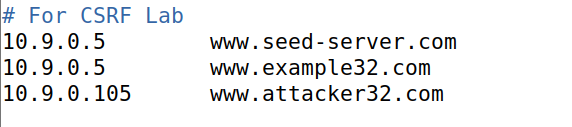
操作系统实验二实验报告

姓名：高昂 学号：57119123

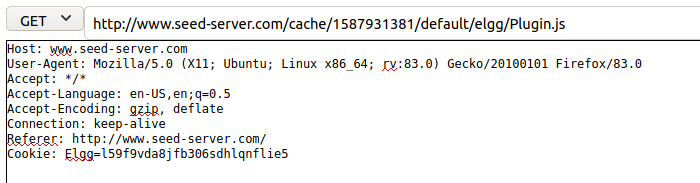
启动客户端

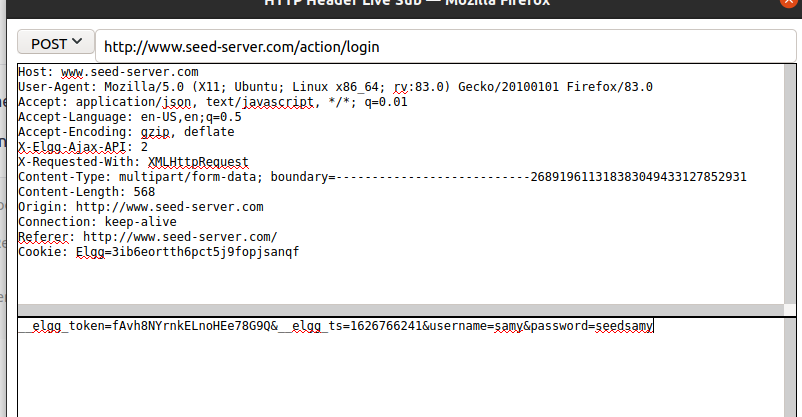




Task 1

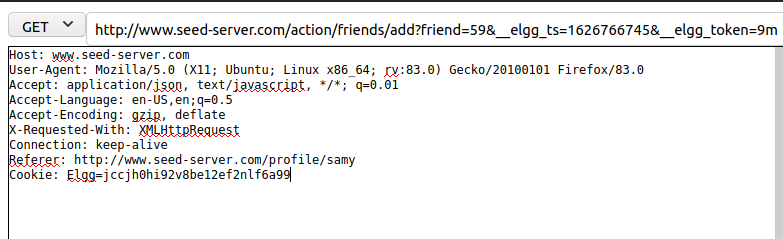
打开 Http Header Live，捕获网站的 get 和 post 请求(登陆Samy）：





Task 2:

