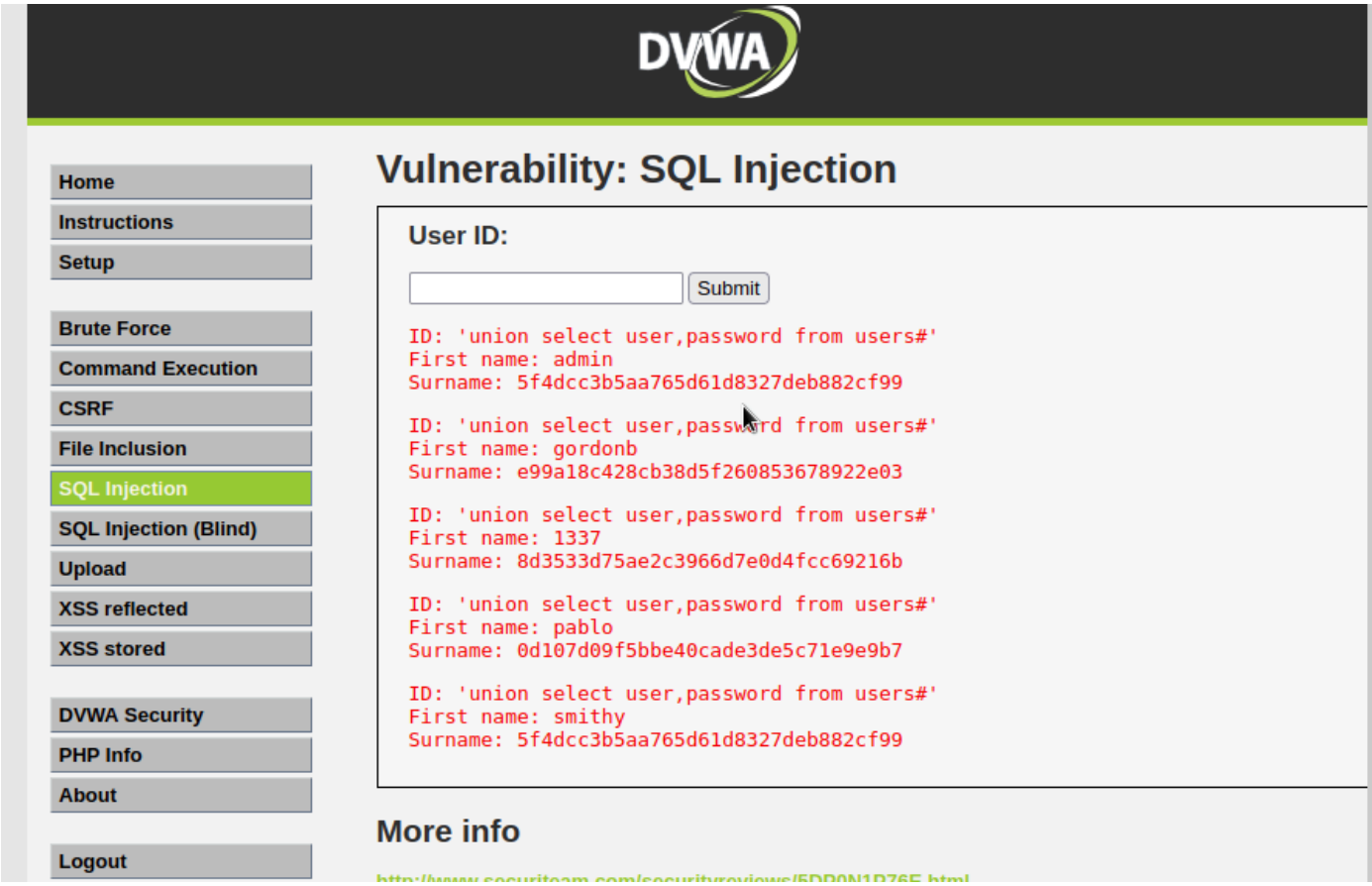
Password Cracking

E’ un processo di recupero delle password.

