本学期实验总体安排

- **实验指导书链接： https://network-security.p.cs-lab.top/**
- **SEED实验室的链接：**
  - https://seedsecuritylabs.org/
  - https://seedsecuritylabs.org/chinese/
- **实验提交地址（校内网/VPN）：** http://grader.tery.top:8000/#/login

网络与系统安全

实验三 XSS

CONTENTS

目录

实验目的

- 1. 掌握 Cross-Site Scripting attack 的基本原理
- 2. 应用 XSS worm 以及了解 self-propagation
- 3. 掌握 Session cookies 的具体使用技巧
- 4. 熟练使用 HTTP GET and POST requests
- 5. 熟悉 CSP 安全政策防止XSS攻击

实验任务

本次实验创建了一个易受XSS攻击的Web应用程序。该Web应用程序存在XSS漏洞。我们的目标是找到利用XSS漏洞的方法，理解攻击可能造成的损害，并掌握可以帮助防御此类攻击的技术。

1、发布恶意消息以显示警告窗口
2、发布恶意消息以显示Cookies
3、窃取受害者的Cookies
4、自动成为受害者的朋友
5、修改受害者的个人资料
6、编写自我传播的跨站脚本蠕虫病毒
7、使用CSP（内容安全策略）抵御XSS攻击

实验原理

◆ XSS 漏洞原理

恶意攻击者在web页面中插入一些恶意的script代码，当用户浏览该页面的时候，那么嵌入到web页面中script代码会执行，因此会达到恶意攻击用户的目的。

类似SQL注入攻击，都是将数据当作代码执行导致的问题。

1、**反射型 XSS**

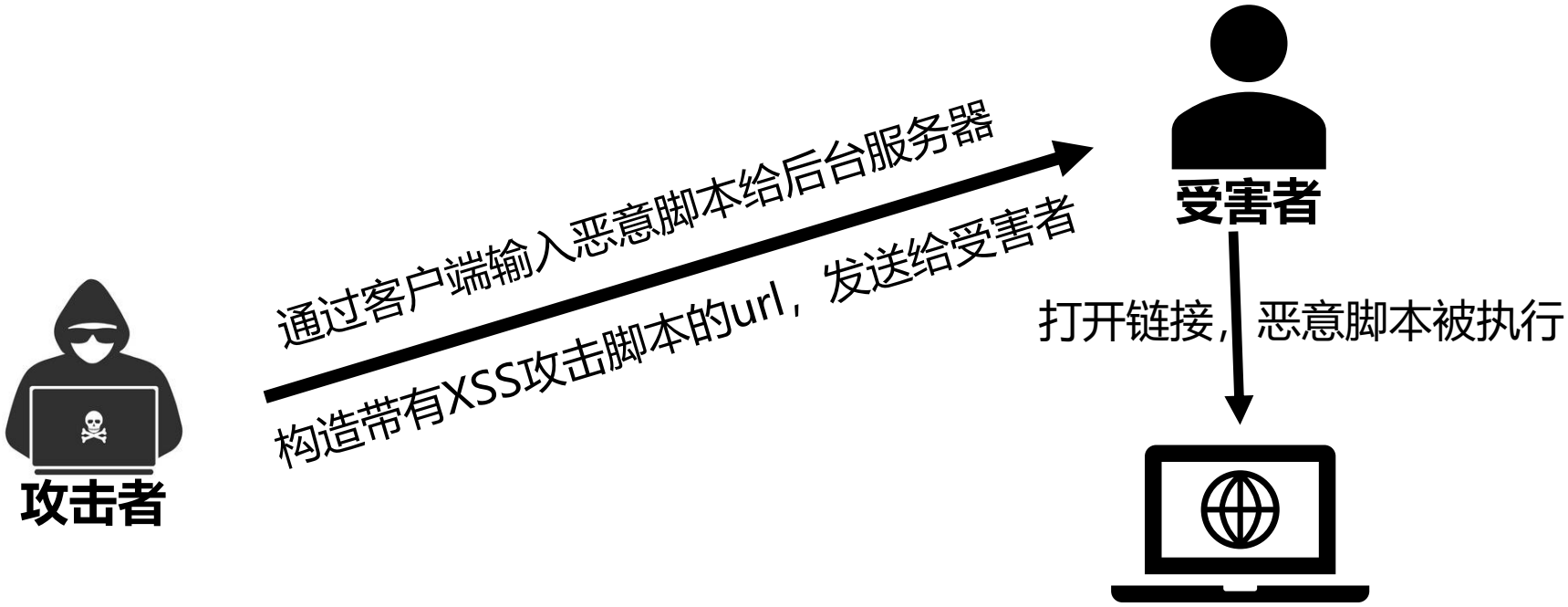
2、**存储型 XSS**

3、**DOM-based型 XSS**

实验原理

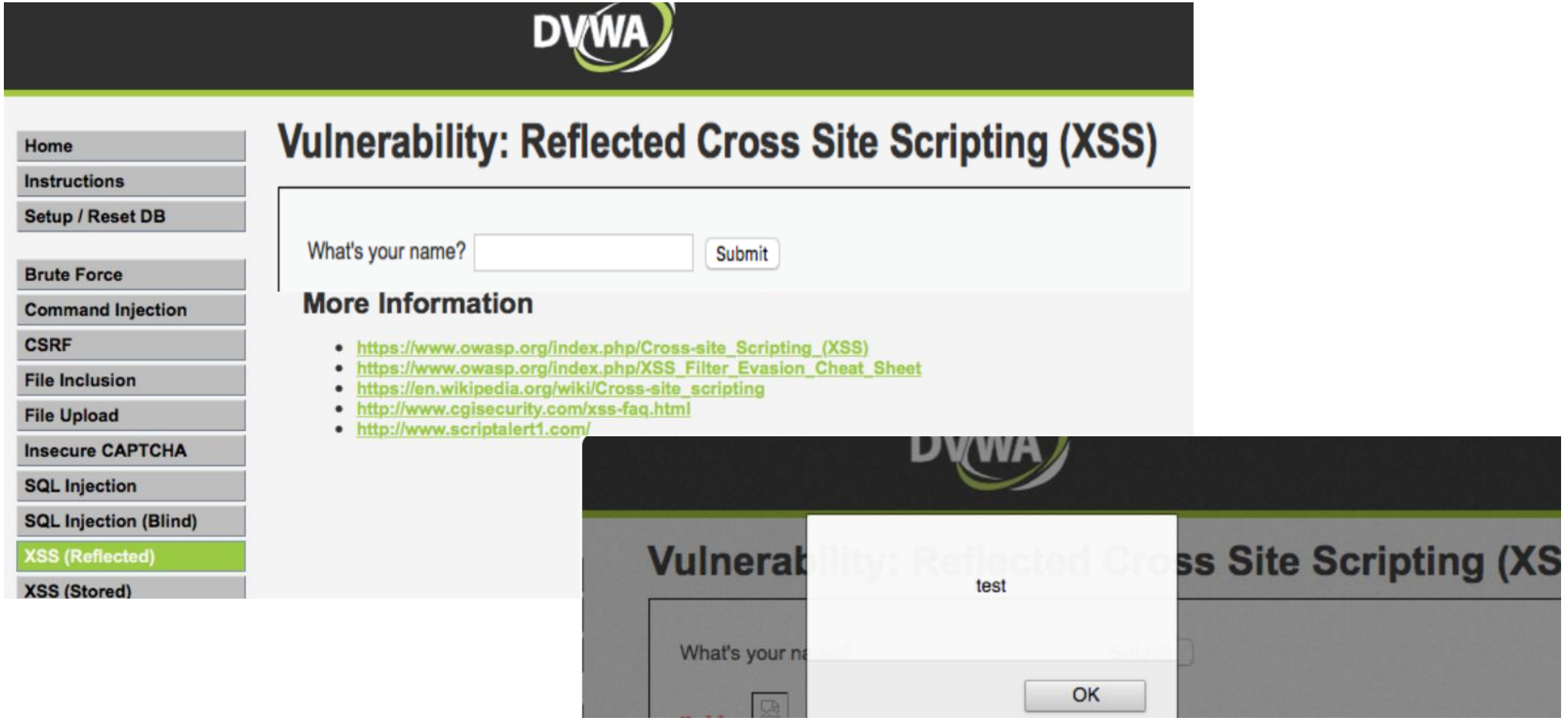
◆ 反射型 XSS

反射型XSS攻击是将注入的**恶意脚本添加到一个网址中**，然后给用户发送这个网址。一旦用户打开这个网址，就会执行脚本并导致攻击。攻击负载和脚本跟随用户点击链接，并被嵌入到响应中，在浏览器上执行。



