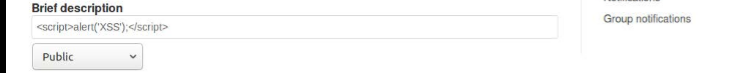
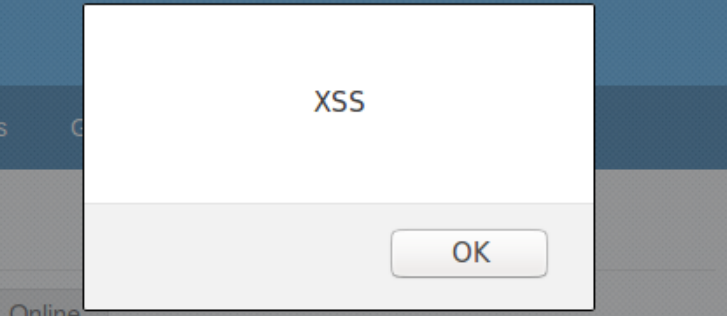
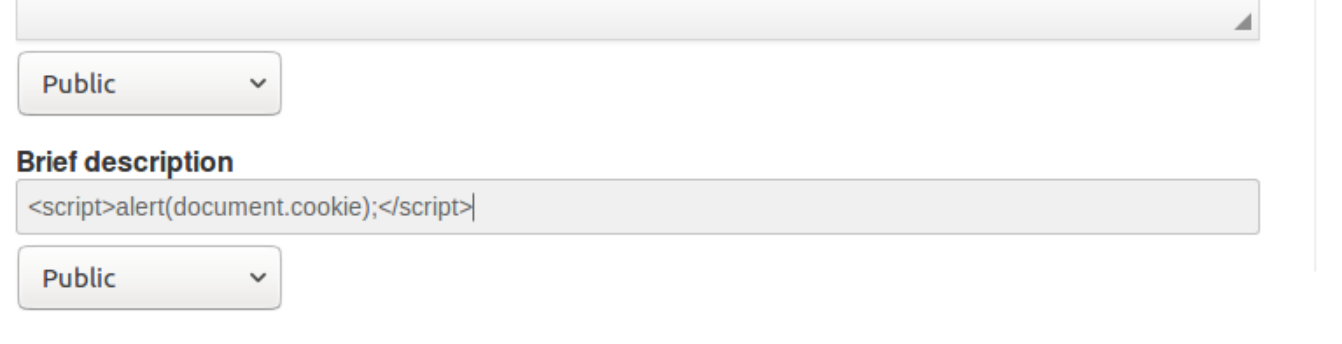
Task 1



