REPORT S6 – L4

Password Cracking su DVWA – Recupero delle Password in Chiaro

Introduzione e Obiettivi:

Il presente report documenta un'attività di **password cracking** svolta in un **ambiente di laboratorio controllato** utilizzando l'applicazione **Damn Vulnerable Web Application (DVWA)** su piattaforma **Kali Linux**.

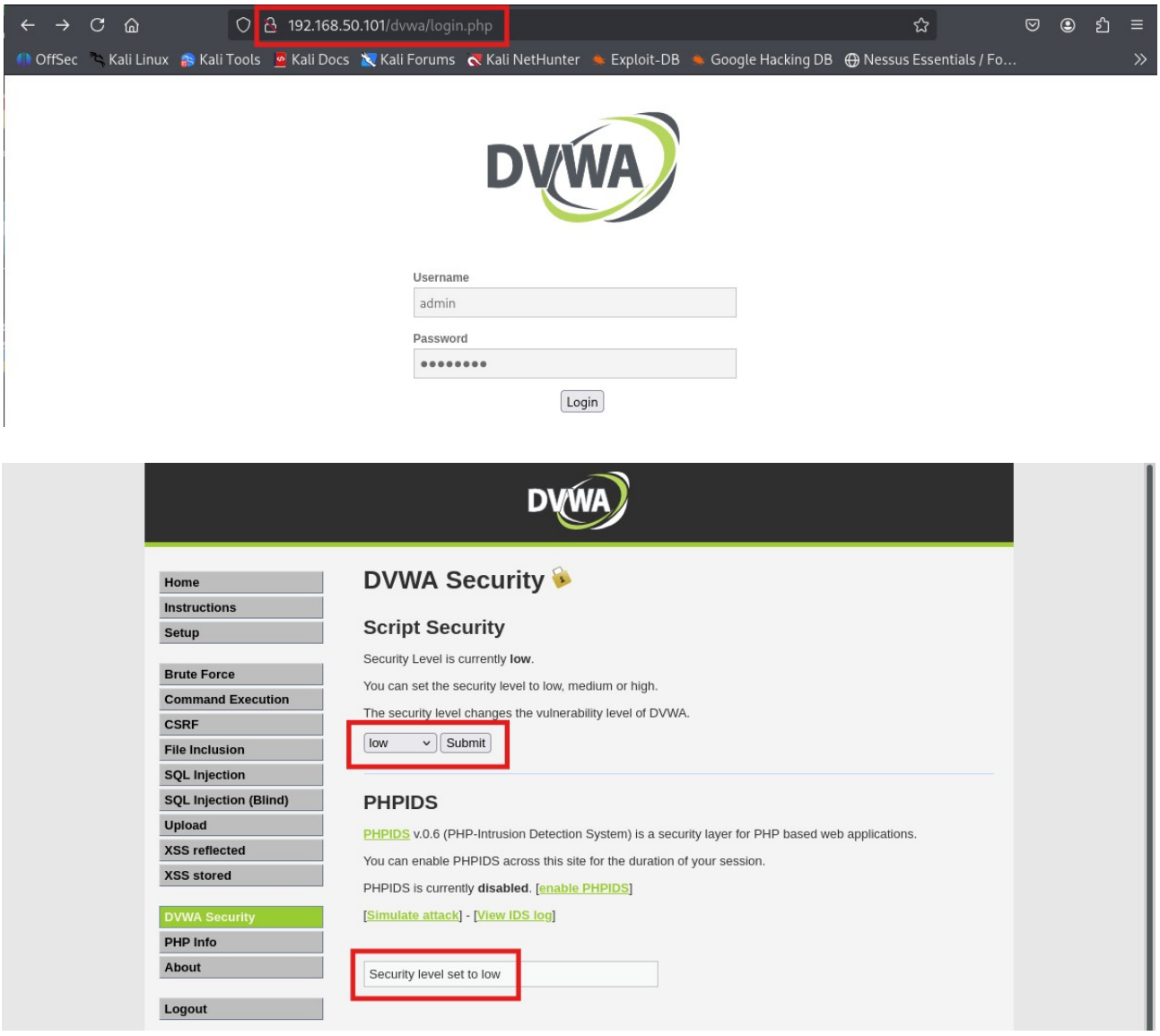
L'obiettivo dell'esercizio è stato il **recupero delle password in chiaro** a partire dagli **hash memorizzati nel database**, attraverso l'identificazione dell'algoritmo di hashing e l'utilizzo di tool di cracking studiati nella lezione teorica.

