**Cross-Site Scripting (XSS) Attack Lab**

作者：黄禧敏

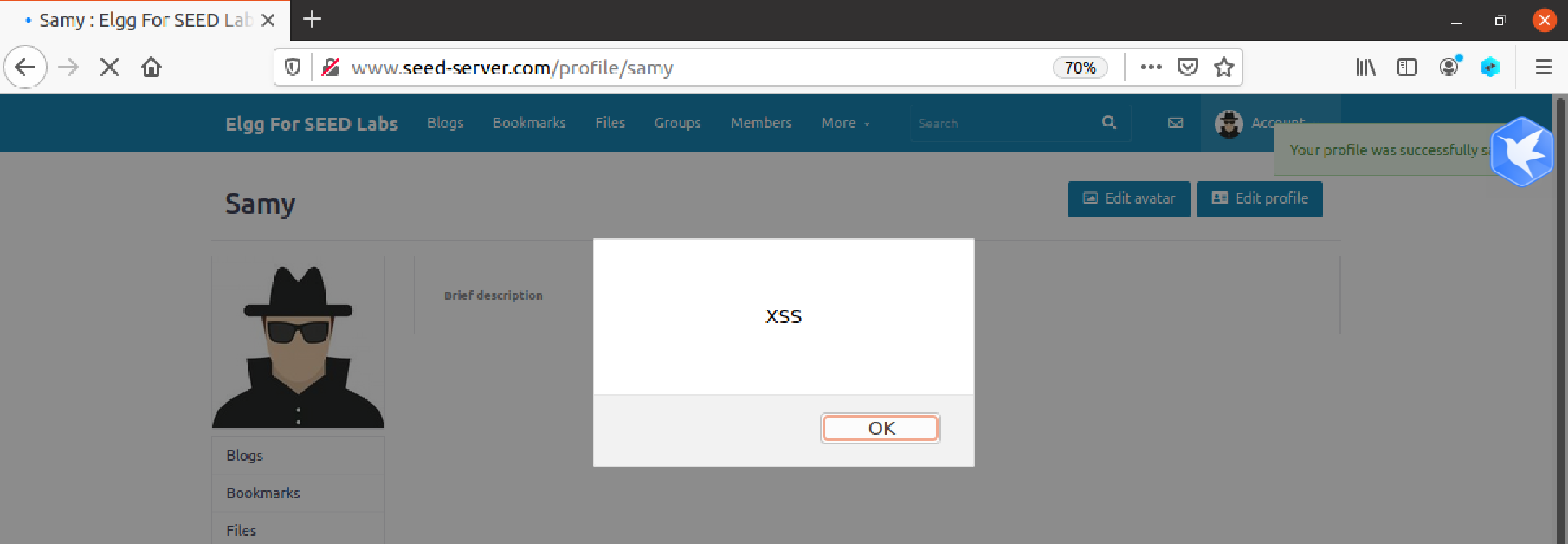
学号：57119109

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

编辑个人资料



显示弹窗

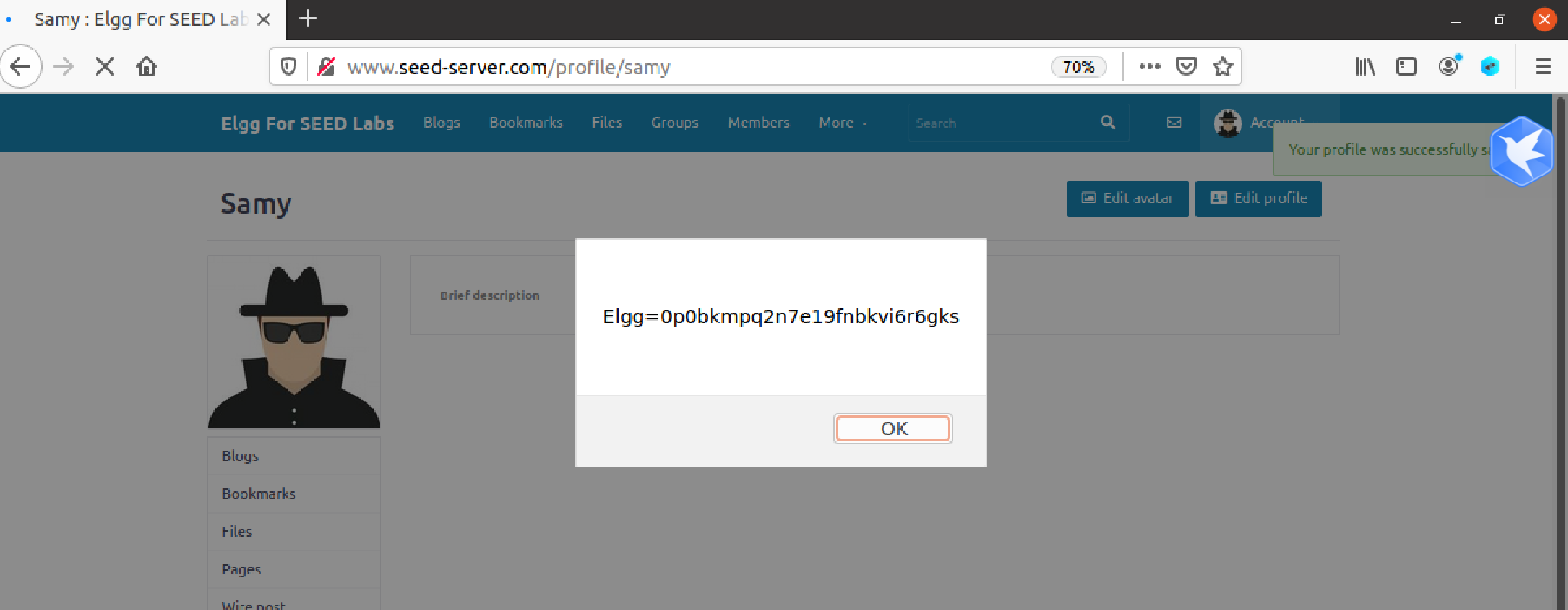


**Task 2: Posting a Malicious Message to Display Cookies**

改为输出cookie

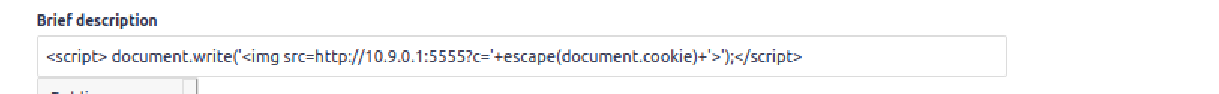


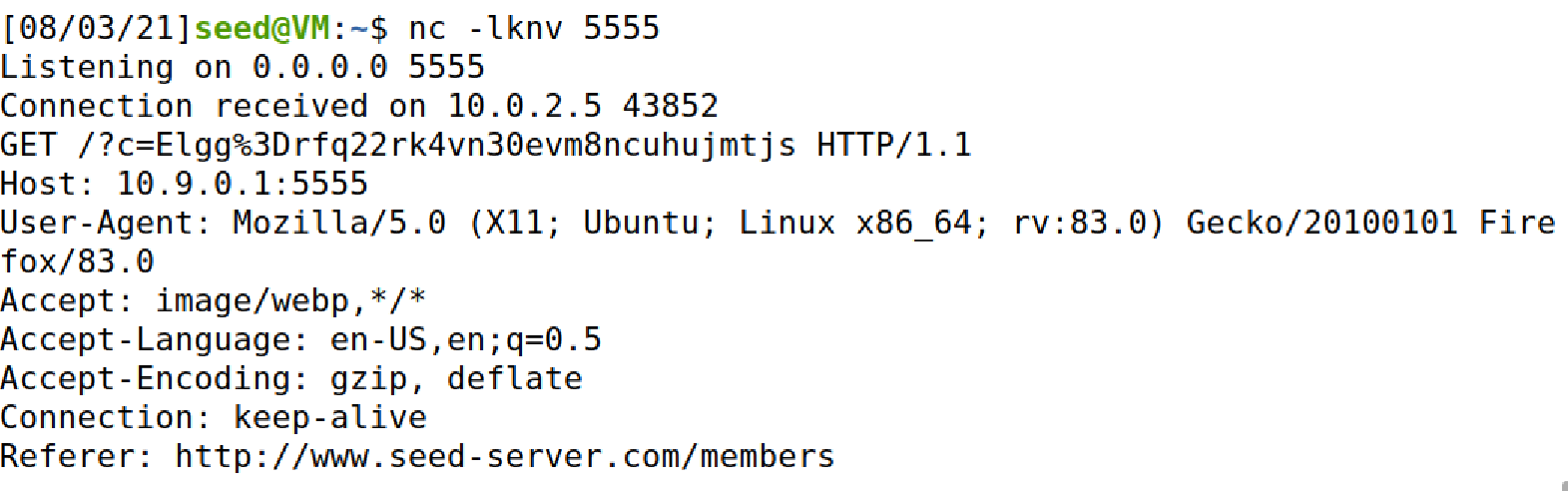
弹窗显示cookie



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

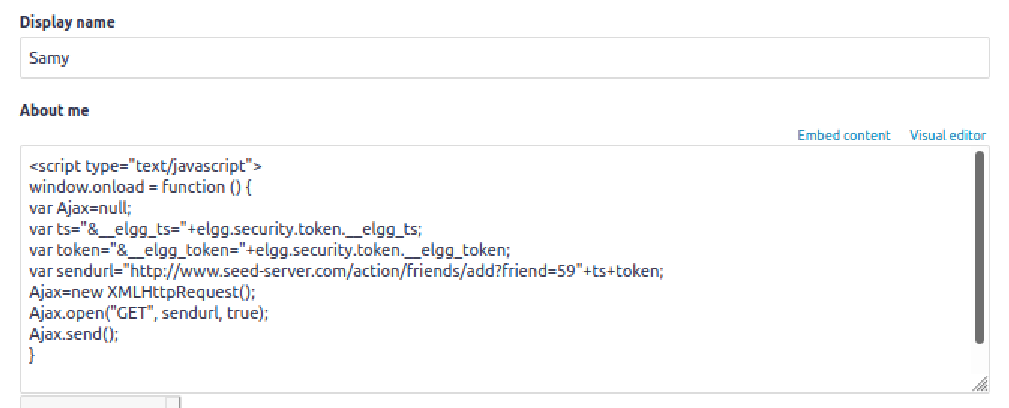
更改个人签名