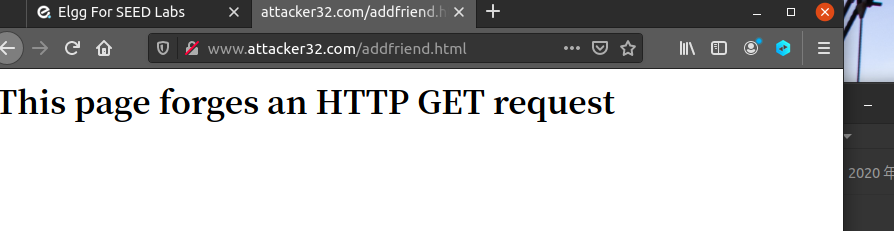
添加好友的请求报文



攻击代码：



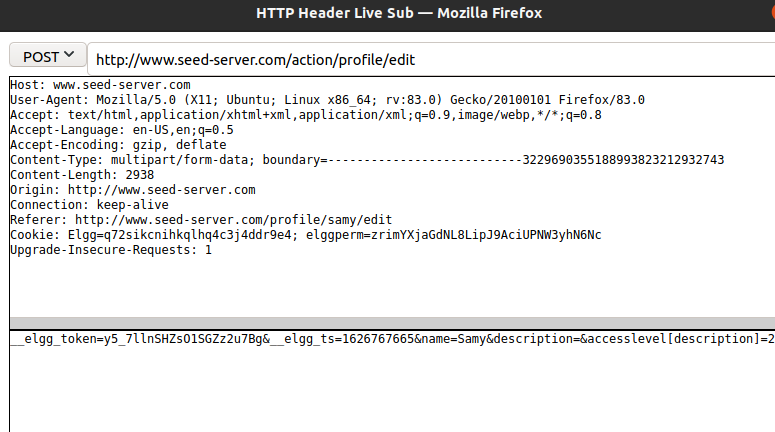
攻击结果



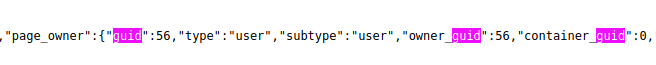


Task 3

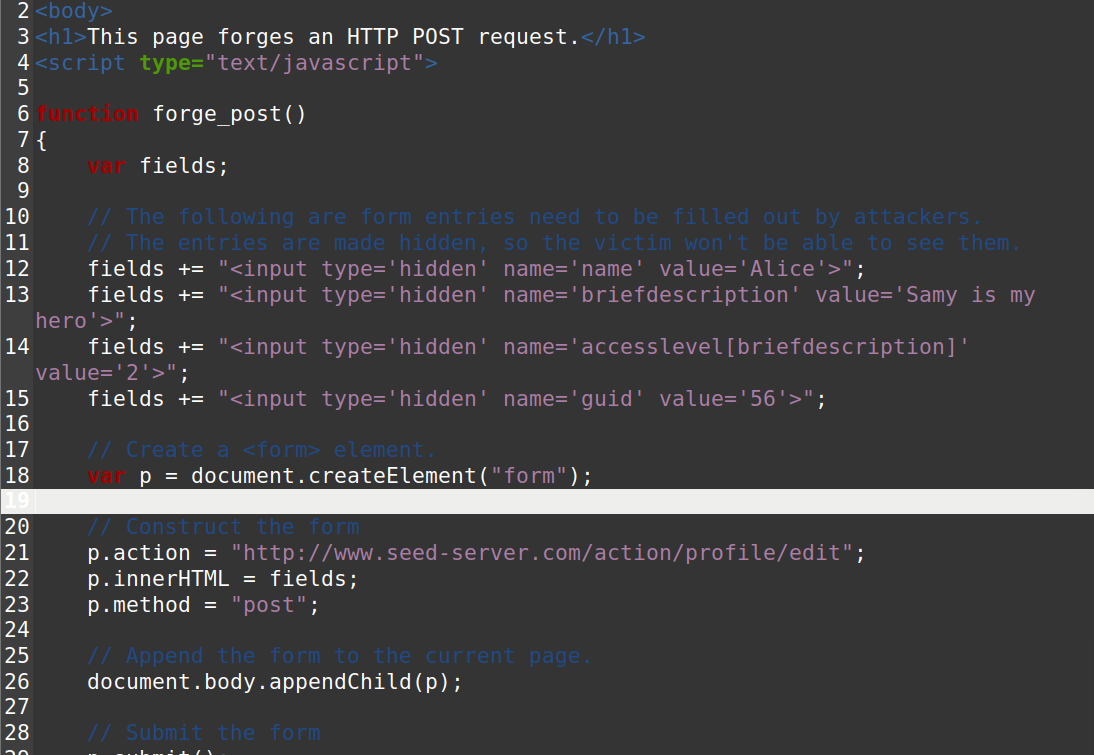
Samy 通过修改自己的简介来获取 post 报文:



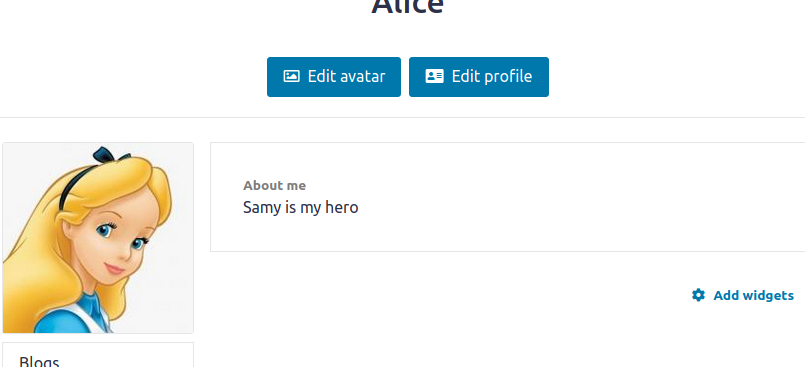
访问alice的主页可以得知pageower（即alice）的guid为56



编写攻击代码



攻击成功

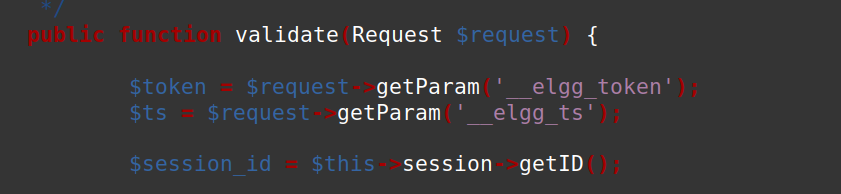


Q1: Boby可以用自己的账号进入Alice的主页，然后查看页面源代码，在其中搜索uid，便可以找到Alice的uid。

Q2: 由于此网站 uid 可通过访问用户主页源代码查出，所以我们可以通过在代码中插入所有用户uid，这样无论谁访问我们的钓鱼网站，就会被攻击。

Task 4

在image\_www/elgg/Csrf.php中开启防御措施(删除return语句)，并重新构建服务器：



然后我们打开 Alice 的账号主页，将之前的攻击结果删除，再次使用 Alice 浏览



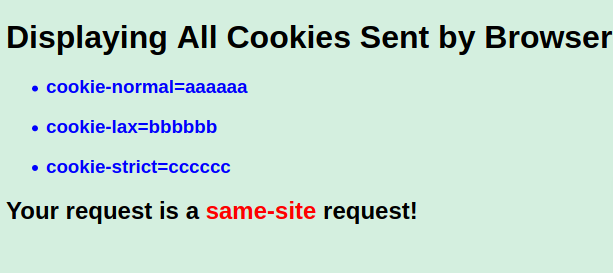
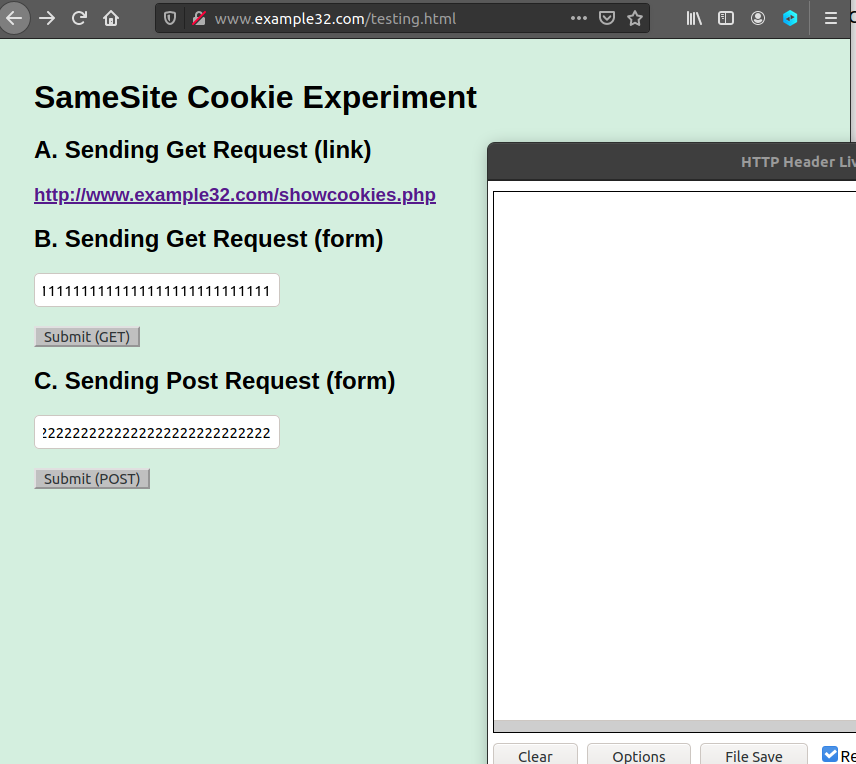