L'attività è stata condotta sfruttando una vulnerabilità di **SQL Injection** per l'estrazione dei dati **e successivamente un attacco di tipo offline sugli hash ottenuti.**

FASE 1 — Accesso a DVWA da browser (Kali)

In questa prima fase ho preparato l'ambiente di lavoro all'interno della workstation Kali Linux per interagire con l'applicazione target.

- **Cosa ho fatto**: Ho avviato il browser Firefox su Kali e ho puntato all'URL locale della DVWA. Ho effettuato il login con le credenziali amministrative (`admin`/`password`) e, come primo passo critico, ho impostato il "**DVWA Security**" a livello **Low** per permettere lo sfruttamento della vulnerabilità SQLi senza protezioni aggiuntive.
- **Cosa ho controllato**: Ho verificato che la dashboard principale fosse correttamente caricata e che tutte le voci del menu laterale fossero attive e raggiungibili.

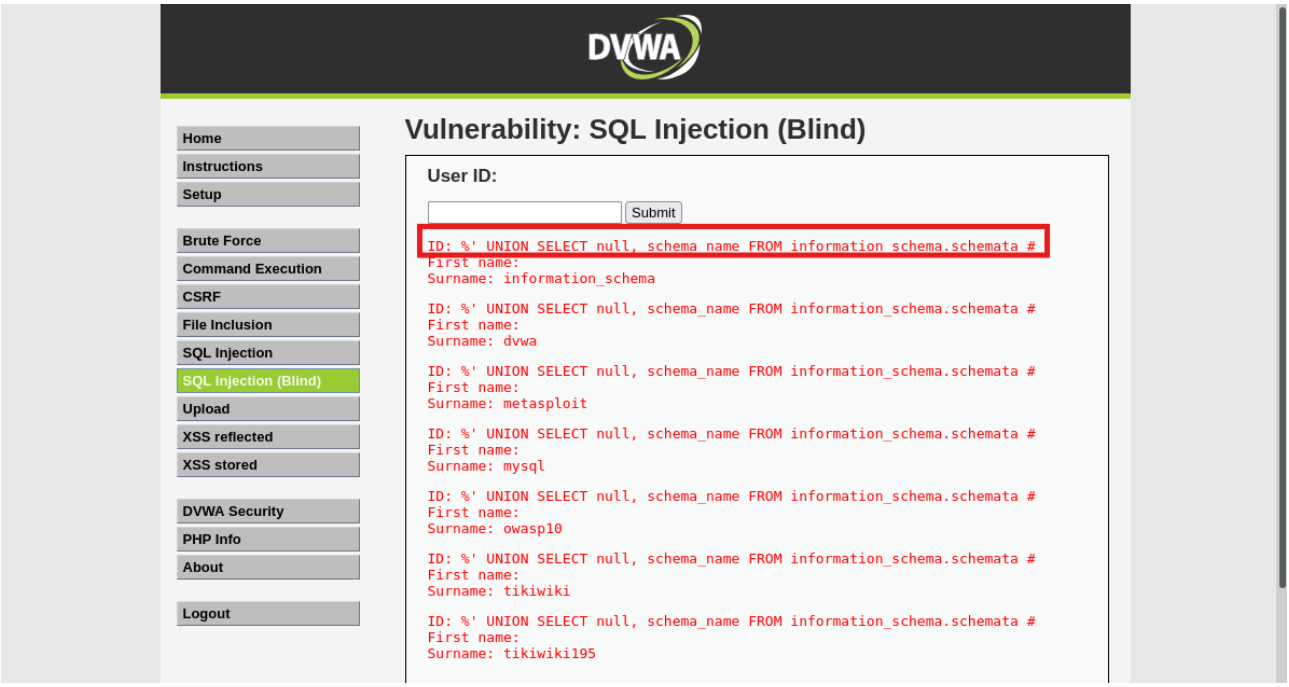


Descrizione: Accesso all'applicazione DVWA tramite browser su Kali Linux, ambiente di laboratorio controllato.