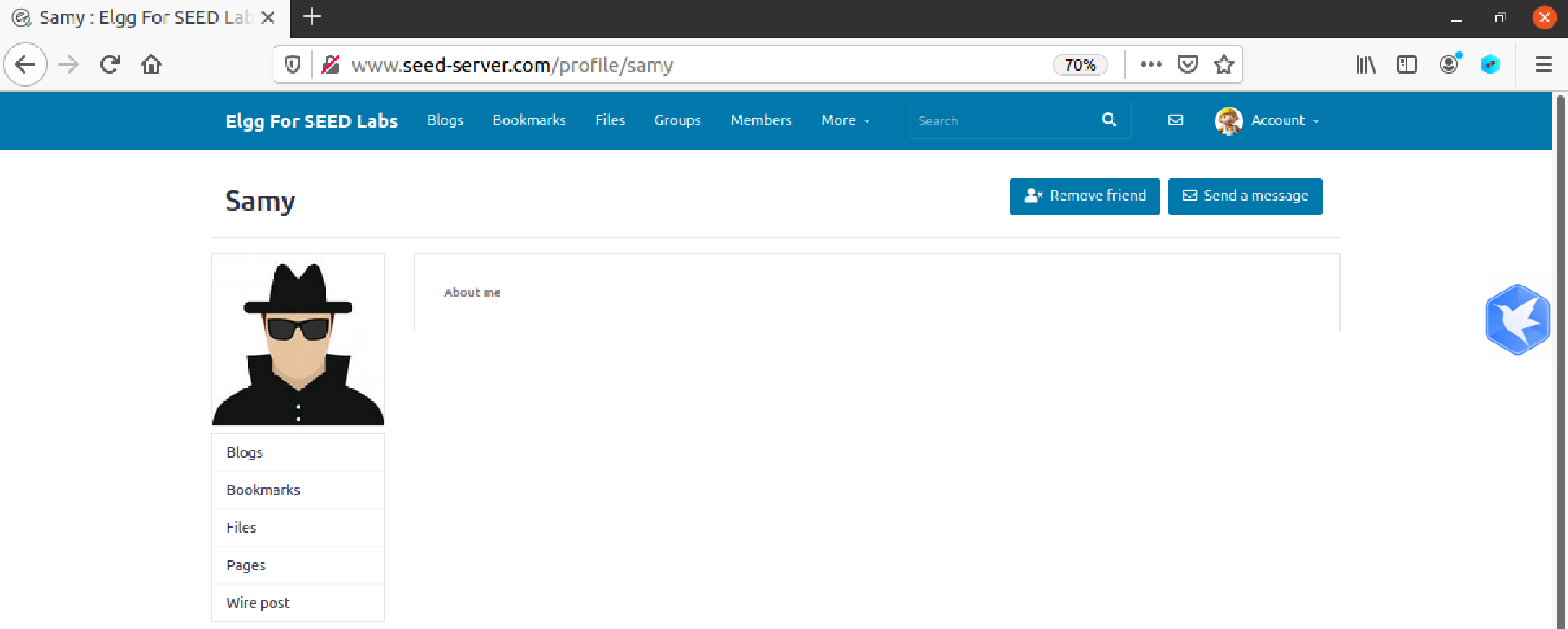


**Task 4: Becoming the Victim’s Friend**

在文本模式下修改samy的about me



登录他人账号，查看samy的个人资料，发现已经自动添加好友；



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

Ts和tocken用于让网站验证用户身份，达到欺骗的效果；

**Question 2:** If the Elgg application only provide the Editor mode for the "About Me" field, i.e.,

you cannot switch to the Text mode, can you still launch a successful attack?

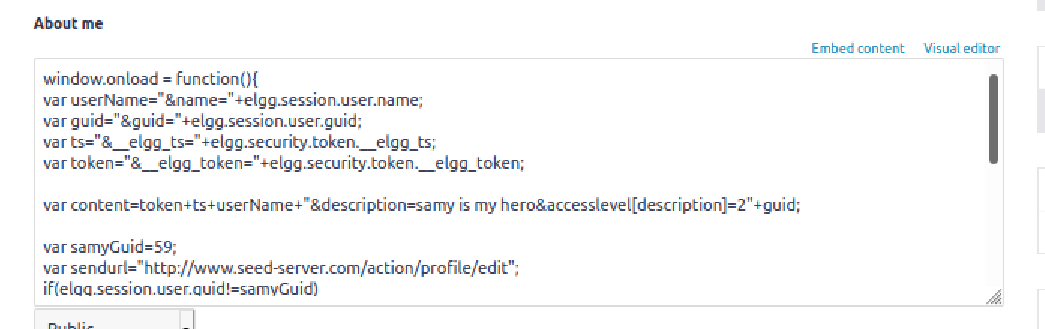
不能成功，因为网站会自动将攻击代码转码成文本显示，不能起到运行效果，可以依旧将代码写入briefdescription;

