Report Tecnico: Password Cracking & Database Exfiltration (DVWA)

Obiettivo: Recupero delle password hashate dal database e successivo cracking.

Target: DVWA (Damn Vulnerable Web App) - Security Level: Low

Studente: Giuseppe Monaco

---

1. Introduzione

L'attività ha avuto come scopo principale il recupero delle password in chiaro degli utenti della piattaforma DVWA. L'operazione è stata condotta seguendo le procedure di Ethical Hacking, sfruttando vulnerabilità note per l'accesso ai dati e utilizzando strumenti di crittoanalisi per il recupero delle credenziali.

Le operazioni si sono articolate nelle seguenti fasi operative, come previsto dalle istruzioni:

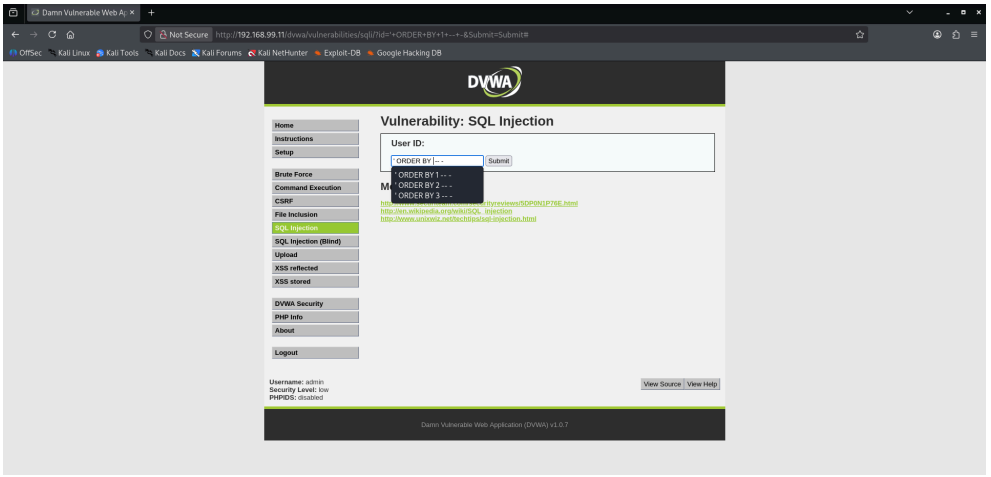
1. **Estrazione:** Accesso al database della DVWA tramite vulnerabilità web (SQL Injection) per l'esfiltrazione delle password hashate;
2. **Identificazione:** Analisi delle stringhe recuperate per confermare la tipologia di algoritmo di hashing, verificato essere MD5;
3. **Cracking:** Configurazione ed esecuzione di attacchi mirati (dizionario e brute force) utilizzando strumenti da riga di comando per decifrare l'intero set di password estratte.

Fase 1: Exploitation e Recupero Dati (SQL Injection)

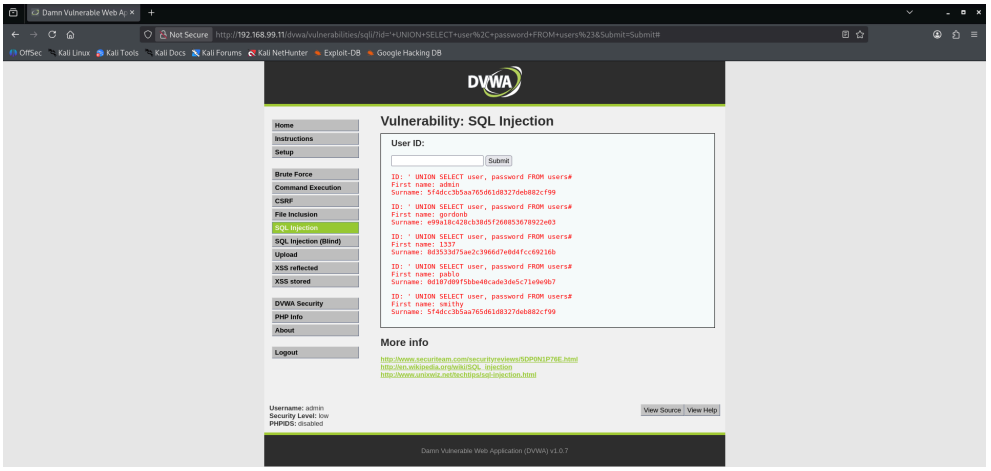
Obiettivo: Accedere alle tabelle del database per estrarre le password hashate.

Per ottenere l'accesso non autorizzato ai dati sensibili, è stata identificata una vulnerabilità di tipo **SQL Injection (SQL)** nel campo di input dell'applicazione.

- **Verifica Vulnerabilità:** L'inserimento di un apice singolo (') ha generato un errore SQL, confermando la mancata sanitizzazione dell'input.
- **Enumerazione:** Tramite clausola `ORDER BY`, è stato determinato che la query originale utilizza 2 colonne.