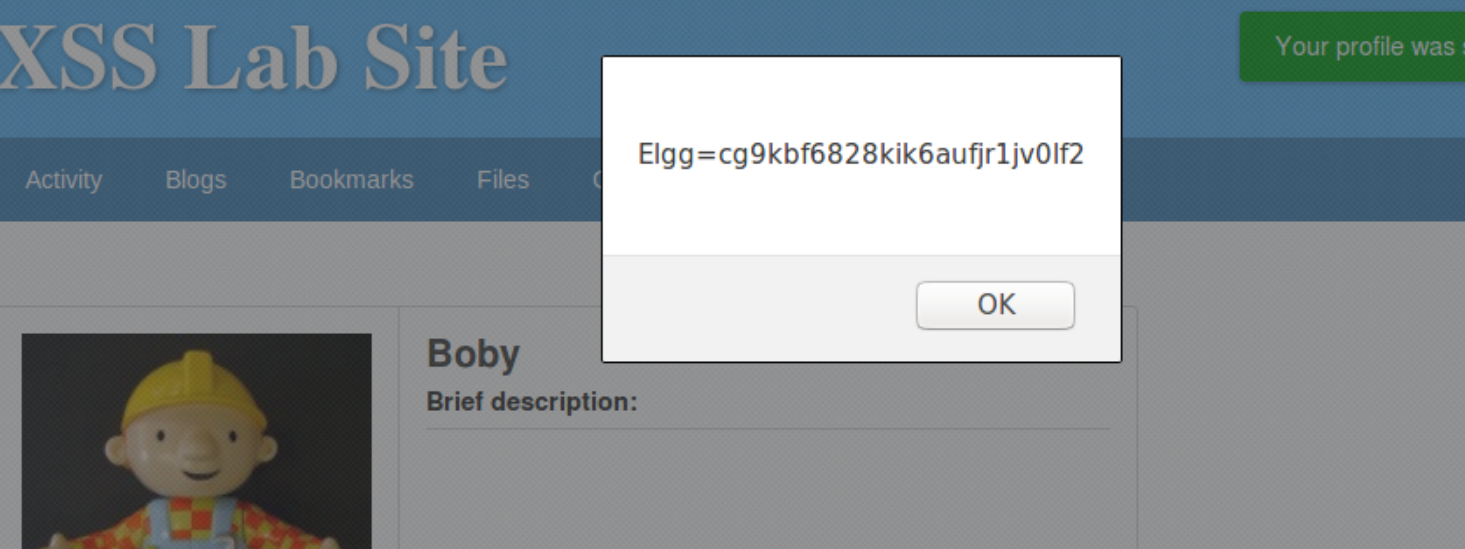


登录Boby的账户，修改签名。登录 Alice 的账户，点击查看 Boby 的个人信息界面，出现警报窗口。

Task 2

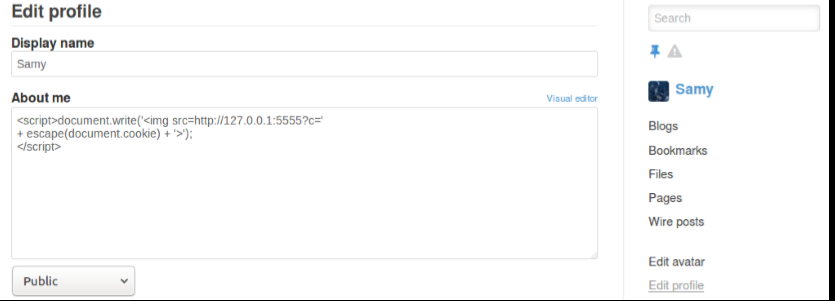


登录Boby的账户，修改签名



登录 Alice 的账户，点击查看 Boby 的个人信息界面，出现警报窗口并显示用户

Task 3



我们先在samy的about me中修改签名如上

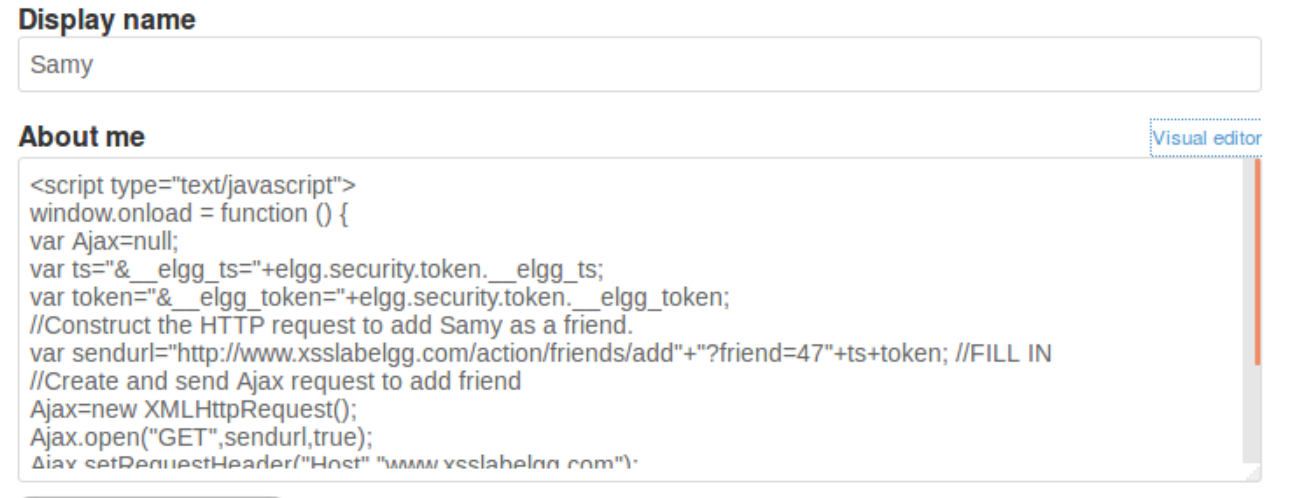