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

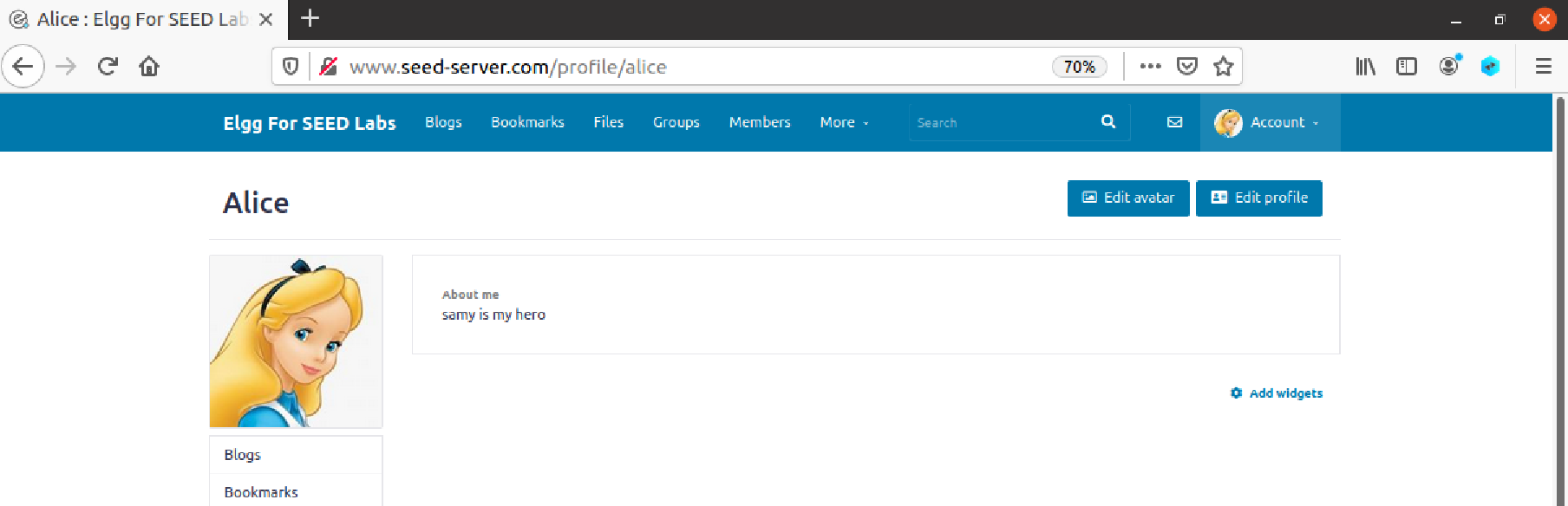
观察post结构



构造攻击代码



登录alice账号查看samy个人资料，返回后发现自己的about me已被修改；



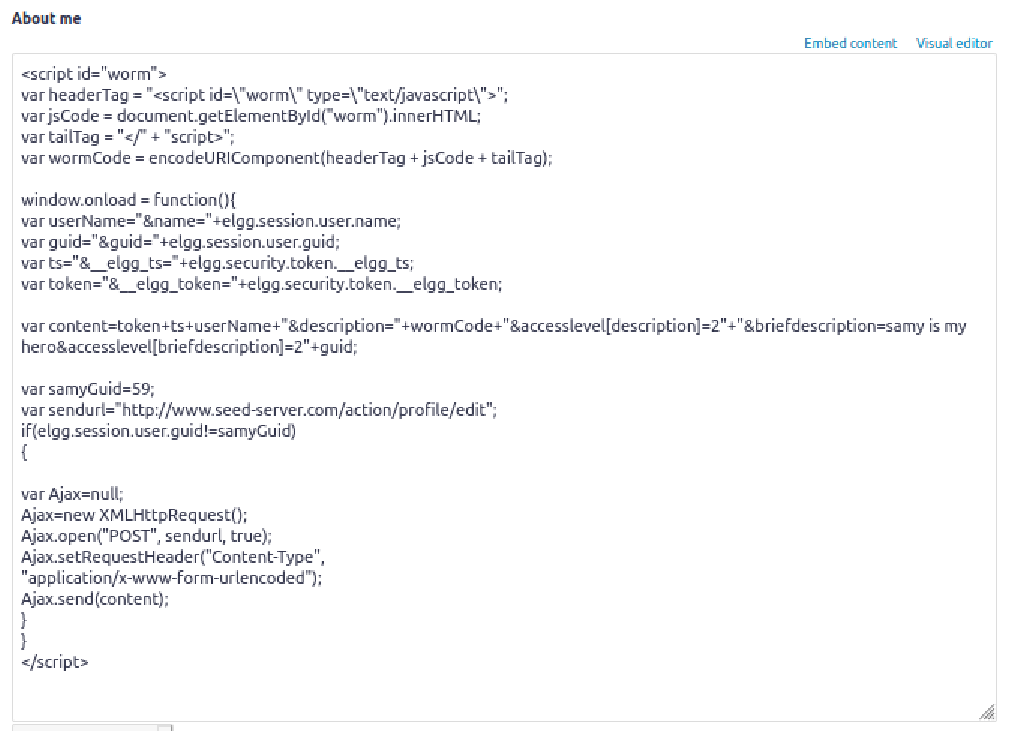
**Question 3:** Why do we need Line ➀? Remove this line, and repeat your attack. Report and explain your observation.

这条语句是为了避免自身about me被修改，一旦自身被修改，那么攻击代码就将被覆盖，从而失效；

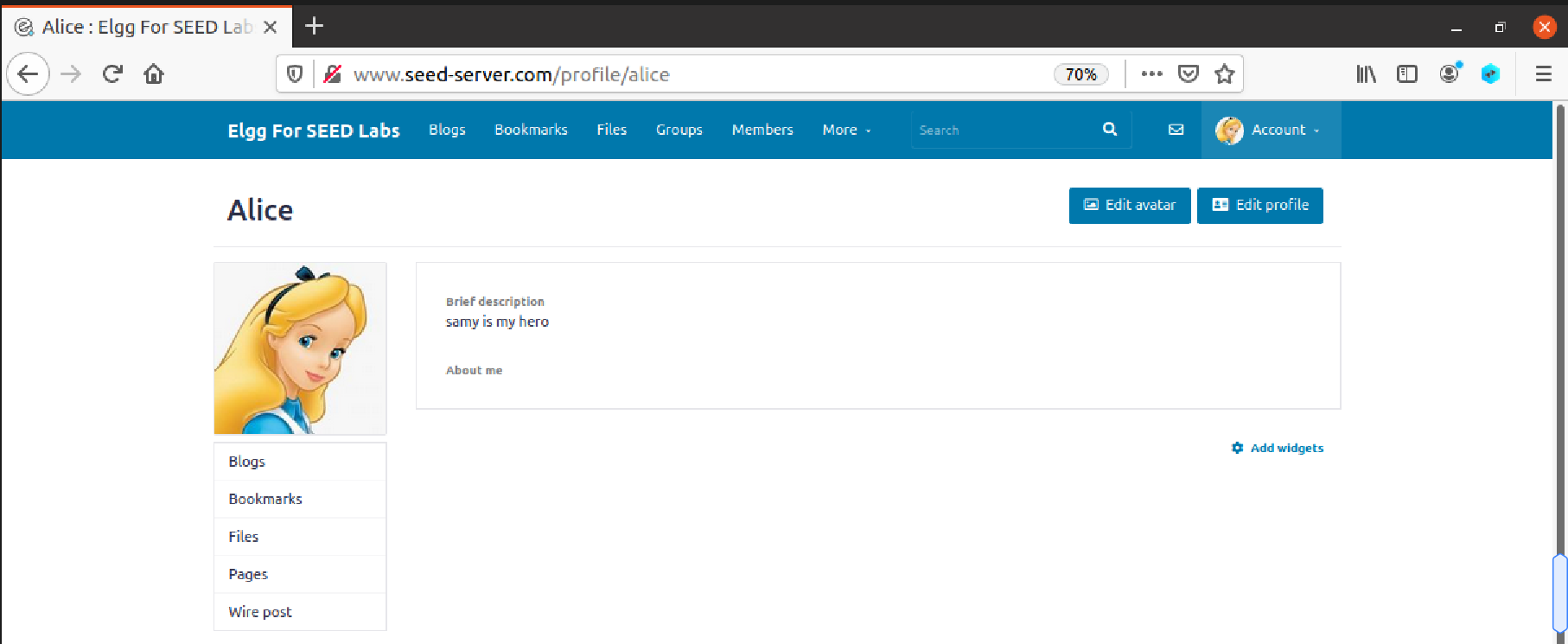
**Task 6: Writing a Self-Propagating XSS Worm**

在samy的about me 中写入worm;

