Cross-Site Request Forgery (CSRF) Attack Lab

作者：黄禧敏

学号：57119109

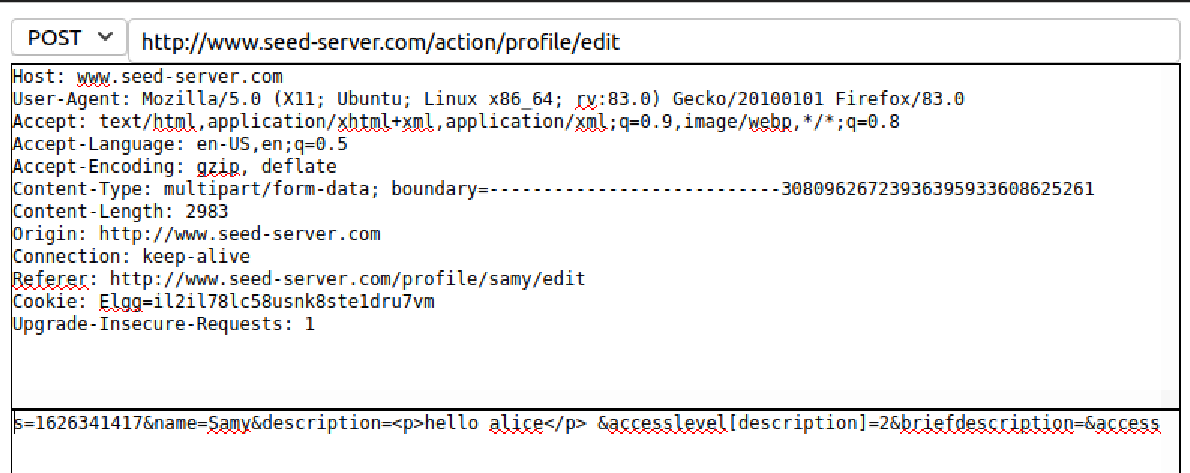
日期：2021/7/17

**Task 1:**

观察HTTP request



Cookie为用户身份标识符



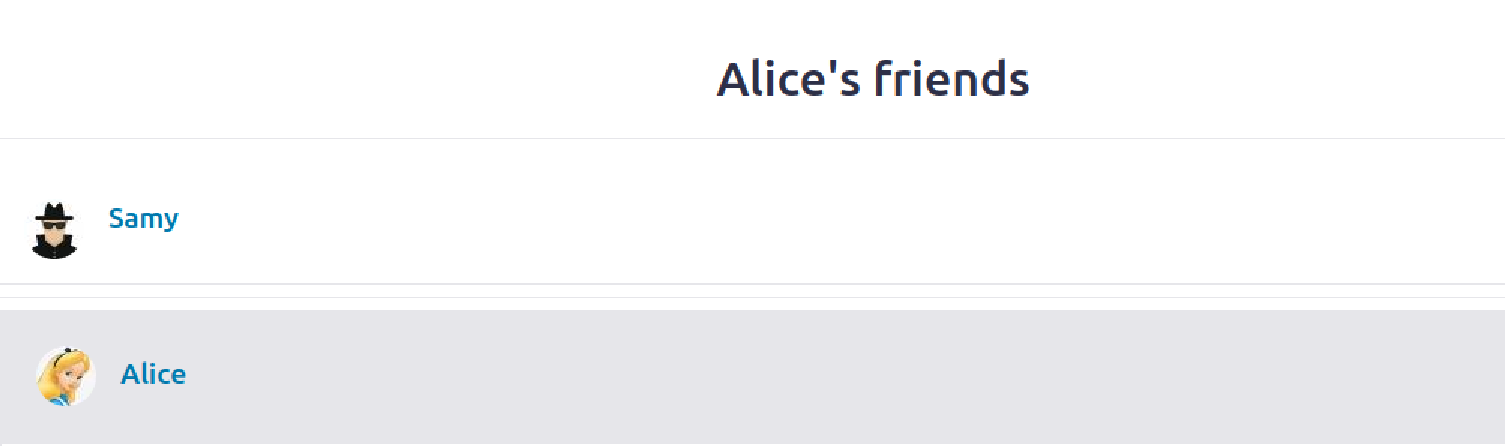
**Task 2:**

CSRF Attack using GET Request

修改恶意网页源码，将目标链接插入某图片标签内，使得目标用户在仅打开网页而不点击的情况下完成攻击；

Friend为目标用户id，samy自己的id为59；



Samy通过邮件将恶意网址链接发给Alice, 诱使Alice点击链接，完成攻击；

**Task 3:**

修改Alice 的个性签名为Samy is my hero.