在终端输入指令监听端口5555的信息，然后登录alice 的账户，点击查看Samy

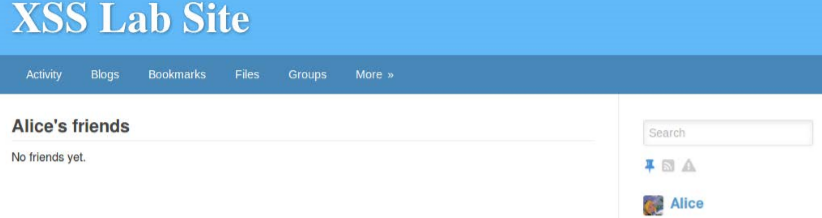
的个人信息界面，发现成功

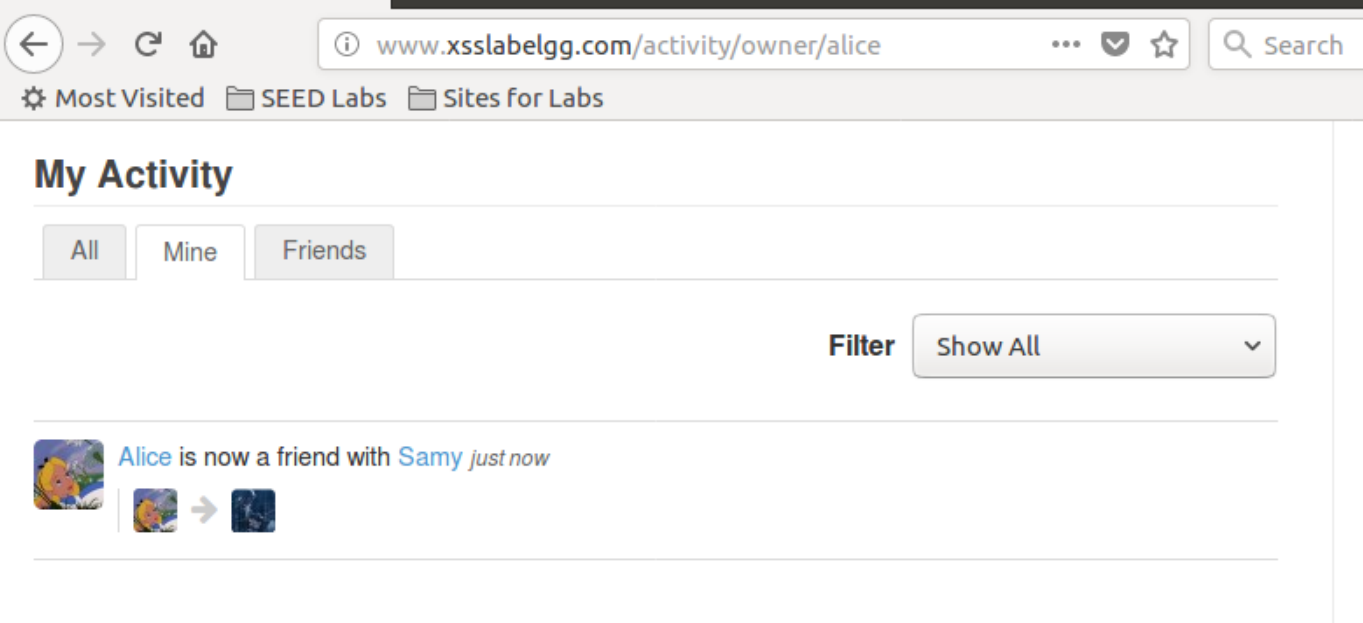
Task 4

我们先抓取的添加好友的HTTP GET请求，可知Samy的用户id 为47。



登录Samy的账户，进入Edit HTML界面修改签名。



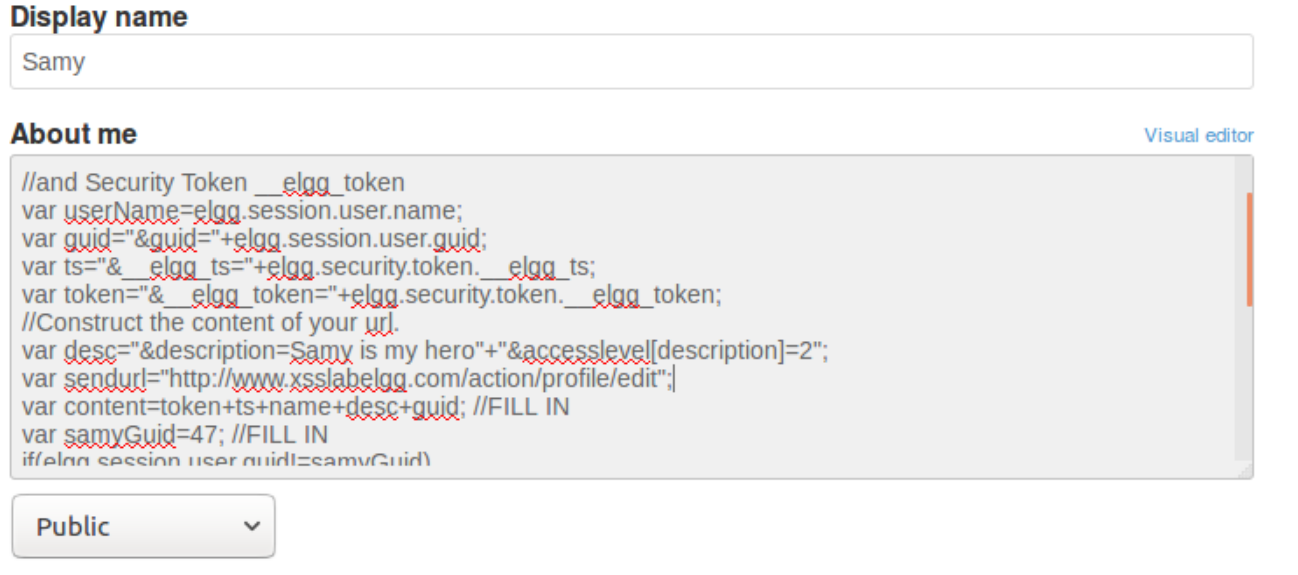


