

L'esercizio di oggi è riuscire a mettere in chiaro delle password presenti su dvwa.

Per risolvere l'esercizio siamo andati a prendere le password presenti nel database e le abbiamo decodificate.

Per ottenere questo risultato ho scelto di utilizzare il metodo sql injection per accedere alle password, e nomi utente relativi, presenti sul server.

Una volta ottenute le combinazioni di nomi utente e password utilizzando john the ripper siamo andati a decodificare le password salvate.

The image shows a Kali Linux terminal window with three main components:

- Left Panel (DVWA Vulnerability: SQL Injection):** A web interface for DVWA. The 'SQL Injection' tab is selected. It shows a 'User ID' input field and a 'Submit' button. Below this, it displays the results of the SQL injection attack, showing a list of user:password pairs extracted from the database.
- Right Panel (Terminal):** A terminal window showing the execution of John the Ripper. The command used is `john --format=raw-md5 /home/kali/Desktop/password`. The output shows the progress of the attack, including the number of password hashes loaded and the time taken to crack the passwords.
- Bottom Panel (Mousepad):** A text editor window showing the output of the John the Ripper attack. It lists the cracked passwords in a numbered list:

```
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38d5f26883678922e03
3 1337:8d353d75ae2c3966d7e0d4fcc69216b
4 pablo:0d18709f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99
6
```

Nell'immagine possiamo vedere a sinistra la sequel injection da cui abbiamo ottenuto le coppie user:password, in basso a destra il file che abbiamo creato con i relativi dati e in alto a destra l'esecuzione di john che ha decodificato le password