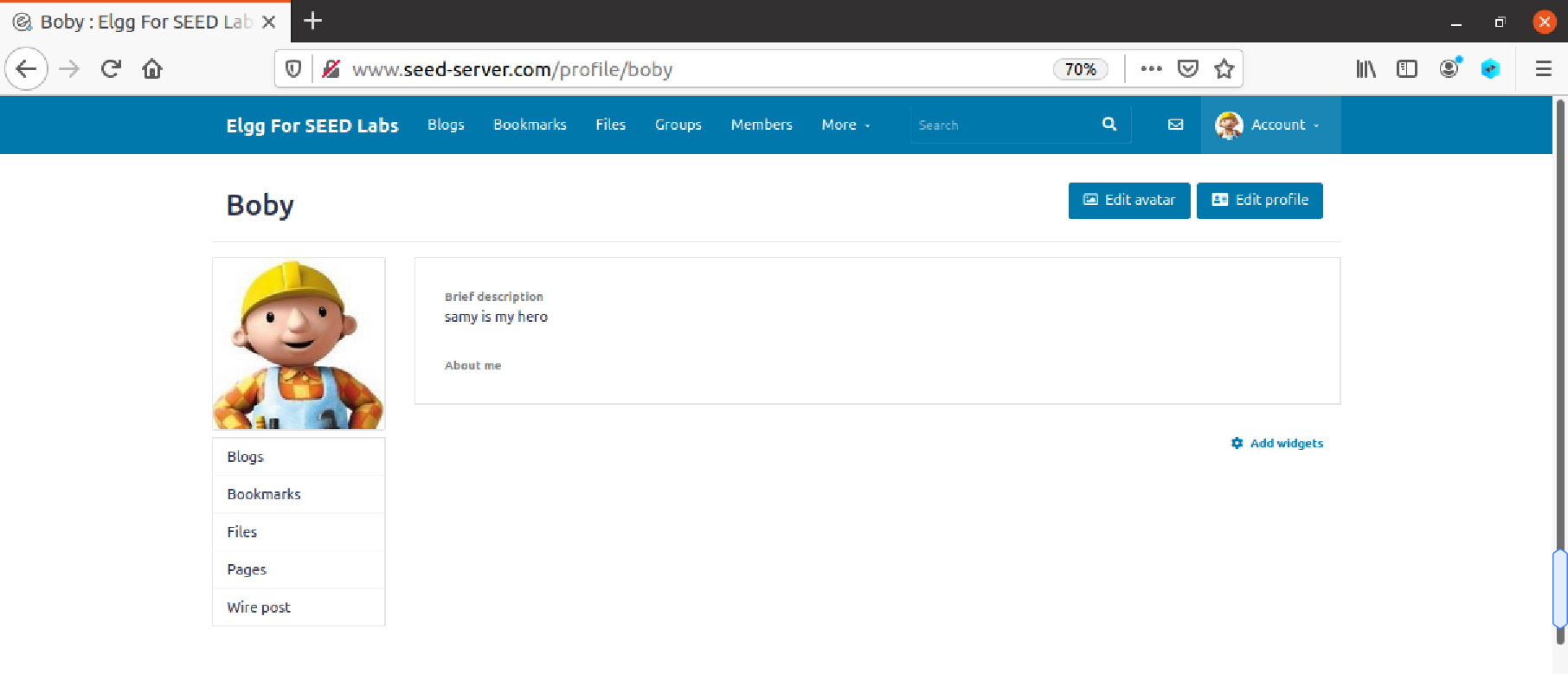
Worm代码将手册提供的alert()替换为上一个task的恶意复制代码;