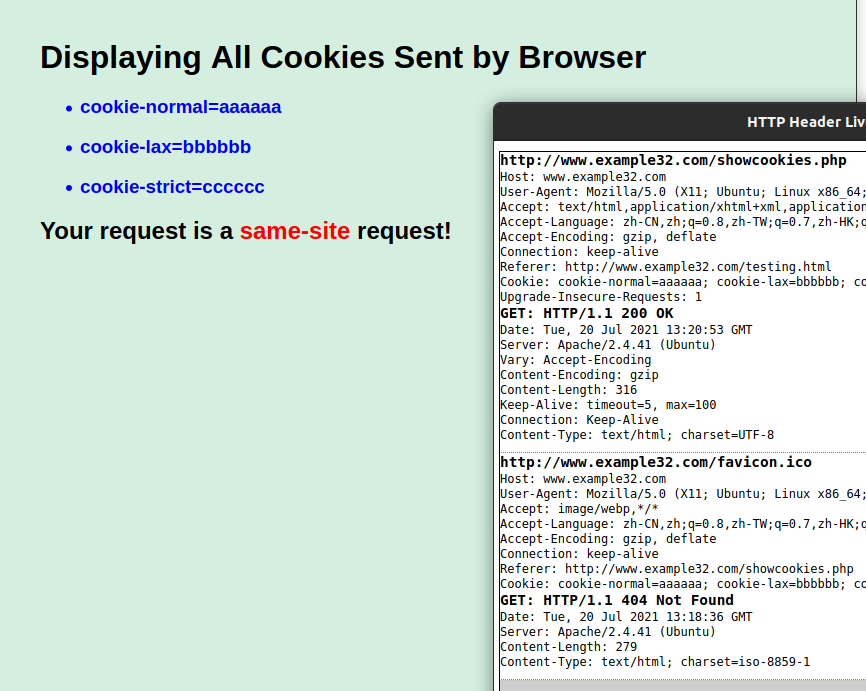
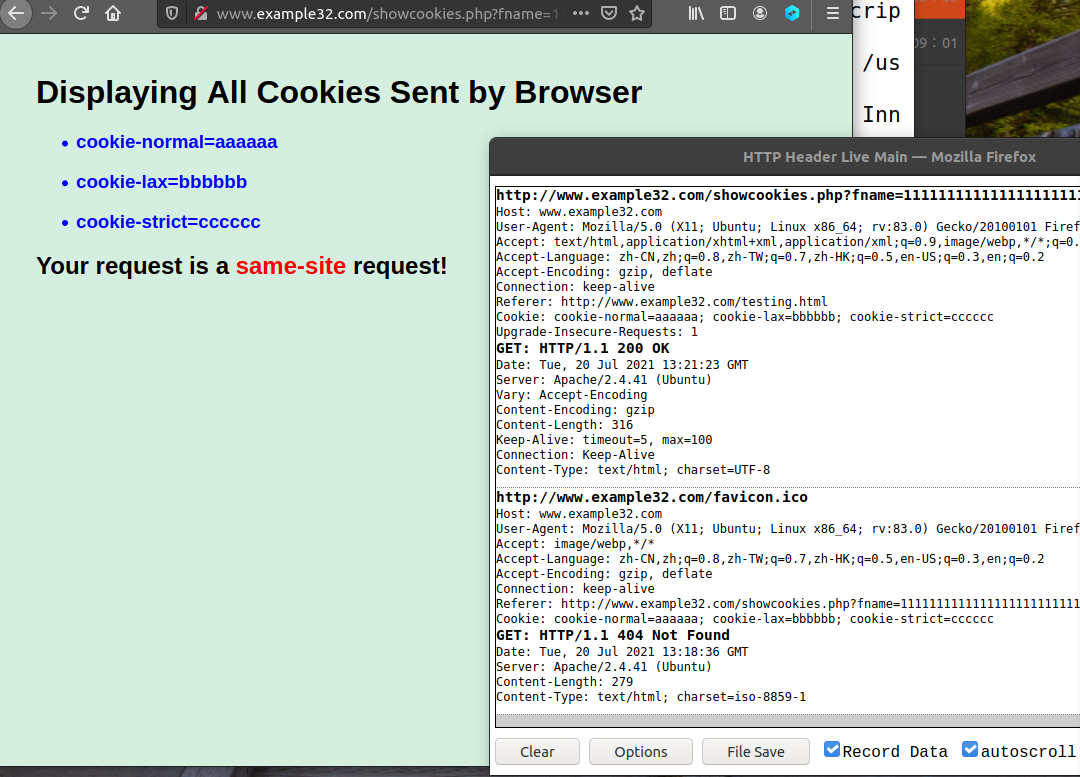
攻击失败

