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.232.46/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.6.1'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.232.46/, Match: 'WordPress 5.6.1'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:02
<==========================================================================
====================================> (348 / 348) 100.00% Time: 00:00:02

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:18
<==========================================================================
==================================> (2568 / 2568) 100.00% Time: 00:00:18

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:01
<==========================================================================
=====================================> (137 / 137) 100.00% Time: 00:00:01

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<==========================================================================
===========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<==========================================================================
======================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] theo
```

```
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 15:45:52 2021
[+] Requests Done: 3170
[+] Cached Requests: 4
[+] Data Sent: 1.02 MB
[+] Data Received: 513.176 KB
[+] Memory used: 209.172 MB
[+] Elapsed time: 00:00:29
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.232.46/ [10.10.232.46]
[+] Started: Mon May 17 15:44:52 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.37 (centos)
 |  - X-Powered-By: PHP/7.2.24
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.232.46/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
```

```
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://10.10.232.46/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://10.10.232.46/wp-
content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.232.46/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.6.1 identified (Insecure, released on 2021-02-03).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.232.46/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.6.1'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.232.46/, Match: 'WordPress 5.6.1'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:02
<==========================================================================
====================================> (348 / 348) 100.00% Time: 00:00:02

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:18
<==========================================================================
==================================> (2568 / 2568) 100.00% Time: 00:00:18

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
```

```
 Checking Config Backups - Time: 00:00:01
<=========================================================================
===================================> (137 / 137) 100.00% Time: 00:00:01

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] theo
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 15:45:20 2021
[+] Requests Done: 3170
[+] Cached Requests: 4
[+] Data Sent: 954.576 KB
[+] Data Received: 513.213 KB
[+] Memory used: 208.5 MB
[+] Elapsed time: 00:00:28
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.232.46/ [10.10.232.46]
[+] Started: Mon May 17 15:44:21 2021
```

```
Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.37 (centos)
 |  - X-Powered-By: PHP/7.2.24
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.232.46/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://10.10.232.46/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://10.10.232.46/wp-
content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.232.46/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.6.1 identified (Insecure, released on 2021-02-03).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.232.46/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.6.1'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.232.46/, Match: 'WordPress 5.6.1'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)
```

```
[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:02
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:02

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:18
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:00:18

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:01
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:01

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] theo
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 15:44:49 2021
[+] Requests Done: 3170
[+] Cached Requests: 4
[+] Data Sent: 1.053 MB
[+] Data Received: 513.194 KB
[+] Memory used: 209.504 MB
[+] Elapsed time: 00:00:28
___________________________________
```

## APPENDIX J – INTERNAL - VANE

```
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.11.187/wordpress/
[+] Started: Mon May 17 17:51:46 2021

[!] The WordPress 'http://10.10.11.187/wordpress/readme.html' file exists
exposing a version number
[+] Interesting header: LINK: <http://internal.thm/blog/index.php/wp-
json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.29 (Ubuntu)
[+] XML-RPC Interface available under:
http://10.10.11.187/wordpress/xmlrpc.php

[+] WordPress version 5.4.2 identified from links opml

[+] WordPress theme in use: twentyseventeen - v2.3

[+] Name: twentyseventeen - v2.3
 |  Location: http://10.10.11.187/wordpress/wp-
content/themes/twentyseventeen/
 |  Readme: http://10.10.11.187/wordpress/wp-
content/themes/twentyseventeen/readme.txt
 |  Style URL: http://10.10.11.187/wordpress/wp-
content/themes/twentyseventeen/style.css
 |  Referenced style.css: http://internal.thm/blog/wp-
content/themes/twentyseventeen/style.css
 |  Theme Name: Twenty Seventeen
 |  Theme URI: https://wordpress.org/themes/twentyseventeen/
 |  Description: Twenty Seventeen brings your site to life with header
video and immersive featured images. With a focus on business sites, it
features multiple sections on the front page as well as widgets,
navigation and social menus, a logo, and more. Personalize its
asymmetrical grid with a custom color scheme and showcase your multimedia
content with post formats. Our default theme for 2017 works great in many
languages, for any abilities, and on any device.
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: one-column, two-columns, right-sidebar, flexible-header,
accessibility-ready, custom-colors, custom-header, custom-menu, custom-
logo, editor-style, featured-images, footer-widgets, post-formats, rtl-
language-support, sticky-post, theme-options, threaded-comments,
translation-ready
 |  Text Domain: twentyseventeen

[+] Enumerating installed plugins  ...
```

```
   Time: 00:00:10
<=========================================================================
==========================================================> (1829 / 1829)
100.00% Time: 00:00:10

[+] No plugins found

[+] Finished: Mon May 17 17:52:02 2021
[+] Memory used: 230.438 MB
[+] Elapsed time: 00:00:15
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.11.187/wordpress/
[+] Started: Mon May 17 17:52:02 2021

[!] The WordPress 'http://10.10.11.187/wordpress/readme.html' file exists
exposing a version number
[+] Interesting header: LINK: <http://internal.thm/blog/index.php/wp-
json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.29 (Ubuntu)
[+] XML-RPC Interface available under:
http://10.10.11.187/wordpress/xmlrpc.php

[+] WordPress version 5.4.2 identified from links opml

[+] WordPress theme in use: twentyseventeen - v2.3

[+] Name: twentyseventeen - v2.3
 |  Location: http://10.10.11.187/wordpress/wp-
content/themes/twentyseventeen/
 |  Readme: http://10.10.11.187/wordpress/wp-
content/themes/twentyseventeen/readme.txt
 |  Style URL: http://10.10.11.187/wordpress/wp-
content/themes/twentyseventeen/style.css
 |  Referenced style.css: http://internal.thm/blog/wp-
content/themes/twentyseventeen/style.css
 |  Theme Name: Twenty Seventeen
 |  Theme URI: https://wordpress.org/themes/twentyseventeen/
 |  Description: Twenty Seventeen brings your site to life with header
video and immersive featured images. With a focus on business sites, it
features multiple sections on the front page as well as widgets,
navigation and social menus, a logo, and more. Personalize its
asymmetrical grid with a custom color scheme and showcase your multimedia
content with post formats. Our default theme for 2017 works great in many
languages, for any abilities, and on any device.
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: one-column, two-columns, right-sidebar, flexible-header,
accessibility-ready, custom-colors, custom-header, custom-menu, custom-
logo, editor-style, featured-images, footer-widgets, post-formats, rtl-
language-support, sticky-post, theme-options, threaded-comments,
translation-ready
```

```
 |  Text Domain: twentyseventeen

[+] Enumerating installed plugins  ...

   Time: 00:00:14
<=========================================================================
==========================================================> (1829 / 1829)
100.00% Time: 00:00:14

[+] No plugins found

[+] Finished: Mon May 17 17:52:21 2021
[+] Memory used: 229.055 MB
[+] Elapsed time: 00:00:18
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.11.187/wordpress/
[+] Started: Mon May 17 17:52:21 2021

[!] The WordPress 'http://10.10.11.187/wordpress/readme.html' file exists
exposing a version number
[+] Interesting header: LINK: <http://internal.thm/blog/index.php/wp-
json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.29 (Ubuntu)
[+] XML-RPC Interface available under:
http://10.10.11.187/wordpress/xmlrpc.php

[+] WordPress version 5.4.2 identified from links opml

[+] WordPress theme in use: twentyseventeen - v2.3

[+] Name: twentyseventeen - v2.3
 |  Location: http://10.10.11.187/wordpress/wp-
content/themes/twentyseventeen/
 |  Readme: http://10.10.11.187/wordpress/wp-
content/themes/twentyseventeen/readme.txt
 |  Style URL: http://10.10.11.187/wordpress/wp-
content/themes/twentyseventeen/style.css
 |  Referenced style.css: http://internal.thm/blog/wp-
content/themes/twentyseventeen/style.css
 |  Theme Name: Twenty Seventeen
 |  Theme URI: https://wordpress.org/themes/twentyseventeen/
 |  Description: Twenty Seventeen brings your site to life with header
video and immersive featured images. With a focus on business sites, it
features multiple sections on the front page as well as widgets,
navigation and social menus, a logo, and more. Personalize its
asymmetrical grid with a custom color scheme and showcase your multimedia
content with post formats. Our default theme for 2017 works great in many
languages, for any abilities, and on any device.
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: one-column, two-columns, right-sidebar, flexible-header,
accessibility-ready, custom-colors, custom-header, custom-menu, custom-
```

```
logo, editor-style, featured-images, footer-widgets, post-formats, rtl-
language-support, sticky-post, theme-options, threaded-comments,
translation-ready
 |  Text Domain: twentyseventeen

[+] Enumerating installed plugins  ...

   Time: 00:00:12
<=========================================================================
==========================================================> (1829 / 1829)
100.00% Time: 00:00:12

[+] No plugins found

[+] Finished: Mon May 17 17:52:37 2021
[+] Memory used: 231.473 MB
[+] Elapsed time: 00:00:16
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.11.187/wordpress/
[+] Started: Mon May 17 17:52:39 2021

[!] The WordPress 'http://10.10.11.187/wordpress/readme.html' file exists
exposing a version number
[+] Interesting header: LINK: <http://internal.thm/blog/index.php/wp-
json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.29 (Ubuntu)
[+] XML-RPC Interface available under:
http://10.10.11.187/wordpress/xmlrpc.php

[+] WordPress version 5.4.2 identified from links opml

[+] WordPress theme in use: twentyseventeen - v2.3

[+] Name: twentyseventeen - v2.3
 |  Location: http://10.10.11.187/wordpress/wp-
content/themes/twentyseventeen/
 |  Readme: http://10.10.11.187/wordpress/wp-
content/themes/twentyseventeen/readme.txt
 |  Style URL: http://10.10.11.187/wordpress/wp-
content/themes/twentyseventeen/style.css
 |  Referenced style.css: http://internal.thm/blog/wp-
content/themes/twentyseventeen/style.css
 |  Theme Name: Twenty Seventeen
 |  Theme URI: https://wordpress.org/themes/twentyseventeen/
 |  Description: Twenty Seventeen brings your site to life with header
video and immersive featured images. With a focus on business sites, it
features multiple sections on the front page as well as widgets,
navigation and social menus, a logo, and more. Personalize its
asymmetrical grid with a custom color scheme and showcase your multimedia
content with post formats. Our default theme for 2017 works great in many
languages, for any abilities, and on any device.
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: one-column, two-columns, right-sidebar, flexible-header,
accessibility-ready, custom-colors, custom-header, custom-menu, custom-
logo, editor-style, featured-images, footer-widgets, post-formats, rtl-
language-support, sticky-post, theme-options, threaded-comments,
translation-ready
 |  Text Domain: twentyseventeen

[+] Enumerating installed plugins  ...

   Time: 00:00:14
<===========================================================================
===========================================================> (1829 / 1829)
100.00% Time: 00:00:14

[+] No plugins found

[+] Finished: Mon May 17 17:52:57 2021
[+] Memory used: 230.41 MB
[+] Elapsed time: 00:00:17
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.11.187/wordpress/
[+] Started: Mon May 17 17:52:58 2021

[!] The WordPress 'http://10.10.11.187/wordpress/readme.html' file exists
exposing a version number
[+] Interesting header: LINK: <http://internal.thm/blog/index.php/wp-
json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.29 (Ubuntu)
[+] XML-RPC Interface available under:
http://10.10.11.187/wordpress/xmlrpc.php

[+] WordPress version 5.4.2 identified from links opml

[+] WordPress theme in use: twentyseventeen - v2.3

[+] Name: twentyseventeen - v2.3
 |  Location: http://10.10.11.187/wordpress/wp-
content/themes/twentyseventeen/
 |  Readme: http://10.10.11.187/wordpress/wp-
content/themes/twentyseventeen/readme.txt
 |  Style URL: http://10.10.11.187/wordpress/wp-
content/themes/twentyseventeen/style.css
 |  Referenced style.css: http://internal.thm/blog/wp-
content/themes/twentyseventeen/style.css
 |  Theme Name: Twenty Seventeen
 |  Theme URI: https://wordpress.org/themes/twentyseventeen/
 |  Description: Twenty Seventeen brings your site to life with header
video and immersive featured images. With a focus on business sites, it
features multiple sections on the front page as well as widgets,
navigation and social menus, a logo, and more. Personalize its
asymmetrical grid with a custom color scheme and showcase your multimedia
content with post formats. Our default theme for 2017 works great in many
languages, for any abilities, and on any device.
```

```
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: one-column, two-columns, right-sidebar, flexible-header,
accessibility-ready, custom-colors, custom-header, custom-menu, custom-
logo, editor-style, featured-images, footer-widgets, post-formats, rtl-
language-support, sticky-post, theme-options, threaded-comments,
translation-ready
 |  Text Domain: twentyseventeen

[+] Enumerating installed plugins  ...

   Time: 00:00:09
<=========================================================================
==========================================================> (1829 / 1829)
100.00% Time: 00:00:09

[+] No plugins found

[+] Finished: Mon May 17 17:53:11 2021
[+] Memory used: 229.289 MB
[+] Elapsed time: 00:00:13
```

## APPENDIX J– INTERNAL - WPSCAN

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

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.11.187/wordpress/ [10.10.11.187]
[+] Started: Mon May 17 17:49:17 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.11.187/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://10.10.11.187/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://10.10.11.187/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.4.2 identified (Insecure, released on 2020-06-10).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.11.187/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.4.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.11.187/wordpress/, Match: 'WordPress 5.4.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:02
<==========================================================================
====================================> (348 / 348) 100.00% Time: 00:00:02

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:18
<==========================================================================
==================================> (2568 / 2568) 100.00% Time: 00:00:18

[i] No Timthumbs Found.
```

```
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:01
<=============================================================================
====================================> (137 / 137) 100.00% Time: 00:00:01

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<=============================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<=============================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:00

[i] No Users Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 17:49:45 2021
[+] Requests Done: 3168
[+] Cached Requests: 4
[+] Data Sent: 888.991 KB
[+] Data Received: 600.744 KB
[+] Memory used: 208.598 MB
[+] Elapsed time: 00:00:27
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.11.187/wordpress/ [10.10.11.187]
[+] Started: Mon May 17 17:49:47 2021

Interesting Finding(s):

[+] Headers
```

```
 | Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.11.187/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://10.10.11.187/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://10.10.11.187/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.4.2 identified (Insecure, released on 2020-06-10).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.11.187/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.4.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.11.187/wordpress/, Match: 'WordPress 5.4.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:02
<=========================================================================
====================================> (348 / 348) 100.00% Time: 00:00:02

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
```

```
 Checking Known Locations - Time: 00:00:18
<========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:00:18

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:01
<========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:01

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:00

[i] No Users Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 17:50:15 2021
[+] Requests Done: 3168
[+] Cached Requests: 4
[+] Data Sent: 839.491 KB
[+] Data Received: 600.781 KB
[+] Memory used: 209.285 MB
[+] Elapsed time: 00:00:27
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
________________________________________________________________
```

```
[+] URL: http://10.10.11.187/wordpress/ [10.10.11.187]
[+] Started: Mon May 17 17:50:17 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.11.187/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://10.10.11.187/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://10.10.11.187/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.4.2 identified (Insecure, released on 2020-06-10).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.11.187/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.4.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.11.187/wordpress/, Match: 'WordPress 5.4.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
```

```
 Checking Known Locations - Time: 00:00:02
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:02

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:18
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:00:18

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:01
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:01

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:00

[i] No Users Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 17:50:44 2021
[+] Requests Done: 3168
[+] Cached Requests: 4
[+] Data Sent: 957.054 KB
[+] Data Received: 600.781 KB
[+] Memory used: 209.062 MB
[+] Elapsed time: 00:00:27
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|
          WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.11.187/wordpress/ [10.10.11.187]
[+] Started: Mon May 17 17:50:46 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.11.187/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://10.10.11.187/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://10.10.11.187/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.4.2 identified (Insecure, released on 2020-06-10).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.11.187/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.4.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.11.187/wordpress/, Match: 'WordPress 5.4.2'

[i] The main theme could not be detected.
```

```
[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:02
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:02

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:18
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:00:18

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:01
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:01

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:00

[i] No Users Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 17:51:12 2021
[+] Requests Done: 3168
[+] Cached Requests: 4
[+] Data Sent: 923.022 KB
[+] Data Received: 600.744 KB
[+] Memory used: 208.238 MB
[+] Elapsed time: 00:00:26
_______________________________________________________________
```

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

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.11.187/wordpress/ [10.10.11.187]
[+] Started: Mon May 17 17:51:14 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.11.187/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://10.10.11.187/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled:
http://10.10.11.187/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.4.2 identified (Insecure, released on 2020-06-10).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.11.187/wordpress/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.4.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.11.187/wordpress/, Match: 'WordPress 5.4.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:02
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:02

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:19
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:00:19

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:01
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:01

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:00

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:00

[i] No Users Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 17:51:42 2021
[+] Requests Done: 3168
[+] Cached Requests: 4
[+] Data Sent: 960.147 KB
[+] Data Received: 600.763 KB
[+] Memory used: 208.559 MB
[+] Elapsed time: 00:00:27
```

## Appendix K – Jack - Vane

```
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.141.112/
[+] Started: Mon May 17 16:27:59 2021

[+] robots.txt available under: 'http://10.10.141.112/robots.txt'
[+] Interesting entry from robots.txt: http://10.10.141.112/wp-
admin/admin-ajax.php
[!] The WordPress 'http://10.10.141.112/readme.html' file exists exposing
a version number
[+] Interesting header: LINK: <http://jack.thm/index.php/wp-json/>;
rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.18 (Ubuntu)
[+] XML-RPC Interface available under: http://10.10.141.112/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://10.10.141.112/wp-content/uploads/

[+] WordPress version 5.3.2 identified from links opml

[+] WordPress theme in use: online-portfolio - v0.0.7

[+] Name: online-portfolio - v0.0.7
 |  Location: http://10.10.141.112/wp-content/themes/online-portfolio/
 |  Readme: http://10.10.141.112/wp-content/themes/online-
portfolio/readme.txt
 |  Style URL: http://10.10.141.112/wp-content/themes/online-
portfolio/style.css
 |  Referenced style.css: http://jack.thm/wp-content/themes/online-
portfolio/style.css
 |  Theme Name: Online Portfolio
 |  Theme URI: https://www.amplethemes.com/downloads/online-protfolio/
 |  Description: Online Portfolio WordPress portfolio theme for building
personal website. You can take full advantage of the free widgets to
create amazing personal website regardless whether you are graphic
designer, painters, artists, web designer, web developer, software
engineer or photographer. You can customize elements and widgets inside
customizer without you having to tweaking any code. The theme comes with
Full width layout, easy Logo upload. Portfolioo is 100% responsive built
with HTML5 and CSS3, it is SEO friendly, mobile optimized and retina
ready, thoroughly tested by WordPress coding standard. Gutenberg ready,
clean and bloat free code, you can flesh out free portfolio, grid,
personal showcase website for free. Perfect Portfolio theme for Graphic
Designers, Web Designers, Web Developers, Artists, Painters and
Photographers.
 |  Author: Ample Themes
 |  Author URI: https://amplethemes.com/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: custom-logo, one-column, two-columns, right-sidebar, left-
sidebar, full-width-template, custom-background, custom-colors, custom-
menu, featured-images, theme-options, threaded-comments, translation-
ready, blog, portfolio, e-commerce, footer-widgets
 |  Text Domain: online-portfolio

[+] Enumerating installed plugins  ...

   Time: 00:02:23
<===========================================================================
==========================================================> (1829 / 1829)
100.00% Time: 00:02:23

[+] We found 2 plugins:

[+] Name: akismet - v3.1.7
 |  Location: http://10.10.141.112/wp-content/plugins/akismet/
 |  Readme: http://10.10.141.112/wp-content/plugins/akismet/readme.txt

[+] Name: user-role-editor - v4.24
 |  Location: http://10.10.141.112/wp-content/plugins/user-role-editor/
 |  Readme: http://10.10.141.112/wp-content/plugins/user-role-
editor/readme.txt

[+] Finished: Mon May 17 16:30:32 2021
[+] Memory used: 210.027 MB
[+] Elapsed time: 00:02:33
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.141.112/
[+] Started: Mon May 17 16:30:33 2021

[+] robots.txt available under: 'http://10.10.141.112/robots.txt'
[+] Interesting entry from robots.txt: http://10.10.141.112/wp-
admin/admin-ajax.php
[!] The WordPress 'http://10.10.141.112/readme.html' file exists exposing
a version number
[+] Interesting header: LINK: <http://jack.thm/index.php/wp-json/>;
rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.18 (Ubuntu)
[+] XML-RPC Interface available under: http://10.10.141.112/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://10.10.141.112/wp-content/uploads/

[+] WordPress version 5.3.2 identified from links opml

[+] WordPress theme in use: online-portfolio - v0.0.7

[+] Name: online-portfolio - v0.0.7
 |  Location: http://10.10.141.112/wp-content/themes/online-portfolio/
 |  Readme: http://10.10.141.112/wp-content/themes/online-
portfolio/readme.txt
```

```
 |  Style URL: http://10.10.141.112/wp-content/themes/online-
portfolio/style.css
 |  Referenced style.css: http://jack.thm/wp-content/themes/online-
portfolio/style.css
 |  Theme Name: Online Portfolio
 |  Theme URI: https://www.amplethemes.com/downloads/online-protfolio/
 |  Description: Online Portfolio WordPress portfolio theme for building
personal website. You can take full advantage of the free widgets to
create amazing personal website regardless whether you are graphic
designer, painters, artists, web designer, web developer, software
engineer or photographer. You can customize elements and widgets inside
customizer without you having to tweaking any code. The theme comes with
Full width layout, easy Logo upload. Portfolioo is 100% responsive built
with HTML5 and CSS3, it is SEO friendly, mobile optimized and retina
ready, thoroughly tested by WordPress coding standard. Gutenberg ready,
clean and bloat free code, you can flesh out free portfolio, grid,
personal showcase website for free. Perfect Portfolio theme for Graphic
Designers, Web Designers, Web Developers, Artists, Painters and
Photographers.
 |  Author: Ample Themes
 |  Author URI: https://amplethemes.com/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: custom-logo, one-column, two-columns, right-sidebar, left-
sidebar, full-width-template, custom-background, custom-colors, custom-
menu, featured-images, theme-options, threaded-comments, translation-
ready, blog, portfolio, e-commerce, footer-widgets
 |  Text Domain: online-portfolio

[+] Enumerating installed plugins  ...