实验原理

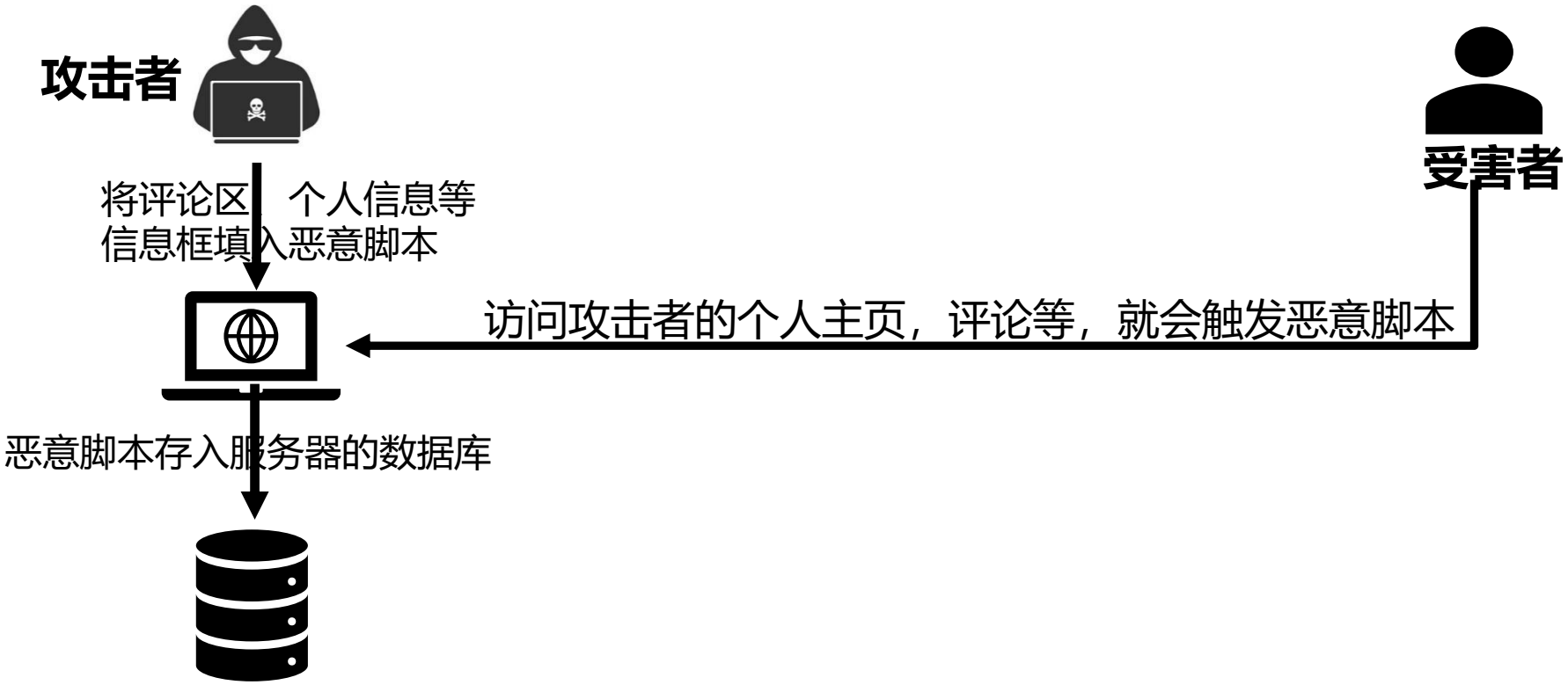
◆ 反射型XSS示例



实验原理

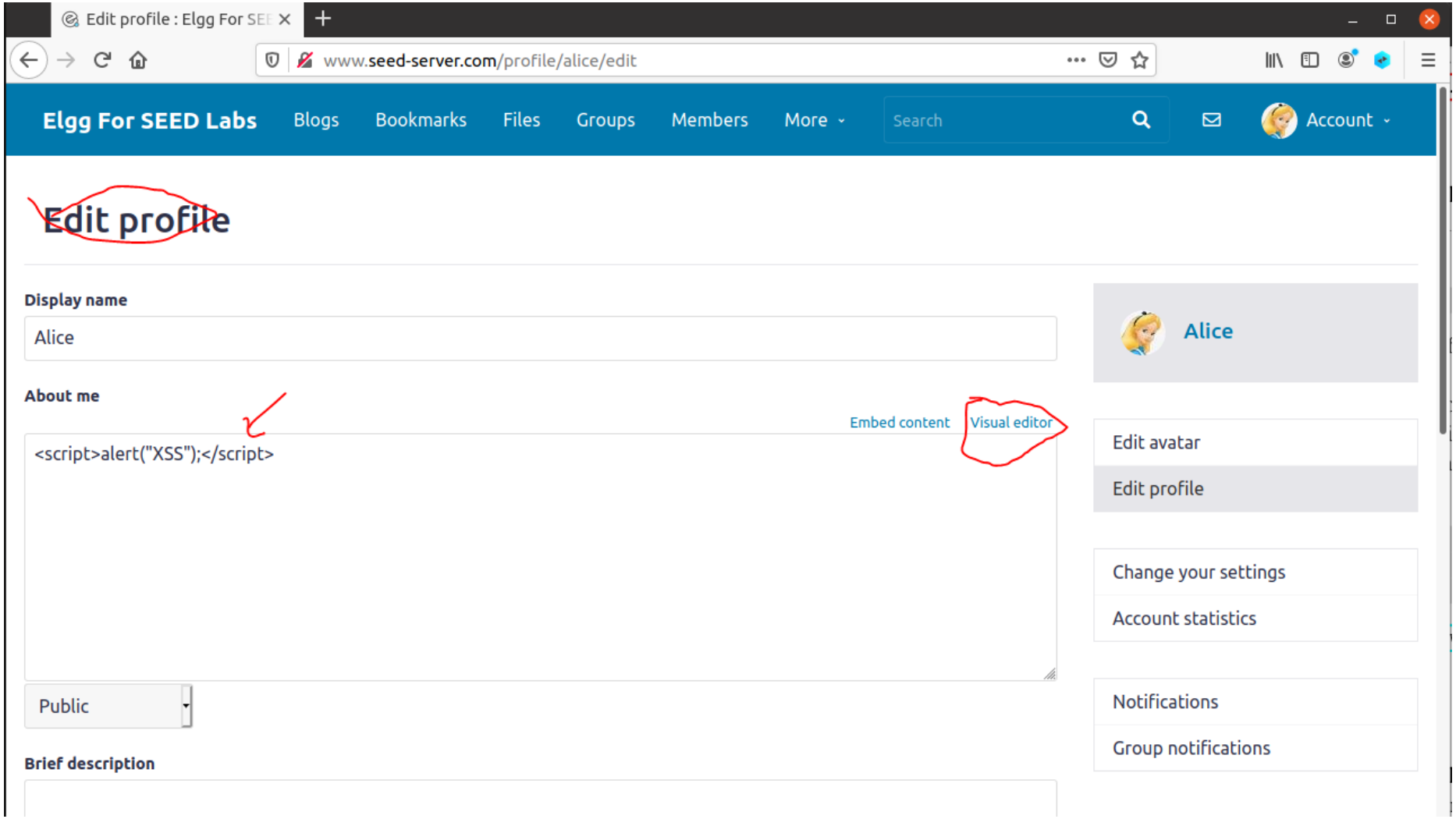
◆存储型 XSS

存储型XSS攻击指的是攻击者将**恶意脚本提交到受害网站的数据库中**，当其他用户浏览包含该恶意脚本链接的页面时，就会执行该脚本。由于是将恶意脚本保存在数据库中，所有访问包含恶意代码的页面的用户都受到攻击。



