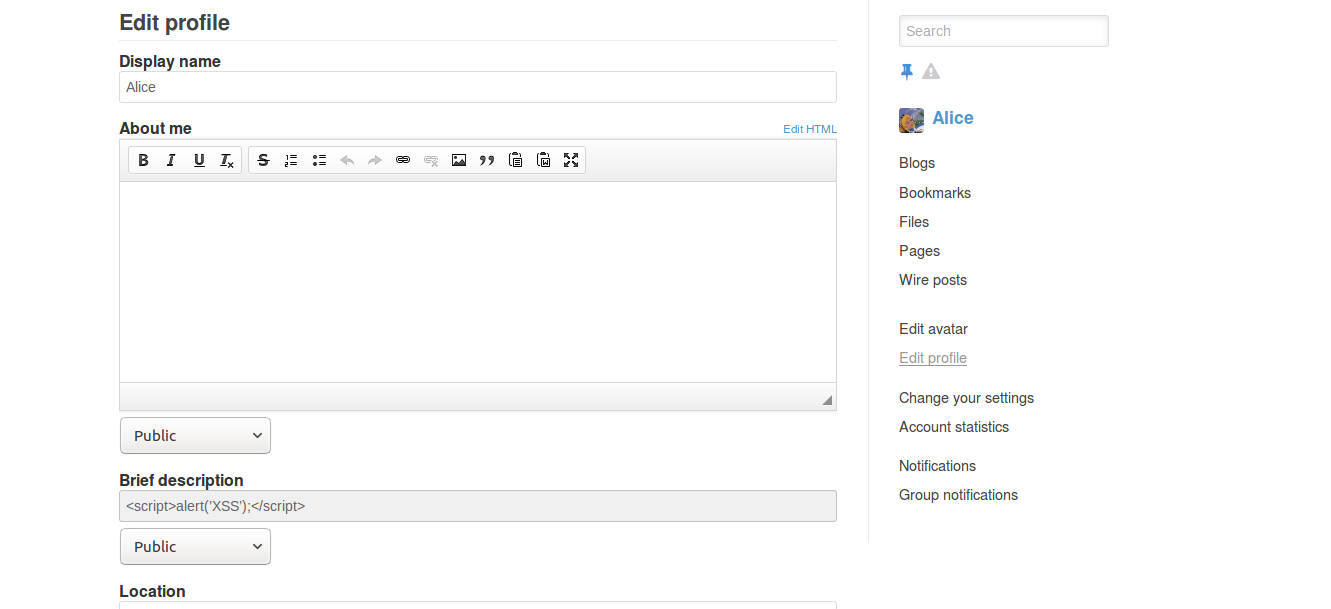
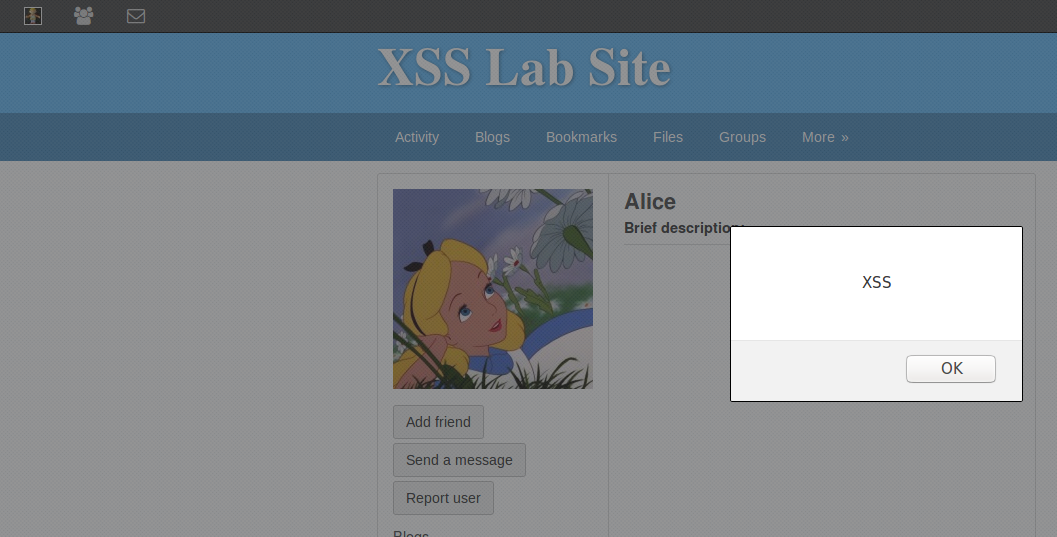
Task1:

