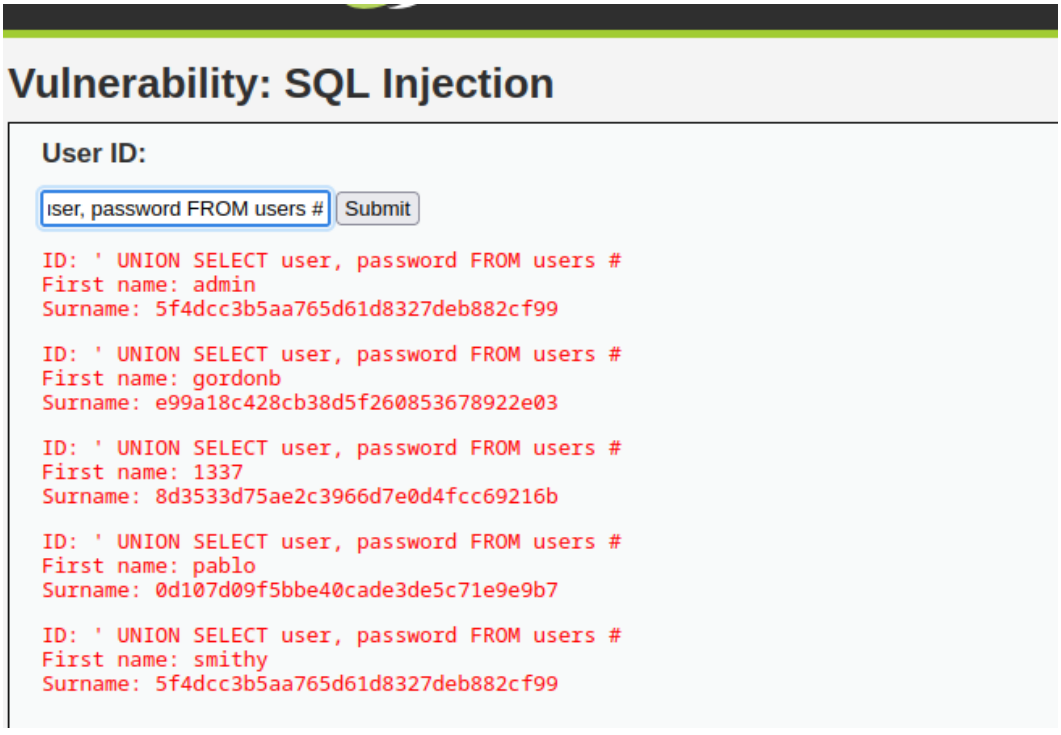
Esercizio 01-03

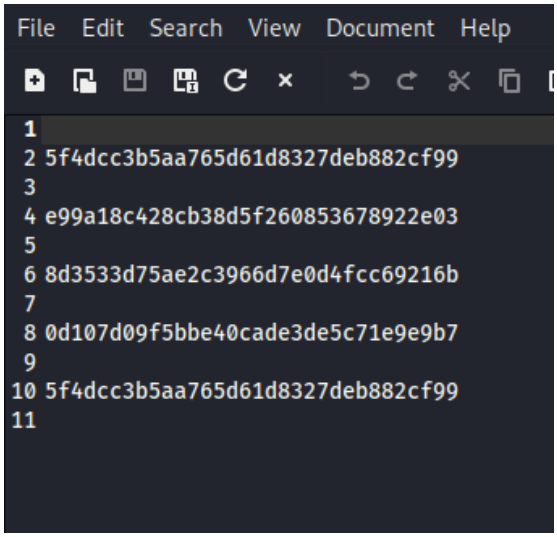
Traccia: recuperare le password dal database di DVWA in formato hash e “scoprirne” il valore in chiaro eseguendo delle sessioni di password cracking. Eseguire la procedura per tutte quante le password trovate.