我们再登录alice的账号，发现一开始alice没有samy的好友，后来点进samy的主页，alice就有了samy的好友

Line1 和 Line2 这两行的代码是为了获取秘密令牌\_elgg\_ts 和\_elgg\_token

可以。可以使用浏览器扩展来删除HTTP 请求中的格式化数据。

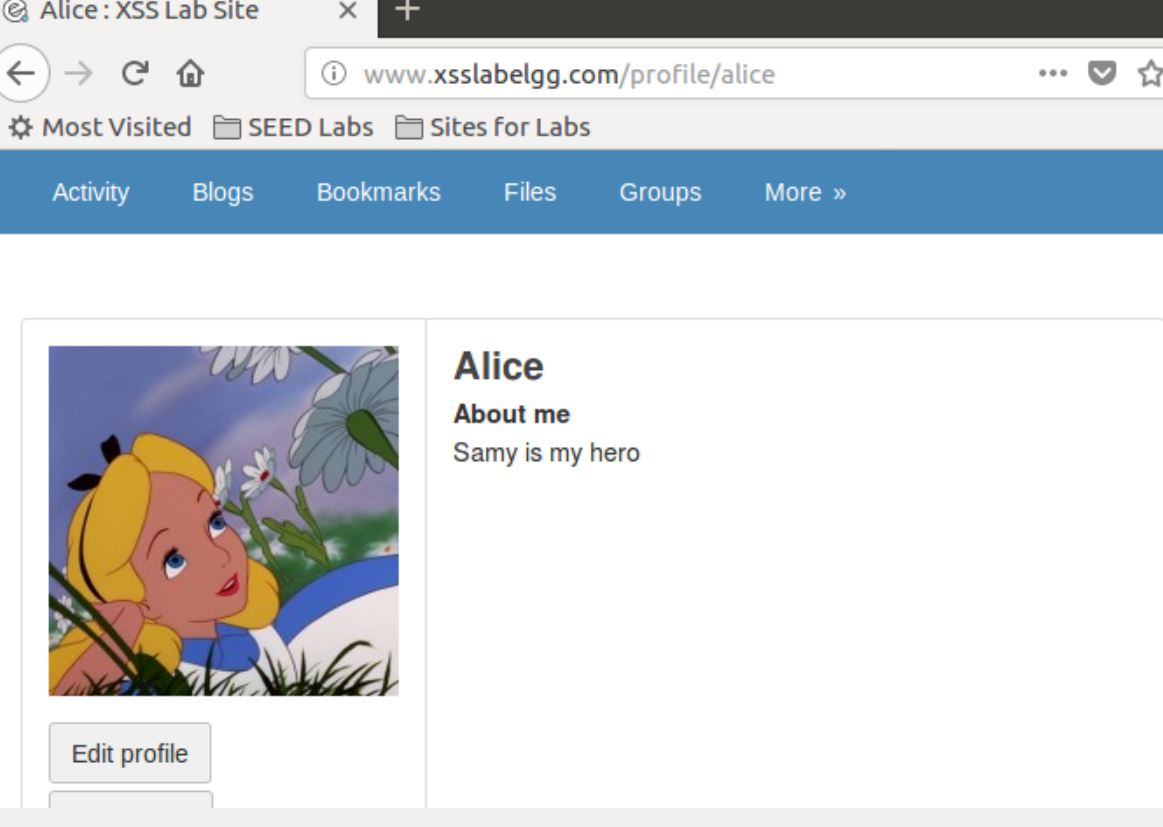
Task 5

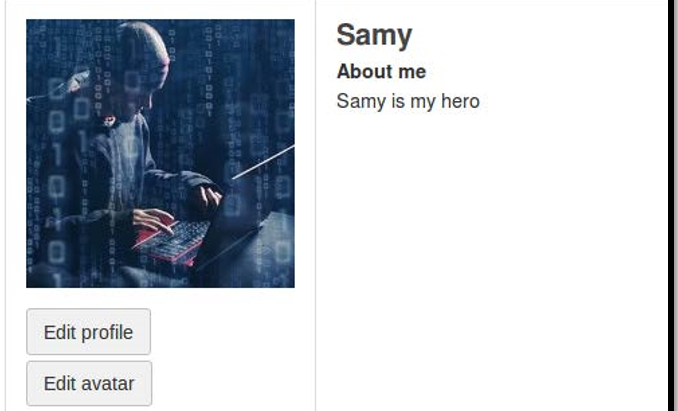


Samy的个人签名修改如上