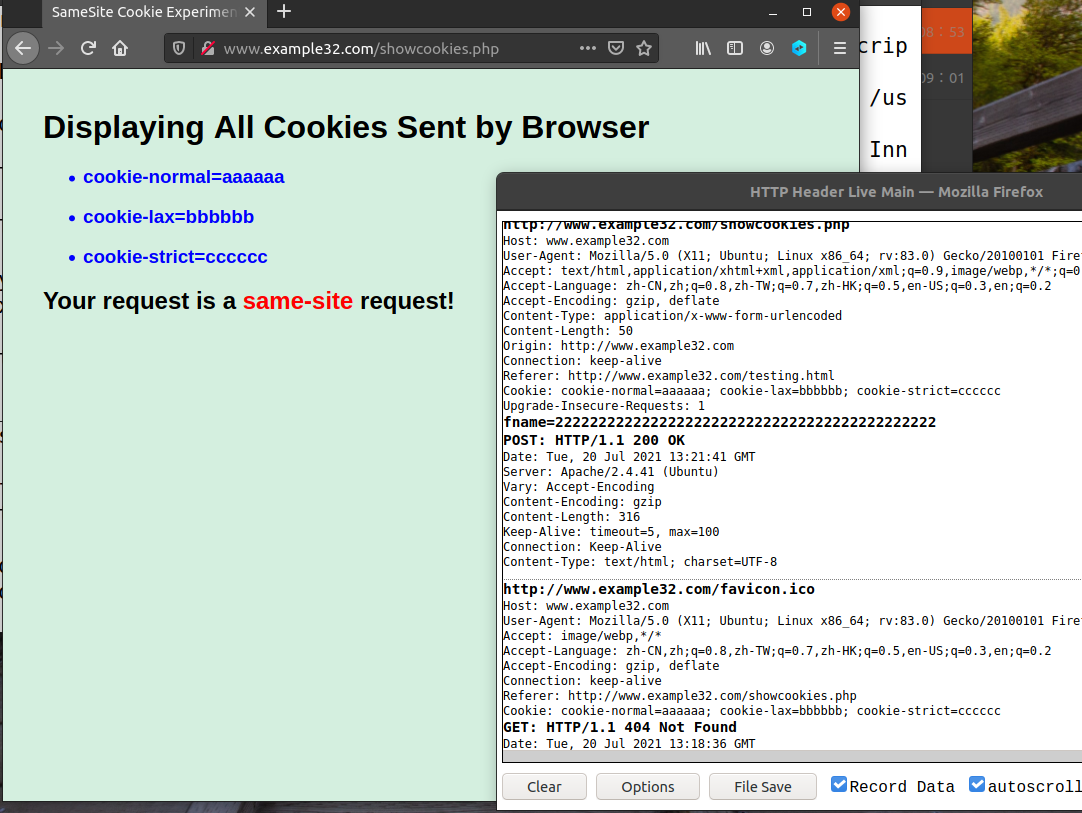
原因

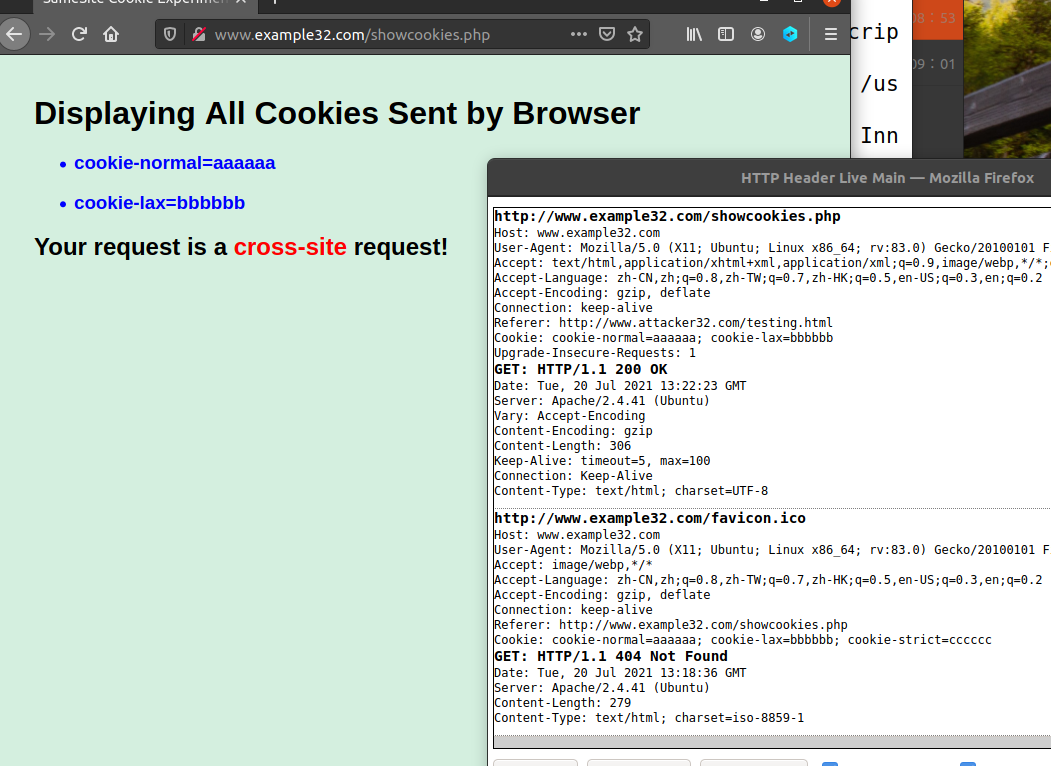
令牌信息是通过数据库中的网站秘密值、时间戳、会话 id、随机生成的会话字符串等信息，经过 MD5 加密后产生的。除非能够直接攻入网站数据库查询这些信息，否则只能暴力破解，所以攻击者的攻击成本大大上升，从而防范 CSRF 攻击。

