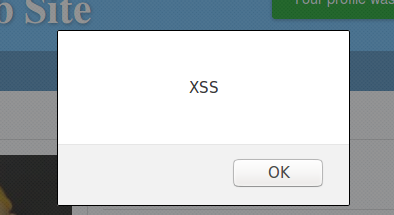
任务一：

直接输入JavaScript程序



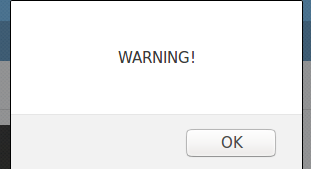
浏览该页面时，程序被执行，出现弹窗：



通过链接引入JavaScript程序：



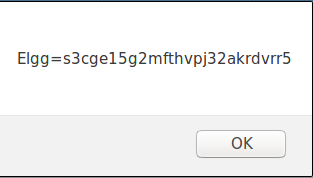




任务二：

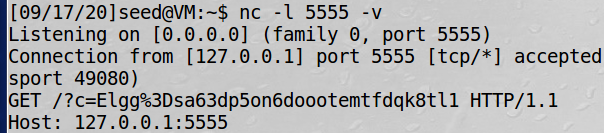


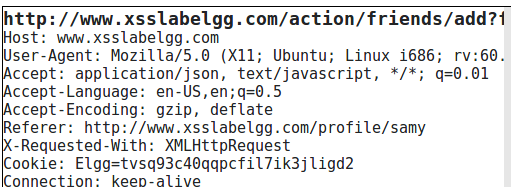
通过javascript语句显示当前用户的cookie



任务三：

通过将用户的cookie值返回到http请求中，向攻击者展示用户cookie  

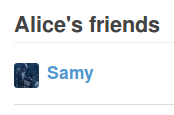



任务四：  
加samy好友的http报文：  




编写samy主页：  

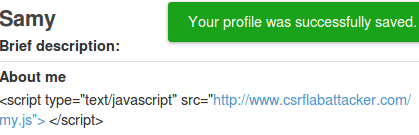

用户浏览samy主页时，被添加为好友



问题一：得到服务器在每个网页上随机插入的一个机密值和时间戳的值，用于验证是否是跨站请求

问题二：不能

如图所示，JavaScript代码被当作文本，不被执行



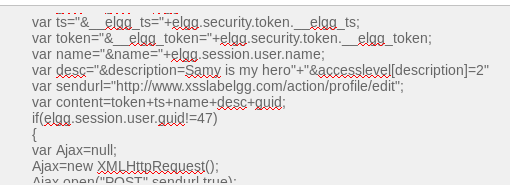
任务五 ：

编辑主页，得到http post报文：

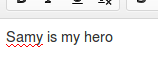






修改samy主页：  


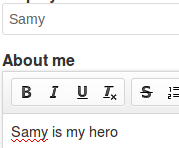
Alice浏览samy主页后，主页上出现文字：



问题三：

避免攻击者samy自己的主页也被攻击

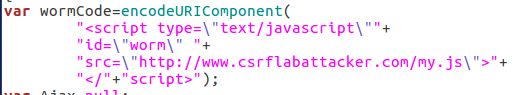
将该条件去掉后：



Samy浏览自己的主页后，自己的主页也被篡改了

任务六：

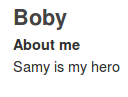
方法一：

修改网页文件：  


将对应文件放入samy主页：  


Bob浏览samy主页：





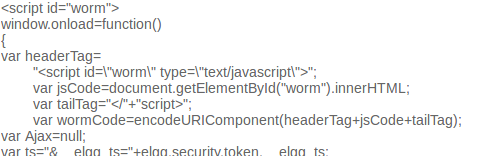
Alice浏览bob主页：

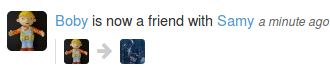
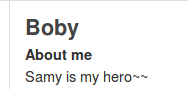




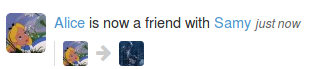
方法二：（DOM）

对于samy的主页程序进行修改：

  
boby浏览samy主页：

Alice浏览boby主页：


Charlie浏览alice主页：


任务七：

修改host文件：  


采用webpage浏览网站结果：

