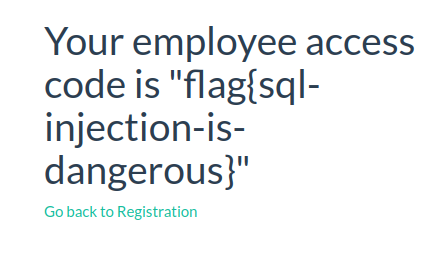
**OWASP Assignment**

Q1)

To Register I needed an Employee Access Code. So I went to the recovery page.

At this page I tried using an SQL Injection

* Tried: ' OR '1'='1’ -> didn’t work
* Tried: ' OR '1'='1 -> worked!



Registered using following account details:

Firstname: Aaron

Lastname: N

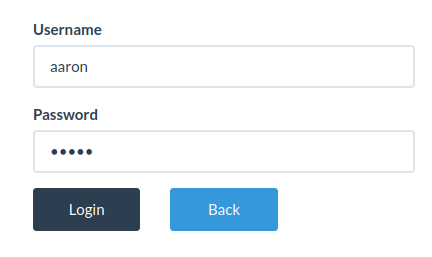
Email: [aaron@gmail.com](mailto:aaron@gmail.com)

Username: aaron

Password: aaron

Employee Access Code: flag{sql-injection-is-dangerous}

After registering, I logged in



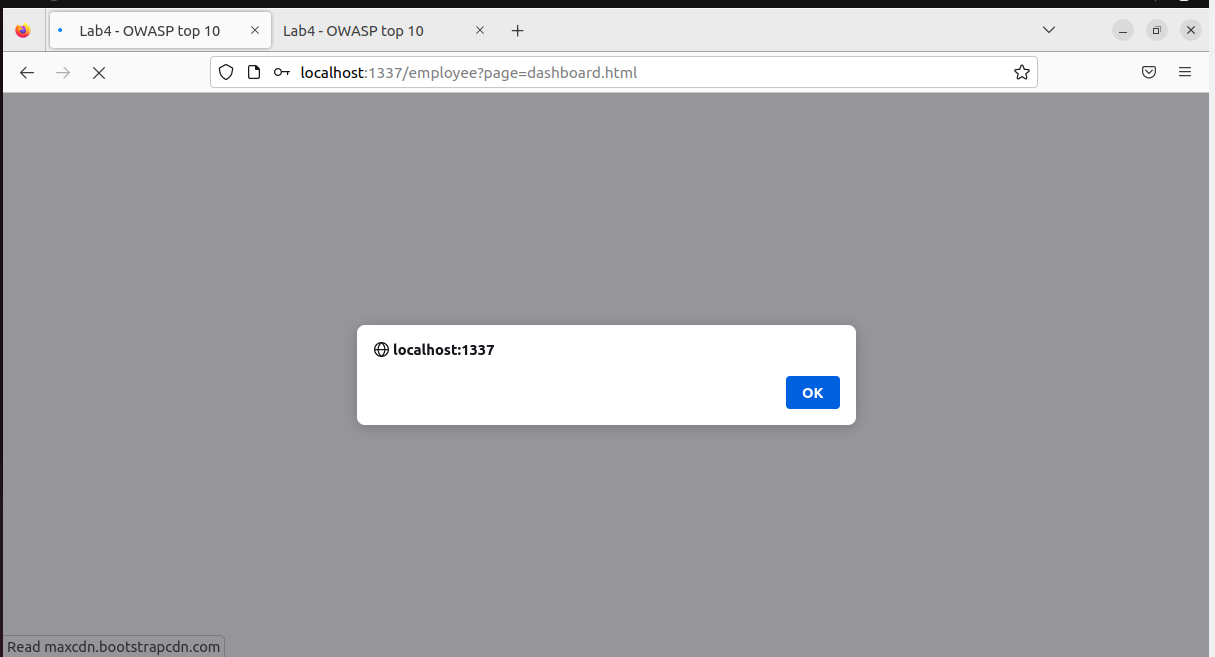
Q2)

[http://localhost:1337/login?redirect=http://localhost:1337/register](http://localhost:1337/login?redirect=http:/localhost:1337/register)

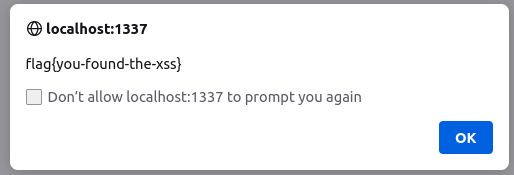
This URL redirects the user to the register page after logging in.

Q3)

From the Profile page, I changed my Firstname to: <script>javascript:alert(document.cookie)</script>



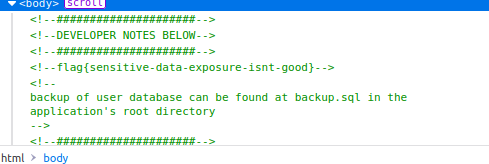
This made this blank alert pop up.



The flag also popped up right after.

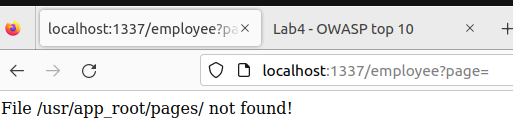
Q4)

By inspecting the dashboard, we can find developer comments in the html body.

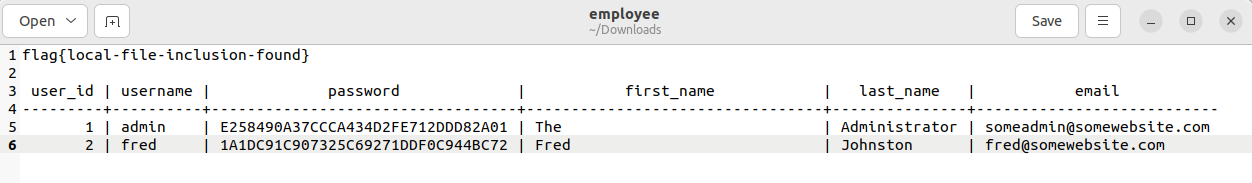


Q5)

I figured out that you can change the URL to access different and possibly restricted pages.



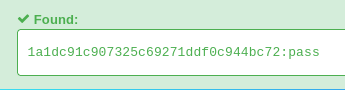
Using info from Q4 I found out localhost:1337/employee?page../backup.sql will open this file



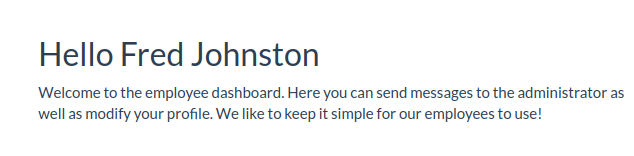
Q6)

Inputting the password directly did not work, likely because it is encrypted.

I guessed it was a hash and used an online MD5 hash decryption site which gave me



Using the password “pass”, I was able to log into Fred’s account.



I didn’t find the flag though, so this may not have been the intended method of exploit for the assignment, but an exploit nonetheless.

Q7)

I was unable to find the right HTML commands to get this to work :(