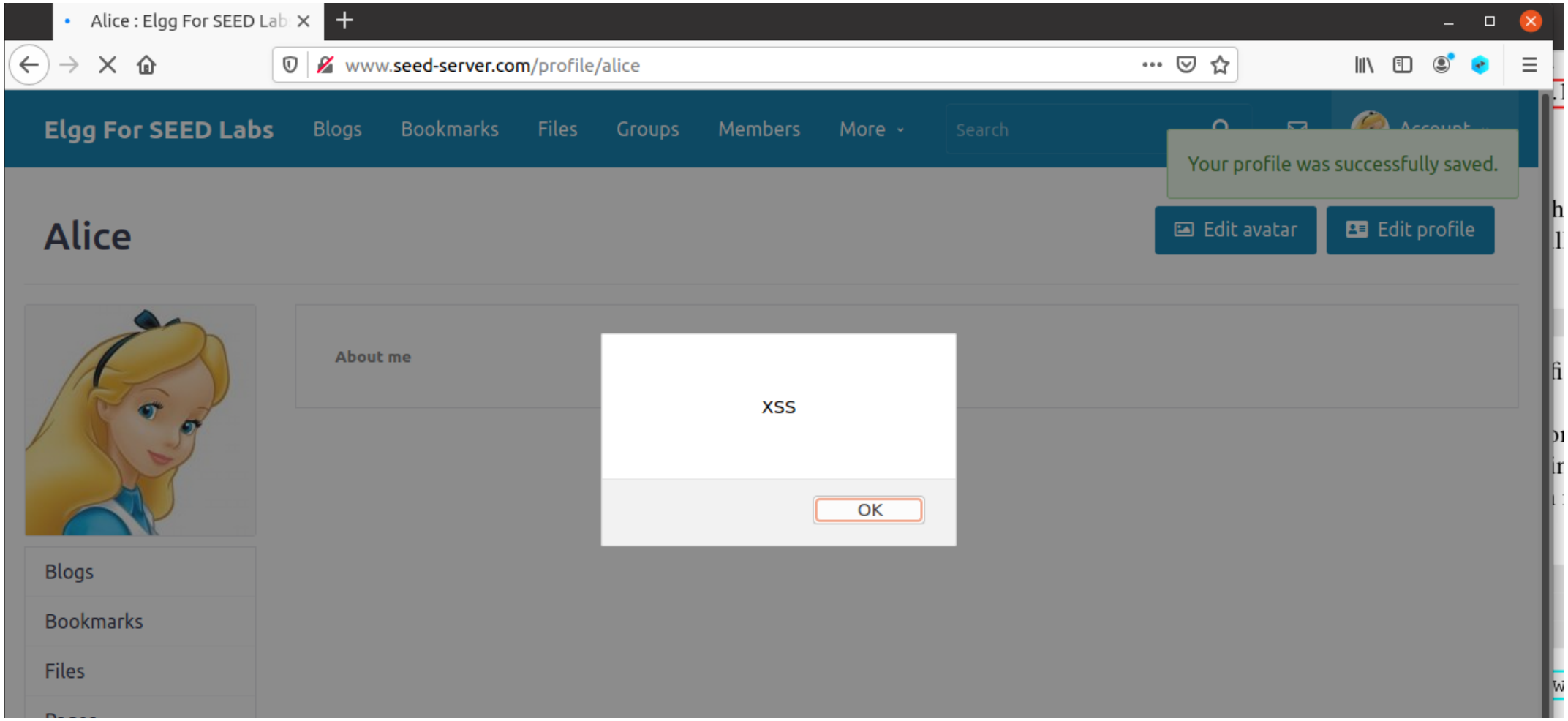
实验原理

◆ 存储型XSS示例