Alice点开Samy的主页，之后发现个人主页被修改；

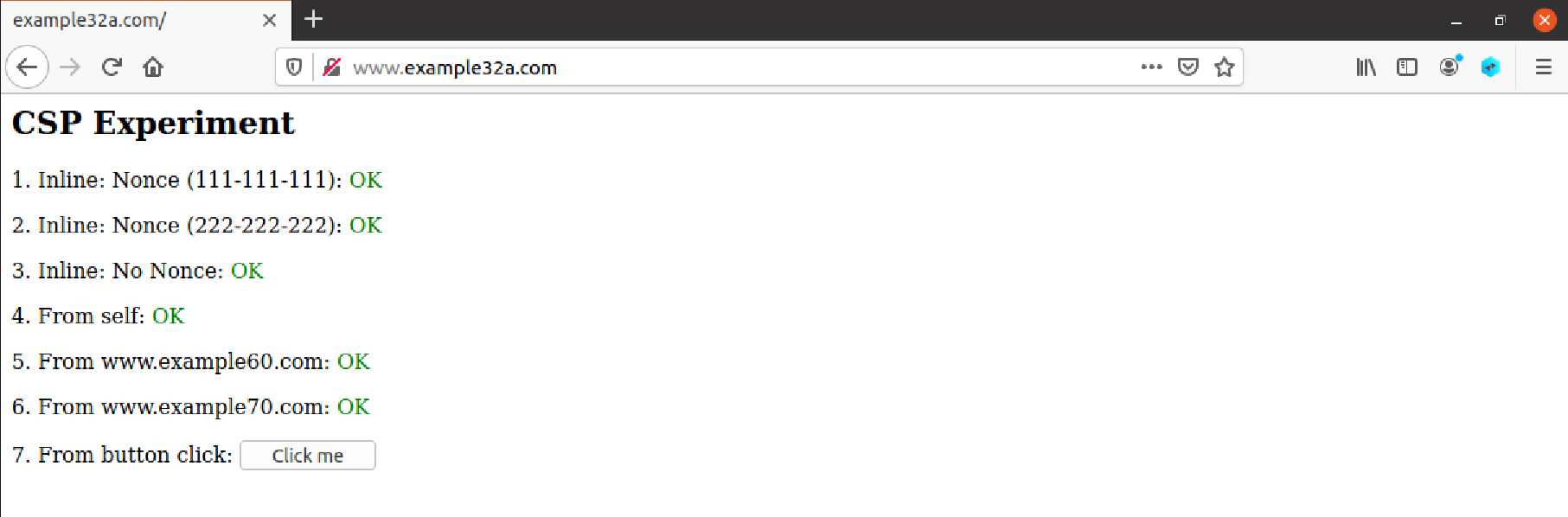


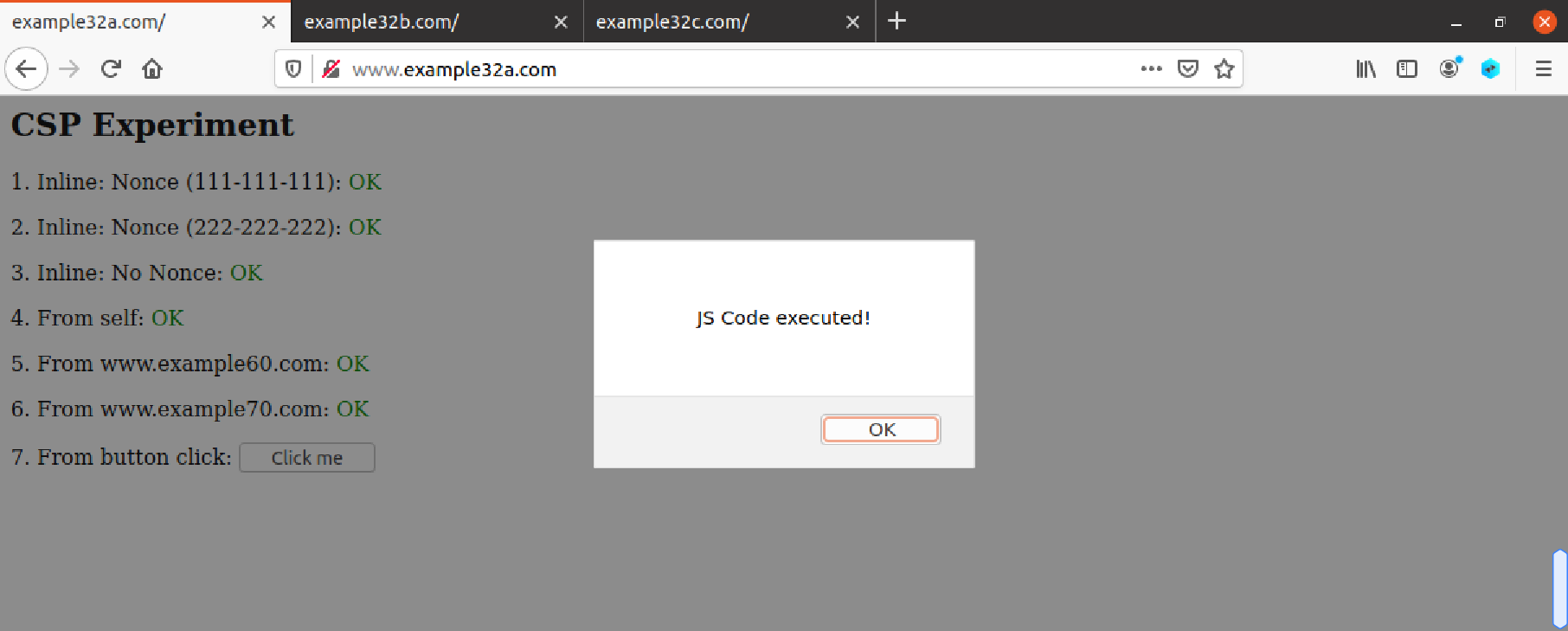
用Boby点开alice主页，之后发现自己的也被修改；

