1. **Accesso al database:**
    - Assicurati di avere accesso al database DVWA. Di solito, DVWA utilizza un database MySQL o MariaDB.
    - Puoi accedere al database con il seguente comando (sostituendo le credenziali con quelle effettive):
    - bash
    - Copia codice
    - mysql -u root -p
        - Qui, -u root indica che stai accedendo come utente root e -p ti chiede di inserire la password.
2. **Seleziona il database DVWA:** Dopo aver effettuato l'accesso, esegui questo comando per selezionare il database:
3. sql
4. Copia codice
5. USE dvwa;
6. **Visualizzazione delle tabelle:** Per vedere tutte le tabelle nel database, puoi usare:
7. sql
8. Copia codice
9. SHOW TABLES;
10. **Recupera le password hashate:** Ora, identifica la tabella che contiene le password. Generalmente, dovrebbe esserci una tabella chiamata qualcosa come users. Puoi visualizzare il contenuto della tabella con:
11. sql
12. Copia codice
13. SELECT * FROM users;

Passo 2: Verifica del Tipo di Hash (MD5)

1. **Controllo del formato degli hash:**Una volta ottenute le password, noterai che sono in formato hash. Gli hash MD5 sono composti da stringhe di 32 caratteri alfanumerici.
    - Un esempio di hash MD5: 5f4dcc3b5aa765d61d8327deb882cf99 (che corrisponde alla password "password").

Passo 3: Cracking delle Password

1. **Tool per il cracking delle password:** I tool più comunemente usati per craccare gli hash MD5 sono:
    - **John the Ripper:** Uno dei più famosi strumenti di cracking delle password.
    - **Hashcat:** Un altro tool potente, supporta molti tipi di hash, inclusi MD5.
2. **Configurazione e uso di John the Ripper:** Se vuoi usare **John the Ripper**, segui questi passaggi:
    - Assicurati di avere John installato:
    - bash
    - Copia codice
    - sudo apt-get install john
    - Crea un file con gli hash da craccare. Puoi salvare gli hash estratti dal database in un file chiamato, ad esempio, hashes.txt.
    - Lancia il cracking con:
    - bash
    - Copia codice
    - john --format=raw-md5 hashes.txt
3. **Utilizzo di Hashcat:** Per usare **Hashcat**:
    - Installa Hashcat (se non è già installato):
    - bash
    - Copia codice
    - sudo apt-get install hashcat
    - Lancia il cracking:
    - bash
    - Copia codice
    - hashcat -m 0 hashes.txt /usr/share/wordlists/rockyou.txt
        - Dove -m 0 indica MD5 e rockyou.txt è un wordlist comune.

Obiettivo finale

L'obiettivo finale è **craccare tutte le password hashate**. Gli strumenti useranno una lista di parole (wordlist) per cercare di indovinare la password corrispondente a ciascun hash.