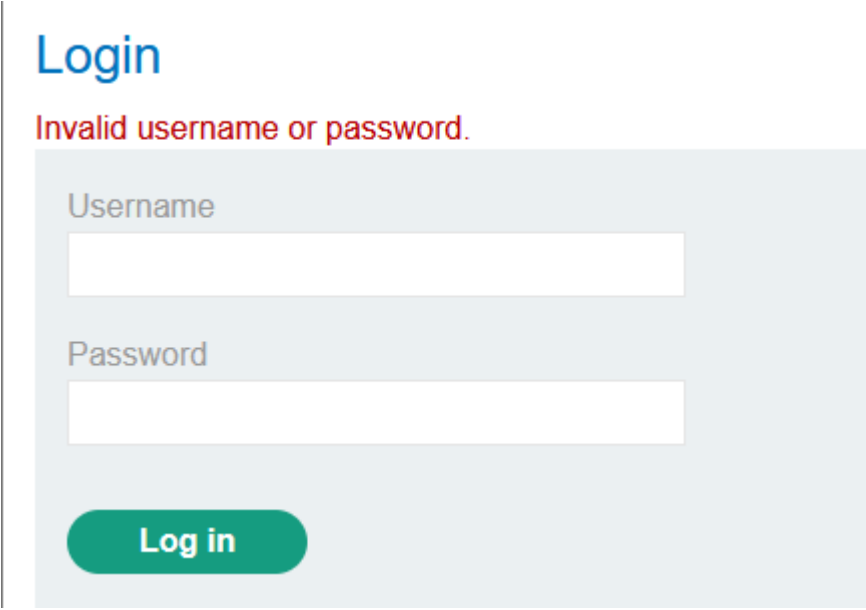


Notes (By manual SQLi)

Lab: SQL injection vulnerability allowing login bypass

1. this is a sqli vuln in the logging functionality
2. that logs in to the application as the `administrator` user.
3. End goal is to perform a sqli attack to login as the administrator user.

▼ Analysis:



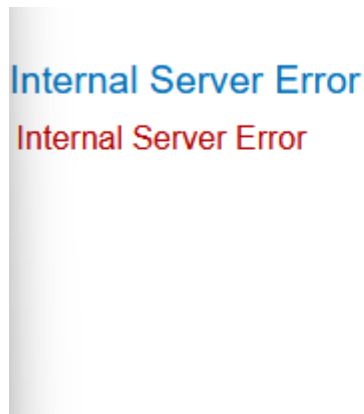
The screenshot shows a web application's login interface. At the top, the word "Login" is displayed in blue. Below it, a red error message reads "Invalid username or password." The login form itself is a light blue box containing two input fields: "Username" and "Password". Below these fields is a green "Log in" button.

this type of thing is called non verbose generic error message. Because if you said only the user name or the password is invalid individually it might be a problem of its own. Because if you do that an attacker can enumerate the user name or password on this system.

In these case we typed a default name and a password like admin admin.

1. I put a quote sign (') in the uname field and typed an arbitrary password and it gave us this

it means something is happening in the backend.



2. as we need the username so the query could be like this

```
SELECT firstname FROM users WHERE username='admin' and password='admin'
```

here the password must not be like the plain text it might be in hashes.

3. But the password won't be a problem because we are going to do something with the username field and that will bypass the password section. So it doesn't matter the password is hashed or not.

4.

```
SELECT firstname FROM users WHERE username=' ' and password='admin'
```

if we put a quote char here it will give us an internal server error. because after a single quote there is one ' and that is an error query.

5.

```
SELECT firstname FROM users WHERE username='admin'--' and password='admin'
```

If we type admin'— it will work as

```
SELECT firstname FROM users WHERE username='admin'
```

but it won't work actually. Because admin is not a user in this system.

6. lets use the name administrator ...

7. and that's all I have entered the webpage as the administrator .

SQL injection vulnerability allowing login bypass



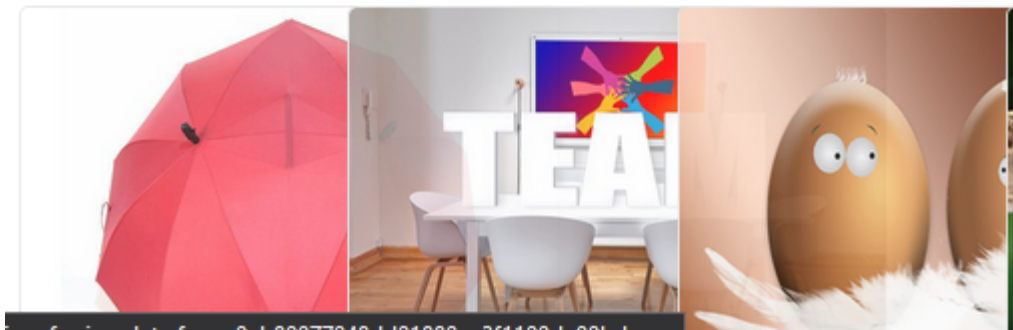
[Back to lab description](#) >>

Congratulations, you solved the lab!

Share your skills!



WE LIKE TO
SHOP 



8. the backend query is `SELECT firstname FROM users WHERE username='administrator'--' and password='admin'`