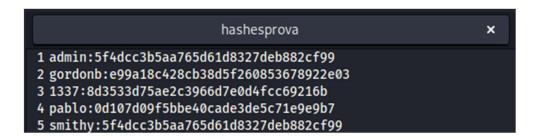
L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate con l'attacco SQL Injection nella DVWA.

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.



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





PRATICA S6L3 – Giorgio Trovesi

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
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

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.

DVWA Security	page.
PHP Info	
About	You have logged in as '1337'
Logout	
Username: 1337 Security Level: low PHPIDS: disabled	