Consegna:

- screenshot della SQLi effettuata ieri
- Spiegazione della sessione password cracking effettuata (tipologia/meccanismo che usa)
- Screenshot dell’esecuzione del cracking password e del risultato (evidenziare la facilità con cui è stata ricavata la password in chiaro)

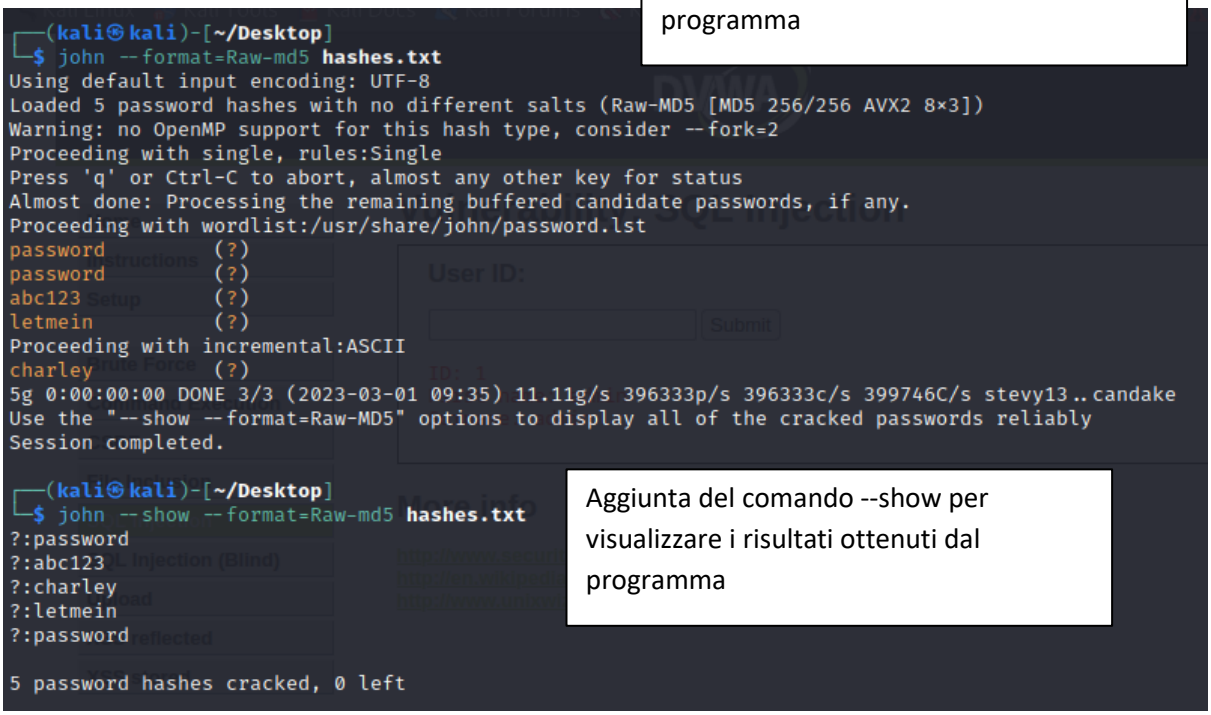
Recupero delle password cifrate in hash





Creazione di un file contenente le 5 password in formato hash per agevolarne la comparazione delle password cifrate

Utilizzo del comando --format=Rax-md5 per specificare il formato di cifrazione al programma



Aggiunta del comando --show per visualizzare i risultati ottenuti dal programma

Per dimostrare ulteriormente la debolezza delle password nonostante fossero archiviate in hash, utilizzo il primo programma per decriptazione hash.

MD5
encript - decript

Il tool on line per criptare e decriptare stringhe in md5

Stringa da criptare | Cripta md5()

Oppure

5f4dcc3b5aa765d61d8327 | Decripta md5()

md5-decript("5f4dcc3b5aa765d61d8327deb882cf99")

password

e99a18c428cb38d5f26085 | Decripta md5()

md5-decript("e99a18c428cb38d5f260853678922e03")

abc123

8d3533d75ae2c3966d7e0 | Decripta md5()

md5-decript("8d3533d75ae2c3966d7e0d4fcc69216b")

charley

0d107d09f5bbe40cade3de | Decripta md5()

md5-decript("0d107d09f5bbe40cade3de5c71e9e9b7")

letmein

5f4dcc3b5aa765d61d8327 | Decripta md5()

md5-decript("5f4dcc3b5aa765d61d8327deb882cf99")

password