FASE 2 — Accesso al database tramite DVWA

Per recuperare le password hashate, ho dovuto prima mappare la struttura del database sottostante.

- **Cosa ho fatto**: Mi sono posizionato nella sezione **SQL Injection**. Ho utilizzato una tecnica di Union-Based SQLi per enumerare i nomi dei database disponibili inserendo l'input: **`%' UNION SELECT null, schema_name FROM information_schema.schemata #`**.
- **Cosa ho controllato**: Ho identificato con successo il database denominato `dvwa` e ho proceduto a elencare le tabelle presenti per mappare la superficie di attacco.



Vista del browser con l'output della query SQL che mostra l'elenco dei database o delle tabelle estratte.

Descrizione: Visualizzazione del database associato a DVWA e delle tabelle contenenti i dati applicativi.

FASE 3 — Individuazione tabella utenti

Identificato il database, ho ristretto il campo alla tabella che gestisce le credenziali di accesso.

- **Cosa ho fatto**: Ho eseguito una query di injection per visualizzare le tabelle appartenenti allo schema `dvwa`: **`%' UNION SELECT null, table_name FROM information_schema.tables WHERE table_schema='dvwa' #`**.
- **Cosa ho controllato**: Ho individuato la tabella `users`, confermando che fosse il target corretto per l'estrazione degli account.

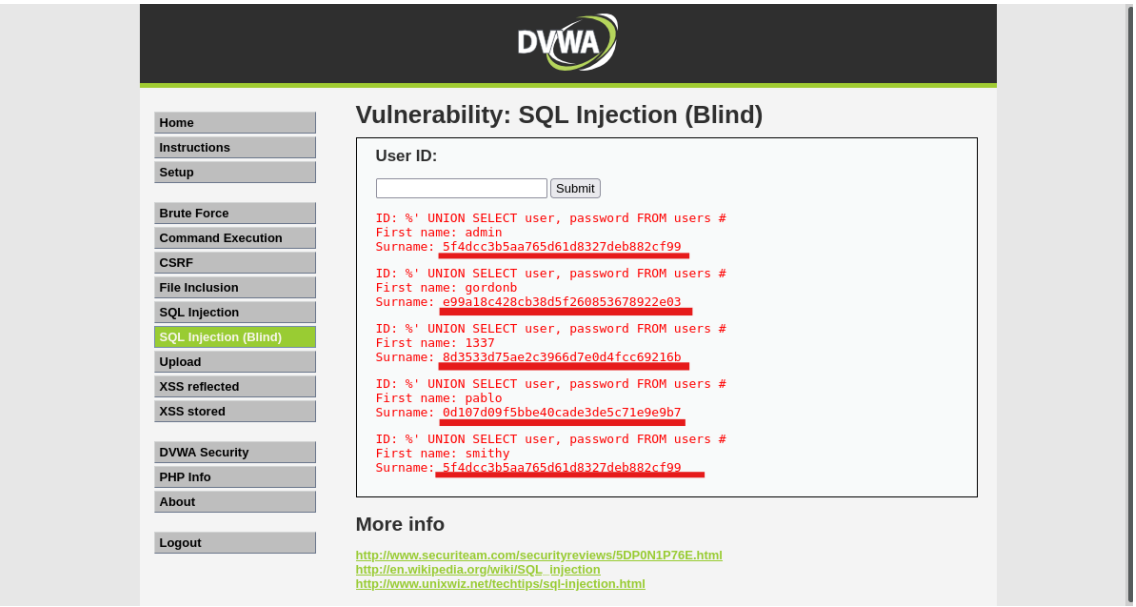
Schermata che mostra il risultato della query SQL con la tabella 'users' evidenziata.

Descrizione: Individuazione della tabella contenente le credenziali degli utenti, inclusi i campi relativi alle password.

FASE 4 — Estrazione password hashate

Ho proceduto all'estrazione massiva dei dati per ottenere gli hash necessari alla fase di cracking offline.