- **Esfiltrazione (Payload):** È stata iniettata una query `UNION SELECT` per unire i risultati legittimi con il contenuto della tabella `users`



  - *Payload utilizzato:* `' UNION SELECT user, password FROM users#`
  - *Risultato:* Il database ha restituito a schermo l'elenco degli utenti (es. admin, gordonb) e le rispettive password in formato hash.

Fase 2: Identificazione e Analisi dell'Hash

Obiettivo: Verificare la tipologia di hash recuperato .

Le stringhe esfiltrate sono state analizzate per determinare l'algoritmo di cifratura utilizzato, passaggio fondamentale per configurare correttamente i tool di cracking.

- **Analisi:** Gli hash presentavano una lunghezza di **32 caratteri** esadecimali.
- **Esito:** La lunghezza e il set di caratteri hanno confermato che si tratta di hash **MD5** (Message Digest 5).
- **Correzione Dati:** Durante l'analisi, è stato individuato un hash corrotto (31 caratteri) relativo all'utente *gordonb*. L'hash è stato corretto manualmente ripristinando il carattere mancante iniziale, permettendo il proseguimento dell'attività.

Fase 3: Password Cracking

Obiettivo: Utilizzare tool specifici e diverse metodologie per recuperare la versione in chiaro di tutte le password .

Per massimizzare le probabilità di successo e recuperare la totalità delle credenziali, la fase di cracking è stata strutturata in due step successivi, utilizzando il tool **John the Ripper**.

4.1. Step 1: Attacco a Dizionario (Dictionary Attack)

In prima istanza, è stato eseguito un attacco basato su wordlist, metodo più rapido ed efficiente per individuare password comuni.

- **Configurazione:** Wordlist `rockyou.txt` standard di Kali Linux.

Comando eseguito:

```
john --format=Raw-MD5
--wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

- **Esito:** Questo attacco ha permesso di decifrare immediatamente la maggior parte degli hash presenti nel database, confermando l'uso di password deboli da parte degli utenti.

4.2. Step 2: Attacco Brute Force (Modalità Incrementale)

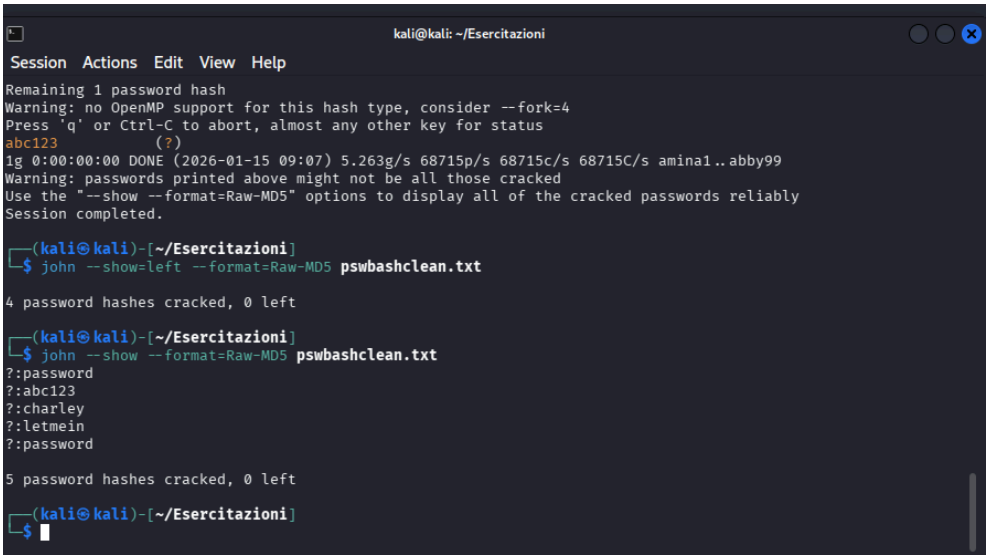
Per tentare di risolvere gli hash residui non individuati tramite il dizionario, si è passati a un attacco di forza bruta puro.

- **Metodologia:** Utilizzo della modalità `--incremental` di John the Ripper. In questa modalità, il tool non utilizza una lista di parole predefinita, ma genera e tenta tutte le possibili combinazioni di caratteri (a-z, 0-9, ecc.) fino a trovare una corrispondenza.

Comando eseguito:

```
john --incremental --format=Raw-MD5 hash.txt
```

- **Analisi:** L'utilizzo combinato di questa tecnica ha permesso di isolare le problematiche relative agli hash rimanenti (inclusa l'identificazione dell'hash corrotto descritta nella Fase 2), garantendo il completamento dell'obiettivo .



Conclusioni

L'esercizio ha dimostrato come una vulnerabilità di iniezione SQL possa portare alla compromissione totale del database utenti. Inoltre, l'utilizzo di un algoritmo di hashing obsoleto (MD5) senza "salt" e l'uso di password deboli (presenti in dizionari comuni) hanno permesso il recupero delle credenziali in tempi estremamente ridotti (meno di 1 secondo).