将代码<script>alert(’XSS’);</script>写入alice的brief description中，效果如图



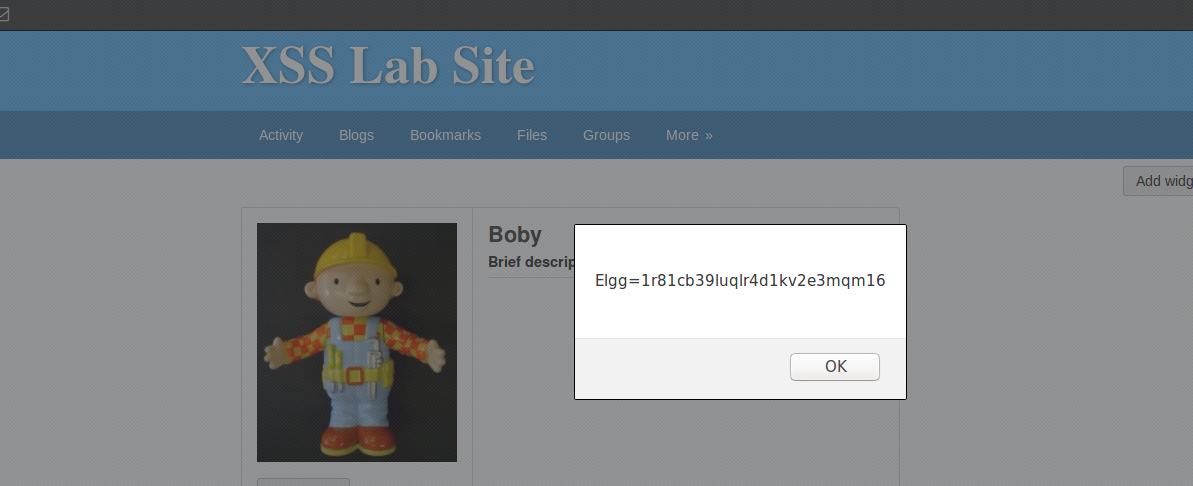
任何用户在看alice的个人简介时都会跳出窗口，如图



Task2:

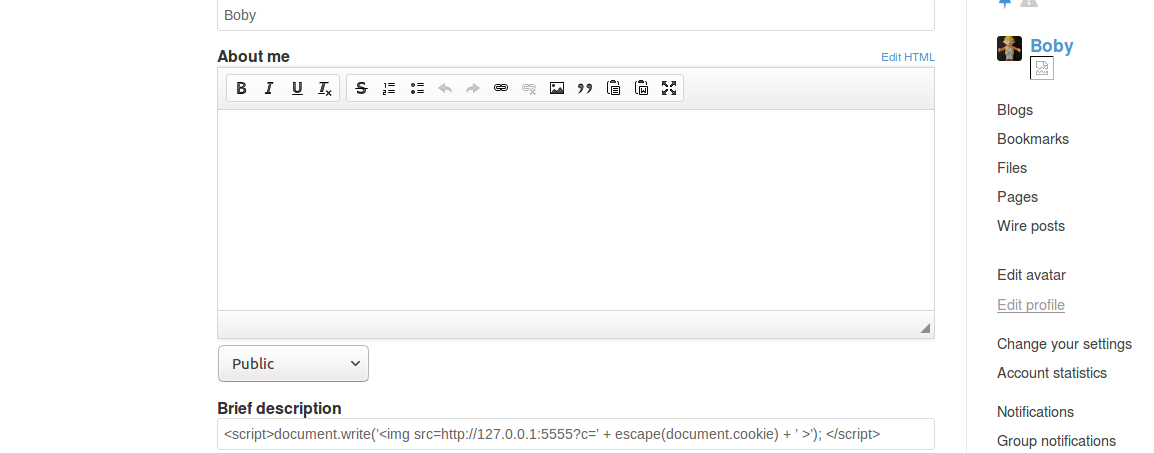
将代码<script>alert(document.cookie);</script>写入boby的brief description中，