Task 5

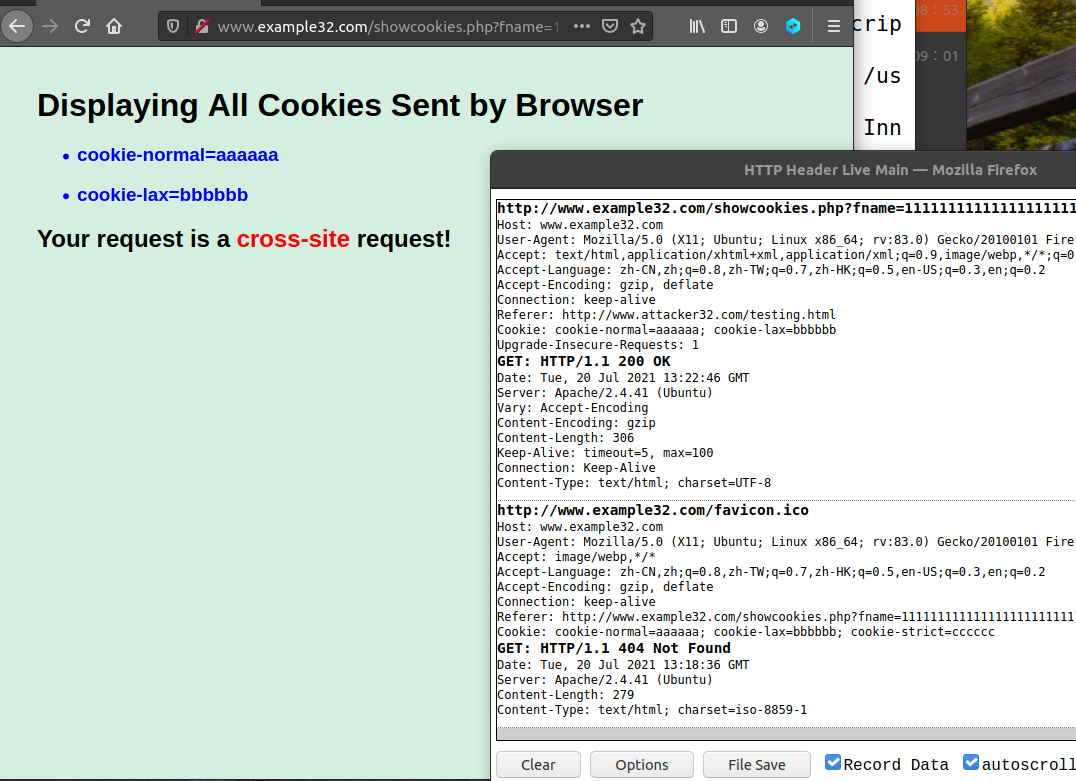




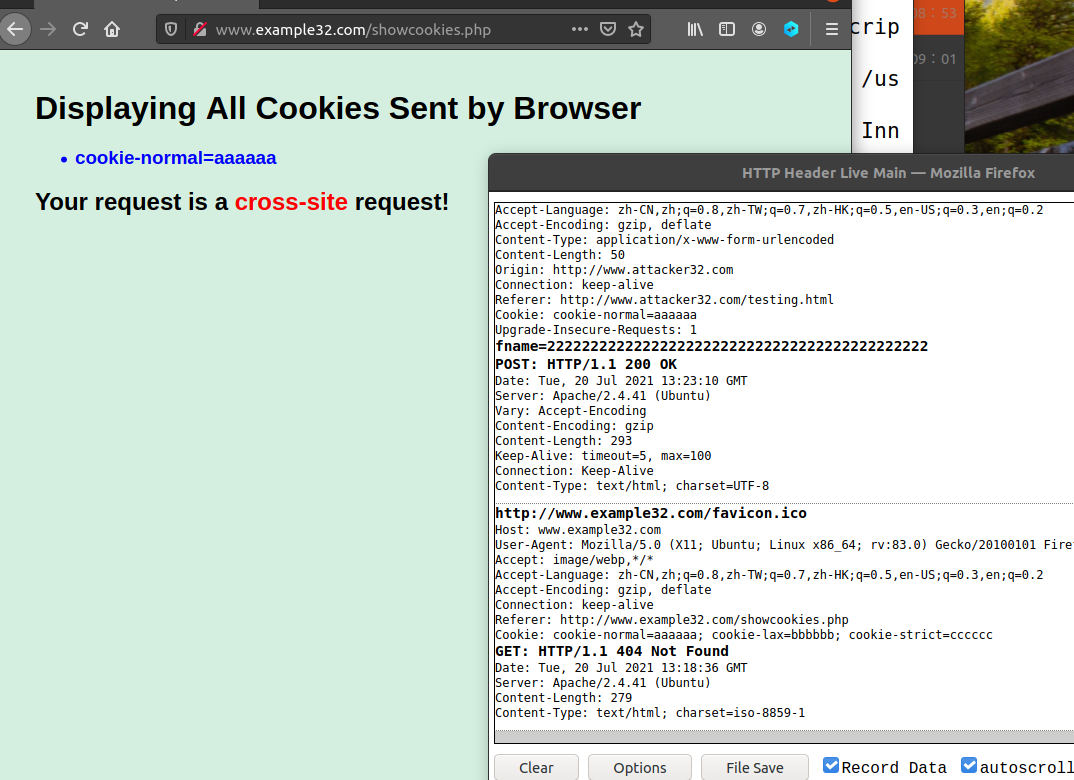




Get



Post



结论：

1. 当前网址和目的网址相同时（same-site），

三种 cookie 都发送。

1. 当前网址和目的网址不同时（cross-site），

Normal-cookie 仍然无差别发送，

Strict\_cookie 不发送，

Lax\_cookie 是在请求数据时发送，在上传数据时不发送。

1. 当在浏览器中设置SameSite来防止CSRF攻击

strict 属性基本可以防范所有 CSRF 攻击，但对使用有一定影响；

lax属性基本可以防范大部分 CSRF 攻击，对使用的影响更小