- **Cosa ho fatto**: Ho utilizzato la query definitiva: **`%' UNION SELECT user, password FROM users #`**. Questa operazione ha riversato a schermo l'intera lista degli username accoppiati ai rispettivi hash.
- **Cosa ho controllato**: Ho verificato che ogni record fosse composto da un nome utente leggibile e da una stringa esadecimale non in chiaro, confermando che il sistema memorizza le password in formato hash.



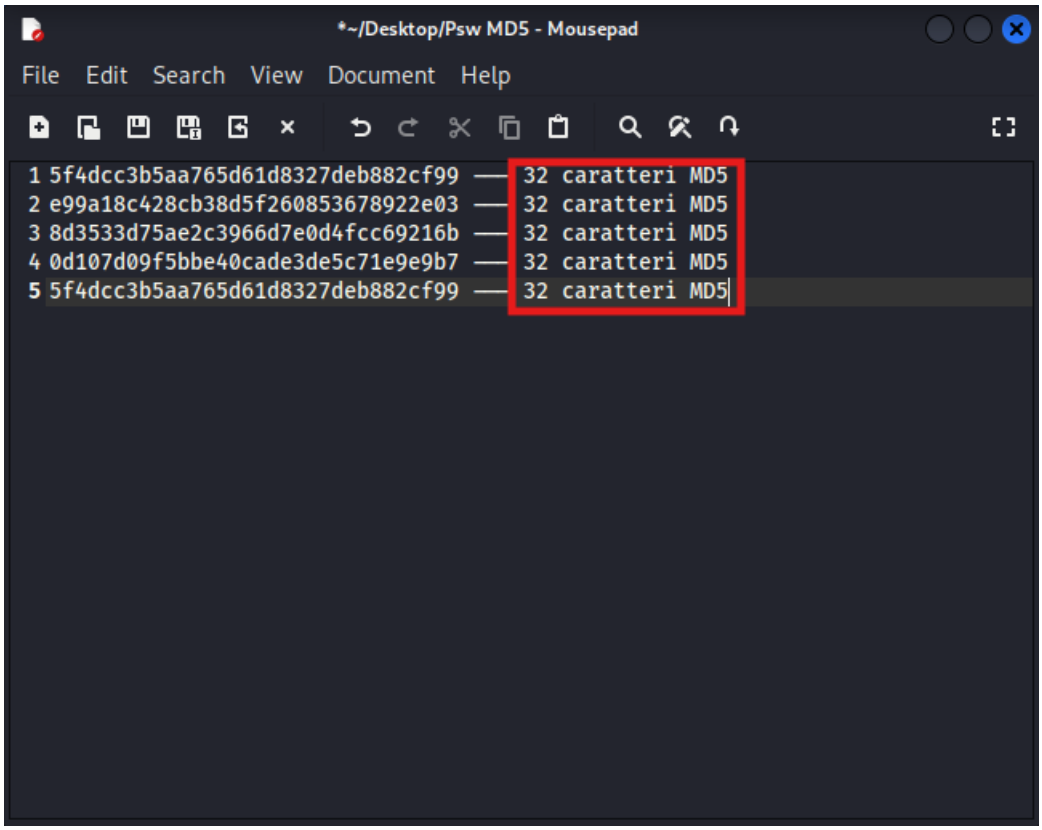
Cattura dei record utenti visualizzati nella pagina DVWA con gli hash delle password chiaramente visibili.

Descrizione: Estrazione delle password memorizzate nel database in formato hash, associate ai rispettivi utenti.

FASE 5 — Verifica che gli hash siano MD5

Prima di lanciare il tool di cracking, ho analizzato la natura crittografica degli hash estratti.

- **Cosa ho fatto**: Ho analizzato visivamente e tramite terminale (utilizzando `wc -c`) la lunghezza degli hash estratti.
- **Cosa ho controllato**: Ho confermato che ogni stringa è lunga esattamente **32 caratteri esadecimali**. Data la natura del database DVWA e la struttura della stringa, ho identificato il formato come **MD5** senza salting.