   Time: 00:04:50
<==========================================================================
==========================================================> (1829 / 1829)
100.00% Time: 00:04:50

[+] We found 2 plugins:

[+] Name: akismet - v3.1.7
 |  Location: http://10.10.141.112/wp-content/plugins/akismet/
 |  Readme: http://10.10.141.112/wp-content/plugins/akismet/readme.txt

[+] Name: user-role-editor - v4.24
 |  Location: http://10.10.141.112/wp-content/plugins/user-role-editor/
 |  Readme: http://10.10.141.112/wp-content/plugins/user-role-
editor/readme.txt

[+] Finished: Mon May 17 16:35:29 2021
[+] Memory used: 205.602 MB
[+] Elapsed time: 00:04:56
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.141.112/
[+] Started: Mon May 17 16:35:30 2021
[+] robots.txt available under: 'http://10.10.141.112/robots.txt'
[+] Interesting entry from robots.txt: http://10.10.141.112/wp-
admin/admin-ajax.php
[!] The WordPress 'http://10.10.141.112/readme.html' file exists exposing
a version number
[+] Interesting header: LINK: <http://jack.thm/index.php/wp-json/>;
rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.18 (Ubuntu)
[+] XML-RPC Interface available under: http://10.10.141.112/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://10.10.141.112/wp-content/uploads/

[+] WordPress version 5.3.2 identified from links opml

[+] WordPress theme in use: online-portfolio - v0.0.7

[+] Name: online-portfolio - v0.0.7
 |  Location: http://10.10.141.112/wp-content/themes/online-portfolio/
 |  Readme: http://10.10.141.112/wp-content/themes/online-
portfolio/readme.txt
 |  Style URL: http://10.10.141.112/wp-content/themes/online-
portfolio/style.css
 |  Referenced style.css: http://jack.thm/wp-content/themes/online-
portfolio/style.css
 |  Theme Name: Online Portfolio
 |  Theme URI: https://www.amplethemes.com/downloads/online-protfolio/
 |  Description: Online Portfolio WordPress portfolio theme for building
personal website. You can take full advantage of the free widgets to
create amazing personal website regardless whether you are graphic
designer, painters, artists, web designer, web developer, software
engineer or photographer. You can customize elements and widgets inside
customizer without you having to tweaking any code. The theme comes with
Full width layout, easy Logo upload. Portfolioo is 100% responsive built
with HTML5 and CSS3, it is SEO friendly, mobile optimized and retina
ready, thoroughly tested by WordPress coding standard. Gutenberg ready,
clean and bloat free code, you can flesh out free portfolio, grid,
personal showcase website for free. Perfect Portfolio theme for Graphic
Designers, Web Designers, Web Developers, Artists, Painters and
Photographers.
 |  Author: Ample Themes
 |  Author URI: https://amplethemes.com/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: custom-logo, one-column, two-columns, right-sidebar, left-
sidebar, full-width-template, custom-background, custom-colors, custom-
menu, featured-images, theme-options, threaded-comments, translation-
ready, blog, portfolio, e-commerce, footer-widgets
 |  Text Domain: online-portfolio

[+] Enumerating installed plugins  ...

   Time: 00:04:51
<==========================================================================
===========================================================> (1829 / 1829)
100.00% Time: 00:04:51

[+] We found 2 plugins:

[+] Name: akismet - v3.1.7
 |  Location: http://10.10.141.112/wp-content/plugins/akismet/
 |  Readme: http://10.10.141.112/wp-content/plugins/akismet/readme.txt

[+] Name: user-role-editor - v4.24
 |  Location: http://10.10.141.112/wp-content/plugins/user-role-editor/
 |  Readme: http://10.10.141.112/wp-content/plugins/user-role-
editor/readme.txt

[+] Finished: Mon May 17 16:40:30 2021
[+] Memory used: 206.762 MB
[+] Elapsed time: 00:04:59
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.141.112/
[+] Started: Mon May 17 16:40:31 2021

[+] robots.txt available under: 'http://10.10.141.112/robots.txt'
[+] Interesting entry from robots.txt: http://10.10.141.112/wp-
admin/admin-ajax.php
[!] The WordPress 'http://10.10.141.112/readme.html' file exists exposing
a version number
[+] Interesting header: LINK: <http://jack.thm/index.php/wp-json/>;
rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.18 (Ubuntu)
[+] XML-RPC Interface available under: http://10.10.141.112/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://10.10.141.112/wp-content/uploads/

[+] WordPress version 5.3.2 identified from links opml

[+] WordPress theme in use: online-portfolio - v0.0.7

[+] Name: online-portfolio - v0.0.7
 |  Location: http://10.10.141.112/wp-content/themes/online-portfolio/
 |  Readme: http://10.10.141.112/wp-content/themes/online-
portfolio/readme.txt
 |  Style URL: http://10.10.141.112/wp-content/themes/online-
portfolio/style.css
 |  Referenced style.css: http://jack.thm/wp-content/themes/online-
portfolio/style.css
 |  Theme Name: Online Portfolio
 |  Theme URI: https://www.amplethemes.com/downloads/online-protfolio/
 |  Description: Online Portfolio WordPress portfolio theme for building
personal website. You can take full advantage of the free widgets to
create amazing personal website regardless whether you are graphic
designer, painters, artists, web designer, web developer, software
engineer or photographer. You can customize elements and widgets inside
customizer without you having to tweaking any code. The theme comes with
Full width layout, easy Logo upload. Portfolioo is 100% responsive built
```

```
with HTML5 and CSS3, it is SEO friendly, mobile optimized and retina
ready, thoroughly tested by WordPress coding standard. Gutenberg ready,
clean and bloat free code, you can flesh out free portfolio, grid,
personal showcase website for free. Perfect Portfolio theme for Graphic
Designers, Web Designers, Web Developers, Artists, Painters and
Photographers.
 |  Author: Ample Themes
 |  Author URI: https://amplethemes.com/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: custom-logo, one-column, two-columns, right-sidebar, left-
sidebar, full-width-template, custom-background, custom-colors, custom-
menu, featured-images, theme-options, threaded-comments, translation-
ready, blog, portfolio, e-commerce, footer-widgets
 |  Text Domain: online-portfolio

[+] Enumerating installed plugins  ...

   Time: 00:04:32
<===========================================================================
===========================================================> (1829 / 1829)
100.00% Time: 00:04:32

[+] We found 2 plugins:

[+] Name: akismet - v3.1.7
 |  Location: http://10.10.141.112/wp-content/plugins/akismet/
 |  Readme: http://10.10.141.112/wp-content/plugins/akismet/readme.txt

[+] Name: user-role-editor - v4.24
 |  Location: http://10.10.141.112/wp-content/plugins/user-role-editor/
 |  Readme: http://10.10.141.112/wp-content/plugins/user-role-
editor/readme.txt

[+] Finished: Mon May 17 16:45:11 2021
[+] Memory used: 213.246 MB
[+] Elapsed time: 00:04:40
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.141.112/
[+] Started: Mon May 17 16:45:12 2021

[+] robots.txt available under: 'http://10.10.141.112/robots.txt'
[+] Interesting entry from robots.txt: http://10.10.141.112/wp-
admin/admin-ajax.php
[!] The WordPress 'http://10.10.141.112/readme.html' file exists exposing
a version number
[+] Interesting header: LINK: <http://jack.thm/index.php/wp-json/>;
rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.18 (Ubuntu)
[+] XML-RPC Interface available under: http://10.10.141.112/xmlrpc.php
[!] Upload directory has directory listing enabled:
http://10.10.141.112/wp-content/uploads/

[+] WordPress version 5.3.2 identified from links opml
[+] WordPress theme in use: online-portfolio - v0.0.7

[+] Name: online-portfolio - v0.0.7
 |  Location: http://10.10.141.112/wp-content/themes/online-portfolio/
 |  Readme: http://10.10.141.112/wp-content/themes/online-
portfolio/readme.txt
 |  Style URL: http://10.10.141.112/wp-content/themes/online-
portfolio/style.css
 |  Referenced style.css: http://jack.thm/wp-content/themes/online-
portfolio/style.css
 |  Theme Name: Online Portfolio
 |  Theme URI: https://www.amplethemes.com/downloads/online-protfolio/
 |  Description: Online Portfolio WordPress portfolio theme for building
personal website. You can take full advantage of the free widgets to
create amazing personal website regardless whether you are graphic
designer, painters, artists, web designer, web developer, software
engineer or photographer. You can customize elements and widgets inside
customizer without you having to tweaking any code. The theme comes with
Full width layout, easy Logo upload. Portfolioo is 100% responsive built
with HTML5 and CSS3, it is SEO friendly, mobile optimized and retina
ready, thoroughly tested by WordPress coding standard. Gutenberg ready,
clean and bloat free code, you can flesh out free portfolio, grid,
personal showcase website for free. Perfect Portfolio theme for Graphic
Designers, Web Designers, Web Developers, Artists, Painters and
Photographers.
 |  Author: Ample Themes
 |  Author URI: https://amplethemes.com/
 |  License: GNU General Public License v2 or later
 |  License URI: http://www.gnu.org/licenses/gpl-2.0.html
 |  Tags: custom-logo, one-column, two-columns, right-sidebar, left-
sidebar, full-width-template, custom-background, custom-colors, custom-
menu, featured-images, theme-options, threaded-comments, translation-
ready, blog, portfolio, e-commerce, footer-widgets
 |  Text Domain: online-portfolio

[+] Enumerating installed plugins  ...

   Time: 00:04:20
<=========================================================================
=============================================================> (1829 / 1829)
100.00% Time: 00:04:20

[+] We found 2 plugins:

[+] Name: akismet - v3.1.7
 |  Location: http://10.10.141.112/wp-content/plugins/akismet/
 |  Readme: http://10.10.141.112/wp-content/plugins/akismet/readme.txt

[+] Name: user-role-editor - v4.24
 |  Location: http://10.10.141.112/wp-content/plugins/user-role-editor/
 |  Readme: http://10.10.141.112/wp-content/plugins/user-role-
editor/readme.txt
```

```
[+] Finished: Mon May 17 16:49:37 2021
[+] Memory used: 206.746 MB
[+] Elapsed time: 00:04:25
```

## Appendix K – Jack - WPScan

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

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.141.112/ [10.10.141.112]
[+] Started: Mon May 17 15:59:08 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.10.141.112/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.141.112/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
```

```
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://10.10.141.112/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://10.10.141.112/wp-
content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.141.112/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.3.2 identified (Insecure, released on 2019-12-18).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.141.112/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.3.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.141.112/, Match: 'WordPress 5.3.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:05
<==========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:05

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:42
<==========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:00:42

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:10
<==========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:10

[i] No Config Backups Found.
```

```
[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:02
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:02

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] jack
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.10.141.112/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] danny
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] wendy
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 16:00:14 2021
[+] Requests Done: 3178
[+] Cached Requests: 5
[+] Data Sent: 1.021 MB
[+] Data Received: 1.156 MB
[+] Memory used: 209.535 MB
[+] Elapsed time: 00:01:06
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
```

```
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.141.112/ [10.10.141.112]
[+] Started: Mon May 17 16:00:16 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.10.141.112/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.141.112/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://10.10.141.112/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://10.10.141.112/wp-
content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.141.112/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.3.2 identified (Insecure, released on 2019-12-18).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.141.112/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.3.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.141.112/, Match: 'WordPress 5.3.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:12
<==========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:12

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:09:12
<==========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:09:12

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:14
<==========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:14

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:07
<==========================================================================
===========================================> (71 / 71) 100.00% Time:
00:00:07

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<==========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] jack
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.10.141.112/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] wendy
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] danny
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 16:10:11 2021
[+] Requests Done: 3178
[+] Cached Requests: 5
[+] Data Sent: 1.061 MB
[+] Data Received: 1.156 MB
[+] Memory used: 208.91 MB
[+] Elapsed time: 00:09:54
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.141.112/ [10.10.141.112]
[+] Started: Mon May 17 16:10:13 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.10.141.112/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.141.112/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://10.10.141.112/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://10.10.141.112/wp-
content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.141.112/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.3.2 identified (Insecure, released on 2019-12-18).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.141.112/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.3.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.141.112/, Match: 'WordPress 5.3.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:37
<=========================================================================
==================================> (348 / 348) 100.00% Time: 00:00:37
```

```
[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:04:16
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:04:16

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:02
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:02

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:01
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:01

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] jack
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.10.141.112/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] wendy
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] danny
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register
```

```
[+] Finished: Mon May 17 16:15:16 2021
[+] Requests Done: 3178
[+] Cached Requests: 5
[+] Data Sent: 1.018 MB
[+] Data Received: 1.156 MB
[+] Memory used: 208.445 MB
[+] Elapsed time: 00:05:02
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.141.112/ [10.10.141.112]
[+] Started: Mon May 17 16:15:18 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.10.141.112/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.141.112/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access
```

```
[+] WordPress readme found: http://10.10.141.112/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://10.10.141.112/wp-
content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.141.112/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.3.2 identified (Insecure, released on 2019-12-18).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.141.112/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.3.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.141.112/, Match: 'WordPress 5.3.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:29
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:29

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:04:34
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:04:34

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:14
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:14

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
```

```
 Checking DB Exports - Time: 00:00:07
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:07

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] jack
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.10.141.112/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] wendy
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] danny
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 16:20:51 2021
[+] Requests Done: 3178
[+] Cached Requests: 5
[+] Data Sent: 1015.008 KB
[+] Data Received: 1.156 MB
[+] Memory used: 209 MB
[+] Elapsed time: 00:05:33
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.141.112/ [10.10.141.112]
[+] Started: Mon May 17 16:20:54 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.10.141.112/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.141.112/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] WordPress readme found: http://10.10.141.112/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://10.10.141.112/wp-
content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.141.112/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299
```

```
[+] WordPress version 5.3.2 identified (Insecure, released on 2019-12-18).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.141.112/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.3.2'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.141.112/, Match: 'WordPress 5.3.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:37
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:37

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:03:42
<=========================================================================
=================================> (2568 / 2568) 100.00% Time: 00:03:42

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:02
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:02

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:01
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:01

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] jack
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.10.141.112/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] wendy
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] danny
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 16:25:23 2021
[+] Requests Done: 3178
[+] Cached Requests: 5
[+] Data Sent: 894.085 KB
[+] Data Received: 1.156 MB
[+] Memory used: 209.91 MB
[+] Elapsed time: 00:04:29
```

