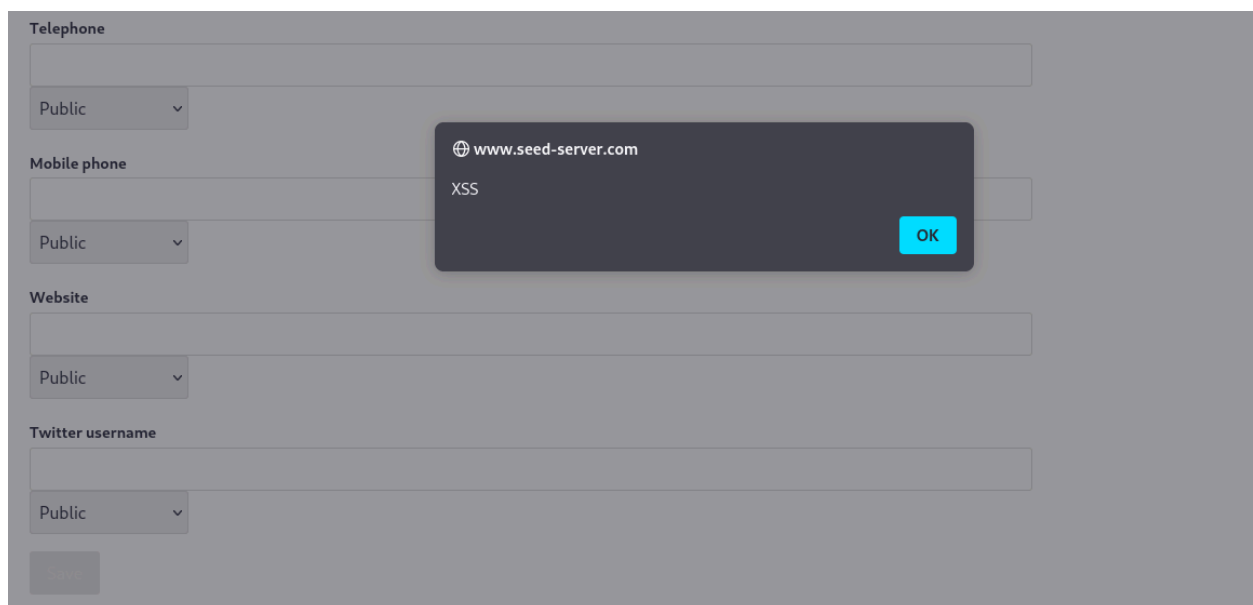Maximiliano Brizzio
CS576 - Lab 3 - XSS

Task 1:

As stated in the lab instructions, I started up the mysql database and the elgg apache web server containers with the command `docker compose up`. Once the services were up and running I opened firefox and went to http://www.seed-server.com/. At the log in page, with the boby:seedboby credentials. I navigated to Boby's profile which was barebones so I decided to add a brief description. I pressed edit profile and scrolled to:
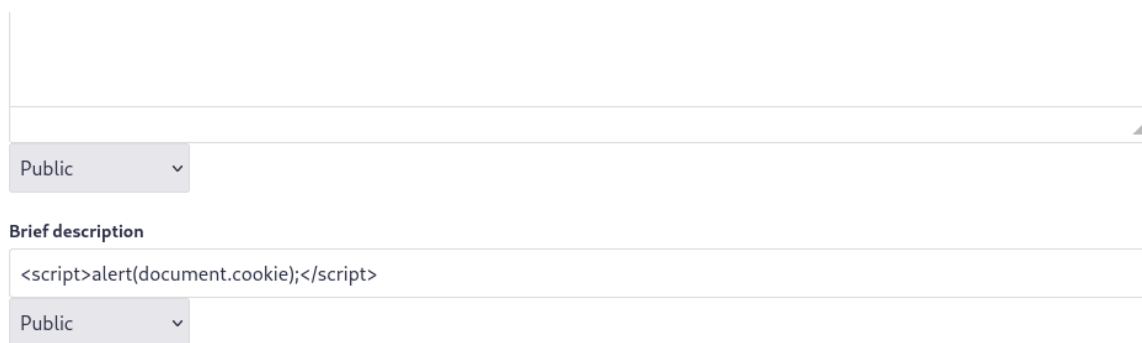