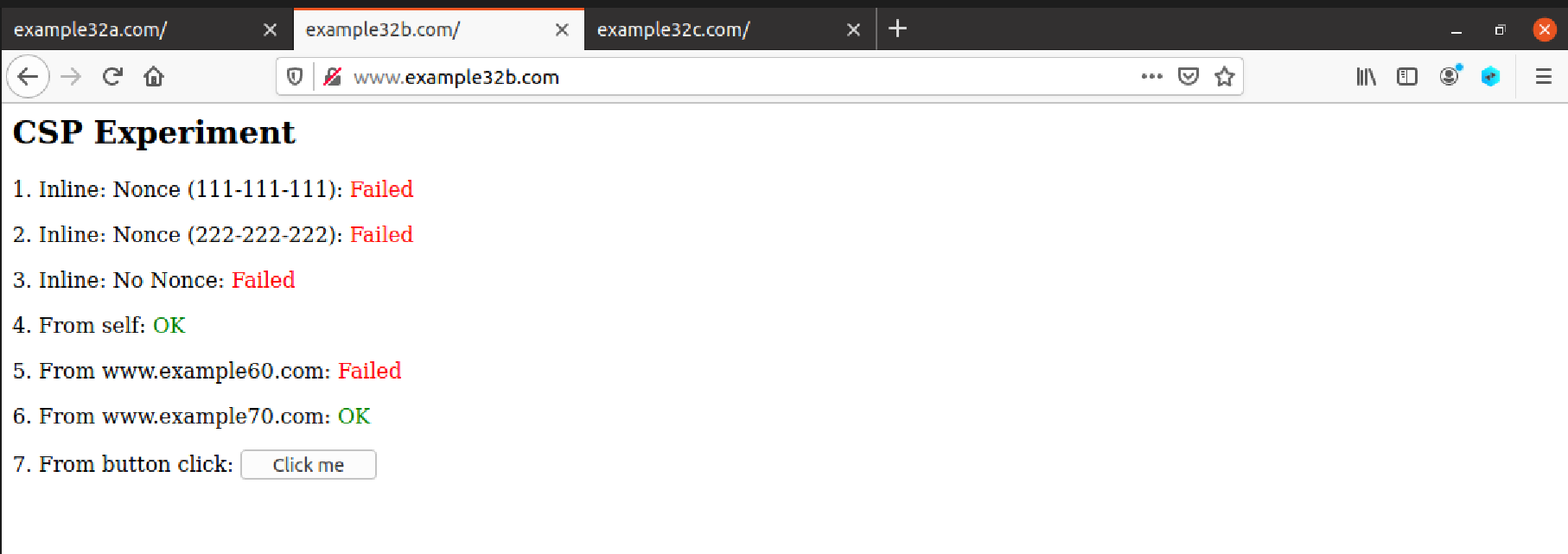


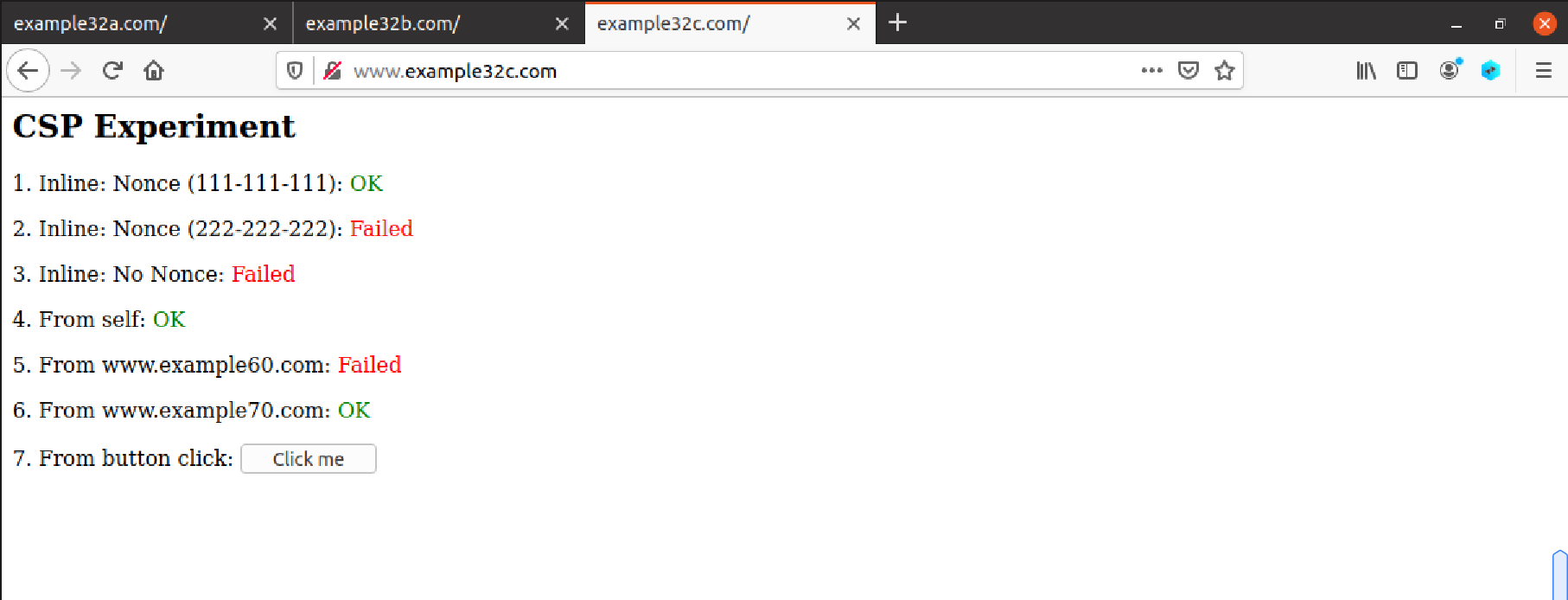
**Task 7: Defeating XSS Attacks Using CSP**