登录 Alice 的账户，点击查看 Samy 的个人信息界面，然后返回自己的个人信息

界面，发现签名已经被修改为Samy is my hero。





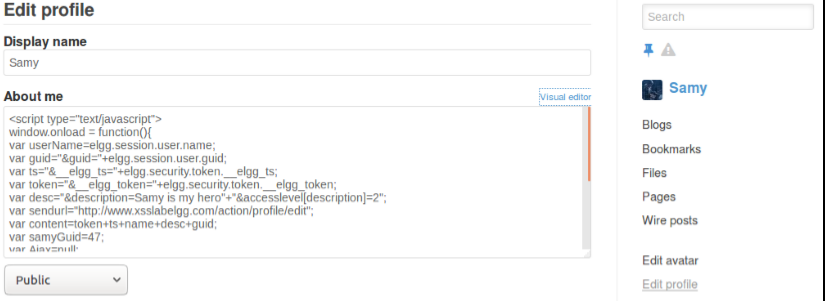
登录Samy的账户修改签名，删除Line1这一行的代码。

我们返回 Samy 的个人信息界面发现自己签名已经被修改为 Samy is my hero，而其

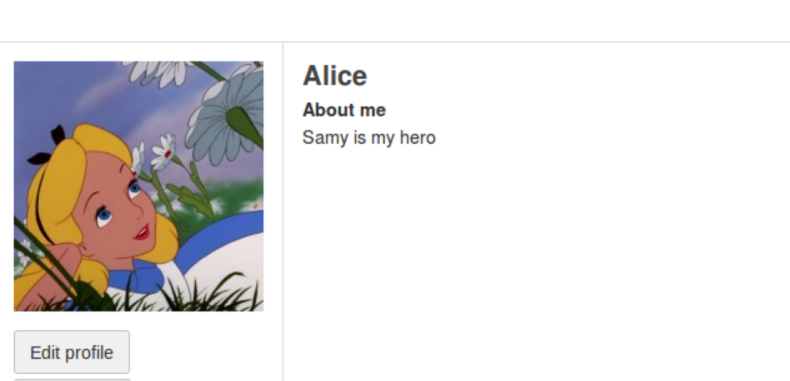
他用户点击查看 Samy 的个人信息界面后签名不会被修改。原因是 Line1 的代码

