

## Task 1:

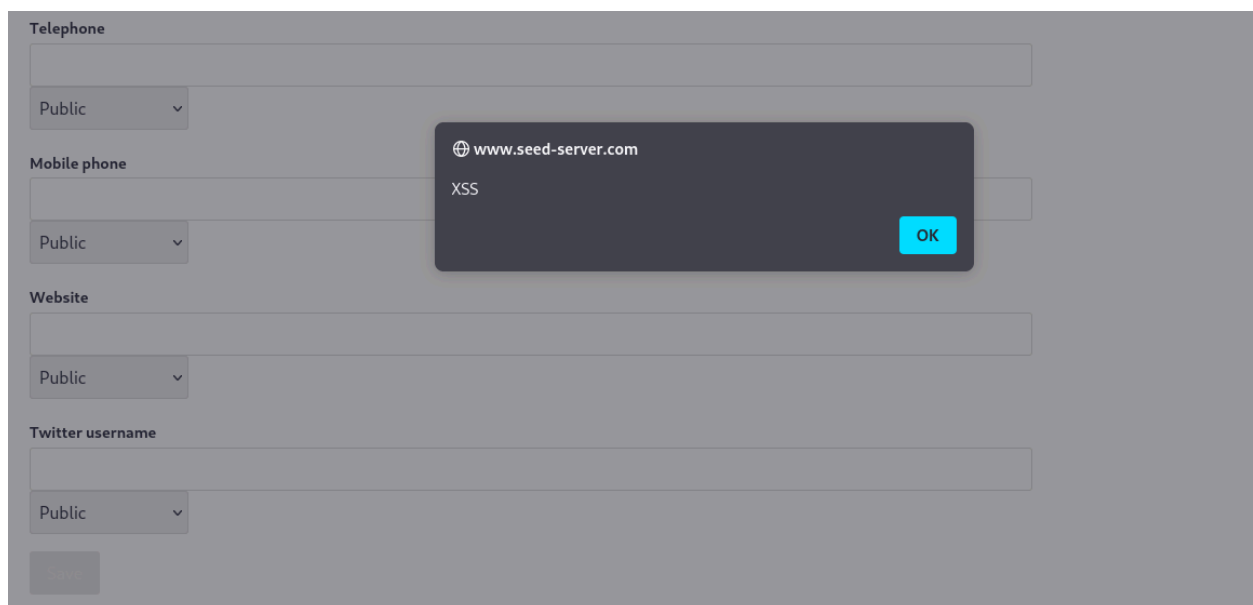
As stated in the lab instructions, I started up the mysql database and the elgg apache web server containers with the command `docker compose up`. Once the services were up and running I opened firefox and went to <http://www.seed-server.com/>. At the log in page, with the boby:seedboby credentials.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

Brief description

`<script>alert('XSS');</script>`

Public

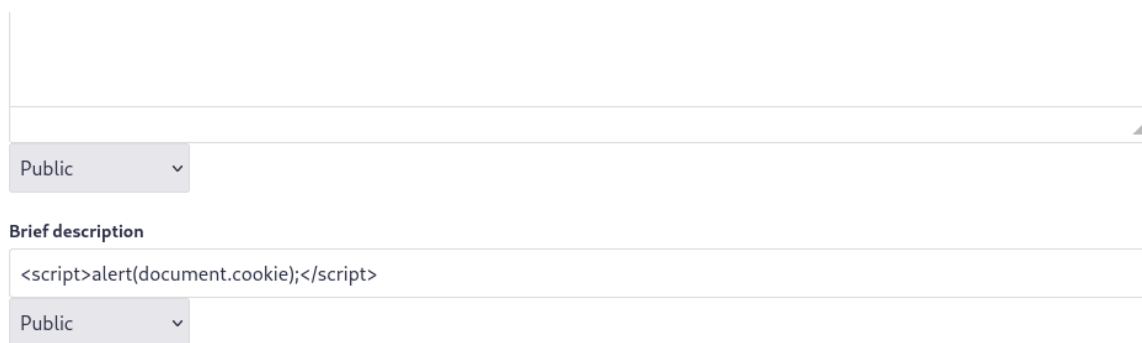
The only thing this code will do is start inline scripting when fed into the HTML code with the single command `alert()` which creates an alert prompt in the browser. With this description, I pressed save and immediately the alert came up:



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

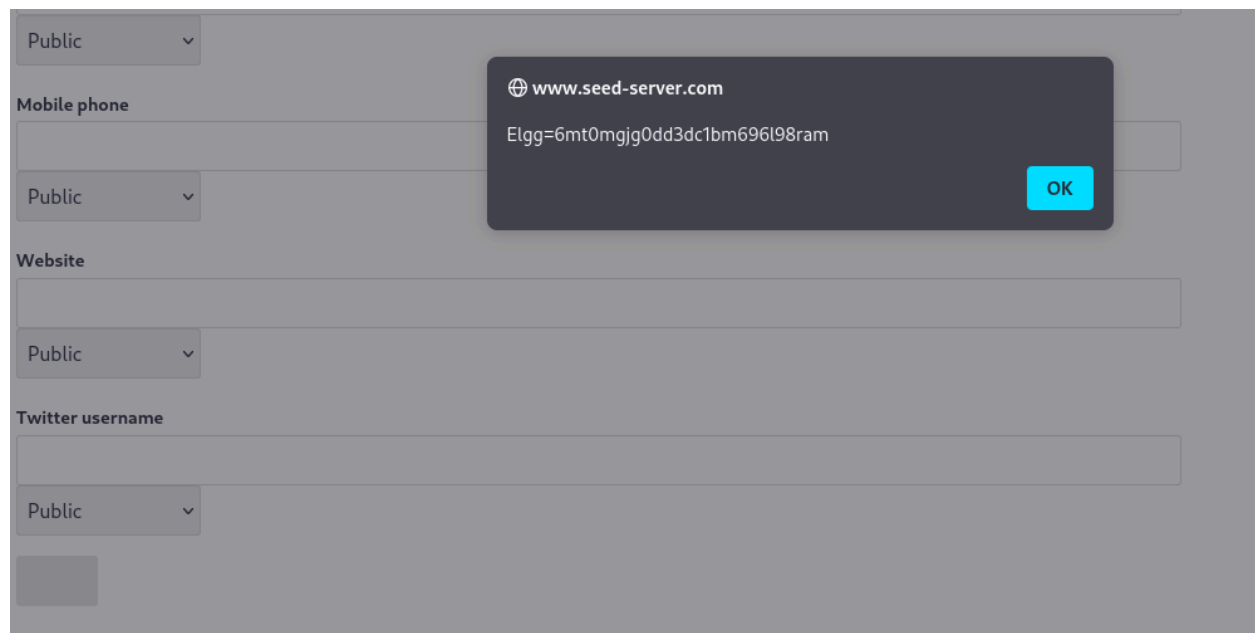
## Task 2:

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>`.



The screenshot shows a portion of a web form. At the top is a large text input field. Below it is a dropdown menu with 'Public' selected. Further down is a section labeled 'Brief description' with a text input field containing the code `<script>alert(document.cookie);</script>`. Below this field is another dropdown menu, also with 'Public' selected.

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



This screenshot shows the same 'Edit profile' form as before, but with a dark grey JavaScript alert box overlaid in the center. The alert box has a globe icon and the text 'www.seed-server.com' at the top. Below that, it displays the cookie string 'Elgg=6mt0mgjg0dd3dc1bm696l98ram'. A red 'OK' button is in the bottom right corner of the alert box. The background form is dimmed, showing the 'Public' dropdowns for 'Mobile phone', 'Website', and 'Twitter username'.