首先登入Samy账号，修改自己的个性签名，使用Http Tool观察Post请求；



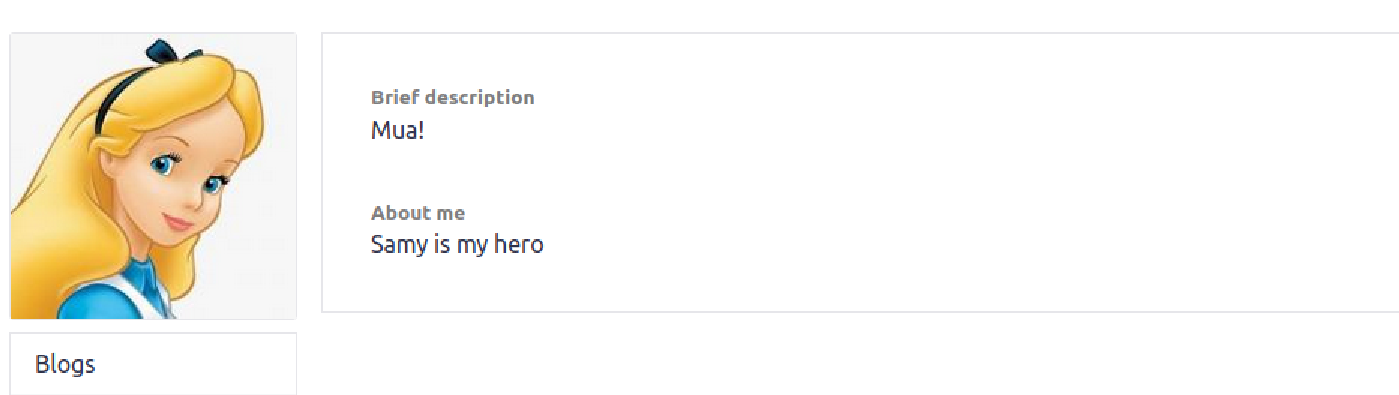
其中下面的briefdescription为个性签名，descripion为about me，guid为用户编号；

根据以上信息修改attacker的网页源码；



注意下面的p.action的网址为点击提交后的post地址；

诱使Alice点开链接后攻击成功；



**Question:**

1. 如何获取特定用户guid：

在member中选择send massage，url中会出现sent\_to，即对应用户的guid；

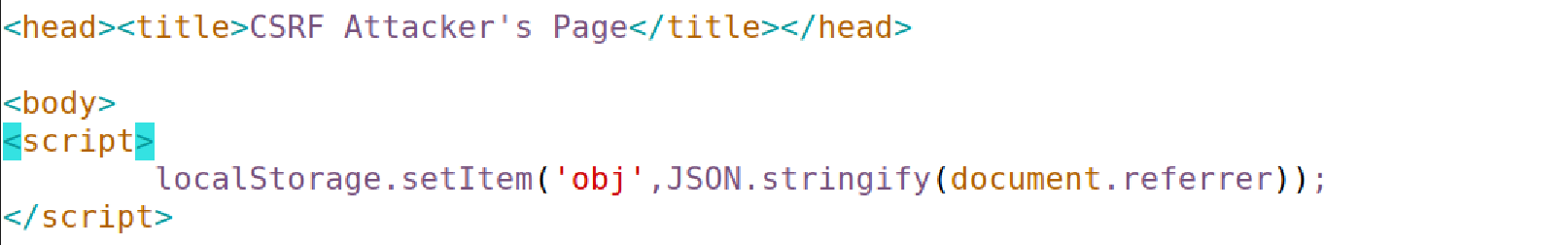


1. 在Samy预先不知道谁点击恶意网站的情况下，如何完成攻击：

可以由question1预先维护一个用户名和guid的对应表，此处由于用户较少，直接维护内置数组；

在index.html页面存储document.referrer，用来判断点击网页的是哪个用户，在editprofile.html中将用户对应guid传入field中，即可完成攻击；

Index.html



Editprofile.html