## Appendix L – Mr Robot – Vane

```
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.172.31/
[+] Started: Mon May 17 18:38:20 2021

[+] robots.txt available under: 'http://10.10.172.31/robots.txt'
[+] Interesting header: SERVER: Apache
[+] Interesting header: X-FRAME-OPTIONS: SAMEORIGIN
[+] Interesting header: X-MOD-PAGESPEED: 1.9.32.3-4523
[+] XML-RPC Interface available under: http://10.10.172.31/xmlrpc.php

[+] WordPress version 4.3.1 identified from links opml
[!] 62 vulnerabilities identified from the version number

[!] Title: WordPress CVE-2018-6389 Denial of Service Vulnerability
    Reference: http://securityaffairs.co/wordpress/68709/hacking/cve-2018-
6389-wordpress-dos-flaw.html
    Reference:
https://github.com/Quitten/WordPress/commit/3463dcbd8d1f2426ba7f58a5293a38
5fcc4e7004
    Reference: https://wpvulndb.com/vulnerabilities/9021
    Reference: https://baraktawily.blogspot.in/2018/02/how-to-dos-29-of-
world-wide-websites.html
    Reference: https://github.com/WazeHell/CVE-2018-6389
    Reference: http://www.securitytracker.com/id/1040347
    Reference: https://baraktawily.blogspot.fr/2018/02/how-to-dos-29-of-
world-wide-websites.html
    Reference: https://thehackernews.com/2018/02/wordpress-dos-
exploit.html
    Reference: https://www.exploit-db.com/exploits/43968/
    Reference: https://github.com/UltimateHackers/Shiva
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-
6389
[i] CVSS: 5.0

[!] Title: WordPress 'ajax-actions.php' Cross Site Request Forgery
Vulnerability
    Reference: http://codex.wordpress.org/Version_4.5
    Reference:
https://github.com/WordPress/WordPress/commit/9b7a7754133c50b82bd9d976fb5b
24094f658aab
    Reference: https://wpvulndb.com/vulnerabilities/8475
    Reference: http://www.debian.org/security/2016/dsa-3681
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
6635
[i] CVSS: 6.8
[i] Fixed in: 4.5

[!] Title: WordPress CVE-2016-6634 Unspecified Cross Site Scripting
Vulnerability
    Reference: http://codex.wordpress.org/Version_4.5
    Reference:
https://core.trac.wordpress.org/query?status=closed&milestone=4.5
    Reference: https://wpvulndb.com/vulnerabilities/8474
    Reference: https://codex.wordpress.org/Version_4.5
    Reference: http://www.securityfocus.com/bid/92390
    Reference: http://www.debian.org/security/2016/dsa-3681
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
6634
[i] CVSS: 4.3
[i] Fixed in: 4.5

[!] Title: WordPress CVE-2016-4029 Security Bypass Vulnerability
    Reference: http://codex.wordpress.org/Version_4.5
    Reference:
https://core.trac.wordpress.org/query?status=closed&milestone=4.5
    Reference: https://codex.wordpress.org/Version_4.5
    Reference: https://wpvulndb.com/vulnerabilities/8473
    Reference: http://www.securitytracker.com/id/1036594
    Reference: http://www.debian.org/security/2016/dsa-3681
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
4029
[i] CVSS: 5.0
[i] Fixed in: 4.5

[!] Title: WordPress allows remote attackers to obtain sensitive revision-
history information by leveraging the ability to read a post, related to
wp-admin/includes/ajax-actions.php and wp-admin/revision.php
    Reference: http://www.securitytracker.com/id/1036163
    Reference: https://codex.wordpress.org/Version_4.5.3
    Reference:
https://github.com/WordPress/WordPress/commit/a2904cc3092c391ac7027bc87f78
06953d1a25a1
    Reference: https://wordpress.org/news/2016/06/wordpress-4-5-3/
    Reference: http://www.debian.org/security/2016/dsa-3639
    Reference: http://www.securityfocus.com/bid/91366
    Reference: https://wpvulndb.com/vulnerabilities/8519
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
5835
[i] CVSS: 5.0
[i] Fixed in: 4.5.3

[!] Title: WordPress allows remote attackers to bypass intended access
restrictions and remove a category attribute from a post via unspecified
vectors
    Reference: http://www.securitytracker.com/id/1036163
    Reference: https://codex.wordpress.org/Version_4.5.3
    Reference: https://wordpress.org/news/2016/06/wordpress-4-5-3/
    Reference: http://www.debian.org/security/2016/dsa-3639
    Reference: http://www.securityfocus.com/bid/91365
    Reference: https://wpvulndb.com/vulnerabilities/8520
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
5837
[i] CVSS: 5.0
[i] Fixed in: 4.5.3

[!] Title: WordPress allows remote attackers to bypass intended password-
change restrictions by leveraging knowledge of a cookie
    Reference: http://www.securitytracker.com/id/1036163
    Reference: https://codex.wordpress.org/Version_4.5.3
    Reference: https://wordpress.org/news/2016/06/wordpress-4-5-3/
    Reference: http://www.debian.org/security/2016/dsa-3639
    Reference: http://www.securityfocus.com/bid/91367
    Reference: https://wpvulndb.com/vulnerabilities/8524
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
5838
[i] CVSS: 5.0
[i] Fixed in: 4.5.3

[!] Title: WordPress allows remote attackers to bypass the
sanitize_file_name protection mechanism via unspecified vectors
    Reference: http://www.securitytracker.com/id/1036163
    Reference: https://codex.wordpress.org/Version_4.5.3
    Reference: https://wordpress.org/news/2016/06/wordpress-4-5-3/
    Reference: http://www.debian.org/security/2016/dsa-3639
    Reference: http://www.securityfocus.com/bid/91364
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
5839
[i] CVSS: 5.0
[i] Fixed in: 4.5.3

[!] Title: The oEmbed protocol implementation in WordPress allows remote
attackers to cause a denial of service via unspecified vectors
```

```
    Reference: http://www.securitytracker.com/id/1036163
    Reference: https://codex.wordpress.org/Version_4.5.3
    Reference: https://wordpress.org/news/2016/06/wordpress-4-5-3/
    Reference: http://www.securityfocus.com/bid/91363
    Reference: https://wpvulndb.com/vulnerabilities/8523
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
5836
[i] CVSS: 5.0
[i] Fixed in: 4.5.3

[!] Title: Cross-site scripting (XSS) vulnerability in the
wp_get_attachment_link function in wp-includes/post-template.php in
WordPress allows remote attackers to inject arbitrary web script or HTML
via a crafted attachment name
    Reference: http://www.securitytracker.com/id/1036163
    Reference: https://codex.wordpress.org/Version_4.5.3
    Reference:
https://github.com/WordPress/WordPress/commit/4372cdf45d0f49c74bbd4d60db72
81de83e32648
    Reference: https://wordpress.org/news/2016/06/wordpress-4-5-3/
    Reference: http://www.debian.org/security/2016/dsa-3639
    Reference: http://www.securityfocus.com/bid/91368
    Reference: https://wpvulndb.com/vulnerabilities/8518
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
5834
[i] CVSS: 4.3
[i] Fixed in: 4.5.3

[!] Title: Cross-site scripting (XSS) vulnerability in the column_title
function in wp-admin/includes/class-wp-media-list-table.php in WordPress
allows remote attackers to inject arbitrary web script or HTML via a
crafted attachment name
    Reference: http://www.securitytracker.com/id/1036163
    Reference: https://codex.wordpress.org/Version_4.5.3
    Reference:
https://github.com/WordPress/WordPress/commit/4372cdf45d0f49c74bbd4d60db72
81de83e32648
    Reference: https://wordpress.org/news/2016/06/wordpress-4-5-3/
    Reference: http://www.securityfocus.com/bid/91368
    Reference: https://wpvulndb.com/vulnerabilities/8518
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
5833
[i] CVSS: 4.3
[i] Fixed in: 4.5.3

[!] Title: The customizer in WordPress allows remote attackers to bypass
intended redirection restrictions via unspecified vectors
    Reference: http://www.securitytracker.com/id/1036163
    Reference: https://codex.wordpress.org/Version_4.5.3
    Reference: https://wordpress.org/news/2016/06/wordpress-4-5-3/
    Reference: http://www.debian.org/security/2016/dsa-3639
    Reference: http://www.securityfocus.com/bid/91362
    Reference: https://wpvulndb.com/vulnerabilities/8522
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
5832
[i] CVSS: 5.0
[i] Fixed in: 4.5.3

[!] Title: Cross-site scripting (XSS) vulnerability in
flash/FlashMediaElement.as in MediaElement.js as used in WordPress allows
remote attackers to inject arbitrary web script or HTML via an obfuscated
form of the jsinitfunction parameter, as demonstrated by
"jsinitfunctio%gn."
    Reference: http://www.openwall.com/lists/oss-security/2016/05/07/2
    Reference: https://codex.wordpress.org/Version_4.5.2
    Reference: https://core.trac.wordpress.org/changeset/37371
    Reference:
https://gist.github.com/cure53/df34ea68c26441f3ae98f821ba1feb9c
    Reference:
https://github.com/johndyer/mediaelement/blob/master/changelog.md
    Reference:
https://github.com/johndyer/mediaelement/commit/34834eef8ac830b9145df169ec
22016a4350f06e
    Reference: https://wordpress.org/news/2016/05/wordpress-4-5-2/
    Reference: https://wpvulndb.com/vulnerabilities/8488
    Reference: http://www.securitytracker.com/id/1035818
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
4567
[i] CVSS: 4.3
[i] Fixed in: 4.5.2

[!] Title: Cross-site scripting (XSS) vulnerability in plupload.flash.swf
in Plupload as used in WordPress allows remote attackers to inject
arbitrary web script or HTML via a Same-Origin Method Execution (SOME)
attack
    Reference: http://www.openwall.com/lists/oss-security/2016/05/07/2
    Reference: http://www.plupload.com/punbb/viewtopic.php?pid=28690
    Reference: https://codex.wordpress.org/Version_4.5.2
    Reference: https://core.trac.wordpress.org/changeset/37382/
    Reference:
https://gist.github.com/cure53/09a81530a44f6b8173f545accc9ed07e
    Reference: https://wordpress.org/news/2016/05/wordpress-4-5-2/
    Reference: https://wpvulndb.com/vulnerabilities/8489
    Reference: http://www.securitytracker.com/id/1035818
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
4566
[i] CVSS: 4.3
[i] Fixed in: 4.5.2

[!] Title: The wp_http_validate_url function in wp-includes/http.php in
WordPress allows remote attackers to conduct server-side request forgery
(SSRF) attacks via a zero value in the first octet of an IPv4 address in
the u parameter to wp-admin/press-this.php
    Reference: https://wordpress.org/news/2016/02/wordpress-4-4-2-
security-and-maintenance-release/
    Reference: https://codex.wordpress.org/Version_4.4.2
    Reference: https://wpvulndb.com/vulnerabilities/8376
    Reference: https://hackerone.com/reports/110801
    Reference: https://core.trac.wordpress.org/changeset/36435
    Reference: http://www.securityfocus.com/bid/82454
    Reference: http://www.securitytracker.com/id/1034933
    Reference: http://www.debian.org/security/2016/dsa-3472
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
2222
[i] CVSS: 5.0
[i] Fixed in: 4.4.2

[!] Title: Open redirect vulnerability in the wp_validate_redirect
function in wp-includes/pluggable.php in WordPress allows remote attackers
to redirect users to arbitrary web sites and conduct phishing attacks via
a malformed URL that triggers incorrect hostname parsing, as demonstrated
by an https:example.com URL
    Reference: https://wordpress.org/news/2016/02/wordpress-4-4-2-
security-and-maintenance-release/
    Reference: https://core.trac.wordpress.org/changeset/36444
    Reference: https://codex.wordpress.org/Version_4.4.2
    Reference: https://wpvulndb.com/vulnerabilities/8377
    Reference: http://www.securityfocus.com/bid/82463
    Reference: http://www.securitytracker.com/id/1034933
    Reference: http://www.debian.org/security/2016/dsa-3472
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
2221
[i] CVSS: 5.8
[i] Fixed in: 4.4.2

[!] Title: Multiple cross-site scripting (XSS) vulnerabilities in wp-
includes/class-wp-theme.php in WordPress allow remote attackers to inject
arbitrary web script or HTML via a (1) stylesheet name or (2) template
name to wp-admin/customize.php
    Reference: https://wordpress.org/news/2016/01/wordpress-4-4-1-
security-and-maintenance-release/
    Reference: https://codex.wordpress.org/Version_4.4.1
    Reference: https://wpvulndb.com/vulnerabilities/8358
    Reference: https://core.trac.wordpress.org/changeset/36185
    Reference: http://www.openwall.com/lists/oss-security/2016/01/08/4
    Reference: http://twitter.com/brutelogic/statuses/685105483397619713
    Reference: http://www.securitytracker.com/id/1034622
    Reference: http://www.debian.org/security/2016/dsa-3444
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
1564
[i] CVSS: 4.3
[i] Fixed in: 4.4.1

[!] Title: WordPress 'wp_ajax_update_plugin()' Function Information
Disclosure Vulnerability
    Reference: http://www.openwall.com/lists/oss-security/2016/08/20/1
    Reference: https://core.trac.wordpress.org/changeset/38168
    Reference: https://core.trac.wordpress.org/ticket/37490
    Reference:
https://sumofpwn.nl/advisory/2016/path_traversal_vulnerability_in_wordpres
s_core_ajax_handlers.html
```

```
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
10148
[i] CVSS: 4.0
[i] Fixed in: 4.6

[!] Title: WordPress Cryptographic Security Bypass Vulnerability
    Reference: http://www.openwall.com/lists/oss-security/2017/01/14/6
    Reference: https://codex.wordpress.org/Version_4.7.1
    Reference:
https://github.com/WordPress/WordPress/commit/cea9e2dc62abf777e06b12ec4ad9
d1aaa49b29f4
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-
security-and-maintenance-release/
    Reference: http://www.securitytracker.com/id/1037591
    Reference: https://wpvulndb.com/vulnerabilities/8721
    Reference: http://www.debian.org/security/2017/dsa-3779
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
5493
[i] CVSS: 5.0
[i] Fixed in: 4.7.1

[!] Title: WordPress Prior to 4.7.1 Cross Site Request Forgery
Vulnerability
    Reference: http://www.openwall.com/lists/oss-security/2017/01/14/6
    Reference: https://codex.wordpress.org/Version_4.7.1
    Reference:
https://github.com/WordPress/WordPress/commit/03e5c0314aeffe6b27f4b98fef84
2bf0fb00c733
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-
security-and-maintenance-release/
    Reference: http://www.securitytracker.com/id/1037591
    Reference: https://wpvulndb.com/vulnerabilities/8720
    Reference: http://www.debian.org/security/2017/dsa-3779
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
5492
[i] CVSS: 6.8
[i] Fixed in: 4.7.1

[!] Title: WordPress Prior to 4.7.1 Security Bypass Vulnerability
    Reference: http://www.openwall.com/lists/oss-security/2017/01/14/6
    Reference: https://codex.wordpress.org/Version_4.7.1
    Reference:
https://github.com/WordPress/WordPress/commit/061e8788814ac87706d8b95688df
276fe3c8596a
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-
security-and-maintenance-release/
    Reference: http://www.securitytracker.com/id/1037591
    Reference: https://wpvulndb.com/vulnerabilities/8719
    Reference: http://www.debian.org/security/2017/dsa-3779
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
5491
[i] CVSS: 5.0
[i] Fixed in: 4.7.1
```

```
[!] Title: WordPress Prior to 4.7.1 Cross Site Scripting Vulnerability
    Reference: http://www.openwall.com/lists/oss-security/2017/01/14/6
    Reference: https://codex.wordpress.org/Version_4.7.1
    Reference:
https://github.com/WordPress/WordPress/commit/ce7fb2934dd111e6353784852de8
aea2a938b359
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-
security-and-maintenance-release/
    Reference: https://www.mehmetince.net/low-severity-wordpress/
    Reference:
https://github.com/WordPress/WordPress/blob/c9ea1de1441bb3bda133bf72d513ca
9de66566c2/wp-admin/update-core.php
    Reference: http://www.securitytracker.com/id/1037591
    Reference: https://wpvulndb.com/vulnerabilities/8718
    Reference: http://www.debian.org/security/2017/dsa-3779
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
5490
[i] CVSS: 4.3
[i] Fixed in: 4.7.1

[!] Title: WordPress Prior to 4.7.1 Cross Site Request Forgery
Vulnerability
    Reference: http://www.openwall.com/lists/oss-security/2017/01/14/6
    Reference: https://codex.wordpress.org/Version_4.7.1
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-
security-and-maintenance-release/
    Reference: http://www.securitytracker.com/id/1037591
    Reference: https://wpvulndb.com/vulnerabilities/8717
    Reference: http://www.debian.org/security/2017/dsa-3779
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
5489
[i] CVSS: 6.8
[i] Fixed in: 4.7.1

[!] Title: WordPress Prior to 4.7.1 Cross Site Scripting Vulnerability
    Reference: http://www.openwall.com/lists/oss-security/2017/01/14/6
    Reference: https://codex.wordpress.org/Version_4.7.1
    Reference:
https://github.com/WordPress/WordPress/commit/c9ea1de1441bb3bda133bf72d513
ca9de66566c2
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-
security-and-maintenance-release/
    Reference:
https://github.com/WordPress/WordPress/blob/c9ea1de1441bb3bda133bf72d513ca
9de66566c2/wp-admin/update-core.php
    Reference: http://www.securitytracker.com/id/1037591
    Reference: https://wpvulndb.com/vulnerabilities/8716
    Reference: http://www.debian.org/security/2017/dsa-3779
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
5488
[i] CVSS: 4.3
[i] Fixed in: 4.7.1

[!] Title: WordPress Prior to 4.7.1 Information Disclosure Vulnerability
```

```
    Reference: http://www.openwall.com/lists/oss-security/2017/01/14/6
    Reference: https://codex.wordpress.org/Version_4.7.1
    Reference:
https://github.com/WordPress/WordPress/commit/daf358983cc1ce0c77bf6d2de2eb
bb43df2add60
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-
security-and-maintenance-release/
    Reference: https://www.wordfence.com/blog/2016/12/wordfence-blocks-
username-harvesting-via-new-rest-api-wp-4-7/
    Reference: http://www.securitytracker.com/id/1037591
    Reference: https://wpvulndb.com/vulnerabilities/8715
    Reference: https://www.exploit-db.com/exploits/41497/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
5487
[i] CVSS: 5.0
[i] Fixed in: 4.7.1

[!] Title: WordPress Prior to 4.7.3 Cross Site Request Forgery
Vulnerability
    Reference: http://openwall.com/lists/oss-security/2017/03/06/7
    Reference: https://codex.wordpress.org/Version_4.7.3
    Reference:
https://github.com/WordPress/WordPress/commit/263831a72d08556bc2f3a328673d
95301a152829
    Reference:
https://sumofpwn.nl/advisory/2016/cross_site_request_forgery_in_wordpress_
press_this_function_allows_dos.html
    Reference: https://wordpress.org/news/2017/03/wordpress-4-7-3-
security-and-maintenance-release/
    Reference: http://www.securitytracker.com/id/1037959
    Reference: https://wpvulndb.com/vulnerabilities/8770
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
6819
[i] CVSS: 4.3
[i] Fixed in: 4.7.3

[!] Title: WordPress Prior to 4.7.3 Multiple Cross Site Scripting
Vulnerabilities
    Reference: https://codex.wordpress.org/Version_4.7.3
    Reference:
https://github.com/WordPress/WordPress/commit/9092fd01e1f452f37c313d38b18f
9fe6907541f9
    Reference: https://wordpress.org/news/2017/03/wordpress-4-7-3-
security-and-maintenance-release/
    Reference:
https://github.com/WordPress/WordPress/commit/419c8d97ce8df7d5004ee0b566bc
5e095f0a6ca8
    Reference:
https://github.com/WordPress/WordPress/commit/28f838ca3ee205b6f39cd2bf23eb
4e5f52796bd7
    Reference: http://openwall.com/lists/oss-security/2017/03/06/8
    Reference:
https://sumofpwn.nl/advisory/2016/wordpress_audio_playlist_functionality_i
s_affected_by_cross_site_scripting.html
```

```
    Reference: http://www.securitytracker.com/id/1037959
    Reference: https://wpvulndb.com/vulnerabilities/8769
    Reference: https://wpvulndb.com/vulnerabilities/8768
    Reference: https://wpvulndb.com/vulnerabilities/8765
    Reference: http://www.debian.org/security/2017/dsa-3815
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
6818
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
6814
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
6817
[i] CVSS: 3.5
[i] Fixed in: 4.7.3

[!] Title: In WordPress (wp-includes/embed.php), there is authenticated
Cross-Site Scripting (XSS) in YouTube URL Embeds
    Reference: https://codex.wordpress.org/Version_4.7.3
    Reference:
https://github.com/WordPress/WordPress/commit/419c8d97ce8df7d5004ee0b566bc
5e095f0a6ca8
    Reference: https://wordpress.org/news/2017/03/wordpress-4-7-3-
security-and-maintenance-release/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
6817
[i] CVSS: 3.5
[i] Fixed in: 4.7.3

[!] Title: WordPress Prior to 4.7.3 Security Bypass Vulnerability
    Reference: https://codex.wordpress.org/Version_4.7.3
    Reference:
https://github.com/WordPress/WordPress/commit/4d80f8b3e1b00a3edcee0774dc9c
2f4c78f9e663
    Reference: https://wordpress.org/news/2017/03/wordpress-4-7-3-
security-and-maintenance-release/
    Reference: http://www.securitytracker.com/id/1037959
    Reference: https://wpvulndb.com/vulnerabilities/8767
    Reference: http://www.debian.org/security/2017/dsa-3815
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
6816
[i] CVSS: 4.0
[i] Fixed in: 4.7.3

[!] Title: WordPress Prior to 4.7.3 URL Redirection Vulnerability
    Reference: https://codex.wordpress.org/Version_4.7.3
    Reference:
https://github.com/WordPress/WordPress/commit/288cd469396cfe7055972b457eb5
89cea51ce40e
    Reference: https://wordpress.org/news/2017/03/wordpress-4-7-3-
security-and-maintenance-release/
    Reference: http://www.securitytracker.com/id/1037959
    Reference: https://wpvulndb.com/vulnerabilities/8766
    Reference: http://www.debian.org/security/2017/dsa-3815
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
6815
```

```
[i] CVSS: 5.8
[i] Fixed in: 4.7.3

[!] Title: In WordPress there is authenticated Cross-Site Scripting (XSS)
via Media File Metadata
    Reference: http://openwall.com/lists/oss-security/2017/03/06/8
    Reference: https://codex.wordpress.org/Version_4.7.3
    Reference:
https://github.com/WordPress/WordPress/commit/28f838ca3ee205b6f39cd2bf23eb
4e5f52796bd7
    Reference:
https://sumofpwn.nl/advisory/2016/wordpress_audio_playlist_functionality_i
s_affected_by_cross_site_scripting.html
    Reference: https://wordpress.org/news/2017/03/wordpress-4-7-3-
security-and-maintenance-release/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
6814
[i] CVSS: 3.5
[i] Fixed in: 4.7.3

[!] Title: WordPress Prior to 4.7.5 Multiple Security Vulnerabilities
    Reference: https://codex.wordpress.org/Version_4.7.5
    Reference:
https://github.com/WordPress/WordPress/commit/e88a48a066ab2200ce3091b131d4
3e2fab2460a4
    Reference: https://wordpress.org/news/2017/05/wordpress-4-7-5/
    Reference:
https://github.com/WordPress/WordPress/commit/38347d7c580be4cdd8476e4bbc65
3d5c79ed9b67
    Reference:
https://github.com/WordPress/WordPress/commit/3d95e3ae816f4d7c638f40d3e936
a4be19724381
    Reference:
https://github.com/WordPress/WordPress/commit/3d10fef22d788f29aed745b0f5ff
6f6baea69af3
    Reference:
https://github.com/WordPress/WordPress/commit/76d77e927bb4d0f87c7262a50e28
d84e01fd2b11
    Reference:
https://github.com/WordPress/WordPress/commit/8c7ea71edbbffca5d9766b7bea7c
7f3722ffafa6
    Reference: http://www.securitytracker.com/id/1038520
    Reference: https://twitter.com/skansing/status/865362551097393153
    Reference: https://wpvulndb.com/vulnerabilities/8815
    Reference: https://wpvulndb.com/vulnerabilities/8817
    Reference: https://wpvulndb.com/vulnerabilities/8818
    Reference: https://wpvulndb.com/vulnerabilities/8820
    Reference: https://wpvulndb.com/vulnerabilities/8816