The only thing this code will do is start inline scripting when fed into the HTML code with the single command `alert()` which creates an alert prompt in the browser.
With this description, I pressed save and immediately the alert came up:

Now back at the profile, everytime I refresh the site, the alert appears. Notably, after doing this for both profiles of Alice and Boby, when navigating to the members page, the alert would appear twice.
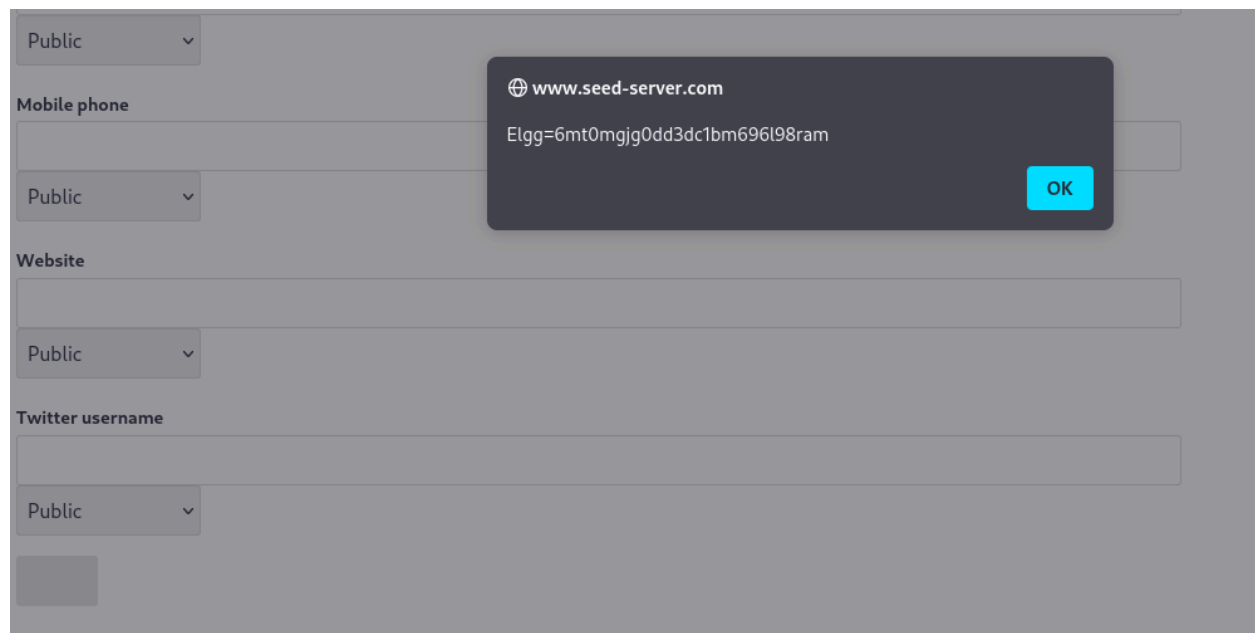
Task 2:

For this task I'm asked to get the user's cookies to appear upon visiting my profile (or in this case Alice's). To begin, I navigate just as I did before to the edit profile page. In the brief description box I type: `<script>alert(document.cookie);</script>.`

Public

Brief description

<script>alert(document.cookie);</script>

Public

Now when I press save, an alert comes up displaying my cookies:

Public

Mobile phone

Public

⊕ www.seed-server.com

Elgg=6mt0mgjg0dd3dc1bm696l98ram

OK

Website

Public

Twitter username

Public