负责判断用户是否为 Samy 本人，避免自己的签名被修改。如今我们删除这行代码，所以samy的个人签名会改变而其他人查看samy不会改变个人签名。

Task 6



我们登录samy的页面修改samy的签名



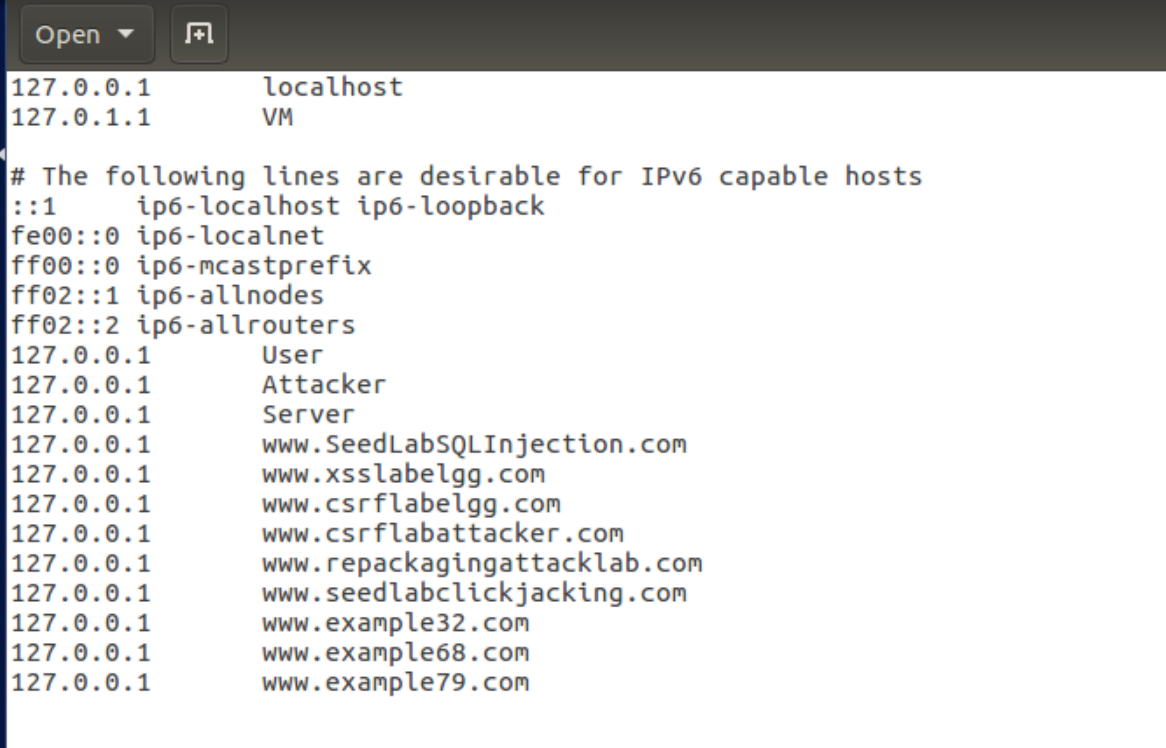


然后我们再登录Alice，用alice的账号登录samy的页面，我们发现alice的签名被修改而且alice有了同样的代码



我们用bob登录访问alice的页面，发现bob的签名同样被改过了

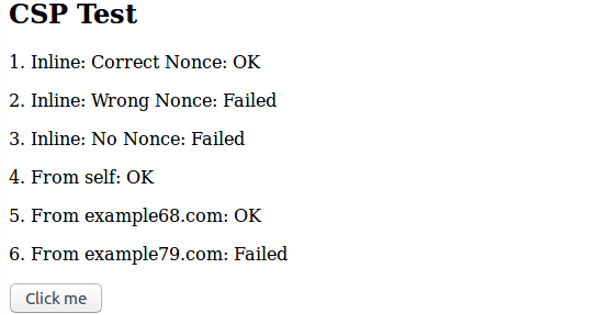
Task 7



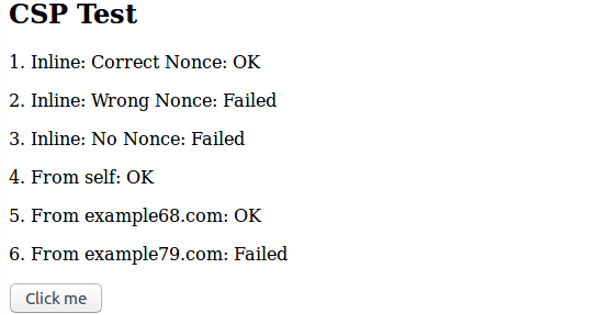
修改/etc/hosts文件

在https://seedsecuritylabs.org/Labs\_16.04/Web/Web\_XSS\_Elgg/中下载csp.zip

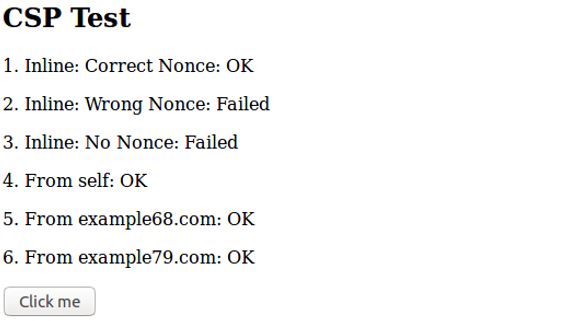
文件，然后进行解压，再运行其中的http\_server.py文件。