原始状态：





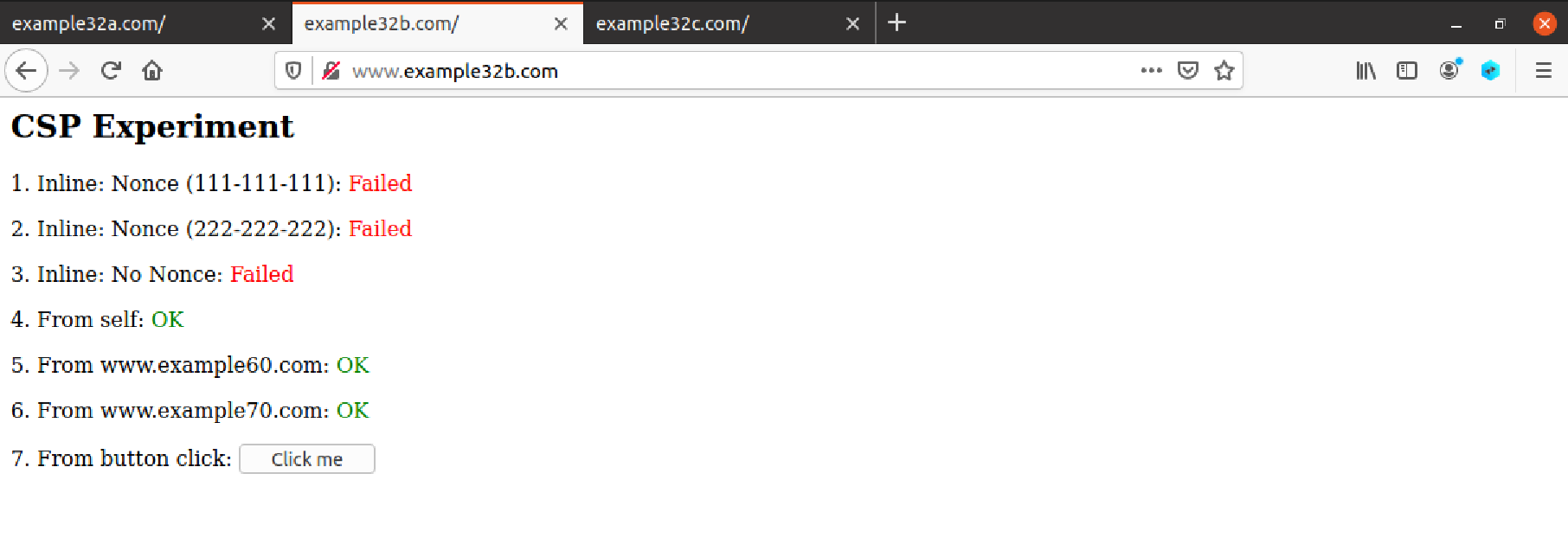




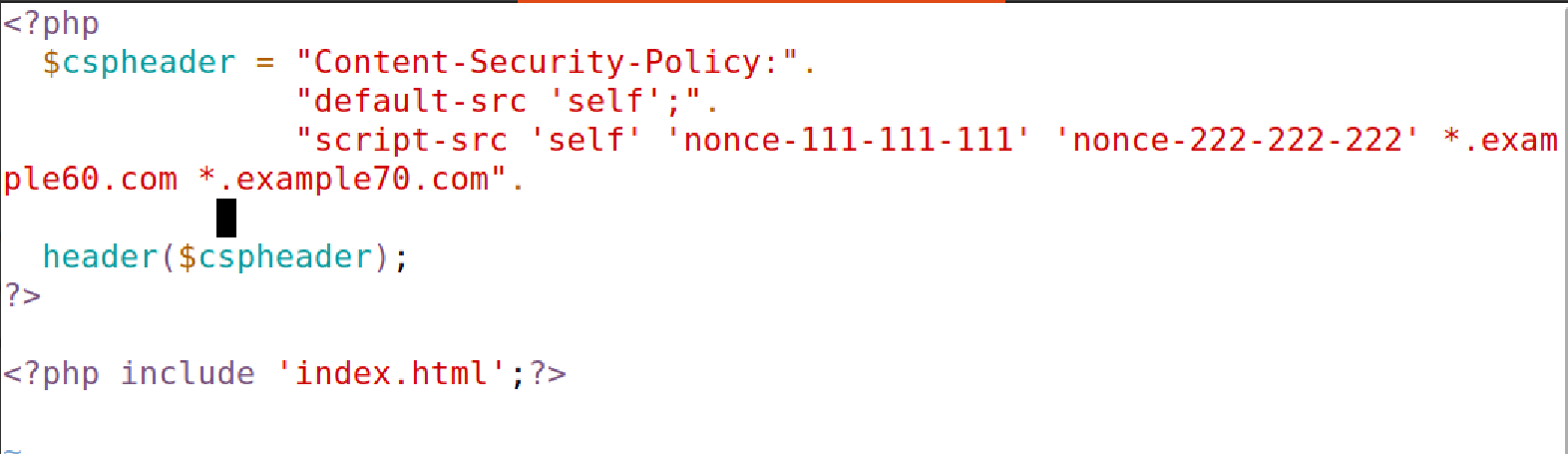
修改apache\_csp.conf

在example32b添加script-src 'self' \*.example60.com \

