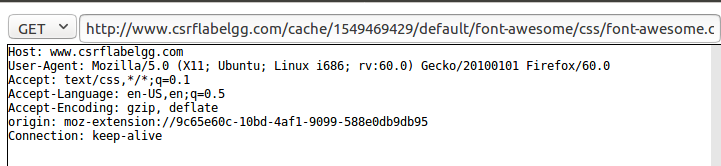
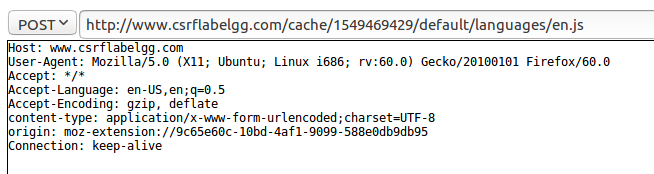
任务一：、

GET：



POST：



变量：

Host：接收请求的服务器地址

User-Agent：发送请求的引用程序名

Accept：发送端希望接收的数据类型

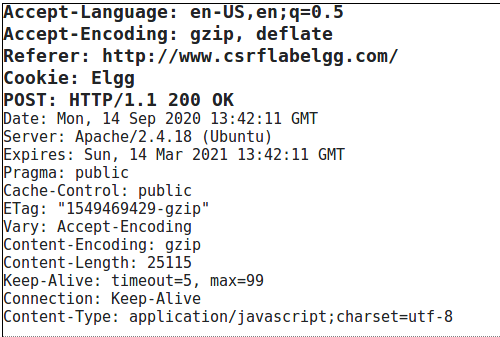
Accept-Encoding：通过服务器端可以发送的编码格式

Accept-Language：通过服务器端可以发送的语言

Origin：当前请求资源所在页面

Connection：指定与连接相关的属性

响应：



变量：

200：请求成功（HTTP对请求成功的标准应答）

Date：响应时间

Expires：响应过期的时间

Server：服务器应用程序软件的名称和版本

Cache-control：缓存机制是否可以缓存及缓存类型

Content-length：响应正文的长度

Content-encoding：响应正文的数据压缩格式

Content-type：响应正文的类型（图片或者二进制字符串）

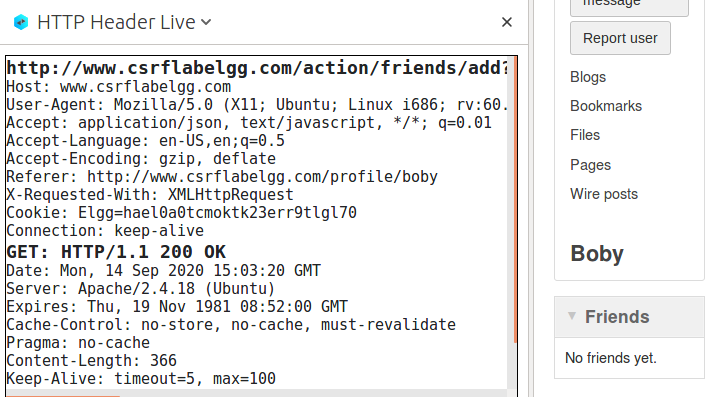
Vary：下游代理使用缓存响应还是从原始服务器请求

Etag：请求变量的实体标签的当前值

Pragma：实现特定的指令

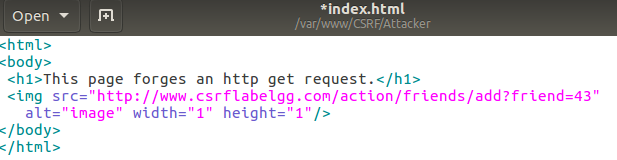
任务二：

1、采用samy账户加账户bob的好友，获取URL信息





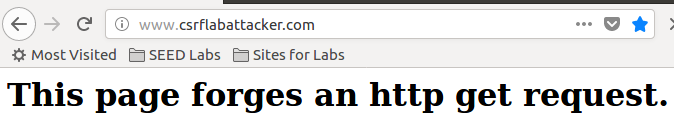
1. 在attack路径下添加index.html文件，其中插入加boby为好友的URL



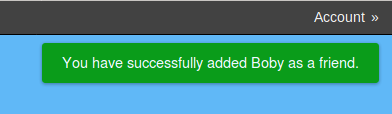
1. boby将攻击网页链接发送给alice

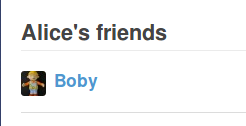


1. alice点击链接，跳转网页：



5、退出网页后显示添加好友成功

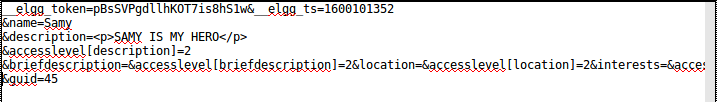




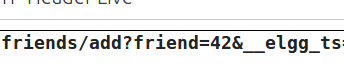
任务三：

1. 用samy账户修改主页信息并观察http报文





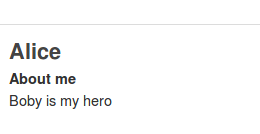
1. 通过加alice好友时获取的http报文信息得到alice的id



1. 编辑攻击网站



4、将攻击网站发送给Alice，Alice访问网站后成功修改主页：



问题一：

通过寻找alice修改主页的源码中找到其user id

或者通过加alice为好友，通过观察http报文找到user id

问题二：

不能。

因为需要提供特定用户id

任务四：

修改函数，开启对策：  


Alice再次点击攻击网站，提示错误，主页修改失败：



原因分析：

服务器在每个网页上随机插入一个机密值，当请求被该页面发出时，该机密值会被包含在请求中。通过这个机密值，服务器可以判断该请求是不是跨站请求。由于在浏览器的控制下，不同页面并不能得到彼此的机密值，并且该机密值对于不同用户而言也是不同的，所以对于攻击者来说机密值不可破解。