在浏览器中输入http://www.example32.com:8000/csptest.html，Fields 1、4、5显示为OK。

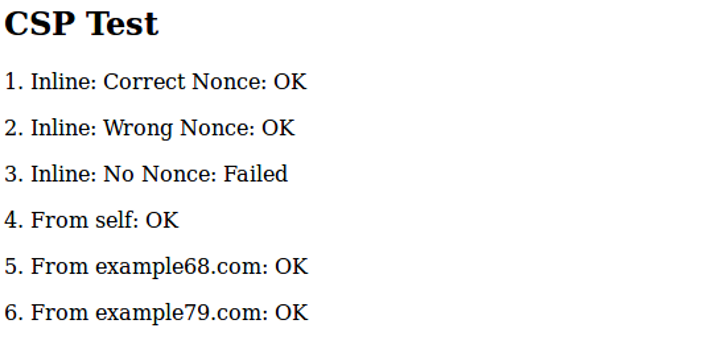


在浏览器中输入http://www.example68.com:8000/csptest.html，Fields 1、4、5显示为OK。



在浏览器中输入http://www.example79.com:8000/csptest.html，Fields 1、4、5、6显示为OK。 他们的结果不一样的原因是http\_server.py只允许含nonce=1rA2345的代码（对应area 1）、来自example68.com:8000的代码（对应area 5）以及网站自身产生的代码（对应area 4）被执行。

接下来我们修改http\_server.py文件，在script-src 后添加 nonce-2rB3333。



重新编译运行修改后的http\_server.py，再次在浏览器中输入http://www.example79.com:8000/csptest.html，Fields 1、2、4、5、6显示为OK。