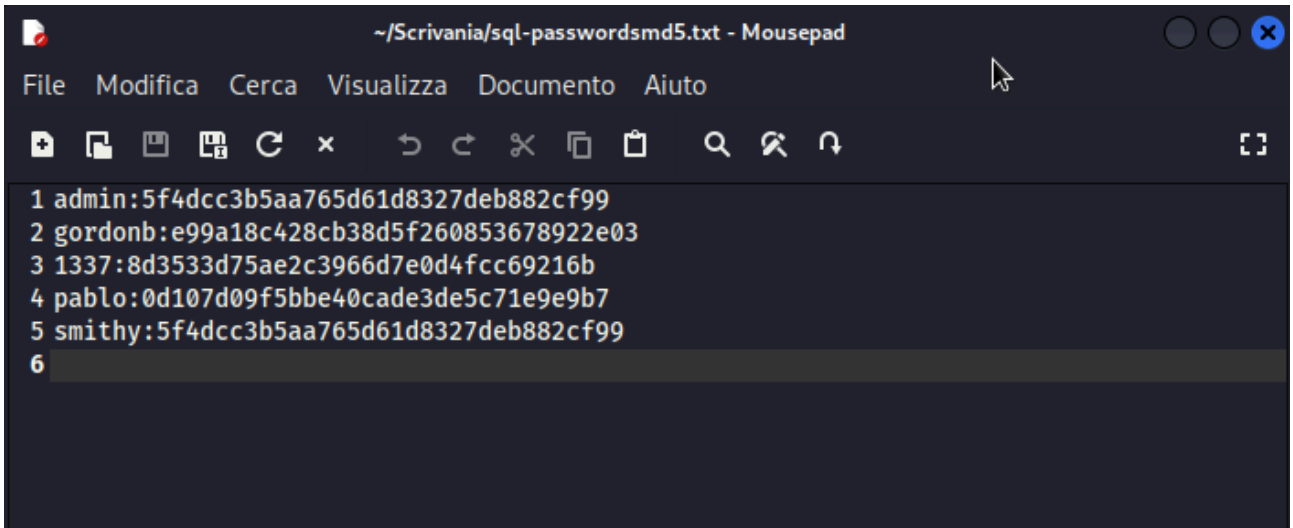
Oggi andremo a provare a craccare le password trovate ieri su DVWA con SQL injection



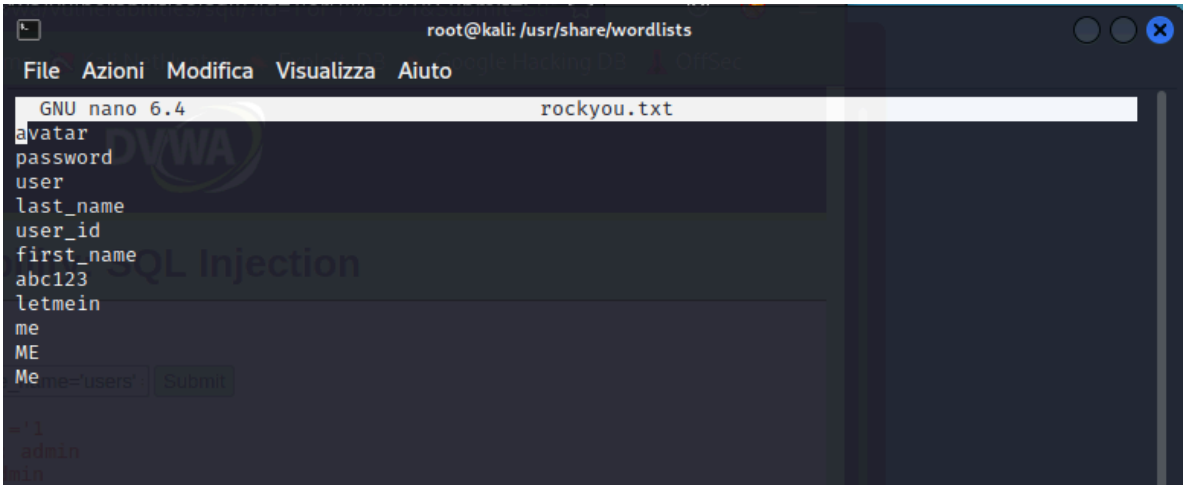
Come si può vedere nell’immagine le password degli utenti sono criptate.

Per andare a decriptare le password ho utilizzato john the ripper.