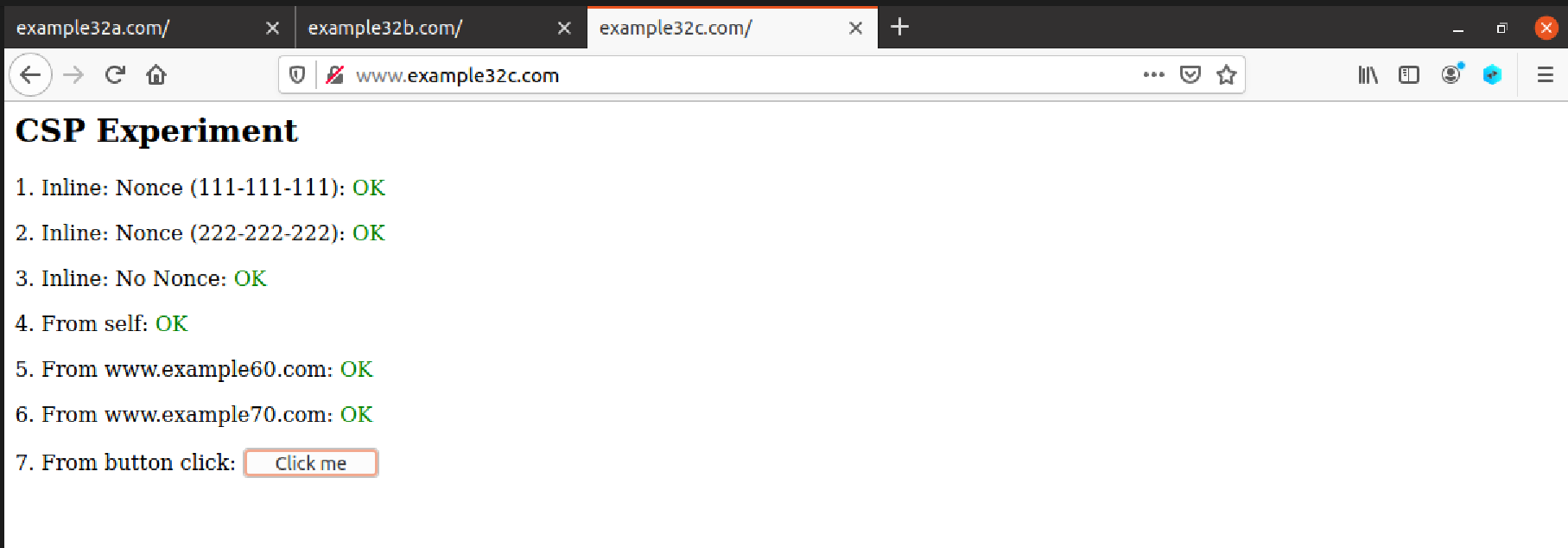
可以看到5变为ok;



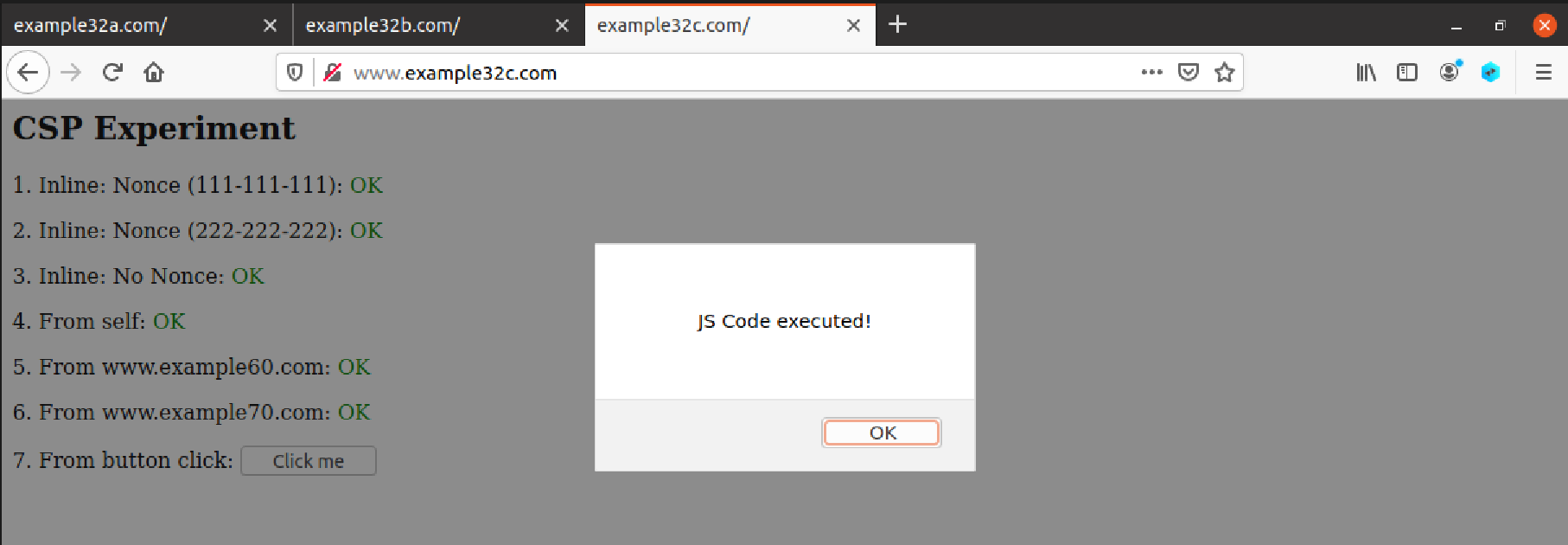
修改phpindex.php



可以看到example32c.com全部选项为ok



点击按钮，可以执行脚本



可以看到，CSP使用的是白名单机制，允许被信任来源的脚本执行；