REPORT S6/L4

Target: DVWA (Damn Vulnerable Web App) - 192.168.50.101

1. Obiettivo

Recuperare le password hashate nel database della DVWA e eseguire sessioni di cracking per recuperare la loro versione in chiaro.

2. Metodologia di Attacco

Il test è stato condotto seguendo tre fasi distinte: Exploitation (SQL Injection), Analisi dei dati ed Esecuzione del Password Cracking.

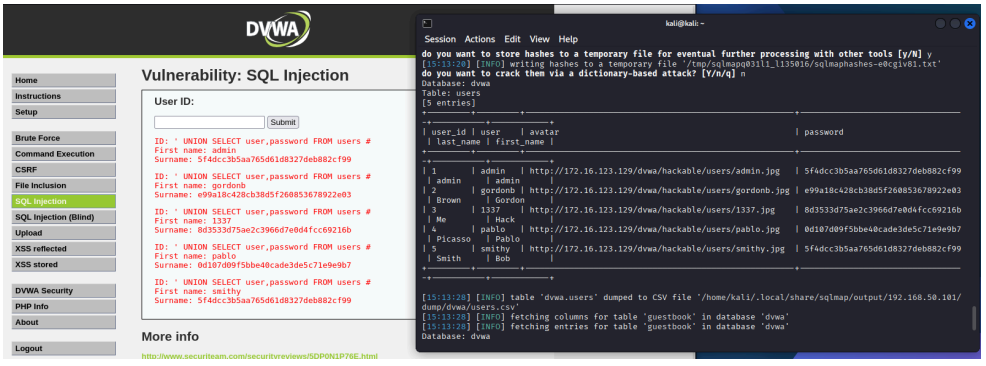
Fase 1: Exploitation ed Esfiltrazione Dati

Dopo aver effettuato l'accesso alla piattaforma, ho abbassato la security da high a low, successivamente mi sono recato nella sezione **SQL Injection** e ho verificato la presenza di una SQL Injection nel parametro **id**.

- **Verifica Manuale:** Ho iniettato un payload di tipo *UNION-Based* per verificare la possibilità di estrarre dati.
    - *Payload:* **' UNION SELECT user,password FROM users #**
    - *Risultato:* L'applicazione ha restituito a schermo gli username e gli hash delle password presenti nel database.
- **Esfiltrazione Automatizzata:** Per ottenere un risultato completo e strutturato del database, ho utilizzato il tool **SQLMap** con i seguenti parametri:

  u="http://192.168.50.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit"
  c="security=low; PHPSESSID=5492ab453bcdcfc57a43006e4d2e5872"
  sqlmap -u $u --cookie=$c -D dvwa --dump-all

*Per ottenere i **cookie di sessione** da inserire in **SQLMap**, ho effettuato un attacco **XSS reflected** all'interno dell'input presente nella sezione XSS reflected (**<script>alert(document.cookie)</script>**)*



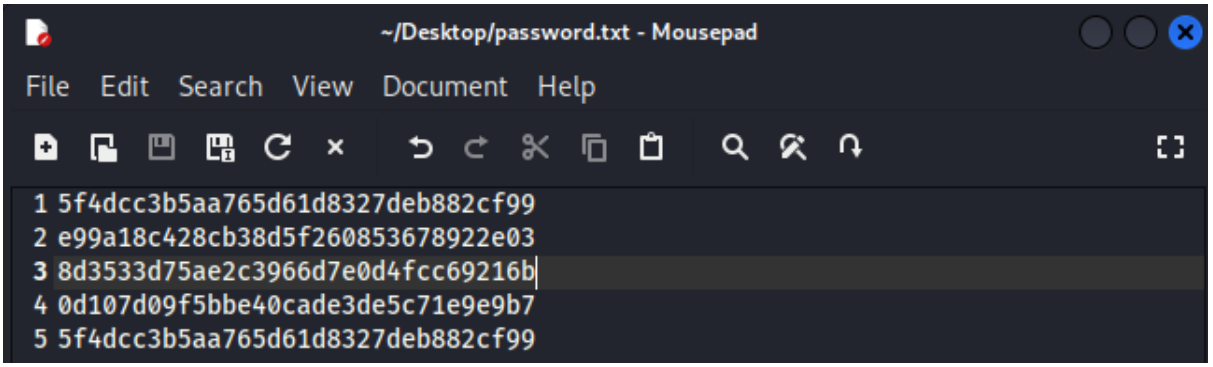
Fase 2: Identificazione e Analisi Hash

Le stringhe recuperate dalla colonna **password** sono state analizzate per identificarne l'algoritmo di cifratura.

- **Analisi:** Conteggio dei caratteri delle stringhe esadecimali.
- **Evidenza:** Tutte le stringhe presentavano una lunghezza fissa di **32 caratteri**.
- **Conclusione:** L'algoritmo utilizzato è **MD5**.

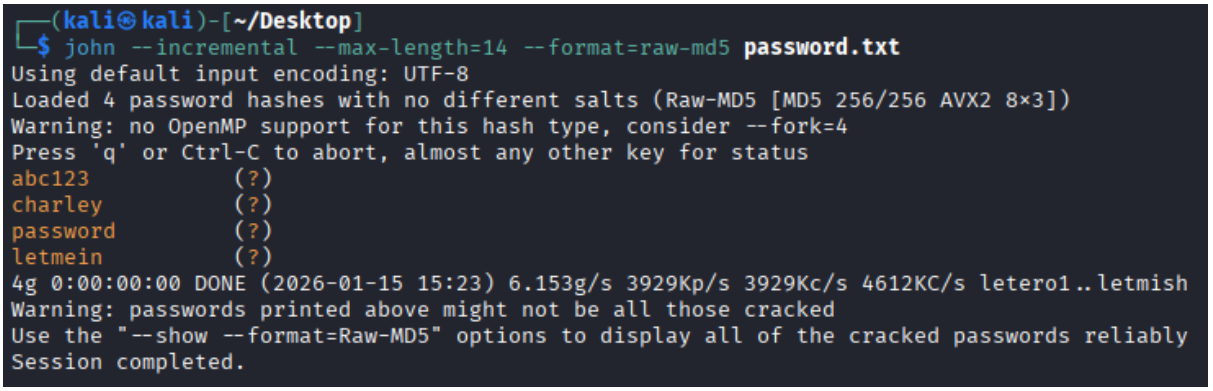
Fase 3: Password Cracking

Gli hash sono stati salvati in un file denominato **password.txt**.



Per il recupero delle password in chiaro ho utilizzato il tool **John the Ripper** in modalità *incremental* (**Brute Force**)

Il comando che ho utilizzato è il seguente: ***john - -incremental - -max-length=14 - -format=raw-md5 password.txt***



3. Risultati Ottenuti

Il processo di cracking ha avuto successo, decifrando il 100% degli hash trovati.

Osservazione: Nonostante nel database fossero presenti **5 utenti**, il tool ha restituito **4 password uniche**. Dall'analisi è emerso che due utenti condividono la stessa stringa di hash. Ciò indica che l'applicazione **non utilizza il Salting**. Se due utenti scelgono la stessa password, l'hash MD5 risultante è identico, permettendo di compromettere due account craccandone uno solo.

4. Conclusioni

Il sistema presenta criticità di livello **Alto**.

1. **Vulnerabilità SQL Injection:** L'input utente non è sanitizzato.
2. **Hashing Debole:** L'uso di MD5 senza salt è obsoleto e insicuro.