    Reference: https://wpvulndb.com/vulnerabilities/8819
    Reference: http://www.debian.org/security/2017/dsa-3870
    Reference: https://www.debian.org/security/2018/dsa-4090
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9065
```

```
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9062
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9063
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9064
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9061
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9066
[i] CVSS: 5.0
[i] Fixed in: 4.7.5

[!] Title: WordPress Prior to 4.7.5 Multiple Security Vulnerabilities
    Reference: https://codex.wordpress.org/Version_4.7.5
    Reference:
https://github.com/WordPress/WordPress/commit/38347d7c580be4cdd8476e4bbc65
3d5c79ed9b67
    Reference: https://wordpress.org/news/2017/05/wordpress-4-7-5/
    Reference:
https://github.com/WordPress/WordPress/commit/3d95e3ae816f4d7c638f40d3e936
a4be19724381
    Reference:
https://github.com/WordPress/WordPress/commit/3d10fef22d788f29aed745b0f5ff
6f6baea69af3
    Reference:
https://github.com/WordPress/WordPress/commit/76d77e927bb4d0f87c7262a50e28
d84e01fd2b11
    Reference:
https://github.com/WordPress/WordPress/commit/e88a48a066ab2200ce3091b131d4
3e2fab2460a4
    Reference:
https://github.com/WordPress/WordPress/commit/8c7ea71edbbffca5d9766b7bea7c
7f3722ffafa6
    Reference: https://twitter.com/skansing/status/865362551097393153
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9064
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9066
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9065
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9063
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9061
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9062
[i] CVSS: 5.0
[i] Fixed in: 4.7.5

[!] Title: In WordPress a cross-site scripting (XSS) vulnerability related
to the Customizer exists, involving an invalid customization session
    Reference: https://codex.wordpress.org/Version_4.7.5
    Reference:
https://github.com/WordPress/WordPress/commit/3d10fef22d788f29aed745b0f5ff
6f6baea69af3
    Reference: https://wordpress.org/news/2017/05/wordpress-4-7-5/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9063
[i] CVSS: 4.3
[i] Fixed in: 4.7.5

[!] Title: In WordPress there is improper handling of post meta data
values in the XML-RPC API
    Reference: https://codex.wordpress.org/Version_4.7.5
    Reference:
https://github.com/WordPress/WordPress/commit/3d95e3ae816f4d7c638f40d3e936
a4be19724381
    Reference: https://wordpress.org/news/2017/05/wordpress-4-7-5/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9062
[i] CVSS: 5.0
[i] Fixed in: 4.7.5

[!] Title: In WordPress a cross-site scripting (XSS) vulnerability exists
when attempting to upload very large files, because the error message does
not properly restrict presentation of the filename
    Reference: https://codex.wordpress.org/Version_4.7.5
    Reference:
https://github.com/WordPress/WordPress/commit/8c7ea71edbbffca5d9766b7bea7c
7f3722ffafa6
    Reference: https://wordpress.org/news/2017/05/wordpress-4-7-5/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9061
[i] CVSS: 4.3
[i] Fixed in: 4.7.5

[!] Title: WordPress Password Reset CVE-2017-8295 Security Bypass
Vulnerability
    Reference: https://exploitbox.io/vuln/WordPress-Exploit-4-7-Unauth-
Password-Reset-0day-CVE-2017-8295.html
    Reference: https://www.exploit-db.com/exploits/41963/
    Reference: http://www.securitytracker.com/id/1038403
    Reference: https://wpvulndb.com/vulnerabilities/8807
    Reference: http://www.debian.org/security/2017/dsa-3870
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
8295
[i] CVSS: 4.3
[i] Fixed in: 4.7.5

[!] Title: Before version 4.8.2, WordPress was vulnerable to a cross-site
scripting attack via shortcodes in the TinyMCE visual editor
    Reference: https://core.trac.wordpress.org/changeset/41395
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-
security-and-maintenance-release/
    Reference: https://wpvulndb.com/vulnerabilities/8914
    Reference: http://www.securitytracker.com/id/1039553
    Reference: https://www.debian.org/security/2017/dsa-3997
    Reference: https://core.trac.wordpress.org/changeset/41393
    Reference: https://core.trac.wordpress.org/changeset/41397
    Reference: https://core.trac.wordpress.org/changeset/41398
    Reference: https://core.trac.wordpress.org/changeset/41412
    Reference: https://core.trac.wordpress.org/changeset/41448
    Reference: https://core.trac.wordpress.org/changeset/41457
    Reference: https://core.trac.wordpress.org/changeset/41470
    Reference: https://core.trac.wordpress.org/changeset/41496
    Reference:
https://github.com/WordPress/WordPress/commit/70b21279098fc973eae803693c07
05a548128e48
    Reference:
https://github.com/WordPress/WordPress/commit/fc930d3daed1c3acef010d04acc2
c5de93cd18ec
    Reference: https://medium.com/websec/wordpress-sqli-bbb2afcc8e94
    Reference: https://medium.com/websec/wordpress-sqli-poc-f1827c20bf8e
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14726
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14723
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14718
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14720
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14721
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14725
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14719
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14722
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14724
[i] CVSS: 4.3
[i] Fixed in: 4.8.2

[!] Title: Before version 4.8.2, WordPress was susceptible to an open
redirect attack in wp-admin/edit-tag-form.php and wp-admin/user-edit.php
    Reference: https://core.trac.wordpress.org/changeset/41398
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-
security-and-maintenance-release/
    Reference: https://wpvulndb.com/vulnerabilities/8910
    Reference: http://www.securitytracker.com/id/1039553
    Reference: https://core.trac.wordpress.org/changeset/41393
    Reference: https://core.trac.wordpress.org/changeset/41395
    Reference: https://core.trac.wordpress.org/changeset/41397
    Reference: https://core.trac.wordpress.org/changeset/41412
    Reference: https://core.trac.wordpress.org/changeset/41448
    Reference: https://core.trac.wordpress.org/changeset/41457
    Reference: https://core.trac.wordpress.org/changeset/41470
    Reference: https://core.trac.wordpress.org/changeset/41496
    Reference:
https://github.com/WordPress/WordPress/commit/70b21279098fc973eae803693c07
05a548128e48
    Reference:
https://github.com/WordPress/WordPress/commit/fc930d3daed1c3acef010d04acc2
c5de93cd18ec
    Reference: https://medium.com/websec/wordpress-sqli-bbb2afcc8e94
    Reference: https://medium.com/websec/wordpress-sqli-poc-f1827c20bf8e
    Reference: https://wpvulndb.com/vulnerabilities/8913
    Reference: https://wpvulndb.com/vulnerabilities/8912
    Reference: https://wpvulndb.com/vulnerabilities/8911
    Reference: https://www.debian.org/security/2017/dsa-3997
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14725
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14719
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14724
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14721
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14723
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14722
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14726
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14718
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14720
[i] CVSS: 4.9
[i] Fixed in: 4.8.2

[!] Title: Before version 4.8.2, WordPress was vulnerable to cross-site
scripting in oEmbed discovery
    Reference: https://core.trac.wordpress.org/changeset/41448
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-
security-and-maintenance-release/
    Reference: https://wpvulndb.com/vulnerabilities/8913
    Reference: http://www.securitytracker.com/id/1039553
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14724
[i] CVSS: 4.3
[i] Fixed in: 4.8.2

[!] Title: Before version 4.8.2, WordPress mishandled % characters and
additional placeholder values in $wpdb->prepare, and thus did not properly
address the possibility of plugins and themes enabling SQL injection
attacks
    Reference: https://core.trac.wordpress.org/changeset/41470
    Reference: https://core.trac.wordpress.org/changeset/41496
    Reference:
https://github.com/WordPress/WordPress/commit/70b21279098fc973eae803693c07
05a548128e48
```

```
    Reference:
https://github.com/WordPress/WordPress/commit/fc930d3daed1c3acef010d04acc2
c5de93cd18ec
    Reference: https://medium.com/websec/wordpress-sqli-bbb2afcc8e94
    Reference: https://medium.com/websec/wordpress-sqli-poc-f1827c20bf8e
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-
security-and-maintenance-release/
    Reference: https://core.trac.wordpress.org/changeset/41393
    Reference: https://core.trac.wordpress.org/changeset/41395
    Reference: https://core.trac.wordpress.org/changeset/41397
    Reference: https://core.trac.wordpress.org/changeset/41398
    Reference: https://core.trac.wordpress.org/changeset/41412
    Reference: https://core.trac.wordpress.org/changeset/41448
    Reference: https://core.trac.wordpress.org/changeset/41457
    Reference: http://www.securitytracker.com/id/1039553
    Reference: https://wpvulndb.com/vulnerabilities/8912
    Reference: https://wpvulndb.com/vulnerabilities/8911
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14723
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14721
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14726
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14718
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14725
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14720
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14724
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14719
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14722
[i] CVSS: 7.5
[i] Fixed in: 4.8.2

[!] Title: Before version 4.8.2, WordPress allowed a Directory Traversal
attack in the Customizer component via a crafted theme filename
    Reference: https://core.trac.wordpress.org/changeset/41397
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-
security-and-maintenance-release/
    Reference: https://wpvulndb.com/vulnerabilities/8912
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14722
[i] CVSS: 5.0
[i] Fixed in: 4.8.2

[!] Title: Before version 4.8.2, WordPress allowed Cross-Site scripting in
the plugin editor via a crafted plugin name
    Reference: https://core.trac.wordpress.org/changeset/41412
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-
security-and-maintenance-release/
```

```
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14721
[i] CVSS: 4.3
[i] Fixed in: 4.8.2

[!] Title: Before version 4.8.2, WordPress allowed a Cross-Site scripting
attack in the template list view via a crafted template name
    Reference: https://core.trac.wordpress.org/changeset/41412
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-
security-and-maintenance-release/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14720
[i] CVSS: 4.3
[i] Fixed in: 4.8.2

[!] Title: Before version 4.8.2, WordPress was vulnerable to a directory
traversal attack during unzip operations in the ZipArchive and PclZip
components
    Reference: https://core.trac.wordpress.org/changeset/41457
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-
security-and-maintenance-release/
    Reference: https://wpvulndb.com/vulnerabilities/8911
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14719
[i] CVSS: 5.0
[i] Fixed in: 4.8.2

[!] Title: Before version 4.8.2, WordPress was susceptible to a Cross-Site
Scripting attack in the link modal via a javascript: or data: URL
    Reference: https://core.trac.wordpress.org/changeset/41393
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-
security-and-maintenance-release/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14718
[i] CVSS: 4.3
[i] Fixed in: 4.8.2

[!] Title: WordPress stores cleartext wp_signups.activation_key values
(but stores the analogous wp_users.user_activation_key values as hashes),
which might make it easier for remote attackers to hijack unactivated user
accounts by leveraging database read access (such as access gained through
an unspecified SQL injection vulnerability)
    Reference: http://www.securitytracker.com/id/1039554
    Reference: https://core.trac.wordpress.org/ticket/38474
    Reference: https://www.debian.org/security/2017/dsa-3997
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14990
[i] CVSS: 4.0
[i] Fixed in: 4.8.3

[!] Title: WordPress through , when domain-based flashmediaelement.swf
sandboxing is not used, allows remote attackers to conduct cross-domain
Flash injection (XSF) attacks by leveraging code contained within the wp-
includes/js/mediaelement/flashmediaelement.swf file
```

```
    Reference: https://opnsec.com/2017/10/cve-2016-9263-unpatched-xsf-
vulnerability-in-wordpress/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
9263
[i] CVSS: 2.6
[i] Fixed in: 4.8.3

[!] Title: WordPress through uses a weak MD5-based password hashing
algorithm, which makes it easier for attackers to determine cleartext
values by leveraging access to the hash values
    Reference: https://core.trac.wordpress.org/ticket/21022
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-
6707
[i] CVSS: 5.0
[i] Fixed in: 4.8.3

[!] Title: wp-includes/feed.php in WordPress does not properly restrict
enclosures in RSS and Atom fields, which might allow attackers to conduct
XSS attacks via a crafted URL
    Reference: https://codex.wordpress.org/Version_4.9.1
    Reference:
https://github.com/WordPress/WordPress/commit/f1de7e42df29395c3314bf85bff3
d1f4f90541de
    Reference: https://wordpress.org/news/2017/11/wordpress-4-9-1-
security-and-maintenance-release/
    Reference: https://wpvulndb.com/vulnerabilities/8967
    Reference: https://www.debian.org/security/2018/dsa-4090
    Reference: https://lists.debian.org/debian-lts-
announce/2017/12/msg00019.html
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
17094
[i] CVSS: 3.5
[i] Fixed in: 4.9.1

[!] Title: wp-includes/general-template.php in WordPress does not properly
restrict the lang attribute of an HTML element, which might allow
attackers to conduct XSS attacks via the language setting of a site
    Reference: https://codex.wordpress.org/Version_4.9.1
    Reference:
https://github.com/WordPress/WordPress/commit/3713ac5ebc90fb2011e98dfd6914
20f43da6c09a
    Reference: https://wordpress.org/news/2017/11/wordpress-4-9-1-
security-and-maintenance-release/
    Reference: https://wpvulndb.com/vulnerabilities/8968
    Reference: https://www.debian.org/security/2018/dsa-4090
    Reference: https://lists.debian.org/debian-lts-
announce/2017/12/msg00019.html
    Reference:
https://github.com/WordPress/WordPress/commit/f1de7e42df29395c3314bf85bff3
d1f4f90541de
    Reference:
https://github.com/WordPress/WordPress/commit/67d03a98c2cae5f41843c897f206
adde299b0509
```

```
    Reference:
https://github.com/WordPress/WordPress/commit/eaf1cfdc1fe0bdffabd8d879c591
b864d833326c
    Reference: https://make.wordpress.org/core/2017/11/28/wordpress-4-9-1-
scheduled-for-november-29th/
    Reference: https://wpvulndb.com/vulnerabilities/8966
    Reference: https://wpvulndb.com/vulnerabilities/8969
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
17093
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
17092
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
17094
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
17091
[i] CVSS: 3.5
[i] Fixed in: 4.9.1

[!] Title: wp-includes/functions.php in WordPress does not require the
unfiltered_html capability for upload of .js files, which might allow
remote attackers to conduct XSS attacks via a crafted file
    Reference: https://codex.wordpress.org/Version_4.9.1
    Reference:
https://github.com/WordPress/WordPress/commit/67d03a98c2cae5f41843c897f206
adde299b0509
    Reference: https://wordpress.org/news/2017/11/wordpress-4-9-1-
security-and-maintenance-release/
    Reference: https://wpvulndb.com/vulnerabilities/8966
    Reference: https://www.debian.org/security/2018/dsa-4090
    Reference:
https://github.com/WordPress/WordPress/commit/3713ac5ebc90fb2011e98dfd6914
20f43da6c09a
    Reference:
https://github.com/WordPress/WordPress/commit/f1de7e42df29395c3314bf85bff3
d1f4f90541de
    Reference:
https://github.com/WordPress/WordPress/commit/eaf1cfdc1fe0bdffabd8d879c591
b864d833326c
    Reference: https://make.wordpress.org/core/2017/11/28/wordpress-4-9-1-
scheduled-for-november-29th/
    Reference: https://lists.debian.org/debian-lts-
announce/2017/12/msg00019.html
    Reference: https://wpvulndb.com/vulnerabilities/8969
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
17092
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
17093
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
17091
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
17094
[i] CVSS: 3.5
[i] Fixed in: 4.9.1
```

```
[!] Title: wp-admin/user-new.php in WordPress sets the newbloguser key to
a string that can be directly derived from the user ID, which allows
remote attackers to bypass intended access restrictions by entering this
string
    Reference: https://codex.wordpress.org/Version_4.9.1
    Reference:
https://github.com/WordPress/WordPress/commit/eaf1cfdc1fe0bdffabd8d879c591
b864d833326c
    Reference: https://wordpress.org/news/2017/11/wordpress-4-9-1-
security-and-maintenance-release/
    Reference: https://wpvulndb.com/vulnerabilities/8969
    Reference: https://www.debian.org/security/2018/dsa-4090
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
17091
[i] CVSS: 6.5
[i] Fixed in: 4.9.1

[!] Title: WordPress has XSS in the Flash fallback files in MediaElement
(under wp-includes/js/mediaelement)
    Reference: https://codex.wordpress.org/Version_4.9.2
    Reference:
https://github.com/WordPress/WordPress/commit/3fe9cb61ee71fcfadb5e00239929
6fcc1198d850
    Reference: https://wordpress.org/news/2018/01/wordpress-4-9-2-
security-and-maintenance-release/
    Reference: https://wpvulndb.com/vulnerabilities/9006
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-
5776
[i] CVSS: 4.3
[i] Fixed in: 4.9.2

[!] Title: WordPress Cross Site Scripting And Directory Traversal
Vulnerabilities
    Reference:
https://github.com/WordPress/WordPress/commit/c9e60dab176635d4bfaaf431c0ea
891e4726d6e0
    Reference:
https://github.com/WordPress/WordPress/commit/54720a14d85bc1197ded7cb09bd3
ea790caa0b6e
    Reference: https://wordpress.org/news/2016/09/wordpress-4-6-1-
security-and-maintenance-release/
    Reference: https://codex.wordpress.org/Version_4.6.1
    Reference: http://www.openwall.com/lists/oss-security/2016/09/08/19
    Reference: http://www.openwall.com/lists/oss-security/2016/09/08/24
    Reference:
https://sumofpwn.nl/advisory/2016/persistent_cross_site_scripting_vulnerab
ility_in_wordpress_due_to_unsafe_processing_of_file_names.html
    Reference: https://wpvulndb.com/vulnerabilities/8615
    Reference: https://wpvulndb.com/vulnerabilities/8616
    Reference: http://www.debian.org/security/2016/dsa-3681
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
7168
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
7169
```

```
[i] CVSS: 3.5
[i] Fixed in: 4.6.1

[!] Title: WordPress CVE-2016-6897 Cross Site Request Forgery
Vulnerability
    Reference: https://core.trac.wordpress.org/ticket/37490
    Reference:
https://sumofpwn.nl/advisory/2016/path_traversal_vulnerability_in_wordpres
s_core_ajax_handlers.html
    Reference: http://www.openwall.com/lists/oss-security/2016/08/20/1
    Reference:
https://github.com/WordPress/WordPress/commit/8c82515ab62b88fb32d01c9778f0
204b296f3568
    Reference: https://wpvulndb.com/vulnerabilities/8606
    Reference: http://www.securitytracker.com/id/1036683
    Reference: https://www.exploit-db.com/exploits/40288/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
6897
[i] CVSS: 4.3
[i] Fixed in: 4.6

[!] Title: WordPress 'ajax-actions.php' Directory Traversal Vulnerability
    Reference: https://core.trac.wordpress.org/ticket/37490#no0
    Reference:
https://sumofpwn.nl/advisory/2016/path_traversal_vulnerability_in_wordpres
s_core_ajax_handlers.html
    Reference: http://www.openwall.com/lists/oss-security/2016/08/20/1
    Reference: https://wpvulndb.com/vulnerabilities/8606
    Reference: http://www.securitytracker.com/id/1036683
    Reference: https://www.exploit-db.com/exploits/40288/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
6896
[i] CVSS: 5.5
[i] Fixed in: 4.6

[!] Title: WordPress Prior to 4.7.2 Multiple Security Vulnerabilities
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-2-
security-release/
    Reference:
https://github.com/WordPress/WordPress/commit/4482f9207027de8f36630737ae08
5110896ea849
    Reference:
https://github.com/WordPress/WordPress/commit/21264a31e0849e6ff793a06a17de
877dd88ea454
    Reference:
https://github.com/WordPress/WordPress/commit/85384297a60900004e27e417eac5
6d24267054cb
    Reference: http://www.openwall.com/lists/oss-security/2017/01/28/5
    Reference: https://codex.wordpress.org/Version_4.7.2
    Reference: http://www.securitytracker.com/id/1037731
    Reference: https://wpvulndb.com/vulnerabilities/8729
    Reference: https://wpvulndb.com/vulnerabilities/8730
    Reference: https://wpvulndb.com/vulnerabilities/8731
    Reference: http://www.debian.org/security/2017/dsa-3779
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
5611
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
5610
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
5612
[i] CVSS: 5.0
[i] Fixed in: 4.7.2

[!] Title: WordPress 'class-wp-rest-posts-controller.php' Privilege
Escalation Vulnerability
    Reference: https://blog.sucuri.net/2017/02/content-injection-
vulnerability-wordpress-rest-api.html
    Reference: https://blogs.akamai.com/2017/02/wordpress-web-api-
vulnerability.html
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-2-
security-release/
[i] Fixed in: 4.7.2

[!] Title: WordPress Prior to 4.8.2 Multiple Input Validation Security
Vulnerabilities (4.3+)
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-
security-and-maintenance-release/
[i] Fixed in: 4.3.12

[!] Title: WordPress versions 4.8.2 and earlier $wpdb->prepare() potential
SQL injection (SQLi).
    Reference:
https://github.com/WordPress/WordPress/commit/a2693fd8602e3263b5925b9d799d
dd577202167d
    Reference: https://wordpress.org/news/2017/10/wordpress-4-8-3-
security-release/
    Reference: https://blog.ircmaxell.com/2017/10/disclosure-wordpress-
wpdb-sql-injection-technical.html
    Reference: https://codex.wordpress.org/Version_4.8.3
    Reference: https://wpvulndb.com/vulnerabilities/8941
    Reference: https://www.debian.org/security/2018/dsa-4090
    Reference: https://lists.debian.org/debian-lts-
announce/2017/11/msg00003.html
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
16510
[i] CVSS: 7.5
[i] Fixed in: 4.8.3

[!] Title: WordPress Prior to 4.9.1 Multiple Security Vulnerabilities
    Reference: https://make.wordpress.org/core/2017/11/28/wordpress-4-9-1-
scheduled-for-november-29th/
    Reference: https://wordpress.org/news/2017/11/wordpress-4-9-1-
