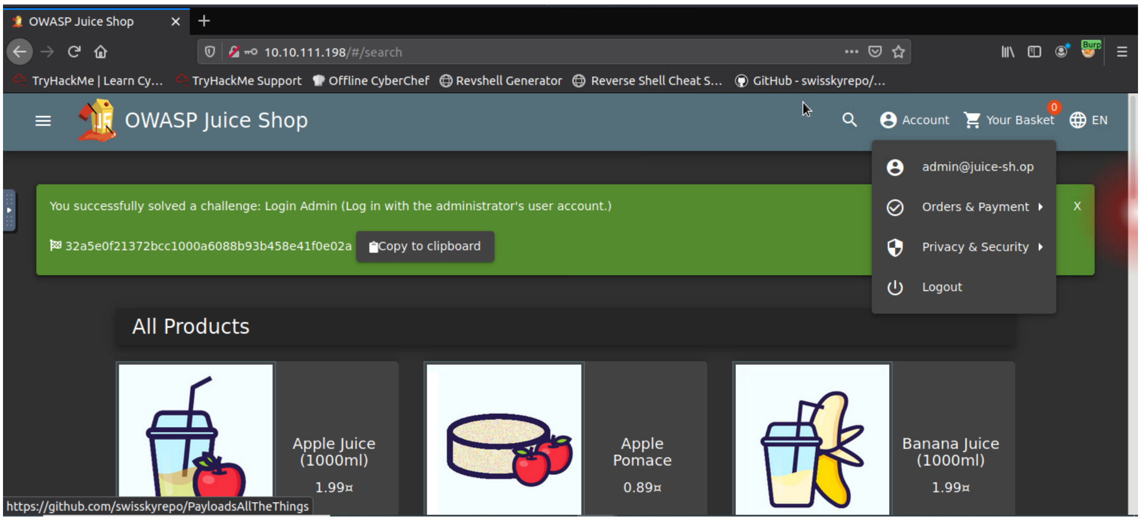
Homework 4

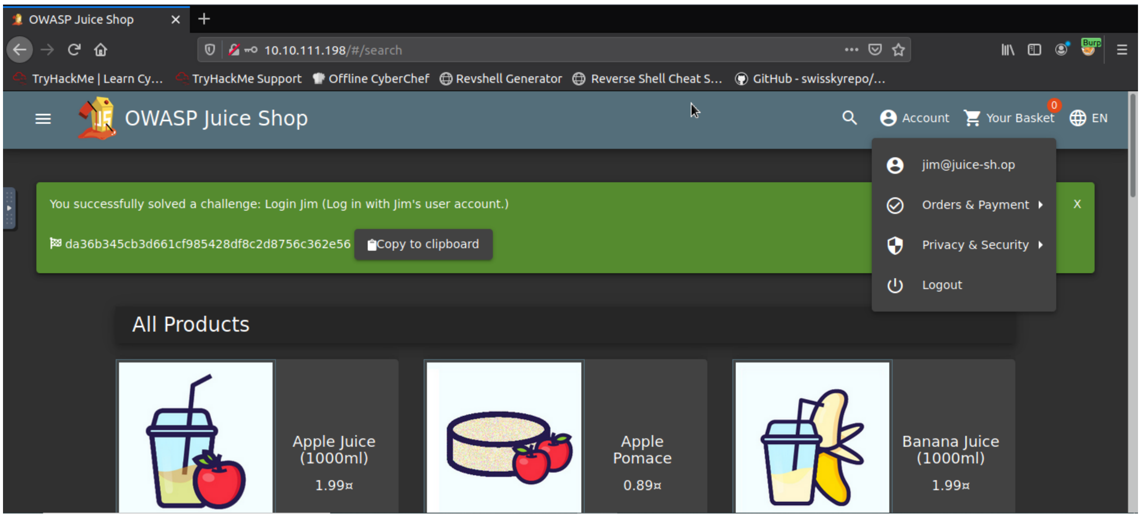
1 To enter the administrator account I had to use burp suite, because first I had to log in and with this tool intercept the data in the log-in, where I edited the email and put ' or 1=1-- in return. This is because the character ' will close the brackets in the SQL query, the 'OR' will return true. As 1=1 is always true. This it will tell the server that the email is valid, and log us into user id 0, which happens to be the administrator account. The -- character is used in SQL to comment out data, any restrictions on the login will no longer work as they are interpreted as a comment



You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)