当boby打开他的个人资料时会弹出窗口显示他的cookie

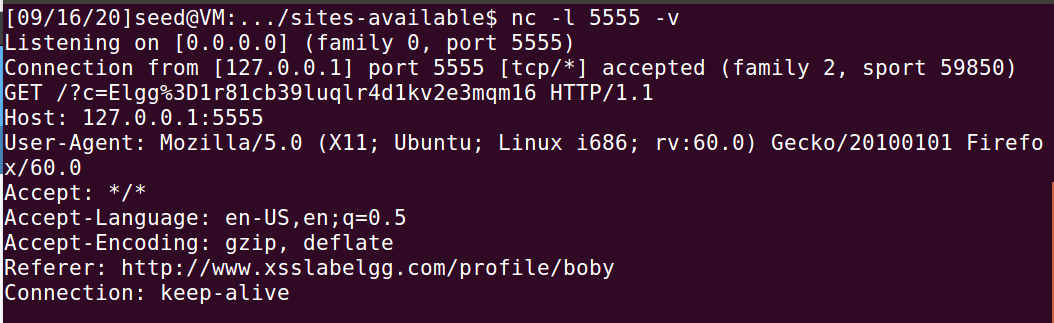


Task3:

在boby的签名中写入代码，将cookie发送到ip127.0.0.1的5555端口

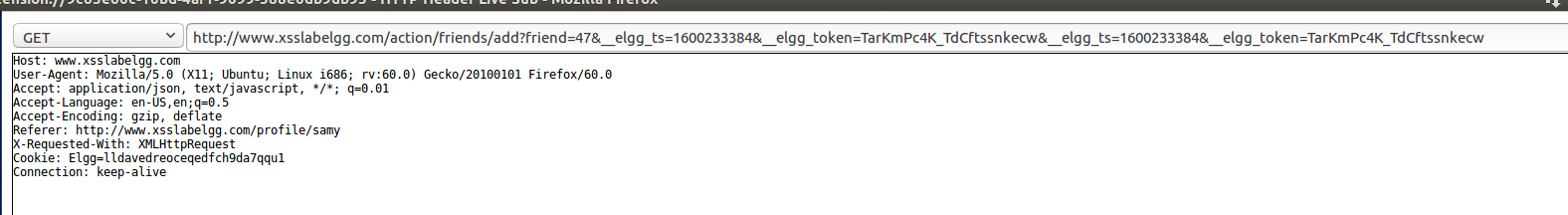


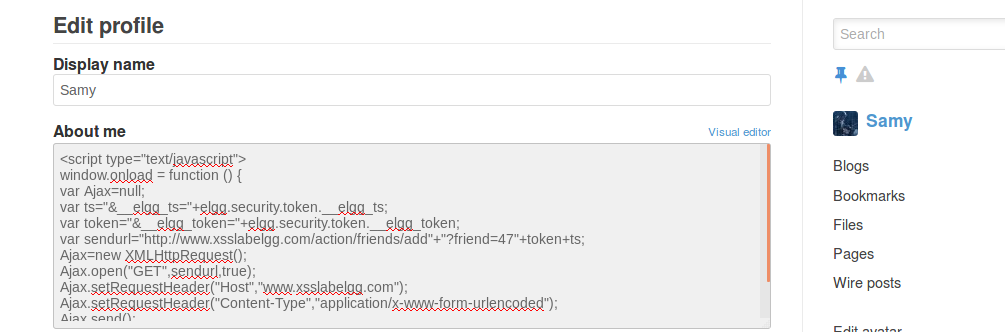
在终端中使用nc命令，可以看到GET报文中有boby的cookie