security-and-maintenance-release/
[i] Fixed in: 4.9.1

[+] Enumerating installed plugins  ...
```

```
   Time: 00:07:33
<=========================================================================
==========================================================> (1829 / 1829)
100.00% Time: 00:07:33

[+] We found 11 plugins:

[+] Name: akismet
 |  Location: http://10.10.172.31/wp-content/plugins/akismet/

[+] Name: all-in-one-seo-pack - v2.0.4
 |  Location: http://10.10.172.31/wp-content/plugins/all-in-one-seo-pack/
 |  Readme: http://10.10.172.31/wp-content/plugins/all-in-one-seo-
pack/readme.txt

[!] Title: All in One SEO Pack <= 2.1.5 - aioseop_functions.php new_meta
Parameter XSS
    Reference: http://blog.sucuri.net/2014/05/vulnerability-found-in-the-
all-in-one-seo-pack-wordpress-plugin.html
    Reference: http://osvdb.org/107640
    Reference: https://wpvulndb.com/vulnerabilities/6888
[i] Fixed in: 2.1.6

[!] Title: All in One SEO Pack <= 2.1.5 - Unspecified Privilege Escalation
    Reference: http://blog.sucuri.net/2014/05/vulnerability-found-in-the-
all-in-one-seo-pack-wordpress-plugin.html
    Reference: http://osvdb.org/107641
    Reference: https://wpvulndb.com/vulnerabilities/6889
[i] Fixed in: 2.1.6

[+] Name: all-in-one-wp-migration - v2.0.4
 |  Location: http://10.10.172.31/wp-content/plugins/all-in-one-wp-
migration/
 |  Readme: http://10.10.172.31/wp-content/plugins/all-in-one-wp-
migration/readme.txt

[+] Name: contact-form-7 - v4.1
 |  Location: http://10.10.172.31/wp-content/plugins/contact-form-7/
 |  Readme: http://10.10.172.31/wp-content/plugins/contact-form-
7/readme.txt

[+] Name: feed
 |  Location: http://10.10.172.31/wp-content/plugins/feed/

[+] We could not determine a version so all vulnerabilities are printed
out

[!] Title: Feed - news_dt.php nid Parameter SQL Injection
    Reference: http://packetstormsecurity.com/files/122260/
    Reference: http://osvdb.org/94804
    Reference: https://wpvulndb.com/vulnerabilities/6965

[+] Name: google-analytics-for-wordpress - v5.3.2
```

```
 |  Location: http://10.10.172.31/wp-content/plugins/google-analytics-for-
wordpress/
 |  Readme: http://10.10.172.31/wp-content/plugins/google-analytics-for-
wordpress/readme.txt

[+] Name: google-sitemap-generator - v4.0.7.1
 |  Location: http://10.10.172.31/wp-content/plugins/google-sitemap-
generator/
 |  Readme: http://10.10.172.31/wp-content/plugins/google-sitemap-
generator/readme.txt

[+] Name: jetpack - v3.3.2
 |  Location: http://10.10.172.31/wp-content/plugins/jetpack/
 |  Readme: http://10.10.172.31/wp-content/plugins/jetpack/readme.txt

[!] Title: ** DISPUTED ** SQL injection vulnerability in
modules/sharedaddy.php in the Jetpack plugin for WordPress allows remote
attackers to execute arbitrary SQL commands via the id parameter
    Reference: http://xforce.iss.net/xforce/xfdb/71404
    Reference: http://www.securityfocus.com/bid/50730
    Reference: http://www.exploit-db.com/exploits/18126
    Reference: https://exchange.xforce.ibmcloud.com/vulnerabilities/71404
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-
4673
[i] CVSS: 7.5

[!] Title: WordPress Jetpack Plugin HTML Injection Vulnerability (2.0+)
    Reference: https://jetpack.com/2016/05/27/jetpack-4-0-3-critical-
security-update/
    Reference: http://wptavern.com/jetpack-4-0-3-patches-a-critical-xss-
vulnerability
[i] Fixed in: 4.0.3

[+] Name: simple-tags - v2.4.1
 |  Location: http://10.10.172.31/wp-content/plugins/simple-tags/
 |  Readme: http://10.10.172.31/wp-content/plugins/simple-tags/readme.txt

[+] Name: wp-mail-smtp - v0.9.5
 |  Location: http://10.10.172.31/wp-content/plugins/wp-mail-smtp/
 |  Readme: http://10.10.172.31/wp-content/plugins/wp-mail-smtp/readme.txt

[+] Name: wptouch - v3.7.3
 |  Location: http://10.10.172.31/wp-content/plugins/wptouch/
 |  Readme: http://10.10.172.31/wp-content/plugins/wptouch/readme.txt

[!] Title: WPtouch 1.9.19.4 - Cross-Site Scripting (XSS)
    Reference: http://www.securityfocus.com/bid/45139
    Reference:
http://www.htbridge.ch/advisory/xss_in_wptouch_wordpress_plugin.html
    Reference: http://osvdb.org/69538
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-
4779
    Reference: https://secunia.com/advisories/42438
    Reference: http://osvdb.org/69538
    Reference: https://wpvulndb.com/vulnerabilities/7120
[i] CVSS: 4.3

[!] Title: SQL injection vulnerability in wptouch/ajax.php in the WPTouch
plugin for WordPress allows remote attackers to execute arbitrary SQL
commands via the id parameter
    Reference: http://www.exploit-db.com/exploits/18039
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-
4803
[i] CVSS: 7.5

[+] Finished: Mon May 17 18:46:10 2021
[+] Memory used: 219.629 MB
[+] Elapsed time: 00:07:50
Vane - a Free WordPress vulnerability scanner
[+] URL: http://10.10.172.31/
[+] Started: Mon May 17 18:47:32 2021

[+] robots.txt available under: 'http://10.10.172.31/robots.txt'
[+] Interesting header: SERVER: Apache
[+] Interesting header: X-FRAME-OPTIONS: SAMEORIGIN
[+] Interesting header: X-MOD-PAGESPEED: 1.9.32.3-4523
[+] XML-RPC Interface available under: http://10.10.172.31/xmlrpc.php
[+] WordPress version 4.3.1 identified from links opml
[!] 62 vulnerabilities identified from the version number

[!] Title: WordPress CVE-2018-6389 Denial of Service Vulnerability
    Reference: http://securityaffairs.co/wordpress/68709/hacking/cve-2018-
6389-wordpress-dos-flaw.html
    Reference:
https://github.com/Quitten/WordPress/commit/3463dcbd8d1f2426ba7f58a5293a38
5fcc4e7004
    Reference: https://wpvulndb.com/vulnerabilities/9021
    Reference: https://baraktawily.blogspot.in/2018/02/how-to-dos-29-of-
world-wide-websites.html
    Reference: https://github.com/WazeHell/CVE-2018-6389
    Reference: http://www.securitytracker.com/id/1040347
    Reference: https://baraktawily.blogspot.fr/2018/02/how-to-dos-29-of-
world-wide-websites.html
    Reference: https://thehackernews.com/2018/02/wordpress-dos-
exploit.html
    Reference: https://www.exploit-db.com/exploits/43968/
    Reference: https://github.com/UltimateHackers/Shiva
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-
6389
[i] CVSS: 5.0

[!] Title: WordPress 'ajax-actions.php' Cross Site Request Forgery
Vulnerability
    Reference: http://codex.wordpress.org/Version_4.5
    Reference:
https://github.com/WordPress/WordPress/commit/9b7a7754133c50b82bd9d976fb5b
24094f658aab
    Reference: https://wpvulndb.com/vulnerabilities/8475
    Reference: http://www.debian.org/security/2016/dsa-3681
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
6635
[i] CVSS: 6.8
[i] Fixed in: 4.5

[!] Title: WordPress CVE-2016-6634 Unspecified Cross Site Scripting
Vulnerability
    Reference: http://codex.wordpress.org/Version_4.5
    Reference:
https://core.trac.wordpress.org/query?status=closed&milestone=4.5
    Reference: https://wpvulndb.com/vulnerabilities/8474
    Reference: https://codex.wordpress.org/Version_4.5
    Reference: http://www.securityfocus.com/bid/92390
    Reference: http://www.debian.org/security/2016/dsa-3681
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
6634
[i] CVSS: 4.3
[i] Fixed in: 4.5

[!] Title: WordPress CVE-2016-4029 Security Bypass Vulnerability
    Reference: http://codex.wordpress.org/Version_4.5
    Reference:
https://core.trac.wordpress.org/query?status=closed&milestone=4.5
    Reference: https://codex.wordpress.org/Version_4.5
    Reference: https://wpvulndb.com/vulnerabilities/8473
    Reference: http://www.securitytracker.com/id/1036594
    Reference: http://www.debian.org/security/2016/dsa-3681
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
4029
[i] CVSS: 5.0
[i] Fixed in: 4.5

[!] Title: WordPress allows remote attackers to obtain sensitive revision-
history information by leveraging the ability to read a post, related to
wp-admin/includes/ajax-actions.php and wp-admin/revision.php
    Reference: http://www.securitytracker.com/id/1036163
    Reference: https://codex.wordpress.org/Version_4.5.3
    Reference:
https://github.com/WordPress/WordPress/commit/a2904cc3092c391ac7027bc87f78
06953d1a25a1
    Reference: https://wordpress.org/news/2016/06/wordpress-4-5-3/
    Reference: http://www.debian.org/security/2016/dsa-3639
    Reference: http://www.securityfocus.com/bid/91366
    Reference: https://wpvulndb.com/vulnerabilities/8519
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
5835
[i] CVSS: 5.0
[i] Fixed in: 4.5.3

[!] Title: WordPress allows remote attackers to bypass intended access
restrictions and remove a category attribute from a post via unspecified
vectors
    Reference: http://www.securitytracker.com/id/1036163
    Reference: https://codex.wordpress.org/Version_4.5.3
    Reference: https://wordpress.org/news/2016/06/wordpress-4-5-3/
    Reference: http://www.debian.org/security/2016/dsa-3639
    Reference: http://www.securityfocus.com/bid/91365
    Reference: https://wpvulndb.com/vulnerabilities/8520
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
5837
[i] CVSS: 5.0
[i] Fixed in: 4.5.3

[!] Title: WordPress allows remote attackers to bypass intended password-
change restrictions by leveraging knowledge of a cookie
    Reference: http://www.securitytracker.com/id/1036163
    Reference: https://codex.wordpress.org/Version_4.5.3
    Reference: https://wordpress.org/news/2016/06/wordpress-4-5-3/
    Reference: http://www.debian.org/security/2016/dsa-3639
    Reference: http://www.securityfocus.com/bid/91367
    Reference: https://wpvulndb.com/vulnerabilities/8524
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
5838
[i] CVSS: 5.0
[i] Fixed in: 4.5.3

[!] Title: WordPress allows remote attackers to bypass the
sanitize_file_name protection mechanism via unspecified vectors
    Reference: http://www.securitytracker.com/id/1036163
    Reference: https://codex.wordpress.org/Version_4.5.3
    Reference: https://wordpress.org/news/2016/06/wordpress-4-5-3/
    Reference: http://www.debian.org/security/2016/dsa-3639
    Reference: http://www.securityfocus.com/bid/91364
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
5839
[i] CVSS: 5.0
[i] Fixed in: 4.5.3

[!] Title: The oEmbed protocol implementation in WordPress allows remote
attackers to cause a denial of service via unspecified vectors
    Reference: http://www.securitytracker.com/id/1036163
    Reference: https://codex.wordpress.org/Version_4.5.3
    Reference: https://wordpress.org/news/2016/06/wordpress-4-5-3/
    Reference: http://www.securityfocus.com/bid/91363
    Reference: https://wpvulndb.com/vulnerabilities/8523
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
5836
[i] CVSS: 5.0
[i] Fixed in: 4.5.3

[!] Title: Cross-site scripting (XSS) vulnerability in the
wp_get_attachment_link function in wp-includes/post-template.php in
WordPress allows remote attackers to inject arbitrary web script or HTML
via a crafted attachment name
    Reference: http://www.securitytracker.com/id/1036163
    Reference: https://codex.wordpress.org/Version_4.5.3
    Reference:
https://github.com/WordPress/WordPress/commit/4372cdf45d0f49c74bbd4d60db72
81de83e32648
    Reference: https://wordpress.org/news/2016/06/wordpress-4-5-3/
    Reference: http://www.debian.org/security/2016/dsa-3639
    Reference: http://www.securityfocus.com/bid/91368
    Reference: https://wpvulndb.com/vulnerabilities/8518
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
5834
[i] CVSS: 4.3
[i] Fixed in: 4.5.3

[!] Title: Cross-site scripting (XSS) vulnerability in the column_title
function in wp-admin/includes/class-wp-media-list-table.php in WordPress
allows remote attackers to inject arbitrary web script or HTML via a
crafted attachment name
    Reference: http://www.securitytracker.com/id/1036163
    Reference: https://codex.wordpress.org/Version_4.5.3
    Reference:
https://github.com/WordPress/WordPress/commit/4372cdf45d0f49c74bbd4d60db72
81de83e32648
    Reference: https://wordpress.org/news/2016/06/wordpress-4-5-3/
    Reference: http://www.securityfocus.com/bid/91368
    Reference: https://wpvulndb.com/vulnerabilities/8518
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
5833
[i] CVSS: 4.3
[i] Fixed in: 4.5.3

[!] Title: The customizer in WordPress allows remote attackers to bypass
intended redirection restrictions via unspecified vectors
    Reference: http://www.securitytracker.com/id/1036163
    Reference: https://codex.wordpress.org/Version_4.5.3
    Reference: https://wordpress.org/news/2016/06/wordpress-4-5-3/
    Reference: http://www.debian.org/security/2016/dsa-3639
    Reference: http://www.securityfocus.com/bid/91362
    Reference: https://wpvulndb.com/vulnerabilities/8522
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
5832
[i] CVSS: 5.0
[i] Fixed in: 4.5.3

[!] Title: Cross-site scripting (XSS) vulnerability in
flash/FlashMediaElement.as in MediaElement.js as used in WordPress allows
remote attackers to inject arbitrary web script or HTML via an obfuscated
form of the jsinitfunction parameter, as demonstrated by
"jsinitfunctio%gn."
    Reference: http://www.openwall.com/lists/oss-security/2016/05/07/2
    Reference: https://codex.wordpress.org/Version_4.5.2
    Reference: https://core.trac.wordpress.org/changeset/37371
    Reference:
https://gist.github.com/cure53/df34ea68c26441f3ae98f821ba1feb9c
    Reference:
https://github.com/johndyer/mediaelement/blob/master/changelog.md
```

```
    Reference:
https://github.com/johndyer/mediaelement/commit/34834eef8ac830b9145df169ec
22016a4350f06e
    Reference: https://wordpress.org/news/2016/05/wordpress-4-5-2/
    Reference: https://wpvulndb.com/vulnerabilities/8488
    Reference: http://www.securitytracker.com/id/1035818
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
4567
[i] CVSS: 4.3
[i] Fixed in: 4.5.2

[!] Title: Cross-site scripting (XSS) vulnerability in plupload.flash.swf
in Plupload as used in WordPress allows remote attackers to inject
arbitrary web script or HTML via a Same-Origin Method Execution (SOME)
attack
    Reference: http://www.openwall.com/lists/oss-security/2016/05/07/2
    Reference: http://www.plupload.com/punbb/viewtopic.php?pid=28690
    Reference: https://codex.wordpress.org/Version_4.5.2
    Reference: https://core.trac.wordpress.org/changeset/37382/
    Reference:
https://gist.github.com/cure53/09a81530a44f6b8173f545accc9ed07e
    Reference: https://wordpress.org/news/2016/05/wordpress-4-5-2/
    Reference: https://wpvulndb.com/vulnerabilities/8489
    Reference: http://www.securitytracker.com/id/1035818
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
4566
[i] CVSS: 4.3
[i] Fixed in: 4.5.2

[!] Title: The wp_http_validate_url function in wp-includes/http.php in
WordPress allows remote attackers to conduct server-side request forgery
(SSRF) attacks via a zero value in the first octet of an IPv4 address in
the u parameter to wp-admin/press-this.php
    Reference: https://wordpress.org/news/2016/02/wordpress-4-4-2-
security-and-maintenance-release/
    Reference: https://codex.wordpress.org/Version_4.4.2
    Reference: https://wpvulndb.com/vulnerabilities/8376
    Reference: https://hackerone.com/reports/110801
    Reference: https://core.trac.wordpress.org/changeset/36435
    Reference: http://www.securityfocus.com/bid/82454
    Reference: http://www.securitytracker.com/id/1034933
    Reference: http://www.debian.org/security/2016/dsa-3472
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
2222
[i] CVSS: 5.0
[i] Fixed in: 4.4.2

[!] Title: Open redirect vulnerability in the wp_validate_redirect
function in wp-includes/pluggable.php in WordPress allows remote attackers
to redirect users to arbitrary web sites and conduct phishing attacks via
a malformed URL that triggers incorrect hostname parsing, as demonstrated
by an https:example.com URL
    Reference: https://wordpress.org/news/2016/02/wordpress-4-4-2-
security-and-maintenance-release/
```

```
    Reference: https://core.trac.wordpress.org/changeset/36444
    Reference: https://codex.wordpress.org/Version_4.4.2
    Reference: https://wpvulndb.com/vulnerabilities/8377
    Reference: http://www.securityfocus.com/bid/82463
    Reference: http://www.securitytracker.com/id/1034933
    Reference: http://www.debian.org/security/2016/dsa-3472
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
2221
[i] CVSS: 5.8
[i] Fixed in: 4.4.2

[!] Title: Multiple cross-site scripting (XSS) vulnerabilities in wp-
includes/class-wp-theme.php in WordPress allow remote attackers to inject
arbitrary web script or HTML via a (1) stylesheet name or (2) template
name to wp-admin/customize.php
    Reference: https://wordpress.org/news/2016/01/wordpress-4-4-1-
security-and-maintenance-release/
    Reference: https://codex.wordpress.org/Version_4.4.1
    Reference: https://wpvulndb.com/vulnerabilities/8358
    Reference: https://core.trac.wordpress.org/changeset/36185
    Reference: http://www.openwall.com/lists/oss-security/2016/01/08/4
    Reference: http://twitter.com/brutelogic/statuses/685105483397619713
    Reference: http://www.securitytracker.com/id/1034622
    Reference: http://www.debian.org/security/2016/dsa-3444
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
1564
[i] CVSS: 4.3
[i] Fixed in: 4.4.1

[!] Title: WordPress 'wp_ajax_update_plugin()' Function Information
Disclosure Vulnerability
    Reference: http://www.openwall.com/lists/oss-security/2016/08/20/1
    Reference: https://core.trac.wordpress.org/changeset/38168
    Reference: https://core.trac.wordpress.org/ticket/37490
    Reference:
https://sumofpwn.nl/advisory/2016/path_traversal_vulnerability_in_wordpres
s_core_ajax_handlers.html
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
10148
[i] CVSS: 4.0
[i] Fixed in: 4.6

[!] Title: WordPress Cryptographic Security Bypass Vulnerability
    Reference: http://www.openwall.com/lists/oss-security/2017/01/14/6
    Reference: https://codex.wordpress.org/Version_4.7.1
    Reference:
https://github.com/WordPress/WordPress/commit/cea9e2dc62abf777e06b12ec4ad9
d1aaa49b29f4
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-
security-and-maintenance-release/
    Reference: http://www.securitytracker.com/id/1037591
    Reference: https://wpvulndb.com/vulnerabilities/8721
    Reference: http://www.debian.org/security/2017/dsa-3779
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
5493
[i] CVSS: 5.0
[i] Fixed in: 4.7.1

[!] Title: WordPress Prior to 4.7.1 Cross Site Request Forgery
Vulnerability
    Reference: http://www.openwall.com/lists/oss-security/2017/01/14/6
    Reference: https://codex.wordpress.org/Version_4.7.1
    Reference:
https://github.com/WordPress/WordPress/commit/03e5c0314aeffe6b27f4b98fef84
2bf0fb00c733
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-
security-and-maintenance-release/
    Reference: http://www.securitytracker.com/id/1037591
    Reference: https://wpvulndb.com/vulnerabilities/8720
    Reference: http://www.debian.org/security/2017/dsa-3779
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
5492
[i] CVSS: 6.8
[i] Fixed in: 4.7.1

[!] Title: WordPress Prior to 4.7.1 Security Bypass Vulnerability
    Reference: http://www.openwall.com/lists/oss-security/2017/01/14/6
    Reference: https://codex.wordpress.org/Version_4.7.1
    Reference:
https://github.com/WordPress/WordPress/commit/061e8788814ac87706d8b95688df
276fe3c8596a
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-
security-and-maintenance-release/
    Reference: http://www.securitytracker.com/id/1037591
    Reference: https://wpvulndb.com/vulnerabilities/8719
    Reference: http://www.debian.org/security/2017/dsa-3779
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
5491
[i] CVSS: 5.0
[i] Fixed in: 4.7.1

[!] Title: WordPress Prior to 4.7.1 Cross Site Scripting Vulnerability
    Reference: http://www.openwall.com/lists/oss-security/2017/01/14/6
    Reference: https://codex.wordpress.org/Version_4.7.1
    Reference:
https://github.com/WordPress/WordPress/commit/ce7fb2934dd111e6353784852de8
aea2a938b359
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-
security-and-maintenance-release/
    Reference: https://www.mehmetince.net/low-severity-wordpress/
    Reference:
https://github.com/WordPress/WordPress/blob/c9ea1de1441bb3bda133bf72d513ca
9de66566c2/wp-admin/update-core.php
    Reference: http://www.securitytracker.com/id/1037591
    Reference: https://wpvulndb.com/vulnerabilities/8718
    Reference: http://www.debian.org/security/2017/dsa-3779
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
5490
[i] CVSS: 4.3
[i] Fixed in: 4.7.1

[!] Title: WordPress Prior to 4.7.1 Cross Site Request Forgery
Vulnerability
    Reference: http://www.openwall.com/lists/oss-security/2017/01/14/6
    Reference: https://codex.wordpress.org/Version_4.7.1
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-
security-and-maintenance-release/
    Reference: http://www.securitytracker.com/id/1037591
    Reference: https://wpvulndb.com/vulnerabilities/8717
    Reference: http://www.debian.org/security/2017/dsa-3779
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
5489
[i] CVSS: 6.8
[i] Fixed in: 4.7.1

[!] Title: WordPress Prior to 4.7.1 Cross Site Scripting Vulnerability
    Reference: http://www.openwall.com/lists/oss-security/2017/01/14/6
    Reference: https://codex.wordpress.org/Version_4.7.1
    Reference:
https://github.com/WordPress/WordPress/commit/c9ea1de1441bb3bda133bf72d513
ca9de66566c2
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-
security-and-maintenance-release/
    Reference:
https://github.com/WordPress/WordPress/blob/c9ea1de1441bb3bda133bf72d513ca
9de66566c2/wp-admin/update-core.php
    Reference: http://www.securitytracker.com/id/1037591
    Reference: https://wpvulndb.com/vulnerabilities/8716
    Reference: http://www.debian.org/security/2017/dsa-3779
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
5488
[i] CVSS: 4.3
[i] Fixed in: 4.7.1

[!] Title: WordPress Prior to 4.7.1 Information Disclosure Vulnerability
    Reference: http://www.openwall.com/lists/oss-security/2017/01/14/6
    Reference: https://codex.wordpress.org/Version_4.7.1
    Reference:
https://github.com/WordPress/WordPress/commit/daf358983cc1ce0c77bf6d2de2eb
bb43df2add60
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-
security-and-maintenance-release/
    Reference: https://www.wordfence.com/blog/2016/12/wordfence-blocks-
username-harvesting-via-new-rest-api-wp-4-7/
    Reference: http://www.securitytracker.com/id/1037591
    Reference: https://wpvulndb.com/vulnerabilities/8715
    Reference: https://www.exploit-db.com/exploits/41497/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
5487
[i] CVSS: 5.0
```

```
[i] Fixed in: 4.7.1

[!] Title: WordPress Prior to 4.7.3 Cross Site Request Forgery
Vulnerability
    Reference: http://openwall.com/lists/oss-security/2017/03/06/7
    Reference: https://codex.wordpress.org/Version_4.7.3
    Reference:
https://github.com/WordPress/WordPress/commit/263831a72d08556bc2f3a328673d
95301a152829
    Reference:
https://sumofpwn.nl/advisory/2016/cross_site_request_forgery_in_wordpress_
press_this_function_allows_dos.html
    Reference: https://wordpress.org/news/2017/03/wordpress-4-7-3-
security-and-maintenance-release/
    Reference: http://www.securitytracker.com/id/1037959
    Reference: https://wpvulndb.com/vulnerabilities/8770
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
6819
[i] CVSS: 4.3
[i] Fixed in: 4.7.3

[!] Title: WordPress Prior to 4.7.3 Multiple Cross Site Scripting
Vulnerabilities
    Reference: https://codex.wordpress.org/Version_4.7.3
