Recupero delle Password in Chiaro

Attività di recupero password dalla Damn Vulnerable Web Application (DVWA). L'operazione ha seguito i seguenti passaggi:

1. **Sfruttamento di una Vulnerabilità SQL Injection**:
    - È stata sfruttata una vulnerabilità SQL injection nella DVWA per estrarre gli hash delle password degli utenti dal database. Questo è visibile nella finestra del browser che mostra la pagina "Vulnerability: SQL Injection" con i risultati di una query di unione.

      ' UNION SELECT user, password FROM users #

2. **Salvataggio degli Hash delle Password**:
    - Gli hash delle password estratti sono stati salvati in un file di testo chiamato "john.txt", visibile nella finestra in alto a sinistra dell'immagine.

3. **Utilizzo di John the Ripper per il Cracking delle Password**:
    - È stato utilizzato lo strumento John the Ripper per tentare di recuperare le password in chiaro dagli hash. Questo è evidenziato nei comandi eseguiti nel terminale:
        - **john --incremental --format=raw-md5 john.txt** per avviare l'attacco.
        - **john --show --format=raw-md5 john.txt** per visualizzare i risultati.

4. **Risultati del Cracking**:
    - L'output mostra che sono state recuperate con successo 5 password in chiaro corrispondenti agli hash.

Questa attività dimostra il processo di recupero e cracking di password hashate da un'applicazione web vulnerabile.