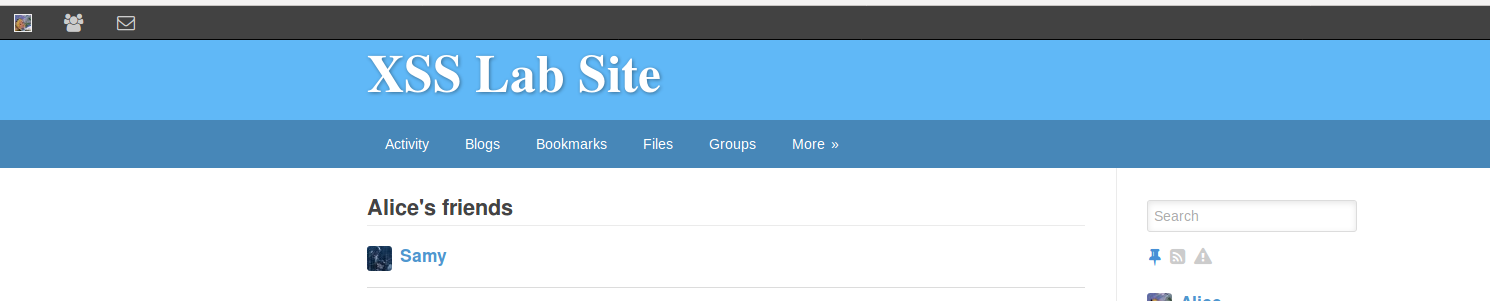
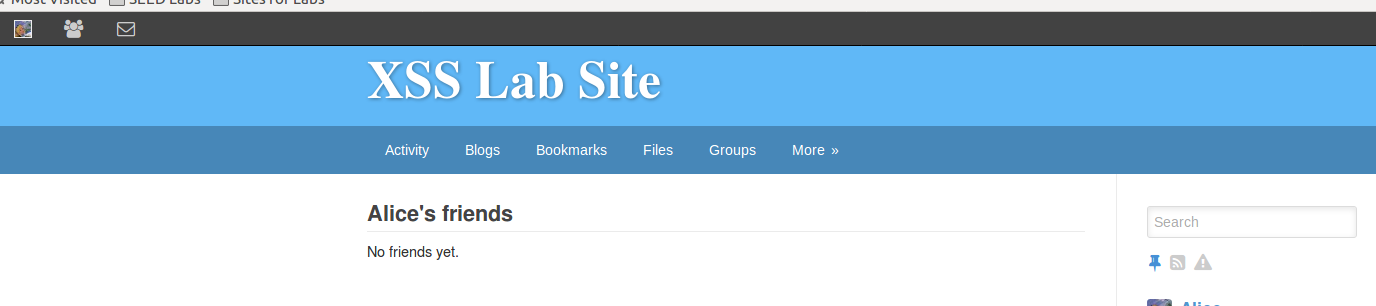
Task4:

抓包查看添加好友的GET报文格式

在samy的个人介绍中写入代码和参数



保存后直接回到samy的个人资料界面发现samy自己添加自己为好友，其他用户访问samy的个人资料也会自动添加其为好友

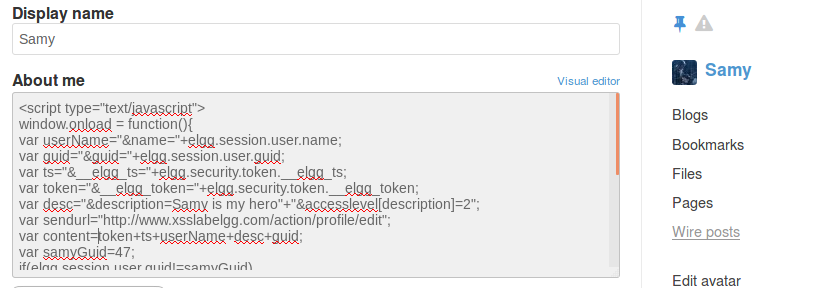


Task5:

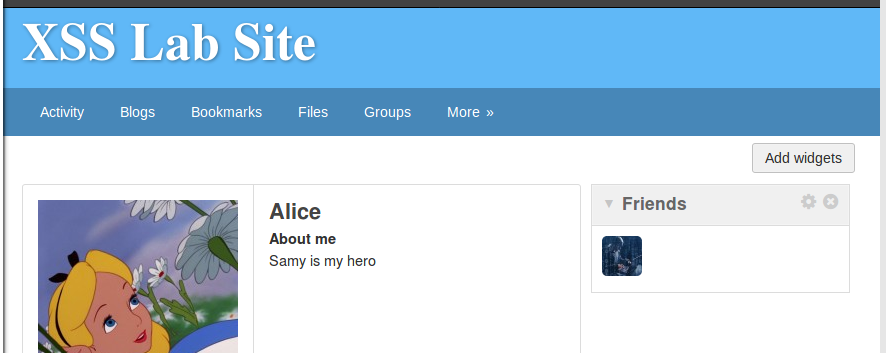
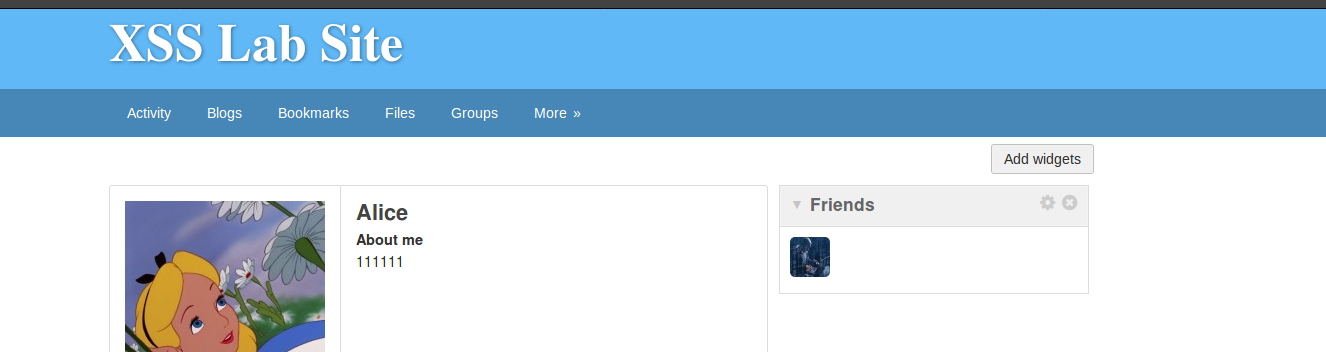
通过抓包查看修改个人介绍的报文格式