    Reference:
https://github.com/WordPress/WordPress/commit/9092fd01e1f452f37c313d38b18f
9fe6907541f9
    Reference: https://wordpress.org/news/2017/03/wordpress-4-7-3-
security-and-maintenance-release/
    Reference:
https://github.com/WordPress/WordPress/commit/419c8d97ce8df7d5004ee0b566bc
5e095f0a6ca8
    Reference:
https://github.com/WordPress/WordPress/commit/28f838ca3ee205b6f39cd2bf23eb
4e5f52796bd7
    Reference: http://openwall.com/lists/oss-security/2017/03/06/8
    Reference:
https://sumofpwn.nl/advisory/2016/wordpress_audio_playlist_functionality_i
s_affected_by_cross_site_scripting.html
    Reference: http://www.securitytracker.com/id/1037959
    Reference: https://wpvulndb.com/vulnerabilities/8769
    Reference: https://wpvulndb.com/vulnerabilities/8768
    Reference: https://wpvulndb.com/vulnerabilities/8765
    Reference: http://www.debian.org/security/2017/dsa-3815
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
6818
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
6814
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
6817
[i] CVSS: 3.5
[i] Fixed in: 4.7.3
```

```
[!] Title: In WordPress (wp-includes/embed.php), there is authenticated
Cross-Site Scripting (XSS) in YouTube URL Embeds
    Reference: https://codex.wordpress.org/Version_4.7.3
    Reference:
https://github.com/WordPress/WordPress/commit/419c8d97ce8df7d5004ee0b566bc
5e095f0a6ca8
    Reference: https://wordpress.org/news/2017/03/wordpress-4-7-3-
security-and-maintenance-release/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
6817
[i] CVSS: 3.5
[i] Fixed in: 4.7.3

[!] Title: WordPress Prior to 4.7.3 Security Bypass Vulnerability
    Reference: https://codex.wordpress.org/Version_4.7.3
    Reference:
https://github.com/WordPress/WordPress/commit/4d80f8b3e1b00a3edcee0774dc9c
2f4c78f9e663
    Reference: https://wordpress.org/news/2017/03/wordpress-4-7-3-
security-and-maintenance-release/
    Reference: http://www.securitytracker.com/id/1037959
    Reference: https://wpvulndb.com/vulnerabilities/8767
    Reference: http://www.debian.org/security/2017/dsa-3815
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
6816
[i] CVSS: 4.0
[i] Fixed in: 4.7.3

[!] Title: WordPress Prior to 4.7.3 URL Redirection Vulnerability
    Reference: https://codex.wordpress.org/Version_4.7.3
    Reference:
https://github.com/WordPress/WordPress/commit/288cd469396cfe7055972b457eb5
89cea51ce40e
    Reference: https://wordpress.org/news/2017/03/wordpress-4-7-3-
security-and-maintenance-release/
    Reference: http://www.securitytracker.com/id/1037959
    Reference: https://wpvulndb.com/vulnerabilities/8766
    Reference: http://www.debian.org/security/2017/dsa-3815
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
6815
[i] CVSS: 5.8
[i] Fixed in: 4.7.3

[!] Title: In WordPress there is authenticated Cross-Site Scripting (XSS)
via Media File Metadata
    Reference: http://openwall.com/lists/oss-security/2017/03/06/8
    Reference: https://codex.wordpress.org/Version_4.7.3
    Reference:
https://github.com/WordPress/WordPress/commit/28f838ca3ee205b6f39cd2bf23eb
4e5f52796bd7
    Reference:
https://sumofpwn.nl/advisory/2016/wordpress_audio_playlist_functionality_i
s_affected_by_cross_site_scripting.html
```

```
    Reference: https://wordpress.org/news/2017/03/wordpress-4-7-3-
security-and-maintenance-release/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
6814
[i] CVSS: 3.5
[i] Fixed in: 4.7.3

[!] Title: WordPress Prior to 4.7.5 Multiple Security Vulnerabilities
    Reference: https://codex.wordpress.org/Version_4.7.5
    Reference:
https://github.com/WordPress/WordPress/commit/e88a48a066ab2200ce3091b131d4
3e2fab2460a4
    Reference: https://wordpress.org/news/2017/05/wordpress-4-7-5/
    Reference:
https://github.com/WordPress/WordPress/commit/38347d7c580be4cdd8476e4bbc65
3d5c79ed9b67
    Reference:
https://github.com/WordPress/WordPress/commit/3d95e3ae816f4d7c638f40d3e936
a4be19724381
    Reference:
https://github.com/WordPress/WordPress/commit/3d10fef22d788f29aed745b0f5ff
6f6baea69af3
    Reference:
https://github.com/WordPress/WordPress/commit/76d77e927bb4d0f87c7262a50e28
d84e01fd2b11
    Reference:
https://github.com/WordPress/WordPress/commit/8c7ea71edbbffca5d9766b7bea7c
7f3722ffafa6
    Reference: http://www.securitytracker.com/id/1038520
    Reference: https://twitter.com/skansing/status/865362551097393153
    Reference: https://wpvulndb.com/vulnerabilities/8815
    Reference: https://wpvulndb.com/vulnerabilities/8817
    Reference: https://wpvulndb.com/vulnerabilities/8818
    Reference: https://wpvulndb.com/vulnerabilities/8820
    Reference: https://wpvulndb.com/vulnerabilities/8816
    Reference: https://wpvulndb.com/vulnerabilities/8819
    Reference: http://www.debian.org/security/2017/dsa-3870
    Reference: https://www.debian.org/security/2018/dsa-4090
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9065
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9062
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9063
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9064
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9061
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9066
[i] CVSS: 5.0
[i] Fixed in: 4.7.5

[!] Title: WordPress Prior to 4.7.5 Multiple Security Vulnerabilities
```

```
    Reference: https://codex.wordpress.org/Version_4.7.5
    Reference:
https://github.com/WordPress/WordPress/commit/38347d7c580be4cdd8476e4bbc65
3d5c79ed9b67
    Reference: https://wordpress.org/news/2017/05/wordpress-4-7-5/
    Reference:
https://github.com/WordPress/WordPress/commit/3d95e3ae816f4d7c638f40d3e936
a4be19724381
    Reference:
https://github.com/WordPress/WordPress/commit/3d10fef22d788f29aed745b0f5ff
6f6baea69af3
    Reference:
https://github.com/WordPress/WordPress/commit/76d77e927bb4d0f87c7262a50e28
d84e01fd2b11
    Reference:
https://github.com/WordPress/WordPress/commit/e88a48a066ab2200ce3091b131d4
3e2fab2460a4
    Reference:
https://github.com/WordPress/WordPress/commit/8c7ea71edbbffca5d9766b7bea7c
7f3722ffafa6
    Reference: https://twitter.com/skansing/status/865362551097393153
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9064
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9066
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9065
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9063
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9061
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9062
[i] CVSS: 5.0
[i] Fixed in: 4.7.5

[!] Title: In WordPress a cross-site scripting (XSS) vulnerability related
to the Customizer exists, involving an invalid customization session
    Reference: https://codex.wordpress.org/Version_4.7.5
    Reference:
https://github.com/WordPress/WordPress/commit/3d10fef22d788f29aed745b0f5ff
6f6baea69af3
    Reference: https://wordpress.org/news/2017/05/wordpress-4-7-5/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9063
[i] CVSS: 4.3
[i] Fixed in: 4.7.5

[!] Title: In WordPress there is improper handling of post meta data
values in the XML-RPC API
    Reference: https://codex.wordpress.org/Version_4.7.5
    Reference:
https://github.com/WordPress/WordPress/commit/3d95e3ae816f4d7c638f40d3e936
a4be19724381
```

```
    Reference: https://wordpress.org/news/2017/05/wordpress-4-7-5/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9062
[i] CVSS: 5.0
[i] Fixed in: 4.7.5

[!] Title: In WordPress a cross-site scripting (XSS) vulnerability exists
when attempting to upload very large files, because the error message does
not properly restrict presentation of the filename
    Reference: https://codex.wordpress.org/Version_4.7.5
    Reference:
https://github.com/WordPress/WordPress/commit/8c7ea71edbbffca5d9766b7bea7c
7f3722ffafa6
    Reference: https://wordpress.org/news/2017/05/wordpress-4-7-5/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
9061
[i] CVSS: 4.3
[i] Fixed in: 4.7.5

[!] Title: WordPress Password Reset CVE-2017-8295 Security Bypass
Vulnerability
    Reference: https://exploitbox.io/vuln/WordPress-Exploit-4-7-Unauth-
Password-Reset-0day-CVE-2017-8295.html
    Reference: https://www.exploit-db.com/exploits/41963/
    Reference: http://www.securitytracker.com/id/1038403
    Reference: https://wpvulndb.com/vulnerabilities/8807
    Reference: http://www.debian.org/security/2017/dsa-3870
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
8295
[i] CVSS: 4.3
[i] Fixed in: 4.7.5

[!] Title: Before version 4.8.2, WordPress was vulnerable to a cross-site
scripting attack via shortcodes in the TinyMCE visual editor
    Reference: https://core.trac.wordpress.org/changeset/41395
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-
security-and-maintenance-release/
    Reference: https://wpvulndb.com/vulnerabilities/8914
    Reference: http://www.securitytracker.com/id/1039553
    Reference: https://www.debian.org/security/2017/dsa-3997
    Reference: https://core.trac.wordpress.org/changeset/41393
    Reference: https://core.trac.wordpress.org/changeset/41397
    Reference: https://core.trac.wordpress.org/changeset/41398
    Reference: https://core.trac.wordpress.org/changeset/41412
    Reference: https://core.trac.wordpress.org/changeset/41448
    Reference: https://core.trac.wordpress.org/changeset/41457
    Reference: https://core.trac.wordpress.org/changeset/41470
    Reference: https://core.trac.wordpress.org/changeset/41496
    Reference:
https://github.com/WordPress/WordPress/commit/70b21279098fc973eae803693c07
05a548128e48
    Reference:
https://github.com/WordPress/WordPress/commit/fc930d3daed1c3acef010d04acc2
c5de93cd18ec
```

```
    Reference: https://medium.com/websec/wordpress-sqli-bbb2afcc8e94
    Reference: https://medium.com/websec/wordpress-sqli-poc-f1827c20bf8e
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14726
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14723
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14718
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14720
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14721
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14725
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14719
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14722
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14724
[i] CVSS: 4.3
[i] Fixed in: 4.8.2

[!] Title: Before version 4.8.2, WordPress was susceptible to an open
redirect attack in wp-admin/edit-tag-form.php and wp-admin/user-edit.php
    Reference: https://core.trac.wordpress.org/changeset/41398
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-
security-and-maintenance-release/
    Reference: https://wpvulndb.com/vulnerabilities/8910
    Reference: http://www.securitytracker.com/id/1039553
    Reference: https://core.trac.wordpress.org/changeset/41393
    Reference: https://core.trac.wordpress.org/changeset/41395
    Reference: https://core.trac.wordpress.org/changeset/41397
    Reference: https://core.trac.wordpress.org/changeset/41412
    Reference: https://core.trac.wordpress.org/changeset/41448
    Reference: https://core.trac.wordpress.org/changeset/41457
    Reference: https://core.trac.wordpress.org/changeset/41470
    Reference: https://core.trac.wordpress.org/changeset/41496
    Reference:
https://github.com/WordPress/WordPress/commit/70b21279098fc973eae803693c07
05a548128e48
    Reference:
https://github.com/WordPress/WordPress/commit/fc930d3daed1c3acef010d04acc2
c5de93cd18ec
    Reference: https://medium.com/websec/wordpress-sqli-bbb2afcc8e94
    Reference: https://medium.com/websec/wordpress-sqli-poc-f1827c20bf8e
    Reference: https://wpvulndb.com/vulnerabilities/8913
    Reference: https://wpvulndb.com/vulnerabilities/8912
    Reference: https://wpvulndb.com/vulnerabilities/8911
    Reference: https://www.debian.org/security/2017/dsa-3997
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14725
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14719
```

```
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14724
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14721
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14723
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14722
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14726
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14718
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14720
[i] CVSS: 4.9
[i] Fixed in: 4.8.2

[!] Title: Before version 4.8.2, WordPress was vulnerable to cross-site
scripting in oEmbed discovery
    Reference: https://core.trac.wordpress.org/changeset/41448
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-
security-and-maintenance-release/
    Reference: https://wpvulndb.com/vulnerabilities/8913
    Reference: http://www.securitytracker.com/id/1039553
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14724
[i] CVSS: 4.3
[i] Fixed in: 4.8.2

[!] Title: Before version 4.8.2, WordPress mishandled % characters and
additional placeholder values in $wpdb->prepare, and thus did not properly
address the possibility of plugins and themes enabling SQL injection
attacks
    Reference: https://core.trac.wordpress.org/changeset/41470
    Reference: https://core.trac.wordpress.org/changeset/41496
    Reference:
https://github.com/WordPress/WordPress/commit/70b21279098fc973eae803693c07
05a548128e48
    Reference:
https://github.com/WordPress/WordPress/commit/fc930d3daed1c3acef010d04acc2
c5de93cd18ec
    Reference: https://medium.com/websec/wordpress-sqli-bbb2afcc8e94
    Reference: https://medium.com/websec/wordpress-sqli-poc-f1827c20bf8e
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-
security-and-maintenance-release/
    Reference: https://core.trac.wordpress.org/changeset/41393
    Reference: https://core.trac.wordpress.org/changeset/41395
    Reference: https://core.trac.wordpress.org/changeset/41397
    Reference: https://core.trac.wordpress.org/changeset/41398
    Reference: https://core.trac.wordpress.org/changeset/41412
    Reference: https://core.trac.wordpress.org/changeset/41448
    Reference: https://core.trac.wordpress.org/changeset/41457
    Reference: http://www.securitytracker.com/id/1039553
    Reference: https://wpvulndb.com/vulnerabilities/8912
    Reference: https://wpvulndb.com/vulnerabilities/8911
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14723
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14721
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14726
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14718
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14725
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14720
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14724
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14719
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14722
[i] CVSS: 7.5
[i] Fixed in: 4.8.2

[!] Title: Before version 4.8.2, WordPress allowed a Directory Traversal
attack in the Customizer component via a crafted theme filename
    Reference: https://core.trac.wordpress.org/changeset/41397
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-
security-and-maintenance-release/
    Reference: https://wpvulndb.com/vulnerabilities/8912
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14722
[i] CVSS: 5.0
[i] Fixed in: 4.8.2

[!] Title: Before version 4.8.2, WordPress allowed Cross-Site scripting in
the plugin editor via a crafted plugin name
    Reference: https://core.trac.wordpress.org/changeset/41412
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-
security-and-maintenance-release/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14721
[i] CVSS: 4.3
[i] Fixed in: 4.8.2

[!] Title: Before version 4.8.2, WordPress allowed a Cross-Site scripting
attack in the template list view via a crafted template name
    Reference: https://core.trac.wordpress.org/changeset/41412
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-
security-and-maintenance-release/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14720
[i] CVSS: 4.3
[i] Fixed in: 4.8.2
```

```
[!] Title: Before version 4.8.2, WordPress was vulnerable to a directory
traversal attack during unzip operations in the ZipArchive and PclZip
components
    Reference: https://core.trac.wordpress.org/changeset/41457
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-
security-and-maintenance-release/
    Reference: https://wpvulndb.com/vulnerabilities/8911
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14719
[i] CVSS: 5.0
[i] Fixed in: 4.8.2

[!] Title: Before version 4.8.2, WordPress was susceptible to a Cross-Site
Scripting attack in the link modal via a javascript: or data: URL
    Reference: https://core.trac.wordpress.org/changeset/41393
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-
security-and-maintenance-release/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14718
[i] CVSS: 4.3
[i] Fixed in: 4.8.2

[!] Title: WordPress stores cleartext wp_signups.activation_key values
(but stores the analogous wp_users.user_activation_key values as hashes),
which might make it easier for remote attackers to hijack unactivated user
accounts by leveraging database read access (such as access gained through
an unspecified SQL injection vulnerability)
    Reference: http://www.securitytracker.com/id/1039554
    Reference: https://core.trac.wordpress.org/ticket/38474
    Reference: https://www.debian.org/security/2017/dsa-3997
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
14990
[i] CVSS: 4.0
[i] Fixed in: 4.8.3

[!] Title: WordPress through , when domain-based flashmediaelement.swf
sandboxing is not used, allows remote attackers to conduct cross-domain
Flash injection (XSF) attacks by leveraging code contained within the wp-
includes/js/mediaelement/flashmediaelement.swf file
    Reference: https://opnsec.com/2017/10/cve-2016-9263-unpatched-xsf-
vulnerability-in-wordpress/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
9263
[i] CVSS: 2.6
[i] Fixed in: 4.8.3

[!] Title: WordPress through uses a weak MD5-based password hashing
algorithm, which makes it easier for attackers to determine cleartext
values by leveraging access to the hash values
    Reference: https://core.trac.wordpress.org/ticket/21022
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-
6707
[i] CVSS: 5.0
[i] Fixed in: 4.8.3
```

```
[!] Title: wp-includes/feed.php in WordPress does not properly restrict
enclosures in RSS and Atom fields, which might allow attackers to conduct
XSS attacks via a crafted URL
    Reference: https://codex.wordpress.org/Version_4.9.1
    Reference:
https://github.com/WordPress/WordPress/commit/f1de7e42df29395c3314bf85bff3
d1f4f90541de
    Reference: https://wordpress.org/news/2017/11/wordpress-4-9-1-
security-and-maintenance-release/
    Reference: https://wpvulndb.com/vulnerabilities/8967
    Reference: https://www.debian.org/security/2018/dsa-4090
    Reference: https://lists.debian.org/debian-lts-
announce/2017/12/msg00019.html
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
17094
[i] CVSS: 3.5
[i] Fixed in: 4.9.1

[!] Title: wp-includes/general-template.php in WordPress does not properly
restrict the lang attribute of an HTML element, which might allow
attackers to conduct XSS attacks via the language setting of a site
    Reference: https://codex.wordpress.org/Version_4.9.1
    Reference:
https://github.com/WordPress/WordPress/commit/3713ac5ebc90fb2011e98dfd6914
20f43da6c09a
    Reference: https://wordpress.org/news/2017/11/wordpress-4-9-1-
security-and-maintenance-release/
    Reference: https://wpvulndb.com/vulnerabilities/8968
    Reference: https://www.debian.org/security/2018/dsa-4090
    Reference: https://lists.debian.org/debian-lts-
announce/2017/12/msg00019.html
    Reference:
https://github.com/WordPress/WordPress/commit/f1de7e42df29395c3314bf85bff3
d1f4f90541de
    Reference:
https://github.com/WordPress/WordPress/commit/67d03a98c2cae5f41843c897f206
adde299b0509
    Reference:
https://github.com/WordPress/WordPress/commit/eaf1cfdc1fe0bdffabd8d879c591
b864d833326c
    Reference: https://make.wordpress.org/core/2017/11/28/wordpress-4-9-1-
scheduled-for-november-29th/
    Reference: https://wpvulndb.com/vulnerabilities/8966
    Reference: https://wpvulndb.com/vulnerabilities/8969
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
17093
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
17092
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
17094
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
17091
[i] CVSS: 3.5
```

```
[i] Fixed in: 4.9.1

[!] Title: wp-includes/functions.php in WordPress does not require the
unfiltered_html capability for upload of .js files, which might allow
remote attackers to conduct XSS attacks via a crafted file
    Reference: https://codex.wordpress.org/Version_4.9.1
    Reference:
https://github.com/WordPress/WordPress/commit/67d03a98c2cae5f41843c897f206
adde299b0509
    Reference: https://wordpress.org/news/2017/11/wordpress-4-9-1-
security-and-maintenance-release/
    Reference: https://wpvulndb.com/vulnerabilities/8966
    Reference: https://www.debian.org/security/2018/dsa-4090
    Reference:
https://github.com/WordPress/WordPress/commit/3713ac5ebc90fb2011e98dfd6914
20f43da6c09a
    Reference:
https://github.com/WordPress/WordPress/commit/f1de7e42df29395c3314bf85bff3
d1f4f90541de
    Reference:
https://github.com/WordPress/WordPress/commit/eaf1cfdc1fe0bdffabd8d879c591
b864d833326c
    Reference: https://make.wordpress.org/core/2017/11/28/wordpress-4-9-1-
scheduled-for-november-29th/
    Reference: https://lists.debian.org/debian-lts-
announce/2017/12/msg00019.html
    Reference: https://wpvulndb.com/vulnerabilities/8969
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
17092
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
17093
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
17091
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
17094
[i] CVSS: 3.5
[i] Fixed in: 4.9.1

[!] Title: wp-admin/user-new.php in WordPress sets the newbloguser key to
a string that can be directly derived from the user ID, which allows
remote attackers to bypass intended access restrictions by entering this
string
    Reference: https://codex.wordpress.org/Version_4.9.1
    Reference:
https://github.com/WordPress/WordPress/commit/eaf1cfdc1fe0bdffabd8d879c591
b864d833326c
    Reference: https://wordpress.org/news/2017/11/wordpress-4-9-1-
security-and-maintenance-release/
    Reference: https://wpvulndb.com/vulnerabilities/8969
    Reference: https://www.debian.org/security/2018/dsa-4090
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
17091
[i] CVSS: 6.5
[i] Fixed in: 4.9.1
```

```
[!] Title: WordPress has XSS in the Flash fallback files in MediaElement
(under wp-includes/js/mediaelement)
    Reference: https://codex.wordpress.org/Version_4.9.2
    Reference:
https://github.com/WordPress/WordPress/commit/3fe9cb61ee71fcfadb5e002399296fcc1198d850
    Reference: https://wordpress.org/news/2018/01/wordpress-4-9-2-security-and-maintenance-release/
    Reference: https://wpvulndb.com/vulnerabilities/9006
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-5776
[i] CVSS: 4.3
[i] Fixed in: 4.9.2

[!] Title: WordPress Cross Site Scripting And Directory Traversal
Vulnerabilities
    Reference:
https://github.com/WordPress/WordPress/commit/c9e60dab176635d4bfaaf431c0ea891e4726d6e0
    Reference:
https://github.com/WordPress/WordPress/commit/54720a14d85bc1197ded7cb09bd3ea790caa0b6e