🏁 32a5e0f21372bcc1000a6088b93b458e41f0e02a

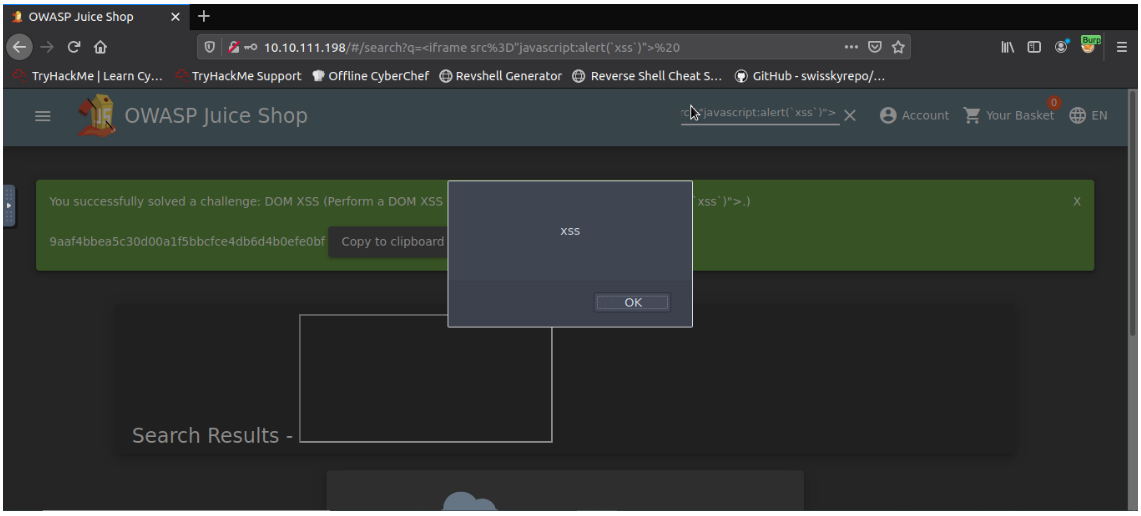
To enter as Jim I did the same as in the admin but in the burp suite, I wrote jim@juice-sh.op'-- . The email address is valid (which will return true), we do not need to force it to be true. And the same works exactly



You successfully solved a challenge: Login Jim (Log in with Jim's user account.)

🏁 da36b345cb3d661cf985428df8c2d8756c362e56

2 For this part I have written in the web search bar a JavaScript script, being this <iframe src="javascript:alert(`xss`)"> . When this bug is generated, we can see that the page is vulnerable to XSS. When this bug is generated, we can see that the page is vulnerable to XSS.



10.10.111.198/#/search?q=<iframe src%3D"javascript:alert(`xss`)">%20

rc="javascript:alert(`xss`)">

You successfully solved a challenge: DOM XSS (Perform a DOM XSS `xss`)">.)

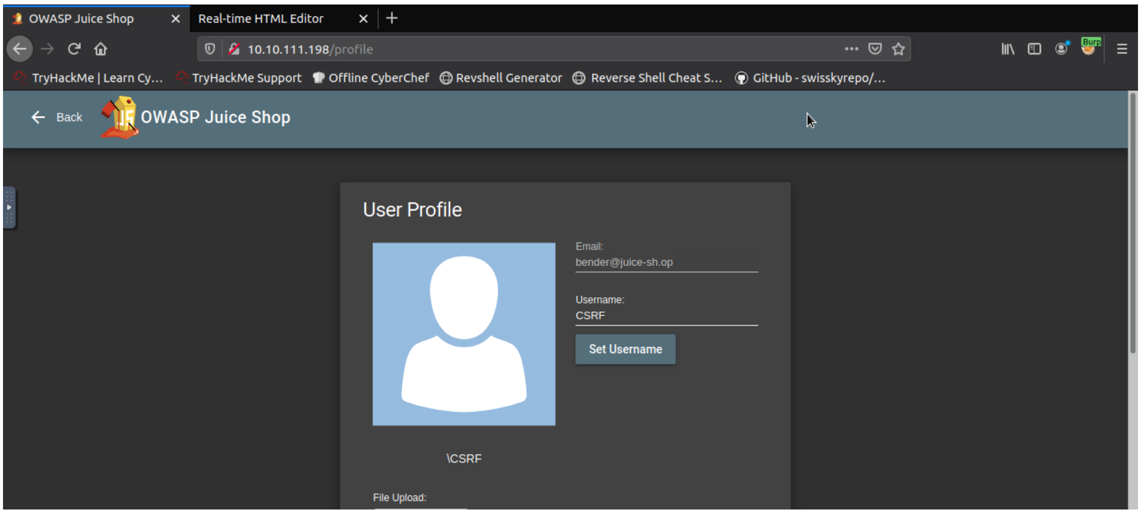
9aaf4bbea5c30d00a1f5bbcfce4db6d4b0efe0bf

xss

3 I navigated to http://htmledit.squarefree.com, with the logged in user that I was going to rename, and with this script I changed it:

```
<form action="http://localhost:3000/profile" method="POST">
  <input name="username" value="CSRF"/>
  <input type="submit"/>
</form>
<script>document.forms[0].submit();</script>
```

And that was enough for the username change and the only way I found to change the name via a CSRF



10.10.111.198/profile

User Profile

Email:
bender@juice-sh.op

Username:
CSRF

\CSRF