在samy的个人介绍中写入代码和参数

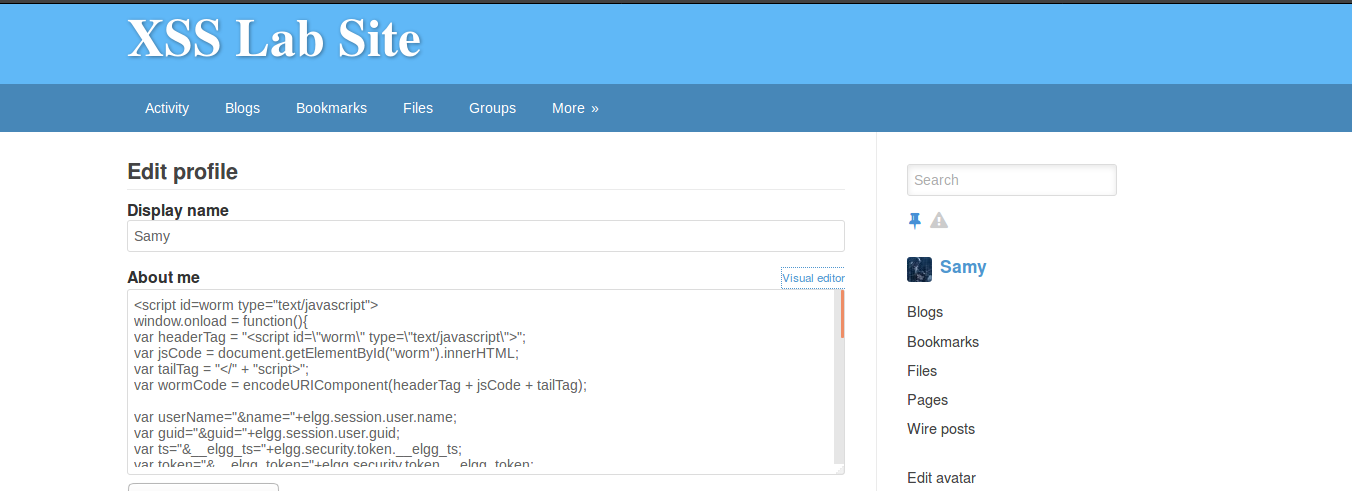


访问samy的个人资料后alice的个人简介从111111变为samy is my hero

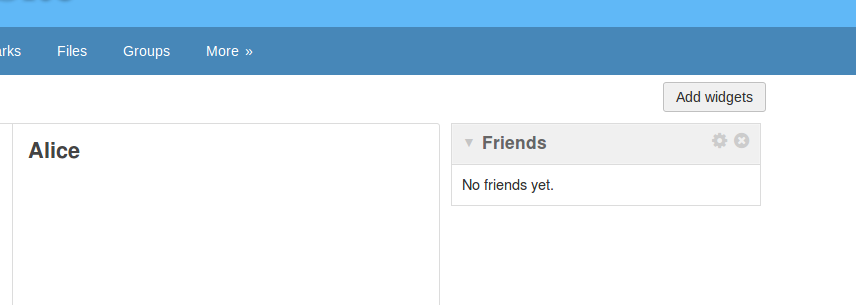


Task6:

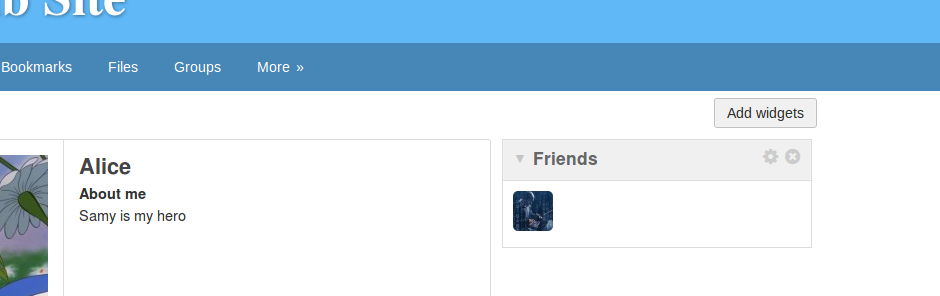
在samy的个人介绍中写入代码和参数，将前两个task的代码综合起来



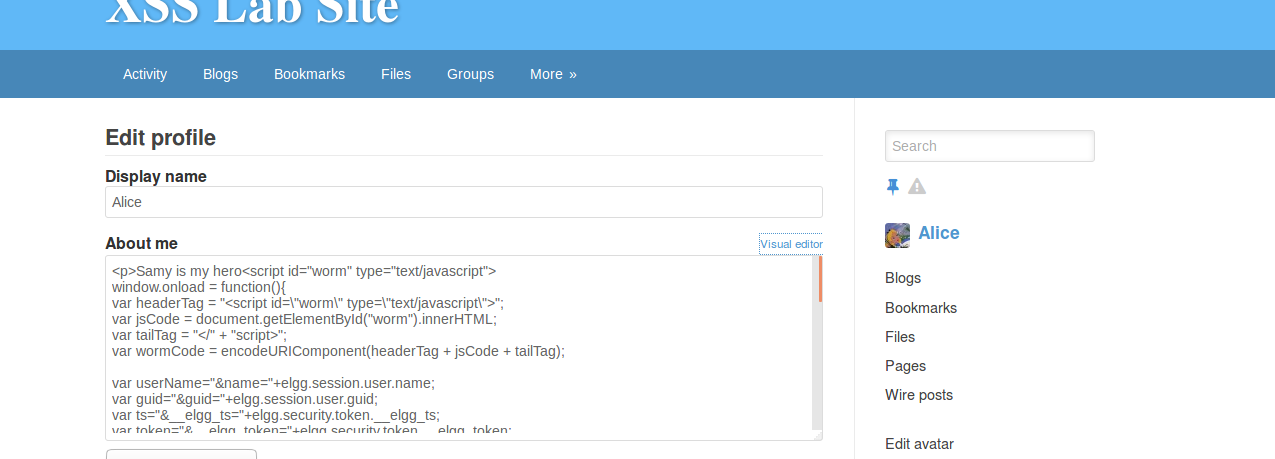
Alice访问samy个人资料前没有好友，个人介绍为空，如图



访问samy的个人资料后，alice自动添加samy为好友并修改了自我介绍，如图



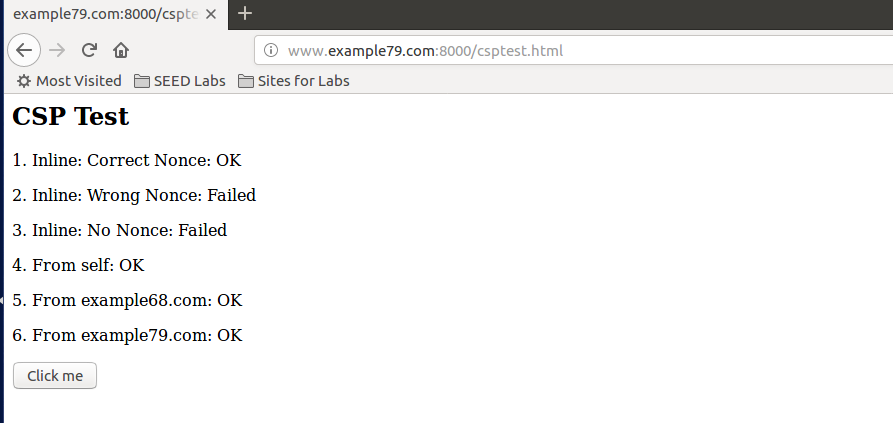
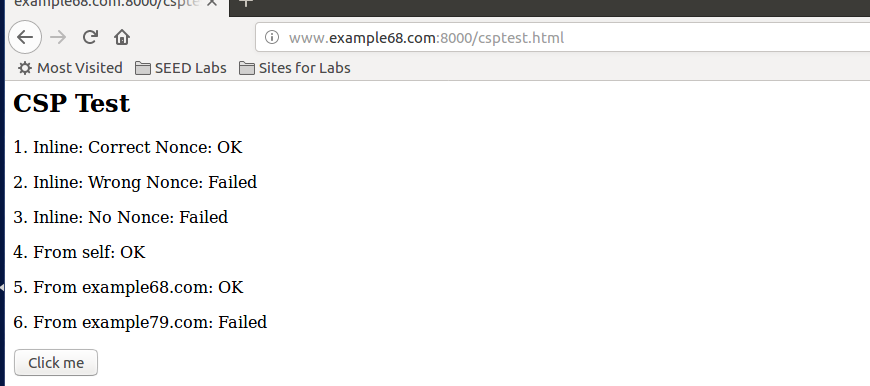
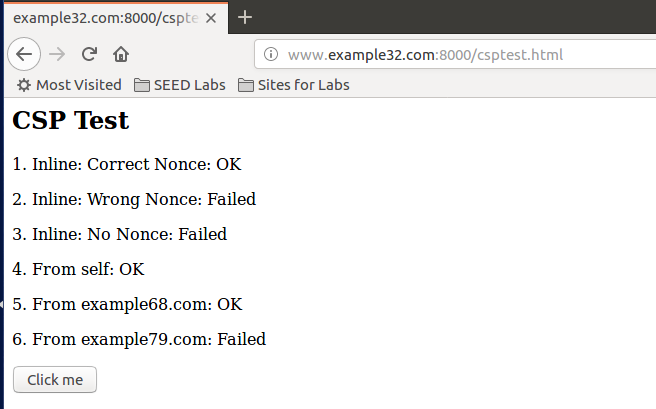
打开个人资料，发现代码已经自动复制到alice的个人介绍中



Task7:

分别访问[www.example32/68/79.com](http://www.example32/68/79.com)，如图

第1、4、5块script始终成功执行，第2、3块时终没有执行，第6块在访问[www.example79](http://www.example79)时执行



将example79.com：8000加入GET头中使得第6块script始终执行，

将nonce-2r83333加入GET头中使得第2块script始终执行，

修改后的server代码如下

