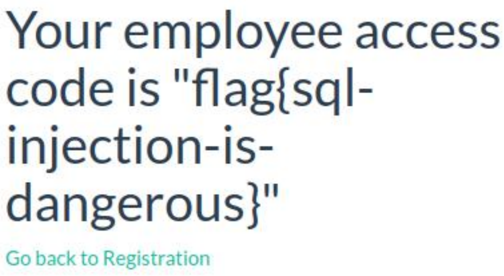
CSI 4139 Assignment 6
Aaron Ng (300176901)
Nov 28, 2022

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

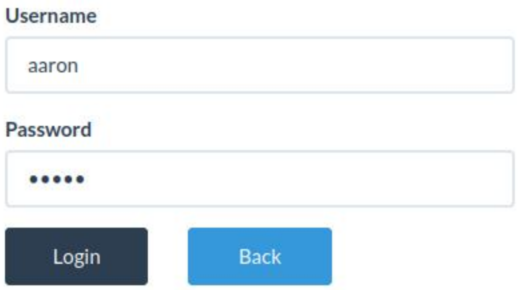
- Tried: ' OR '1'='1’ -> didn’t work
- Tried: ' OR '1'='1 -> worked!



Your employee access code is "flag{sql-injection-is-dangerous}"

Registered using following account details:
Firstname: Aaron
Lastname: N
Email: aaron@gmail.com
Username: aaron
Password: aaron
Employee Access Code: flag{sql-injection-is-dangerous}

After registering, I logged in



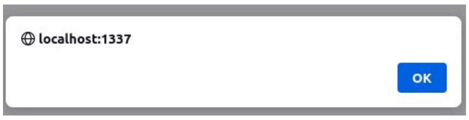
Username: aaron
Password: •••••

Q2)
http://localhost:1337/login?redirect=http://localhost:1337/register
This URL redirects the user to the register page after logging in.

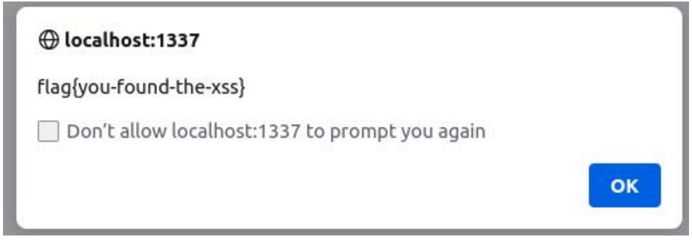
CSI 4139 Assignment 6
Aaron Ng (300176901)
Nov 28, 2022

Q3)

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



This made this blank alert pop up.

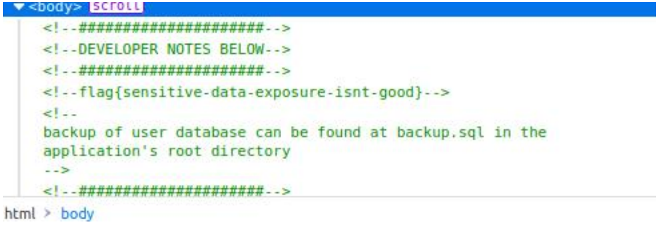


flag{you-found-the-xss}

The flag also popped up right after.

Q4)

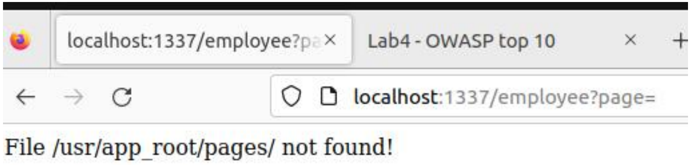
By inspecting the dashboard, we can find developer comments in the html body.



```
▼ <body> scroll
  <!--######################-->
  <!--DEVELOPER NOTES BELOW-->
  <!--######################-->
  <!--flag{sensitive-data-exposure-isnt-good}-->
  <!--
  backup of user database can be found at backup.sql in the
  application's root directory
  -->
  <!--######################-->
```

Q5)

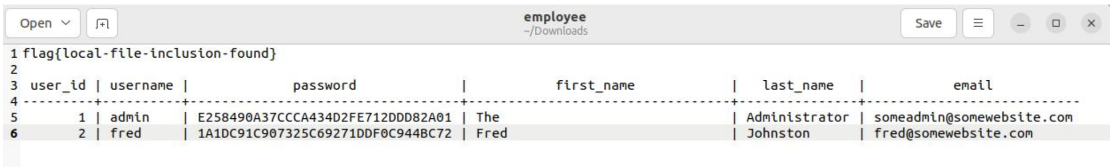
I figured out that you can change the URL to access different and possibly restricted pages.



localhost:1337/employee?page=

File /usr/app_root/pages/ not found!

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



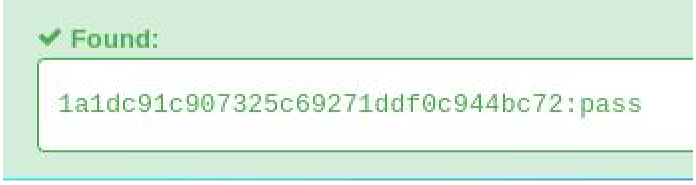
```
flag{local-file-inclusion-found}

 user_id | username |             password             |            first_name            |   last_name   |          email
---------+----------+----------------------------------+----------------------------------+---------------+---------------------------
       1 | admin    | E258490A37CCCA434D2FE712DDD82A01 | The                              | Administrator | someadmin@somewebsite.com
       2 | fred     | 1A1DC91C907325C69271DDF0C944BC72 | Fred                             | Johnston      | fred@somewebsite.com
```

CSI 4139 Assignment 6
Aaron Ng (300176901)
Nov 28, 2022

Q6)

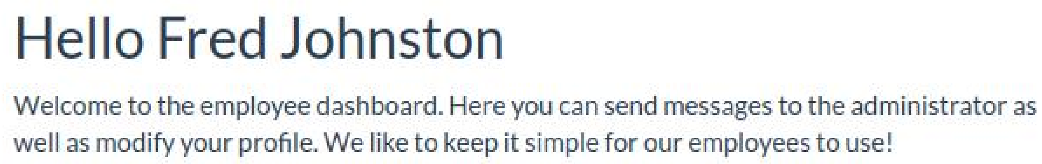
Inputting the password directly did not work, likely because it is encrypted.
I guessed it was a hash and used an online MD5 hash decryption site which gave me



✔ Found:

```
1a1dc91c907325c69271ddf0c944bc72:pass
```

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



Hello Fred Johnston

Welcome to the employee dashboard. Here you can send messages to the administrator as well as modify your profile. We like to keep it simple for our employees to use!

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 :(