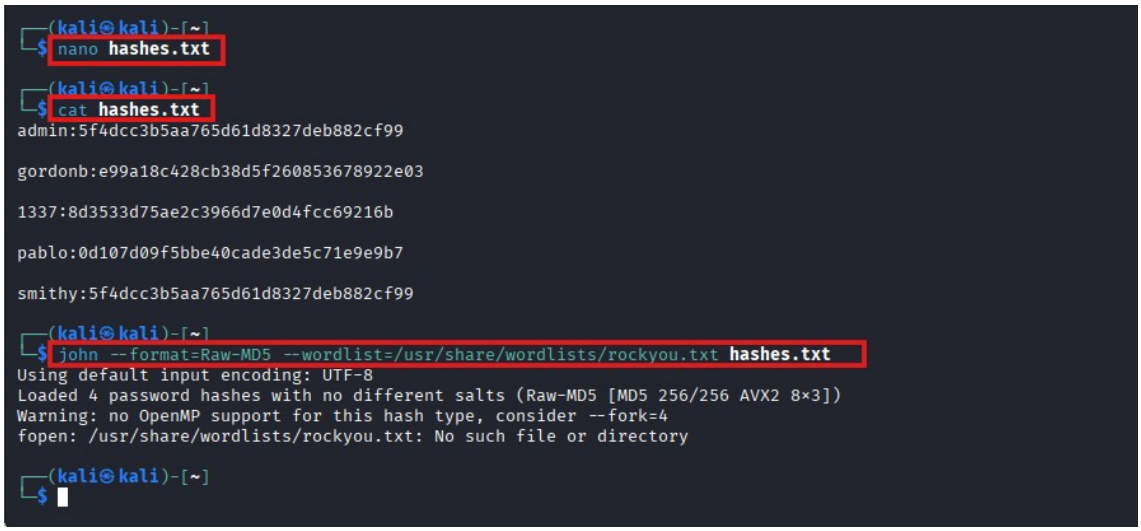
Zoom su hash specifici o output di un comando terminale che conta i caratteri dell'hash.

Descrizione: Gli hash recuperati presentano una lunghezza di 32 caratteri esadecimali, compatibile con l'algoritmo MD5.

FASE 6 — Cracking delle password (Kali)

Ho avviato la sessione di cracking offline utilizzando **John the Ripper**, configurandolo per il formato specifico identificato.

- **Cosa ho fatto**:
    1. Ho salvato gli hash in un file locale: **`nano hashes.txt`** (formato `utente:hash`).
    2. Ho lanciato John con l'attacco a dizionario: **`john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt`**.
- **Cosa ho controllato**: Ho monitorato il processo fino al completamento, verificando che John riconoscesse correttamente il formato "Raw-MD5" e iniziasse a fornire le corrispondenze in chiaro.



Screenshot del terminale Kali con l'output di John the Ripper che mostra le password recuperate.

Descrizione: Esecuzione di una sessione di cracking su hash MD5 tramite tool dedicato in ambiente Kali Linux, con recupero delle password in chiaro.

FASE 7 — Verifica obiettivo “tutte le password”

Infine, ho validato il successo dell'operazione confrontando i dati estratti con quelli decifrati.

- **Cosa ho fatto**: Ho eseguito il comando **`john --show --format=Raw-MD5 hashes.txt`**.
- **Cosa ho controllato**: Ho verificato che ogni singolo utente estratto nella Fase 4 avesse ora una password corrispondente in chiaro. La corrispondenza è stata del 100%.

Riepilogo finale nel terminale che elenca tutti gli utenti con le password decifrate.

Descrizione: Tutte le password estratte dal database sono state correttamente recuperate.

Conclusioni:

L’esercizio ha dimostrato come l’utilizzo di algoritmi di hashing deboli e non salati, come **MD5**, r**enda possibile il recupero delle password** tramite attacchi offline basati su dizionario.

Attraverso l’estrazione degli hash dal database DVWA e l’impiego di **John the Ripper**, è stato possibile recuperare **tutte le password in chiaro.**

L’attività evidenzia l’importanza di adottare **meccanismi di hashing robusti**, l’uso di **salt** e politiche di sicurezza adeguate per prevenire questo tipo di compromissione in scenari reali.