    Reference: https://wordpress.org/news/2016/09/wordpress-4-6-1-security-and-maintenance-release/
    Reference: https://codex.wordpress.org/Version_4.6.1
    Reference: http://www.openwall.com/lists/oss-security/2016/09/08/19
    Reference: http://www.openwall.com/lists/oss-security/2016/09/08/24
    Reference:
https://sumofpwn.nl/advisory/2016/persistent_cross_site_scripting_vulnerability_in_wordpress_due_to_unsafe_processing_of_file_names.html
    Reference: https://wpvulndb.com/vulnerabilities/8615
    Reference: https://wpvulndb.com/vulnerabilities/8616
    Reference: http://www.debian.org/security/2016/dsa-3681
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7168
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7169
[i] CVSS: 3.5
[i] Fixed in: 4.6.1

[!] Title: WordPress CVE-2016-6897 Cross Site Request Forgery
Vulnerability
    Reference: https://core.trac.wordpress.org/ticket/37490
    Reference:
https://sumofpwn.nl/advisory/2016/path_traversal_vulnerability_in_wordpress_core_ajax_handlers.html
    Reference: http://www.openwall.com/lists/oss-security/2016/08/20/1
    Reference:
https://github.com/WordPress/WordPress/commit/8c82515ab62b88fb32d01c9778f0204b296f3568
    Reference: https://wpvulndb.com/vulnerabilities/8606
    Reference: http://www.securitytracker.com/id/1036683
    Reference: https://www.exploit-db.com/exploits/40288/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
6897
[i] CVSS: 4.3
[i] Fixed in: 4.6

[!] Title: WordPress 'ajax-actions.php' Directory Traversal Vulnerability
    Reference: https://core.trac.wordpress.org/ticket/37490#no0
    Reference:
https://sumofpwn.nl/advisory/2016/path_traversal_vulnerability_in_wordpres
s_core_ajax_handlers.html
    Reference: http://www.openwall.com/lists/oss-security/2016/08/20/1
    Reference: https://wpvulndb.com/vulnerabilities/8606
    Reference: http://www.securitytracker.com/id/1036683
    Reference: https://www.exploit-db.com/exploits/40288/
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-
6896
[i] CVSS: 5.5
[i] Fixed in: 4.6

[!] Title: WordPress Prior to 4.7.2 Multiple Security Vulnerabilities
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-2-
security-release/
    Reference:
https://github.com/WordPress/WordPress/commit/4482f9207027de8f36630737ae08
5110896ea849
    Reference:
https://github.com/WordPress/WordPress/commit/21264a31e0849e6ff793a06a17de
877dd88ea454
    Reference:
https://github.com/WordPress/WordPress/commit/85384297a60900004e27e417eac5
6d24267054cb
    Reference: http://www.openwall.com/lists/oss-security/2017/01/28/5
    Reference: https://codex.wordpress.org/Version_4.7.2
    Reference: http://www.securitytracker.com/id/1037731
    Reference: https://wpvulndb.com/vulnerabilities/8729
    Reference: https://wpvulndb.com/vulnerabilities/8730
    Reference: https://wpvulndb.com/vulnerabilities/8731
    Reference: http://www.debian.org/security/2017/dsa-3779
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
5611
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
5610
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
5612
[i] CVSS: 5.0
[i] Fixed in: 4.7.2

[!] Title: WordPress 'class-wp-rest-posts-controller.php' Privilege
Escalation Vulnerability
    Reference: https://blog.sucuri.net/2017/02/content-injection-
vulnerability-wordpress-rest-api.html
    Reference: https://blogs.akamai.com/2017/02/wordpress-web-api-
vulnerability.html
```

```
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-2-
security-release/
[i] Fixed in: 4.7.2

[!] Title: WordPress Prior to 4.8.2 Multiple Input Validation Security
Vulnerabilities (4.3+)
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-
security-and-maintenance-release/
[i] Fixed in: 4.3.12

[!] Title: WordPress versions 4.8.2 and earlier $wpdb->prepare() potential
SQL injection (SQLi).
    Reference:
https://github.com/WordPress/WordPress/commit/a2693fd8602e3263b5925b9d799d
dd577202167d
    Reference: https://wordpress.org/news/2017/10/wordpress-4-8-3-
security-release/
    Reference: https://blog.ircmaxell.com/2017/10/disclosure-wordpress-
wpdb-sql-injection-technical.html
    Reference: https://codex.wordpress.org/Version_4.8.3
    Reference: https://wpvulndb.com/vulnerabilities/8941
    Reference: https://www.debian.org/security/2018/dsa-4090
    Reference: https://lists.debian.org/debian-lts-
announce/2017/11/msg00003.html
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-
16510
[i] CVSS: 7.5
[i] Fixed in: 4.8.3

[!] Title: WordPress Prior to 4.9.1 Multiple Security Vulnerabilities
    Reference: https://make.wordpress.org/core/2017/11/28/wordpress-4-9-1-
scheduled-for-november-29th/
    Reference: https://wordpress.org/news/2017/11/wordpress-4-9-1-
security-and-maintenance-release/
[i] Fixed in: 4.9.1

[+] Enumerating installed plugins  ...

   Time: 00:03:49
<=========================================================================
==========================================================> (1829 / 1829)
100.00% Time: 00:03:49

[+] We found 11 plugins:

[+] Name: akismet
 |  Location: http://10.10.172.31/wp-content/plugins/akismet/

[+] Name: all-in-one-seo-pack - v2.0.4
 |  Location: http://10.10.172.31/wp-content/plugins/all-in-one-seo-pack/
 |  Readme: http://10.10.172.31/wp-content/plugins/all-in-one-seo-
pack/readme.txt
```

```
[!] Title: All in One SEO Pack <= 2.1.5 - aioseop_functions.php new_meta
Parameter XSS
    Reference: http://blog.sucuri.net/2014/05/vulnerability-found-in-the-
all-in-one-seo-pack-wordpress-plugin.html
    Reference: http://osvdb.org/107640
    Reference: https://wpvulndb.com/vulnerabilities/6888
[i] Fixed in: 2.1.6

[!] Title: All in One SEO Pack <= 2.1.5 - Unspecified Privilege Escalation
    Reference: http://blog.sucuri.net/2014/05/vulnerability-found-in-the-
all-in-one-seo-pack-wordpress-plugin.html
    Reference: http://osvdb.org/107641
    Reference: https://wpvulndb.com/vulnerabilities/6889
[i] Fixed in: 2.1.6

[+] Name: all-in-one-wp-migration - v2.0.4
 |  Location: http://10.10.172.31/wp-content/plugins/all-in-one-wp-
migration/
 |  Readme: http://10.10.172.31/wp-content/plugins/all-in-one-wp-
migration/readme.txt

[+] Name: contact-form-7 - v4.1
 |  Location: http://10.10.172.31/wp-content/plugins/contact-form-7/
 |  Readme: http://10.10.172.31/wp-content/plugins/contact-form-
7/readme.txt

[+] Name: feed
 |  Location: http://10.10.172.31/wp-content/plugins/feed/

[+] We could not determine a version so all vulnerabilities are printed
out

[!] Title: Feed - news_dt.php nid Parameter SQL Injection
    Reference: http://packetstormsecurity.com/files/122260/
    Reference: http://osvdb.org/94804
    Reference: https://wpvulndb.com/vulnerabilities/6965

[+] Name: google-analytics-for-wordpress - v5.3.2
 |  Location: http://10.10.172.31/wp-content/plugins/google-analytics-for-
wordpress/
 |  Readme: http://10.10.172.31/wp-content/plugins/google-analytics-for-
wordpress/readme.txt

[+] Name: google-sitemap-generator - v4.0.7.1
 |  Location: http://10.10.172.31/wp-content/plugins/google-sitemap-
generator/
 |  Readme: http://10.10.172.31/wp-content/plugins/google-sitemap-
generator/readme.txt

[+] Name: jetpack - v3.3.2
 |  Location: http://10.10.172.31/wp-content/plugins/jetpack/
 |  Readme: http://10.10.172.31/wp-content/plugins/jetpack/readme.txt
```

```
[!] Title: ** DISPUTED ** SQL injection vulnerability in
modules/sharedaddy.php in the Jetpack plugin for WordPress allows remote
attackers to execute arbitrary SQL commands via the id parameter
    Reference: http://xforce.iss.net/xforce/xfdb/71404
    Reference: http://www.securityfocus.com/bid/50730
    Reference: http://www.exploit-db.com/exploits/18126
    Reference: https://exchange.xforce.ibmcloud.com/vulnerabilities/71404
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-
4673
[i] CVSS: 7.5

[!] Title: WordPress Jetpack Plugin HTML Injection Vulnerability (2.0+)
    Reference: https://jetpack.com/2016/05/27/jetpack-4-0-3-critical-
security-update/
    Reference: http://wptavern.com/jetpack-4-0-3-patches-a-critical-xss-
vulnerability
[i] Fixed in: 4.0.3

[+] Name: simple-tags - v2.4.1
 |  Location: http://10.10.172.31/wp-content/plugins/simple-tags/
 |  Readme: http://10.10.172.31/wp-content/plugins/simple-tags/readme.txt

[+] Name: wp-mail-smtp - v0.9.5
 |  Location: http://10.10.172.31/wp-content/plugins/wp-mail-smtp/
 |  Readme: http://10.10.172.31/wp-content/plugins/wp-mail-smtp/readme.txt

[+] Name: wptouch - v3.7.3
 |  Location: http://10.10.172.31/wp-content/plugins/wptouch/
 |  Readme: http://10.10.172.31/wp-content/plugins/wptouch/readme.txt

[!] Title: WPtouch 1.9.19.4 - Cross-Site Scripting (XSS)
    Reference: http://www.securityfocus.com/bid/45139
    Reference:
http://www.htbridge.ch/advisory/xss_in_wptouch_wordpress_plugin.html
    Reference: http://osvdb.org/69538
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-
4779
    Reference: https://secunia.com/advisories/42438
    Reference: http://osvdb.org/69538
    Reference: https://wpvulndb.com/vulnerabilities/7120
[i] CVSS: 4.3

[!] Title: SQL injection vulnerability in wptouch/ajax.php in the WPTouch
plugin for WordPress allows remote attackers to execute arbitrary SQL
commands via the id parameter
    Reference: http://www.exploit-db.com/exploits/18039
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-
4803
[i] CVSS: 7.5

[+] Finished: Mon May 17 18:53:21 2021
[+] Memory used: 226.328 MB
[+] Elapsed time: 00:04:07
[+] Enumerating installed plugins  ...
```

```
   Time: 00:03:49
<==========================================================================
===============================================================> (1829 / 1829)
100.00% Time: 00:03:49

[+] We found 11 plugins:

[+] Name: akismet
 |  Location: http://10.10.172.31/wp-content/plugins/akismet/

[+] Name: all-in-one-seo-pack - v2.0.4
 |  Location: http://10.10.172.31/wp-content/plugins/all-in-one-seo-pack/
 |  Readme: http://10.10.172.31/wp-content/plugins/all-in-one-seo-
pack/readme.txt

[!] Title: All in One SEO Pack <= 2.1.5 - aioseop_functions.php new_meta
Parameter XSS
    Reference: http://blog.sucuri.net/2014/05/vulnerability-found-in-the-
all-in-one-seo-pack-wordpress-plugin.html
    Reference: http://osvdb.org/107640
    Reference: https://wpvulndb.com/vulnerabilities/6888
[i] Fixed in: 2.1.6

[!] Title: All in One SEO Pack <= 2.1.5 - Unspecified Privilege Escalation
    Reference: http://blog.sucuri.net/2014/05/vulnerability-found-in-the-
all-in-one-seo-pack-wordpress-plugin.html
    Reference: http://osvdb.org/107641
    Reference: https://wpvulndb.com/vulnerabilities/6889
[i] Fixed in: 2.1.6

[+] Name: all-in-one-wp-migration - v2.0.4
 |  Location: http://10.10.172.31/wp-content/plugins/all-in-one-wp-
migration/
 |  Readme: http://10.10.172.31/wp-content/plugins/all-in-one-wp-
migration/readme.txt

[+] Name: contact-form-7 - v4.1
 |  Location: http://10.10.172.31/wp-content/plugins/contact-form-7/
 |  Readme: http://10.10.172.31/wp-content/plugins/contact-form-
7/readme.txt

[+] Name: feed
 |  Location: http://10.10.172.31/wp-content/plugins/feed/

[+] We could not determine a version so all vulnerabilities are printed
out

[!] Title: Feed - news_dt.php nid Parameter SQL Injection
    Reference: http://packetstormsecurity.com/files/122260/
    Reference: http://osvdb.org/94804
    Reference: https://wpvulndb.com/vulnerabilities/6965

[+] Name: google-analytics-for-wordpress - v5.3.2
```

```
 |  Location: http://10.10.172.31/wp-content/plugins/google-analytics-for-
wordpress/
 |  Readme: http://10.10.172.31/wp-content/plugins/google-analytics-for-
wordpress/readme.txt

[+] Name: google-sitemap-generator - v4.0.7.1
 |  Location: http://10.10.172.31/wp-content/plugins/google-sitemap-
generator/
 |  Readme: http://10.10.172.31/wp-content/plugins/google-sitemap-
generator/readme.txt

[+] Name: jetpack - v3.3.2
 |  Location: http://10.10.172.31/wp-content/plugins/jetpack/
 |  Readme: http://10.10.172.31/wp-content/plugins/jetpack/readme.txt

[!] Title: ** DISPUTED ** SQL injection vulnerability in
modules/sharedaddy.php in the Jetpack plugin for WordPress allows remote
attackers to execute arbitrary SQL commands via the id parameter
    Reference: http://xforce.iss.net/xforce/xfdb/71404
    Reference: http://www.securityfocus.com/bid/50730
    Reference: http://www.exploit-db.com/exploits/18126
    Reference: https://exchange.xforce.ibmcloud.com/vulnerabilities/71404
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-
4673
[i] CVSS: 7.5

[!] Title: WordPress Jetpack Plugin HTML Injection Vulnerability (2.0+)
    Reference: https://jetpack.com/2016/05/27/jetpack-4-0-3-critical-
security-update/
    Reference: http://wptavern.com/jetpack-4-0-3-patches-a-critical-xss-
vulnerability
[i] Fixed in: 4.0.3

[+] Name: simple-tags - v2.4.1
 |  Location: http://10.10.172.31/wp-content/plugins/simple-tags/
 |  Readme: http://10.10.172.31/wp-content/plugins/simple-tags/readme.txt

[+] Name: wp-mail-smtp - v0.9.5
 |  Location: http://10.10.172.31/wp-content/plugins/wp-mail-smtp/
 |  Readme: http://10.10.172.31/wp-content/plugins/wp-mail-smtp/readme.txt

[+] Name: wptouch - v3.7.3
 |  Location: http://10.10.172.31/wp-content/plugins/wptouch/
 |  Readme: http://10.10.172.31/wp-content/plugins/wptouch/readme.txt

[!] Title: WPtouch 1.9.19.4 - Cross-Site Scripting (XSS)
    Reference: http://www.securityfocus.com/bid/45139
    Reference:
http://www.htbridge.ch/advisory/xss_in_wptouch_wordpress_plugin.html
    Reference: http://osvdb.org/69538
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-
4779
    Reference: https://secunia.com/advisories/42438
    Reference: http://osvdb.org/69538
    Reference: https://wpvulndb.com/vulnerabilities/7120
[i] CVSS: 4.3

[!] Title: SQL injection vulnerability in wptouch/ajax.php in the WPTouch
plugin for WordPress allows remote attackers to execute arbitrary SQL
commands via the id parameter
    Reference: http://www.exploit-db.com/exploits/18039
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-
4803
[i] CVSS: 7.5

[+] Finished: Mon May 17 18:58:21 2021
[+] Memory used: 226.328 MB
[+] Elapsed time: 00:04:07
[+] Enumerating installed plugins  ...

   Time: 00:03:49
<=========================================================================
==========================================================> (1829 / 1829)
100.00% Time: 00:03:49

[+] We found 11 plugins:

[+] Name: akismet
 |  Location: http://10.10.172.31/wp-content/plugins/akismet/

[+] Name: all-in-one-seo-pack - v2.0.4
 |  Location: http://10.10.172.31/wp-content/plugins/all-in-one-seo-pack/
 |  Readme: http://10.10.172.31/wp-content/plugins/all-in-one-seo-
pack/readme.txt

[!] Title: All in One SEO Pack <= 2.1.5 - aioseop_functions.php new_meta
Parameter XSS
    Reference: http://blog.sucuri.net/2014/05/vulnerability-found-in-the-
all-in-one-seo-pack-wordpress-plugin.html
    Reference: http://osvdb.org/107640
    Reference: https://wpvulndb.com/vulnerabilities/6888
[i] Fixed in: 2.1.6

[!] Title: All in One SEO Pack <= 2.1.5 - Unspecified Privilege Escalation
    Reference: http://blog.sucuri.net/2014/05/vulnerability-found-in-the-
all-in-one-seo-pack-wordpress-plugin.html
    Reference: http://osvdb.org/107641
    Reference: https://wpvulndb.com/vulnerabilities/6889
[i] Fixed in: 2.1.6

[+] Name: all-in-one-wp-migration - v2.0.4
 |  Location: http://10.10.172.31/wp-content/plugins/all-in-one-wp-
migration/
 |  Readme: http://10.10.172.31/wp-content/plugins/all-in-one-wp-
migration/readme.txt

[+] Name: contact-form-7 - v4.1
 |  Location: http://10.10.172.31/wp-content/plugins/contact-form-7/
 |  Readme: http://10.10.172.31/wp-content/plugins/contact-form-
7/readme.txt

[+] Name: feed
 |  Location: http://10.10.172.31/wp-content/plugins/feed/

[+] We could not determine a version so all vulnerabilities are printed
out

[!] Title: Feed - news_dt.php nid Parameter SQL Injection
    Reference: http://packetstormsecurity.com/files/122260/
    Reference: http://osvdb.org/94804
    Reference: https://wpvulndb.com/vulnerabilities/6965

[+] Name: google-analytics-for-wordpress - v5.3.2
 |  Location: http://10.10.172.31/wp-content/plugins/google-analytics-for-
wordpress/
 |  Readme: http://10.10.172.31/wp-content/plugins/google-analytics-for-
wordpress/readme.txt

[+] Name: google-sitemap-generator - v4.0.7.1
 |  Location: http://10.10.172.31/wp-content/plugins/google-sitemap-
generator/
 |  Readme: http://10.10.172.31/wp-content/plugins/google-sitemap-
generator/readme.txt

[+] Name: jetpack - v3.3.2
 |  Location: http://10.10.172.31/wp-content/plugins/jetpack/
 |  Readme: http://10.10.172.31/wp-content/plugins/jetpack/readme.txt

[!] Title: ** DISPUTED ** SQL injection vulnerability in
modules/sharedaddy.php in the Jetpack plugin for WordPress allows remote
attackers to execute arbitrary SQL commands via the id parameter
    Reference: http://xforce.iss.net/xforce/xfdb/71404
    Reference: http://www.securityfocus.com/bid/50730
    Reference: http://www.exploit-db.com/exploits/18126
    Reference: https://exchange.xforce.ibmcloud.com/vulnerabilities/71404
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-
4673
[i] CVSS: 7.5

[!] Title: WordPress Jetpack Plugin HTML Injection Vulnerability (2.0+)
    Reference: https://jetpack.com/2016/05/27/jetpack-4-0-3-critical-
security-update/
    Reference: http://wptavern.com/jetpack-4-0-3-patches-a-critical-xss-
vulnerability
[i] Fixed in: 4.0.3

[+] Name: simple-tags - v2.4.1
 |  Location: http://10.10.172.31/wp-content/plugins/simple-tags/
 |  Readme: http://10.10.172.31/wp-content/plugins/simple-tags/readme.txt

[+] Name: wp-mail-smtp - v0.9.5
 |  Location: http://10.10.172.31/wp-content/plugins/wp-mail-smtp/
 |  Readme: http://10.10.172.31/wp-content/plugins/wp-mail-smtp/readme.txt

[+] Name: wptouch - v3.7.3
 |  Location: http://10.10.172.31/wp-content/plugins/wptouch/
 |  Readme: http://10.10.172.31/wp-content/plugins/wptouch/readme.txt

[!] Title: WPtouch 1.9.19.4 - Cross-Site Scripting (XSS)
    Reference: http://www.securityfocus.com/bid/45139
    Reference:
http://www.htbridge.ch/advisory/xss_in_wptouch_wordpress_plugin.html
    Reference: http://osvdb.org/69538
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-
4779
    Reference: https://secunia.com/advisories/42438
    Reference: http://osvdb.org/69538
    Reference: https://wpvulndb.com/vulnerabilities/7120
[i] CVSS: 4.3

[!] Title: SQL injection vulnerability in wptouch/ajax.php in the WPTouch
plugin for WordPress allows remote attackers to execute arbitrary SQL
commands via the id parameter
    Reference: http://www.exploit-db.com/exploits/18039
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-
4803
[i] CVSS: 7.5

[+] Finished: Mon May 17 18:53:21 2021
[+] Memory used: 226.328 MB
[+] Elapsed time: 00:04:07
[+] Enumerating installed plugins  ...

   Time: 00:03:49
<=========================================================================
==========================================================> (1829 / 1829)
100.00% Time: 00:03:49

[+] We found 11 plugins:

[+] Name: akismet
 |  Location: http://10.10.172.31/wp-content/plugins/akismet/

[+] Name: all-in-one-seo-pack - v2.0.4
 |  Location: http://10.10.172.31/wp-content/plugins/all-in-one-seo-pack/
 |  Readme: http://10.10.172.31/wp-content/plugins/all-in-one-seo-
pack/readme.txt

[!] Title: All in One SEO Pack <= 2.1.5 - aioseop_functions.php new_meta
Parameter XSS
    Reference: http://blog.sucuri.net/2014/05/vulnerability-found-in-the-
all-in-one-seo-pack-wordpress-plugin.html
    Reference: http://osvdb.org/107640
    Reference: https://wpvulndb.com/vulnerabilities/6888
[i] Fixed in: 2.1.6
```

```
[!] Title: All in One SEO Pack <= 2.1.5 - Unspecified Privilege Escalation
    Reference: http://blog.sucuri.net/2014/05/vulnerability-found-in-the-
all-in-one-seo-pack-wordpress-plugin.html
    Reference: http://osvdb.org/107641
    Reference: https://wpvulndb.com/vulnerabilities/6889
[i] Fixed in: 2.1.6

[+] Name: all-in-one-wp-migration - v2.0.4
 |  Location: http://10.10.172.31/wp-content/plugins/all-in-one-wp-
migration/
 |  Readme: http://10.10.172.31/wp-content/plugins/all-in-one-wp-
migration/readme.txt

[+] Name: contact-form-7 - v4.1
 |  Location: http://10.10.172.31/wp-content/plugins/contact-form-7/
 |  Readme: http://10.10.172.31/wp-content/plugins/contact-form-
7/readme.txt

[+] Name: feed
 |  Location: http://10.10.172.31/wp-content/plugins/feed/

[+] We could not determine a version so all vulnerabilities are printed
out

[!] Title: Feed - news_dt.php nid Parameter SQL Injection
    Reference: http://packetstormsecurity.com/files/122260/
    Reference: http://osvdb.org/94804
    Reference: https://wpvulndb.com/vulnerabilities/6965

[+] Name: google-analytics-for-wordpress - v5.3.2
 |  Location: http://10.10.172.31/wp-content/plugins/google-analytics-for-
wordpress/
 |  Readme: http://10.10.172.31/wp-content/plugins/google-analytics-for-
wordpress/readme.txt

[+] Name: google-sitemap-generator - v4.0.7.1
 |  Location: http://10.10.172.31/wp-content/plugins/google-sitemap-
generator/
 |  Readme: http://10.10.172.31/wp-content/plugins/google-sitemap-
generator/readme.txt

[+] Name: jetpack - v3.3.2
 |  Location: http://10.10.172.31/wp-content/plugins/jetpack/
 |  Readme: http://10.10.172.31/wp-content/plugins/jetpack/readme.txt

[!] Title: ** DISPUTED ** SQL injection vulnerability in
modules/sharedaddy.php in the Jetpack plugin for WordPress allows remote
attackers to execute arbitrary SQL commands via the id parameter
    Reference: http://xforce.iss.net/xforce/xfdb/71404
    Reference: http://www.securityfocus.com/bid/50730
    Reference: http://www.exploit-db.com/exploits/18126
    Reference: https://exchange.xforce.ibmcloud.com/vulnerabilities/71404
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-
4673
```

```
[i] CVSS: 7.5

[!] Title: WordPress Jetpack Plugin HTML Injection Vulnerability (2.0+)
    Reference: https://jetpack.com/2016/05/27/jetpack-4-0-3-critical-
security-update/
    Reference: http://wptavern.com/jetpack-4-0-3-patches-a-critical-xss-
vulnerability
[i] Fixed in: 4.0.3

[+] Name: simple-tags - v2.4.1
 |  Location: http://10.10.172.31/wp-content/plugins/simple-tags/
 |  Readme: http://10.10.172.31/wp-content/plugins/simple-tags/readme.txt

[+] Name: wp-mail-smtp - v0.9.5
 |  Location: http://10.10.172.31/wp-content/plugins/wp-mail-smtp/
 |  Readme: http://10.10.172.31/wp-content/plugins/wp-mail-smtp/readme.txt

[+] Name: wptouch - v3.7.3
 |  Location: http://10.10.172.31/wp-content/plugins/wptouch/
 |  Readme: http://10.10.172.31/wp-content/plugins/wptouch/readme.txt

[!] Title: WPtouch 1.9.19.4 - Cross-Site Scripting (XSS)
    Reference: http://www.securityfocus.com/bid/45139
    Reference:
http://www.htbridge.ch/advisory/xss_in_wptouch_wordpress_plugin.html
    Reference: http://osvdb.org/69538
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-
4779
    Reference: https://secunia.com/advisories/42438
    Reference: http://osvdb.org/69538
    Reference: https://wpvulndb.com/vulnerabilities/7120
[i] CVSS: 4.3

[!] Title: SQL injection vulnerability in wptouch/ajax.php in the WPTouch
plugin for WordPress allows remote attackers to execute arbitrary SQL
commands via the id parameter
    Reference: http://www.exploit-db.com/exploits/18039
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-
4803
[i] CVSS: 7.5

[+] Finished: Mon May 17 18:53:21 2021
[+] Memory used: 226.328 MB
[+] Elapsed time: 00:04:07
```