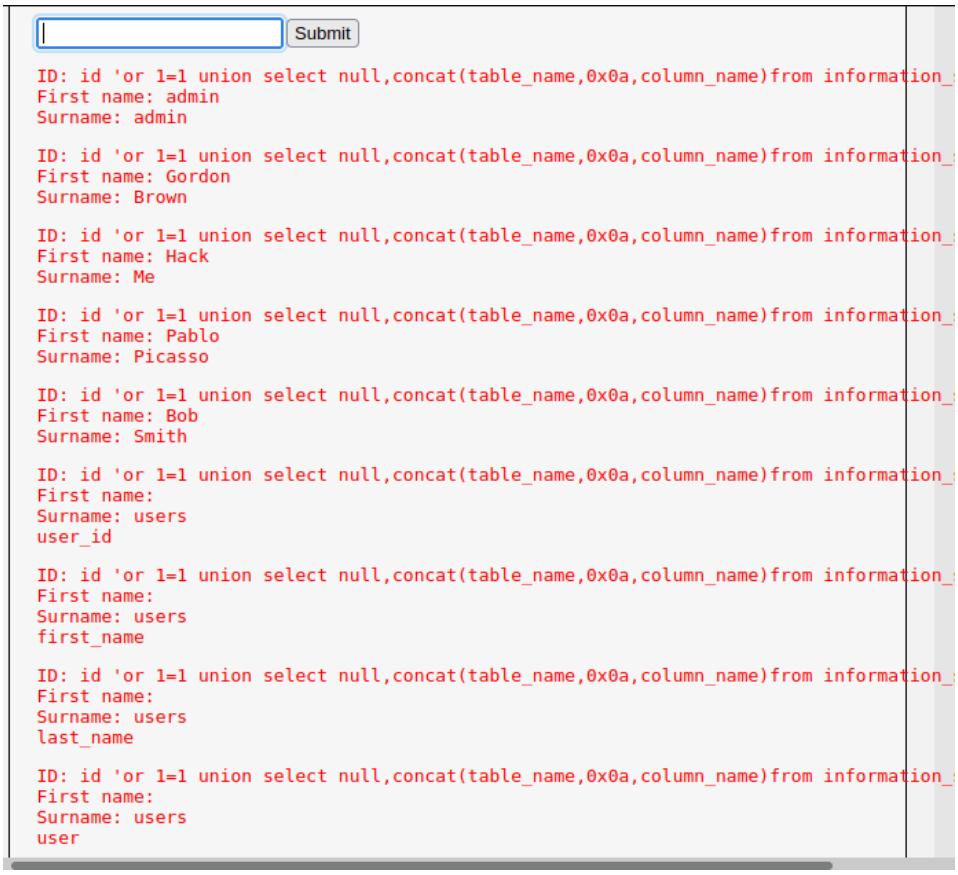
John the Ripper è uno strumento libero per il cracking delle password.



L’immagine che troviamo nella pagina precedente è un file con i nomi degli utenti e le password criptate, per poi metterle a confronto con un database di password per decriptarle.



Le password che sono state inserire in questo file sono state messe basandomi sui resultati di union dato che non riuscivo farlo funzionare con il file di john the ripper.



Il primo risultato che ho ottenuto è questo:

```
┌──(root㉿kali)-[/home/kali/Scrivania]
└─# john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt sql-passwordsmd5.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD 4×2])
Warning: no OpenMP support for this hash type, consider --fork=6
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 6 candidates left, minimum 8 needed for performance.
password         (admin)
1g 0:00:00:00 DONE (2022-08-10 18:31) 50.00g/s 300.0p/s 300.0c/s 1200C/s avatar..first_name
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.
```

Il quale mi mostra una password soltanto, rifacendo il comando non mostrava più niente.

```
┌──(root㉿kali)-[/home/kali/Scrivania]
└─# john --format=raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt sql-passwordsmd5.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD 4×2])
Remaining 3 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=6
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 6 candidates left, minimum 8 needed for performance.
0g 0:00:00:00 DONE (2022-08-10 18:40) 0g/s 600.0p/s 600.0c/s 1800C/s avatar..first_name
Session completed.
```

Aggiungendo altre password nella file rockyou.txt, ottenendo questo risultato:

```
┌──(root㉿kali)-[/home/kali/Scrivania]
└─# john --format=raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt sql-passwordsmd5.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD 4×2])
Remaining 3 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=6
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123           (gordonb)
letmein          (pablo)
2g 0:00:00:00 DONE (2022-08-10 18:44) 200.0g/s 1100p/s 1100c/s 3300C/s avatar..Me
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.
```

Ho utilizzato il comando john —format=raw-MD5 sql-passwordsm5.txt —show per vedere le password decriptate.

```
┌──(root㉿kali)-[/home/kali/Scrivania]
└─# john --format=raw-MD5 sql-passwordsmd5.txt --show
admin:password
gordonb:abc123
pablo:letmein
smithy:password

4 password hashes cracked, 1 left
```