## APPENDIX L – MR ROBOT - WPSCAN

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

        WordPress Security Scanner by the WPScan Team
                       Version 3.8.10
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.172.31/ [10.10.172.31]
[+] Started: Mon May 17 17:59:18 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache
 |  - X-Mod-Pagespeed: 1.9.32.3-4523
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.10.172.31/robots.txt
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.172.31/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] The external WP-Cron seems to be enabled: http://10.10.172.31/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.3.1 identified (Insecure, released on 2015-09-15).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.172.31/37cec58.html, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=4.3.1'
```

```
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.172.31/37cec58.html, Match: 'WordPress 4.3.1'

[+] WordPress theme in use: twentyfifteen
 | Location: http://10.10.172.31/wp-content/themes/twentyfifteen/
 | Last Updated: 2021-03-09T00:00:00.000Z
 | Readme: http://10.10.172.31/wp-content/themes/twentyfifteen/readme.txt
 | [!] The version is out of date, the latest version is 2.9
 | Style URL: http://10.10.172.31/wp-
content/themes/twentyfifteen/style.css?ver=4.3.1
 | Style Name: Twenty Fifteen
 | Style URI: https://wordpress.org/themes/twentyfifteen/
 | Description: Our 2015 default theme is clean, blog-focused, and
designed for clarity. Twenty Fifteen's simple, st...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In 404 Page (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.10.172.31/wp-
content/themes/twentyfifteen/style.css?ver=4.3.1, Match: 'Version: 1.3'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:43
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:43
[+] Checking Theme Versions (via Passive and Aggressive Methods)

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:03:10
<=========================================================================
=================================> (2575 / 2575) 100.00% Time: 00:03:10

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:19
<=========================================================================
===================================> (137 / 137) 100.00% Time: 00:00:19

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:09
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:09

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:00

[i] No Users Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 18:03:51 2021
[+] Requests Done: 3193
[+] Cached Requests: 10
[+] Data Sent: 1.024 MB
[+] Data Received: 1.259 MB
[+] Memory used: 254.57 MB
[+] Elapsed time: 00:04:32
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.172.31/ [10.10.172.31]
[+] Started: Mon May 17 18:03:53 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache
 |  - X-Mod-Pagespeed: 1.9.32.3-4523
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.10.172.31/robots.txt
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%
```

```
[+] XML-RPC seems to be enabled: http://10.10.172.31/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] The external WP-Cron seems to be enabled: http://10.10.172.31/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.3.1 identified (Insecure, released on 2015-09-15).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.172.31/59ddf97.html, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=4.3.1'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.172.31/59ddf97.html, Match: 'WordPress 4.3.1'

[+] WordPress theme in use: twentyfifteen
 | Location: http://10.10.172.31/wp-content/themes/twentyfifteen/
 | Last Updated: 2021-03-09T00:00:00.000Z
 | Readme: http://10.10.172.31/wp-content/themes/twentyfifteen/readme.txt
 | [!] The version is out of date, the latest version is 2.9
 | Style URL: http://10.10.172.31/wp-
content/themes/twentyfifteen/style.css?ver=4.3.1
 | Style Name: Twenty Fifteen
 | Style URI: https://wordpress.org/themes/twentyfifteen/
 | Description: Our 2015 default theme is clean, blog-focused, and
designed for clarity. Twenty Fifteen's simple, st...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In 404 Page (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.10.172.31/wp-
content/themes/twentyfifteen/style.css?ver=4.3.1, Match: 'Version: 1.3'

[+] Enumerating All Plugins (via Passive Methods)
```

```
[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:48
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:48
[+] Checking Theme Versions (via Passive and Aggressive Methods)

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:06:01
<=========================================================================
=================================> (2575 / 2575) 100.00% Time: 00:06:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:19
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:19

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:09
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:09

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:01

[i] No Users Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 18:11:21 2021
[+] Requests Done: 3193
[+] Cached Requests: 10
[+] Data Sent: 1011.827 KB
[+] Data Received: 1.259 MB
[+] Memory used: 253.457 MB
[+] Elapsed time: 00:07:28
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.172.31/ [10.10.172.31]
[+] Started: Mon May 17 18:11:23 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache
 |  - X-Mod-Pagespeed: 1.9.32.3-4523
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.10.172.31/robots.txt
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.172.31/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] The external WP-Cron seems to be enabled: http://10.10.172.31/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.3.1 identified (Insecure, released on 2015-09-15).
```

```
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.172.31/7182b06.html, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=4.3.1'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.172.31/7182b06.html, Match: 'WordPress 4.3.1'

[+] WordPress theme in use: twentyfifteen
 | Location: http://10.10.172.31/wp-content/themes/twentyfifteen/
 | Last Updated: 2021-03-09T00:00:00.000Z
 | Readme: http://10.10.172.31/wp-content/themes/twentyfifteen/readme.txt
 | [!] The version is out of date, the latest version is 2.9
 | Style URL: http://10.10.172.31/wp-
content/themes/twentyfifteen/style.css?ver=4.3.1
 | Style Name: Twenty Fifteen
 | Style URI: https://wordpress.org/themes/twentyfifteen/
 | Description: Our 2015 default theme is clean, blog-focused, and
designed for clarity. Twenty Fifteen's simple, st...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In 404 Page (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.10.172.31/wp-
content/themes/twentyfifteen/style.css?ver=4.3.1, Match: 'Version: 1.3'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:48
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:48
[+] Checking Theme Versions (via Passive and Aggressive Methods)

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:04:34
<=========================================================================
=================================> (2575 / 2575) 100.00% Time: 00:04:34

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:19
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:19

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
```

```
 Checking DB Exports - Time: 00:00:09
<==========================================================================
=========================================> (71 / 71) 100.00% Time:
00:00:09

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<==========================================================================
====================================> (10 / 10) 100.00% Time: 00:00:01

[i] No Users Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 18:17:24 2021
[+] Requests Done: 3193
[+] Cached Requests: 10
[+] Data Sent: 915.073 KB
[+] Data Received: 1.259 MB
[+] Memory used: 252.957 MB
[+] Elapsed time: 00:06:00
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.172.31/ [10.10.172.31]
[+] Started: Mon May 17 18:17:27 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache
 |  - X-Mod-Pagespeed: 1.9.32.3-4523
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.10.172.31/robots.txt
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.172.31/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] The external WP-Cron seems to be enabled: http://10.10.172.31/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.3.1 identified (Insecure, released on 2015-09-15).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.172.31/780dbde.html, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=4.3.1'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.172.31/780dbde.html, Match: 'WordPress 4.3.1'

[+] WordPress theme in use: twentyfifteen
 | Location: http://10.10.172.31/wp-content/themes/twentyfifteen/
 | Last Updated: 2021-03-09T00:00:00.000Z
 | Readme: http://10.10.172.31/wp-content/themes/twentyfifteen/readme.txt
 | [!] The version is out of date, the latest version is 2.9
 | Style URL: http://10.10.172.31/wp-
content/themes/twentyfifteen/style.css?ver=4.3.1
 | Style Name: Twenty Fifteen
 | Style URI: https://wordpress.org/themes/twentyfifteen/
 | Description: Our 2015 default theme is clean, blog-focused, and
designed for clarity. Twenty Fifteen's simple, st...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In 404 Page (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.10.172.31/wp-
content/themes/twentyfifteen/style.css?ver=4.3.1, Match: 'Version: 1.3'
```

```
[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:48
<=========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:48
[+] Checking Theme Versions (via Passive and Aggressive Methods)

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:06:00
<=========================================================================
=================================> (2575 / 2575) 100.00% Time: 00:06:00

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:19
<=========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:19

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:09
<=========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:09

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<=========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:01

[i] No Users Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 18:24:55 2021
[+] Requests Done: 3193
[+] Cached Requests: 10
[+] Data Sent: 905.71 KB
[+] Data Received: 1.259 MB
[+] Memory used: 253.66 MB
[+] Elapsed time: 00:07:28
```

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

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.172.31/ [10.10.172.31]
[+] Started: Mon May 17 18:24:57 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache
 |  - X-Mod-Pagespeed: 1.9.32.3-4523
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.10.172.31/robots.txt
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.172.31/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_s
canner
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_
login
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingbac
k_access

[+] The external WP-Cron seems to be enabled: http://10.10.172.31/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299
```

```
[+] WordPress version 4.3.1 identified (Insecure, released on 2015-09-15).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.172.31/bceb3a3.html, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=4.3.1'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.172.31/bceb3a3.html, Match: 'WordPress 4.3.1'

[+] WordPress theme in use: twentyfifteen
 | Location: http://10.10.172.31/wp-content/themes/twentyfifteen/
 | Last Updated: 2021-03-09T00:00:00.000Z
 | Readme: http://10.10.172.31/wp-content/themes/twentyfifteen/readme.txt
 | [!] The version is out of date, the latest version is 2.9
 | Style URL: http://10.10.172.31/wp-
content/themes/twentyfifteen/style.css?ver=4.3.1
 | Style Name: Twenty Fifteen
 | Style URI: https://wordpress.org/themes/twentyfifteen/
 | Description: Our 2015 default theme is clean, blog-focused, and
designed for clarity. Twenty Fifteen's simple, st...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In 404 Page (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.10.172.31/wp-
content/themes/twentyfifteen/style.css?ver=4.3.1, Match: 'Version: 1.3'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:09
<==========================================================================
===================================> (348 / 348) 100.00% Time: 00:00:09
[+] Checking Theme Versions (via Passive and Aggressive Methods)

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:05:13
<==========================================================================
=================================> (2575 / 2575) 100.00% Time: 00:05:13

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:21
<==========================================================================
====================================> (137 / 137) 100.00% Time: 00:00:21

[i] No Config Backups Found.
```

```
[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:11
<========================================================================
==========================================> (71 / 71) 100.00% Time:
00:00:11

[i] No DB Exports Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<========================================================================
=====================================> (10 / 10) 100.00% Time: 00:00:01

[i] No Users Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not
been output.
[!] You can get a free API token with 50 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon May 17 18:31:02 2021
[+] Requests Done: 3193
[+] Cached Requests: 10
[+] Data Sent: 961.89 KB
[+] Data Received: 1.259 MB
[+] Memory used: 252.965 MB
[+] Elapsed time: 00:06:05
```