实验原理

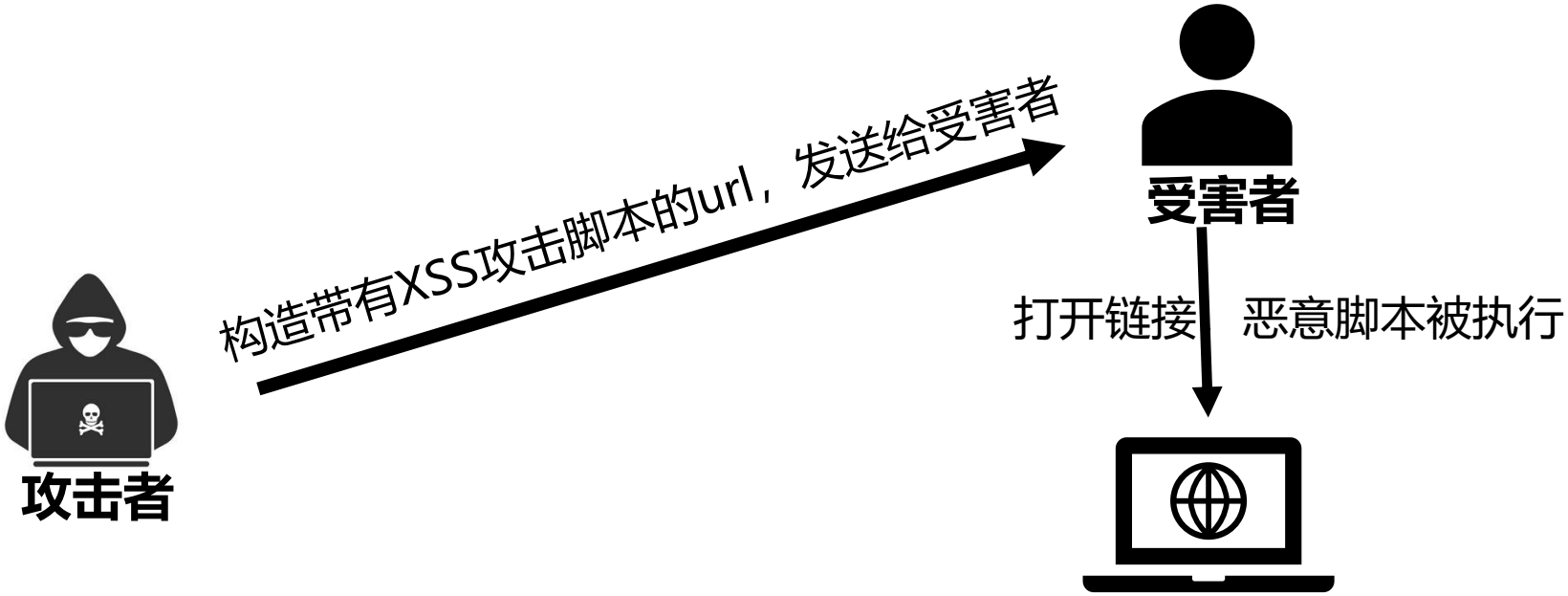
◆ 存储型XSS示例



实验原理

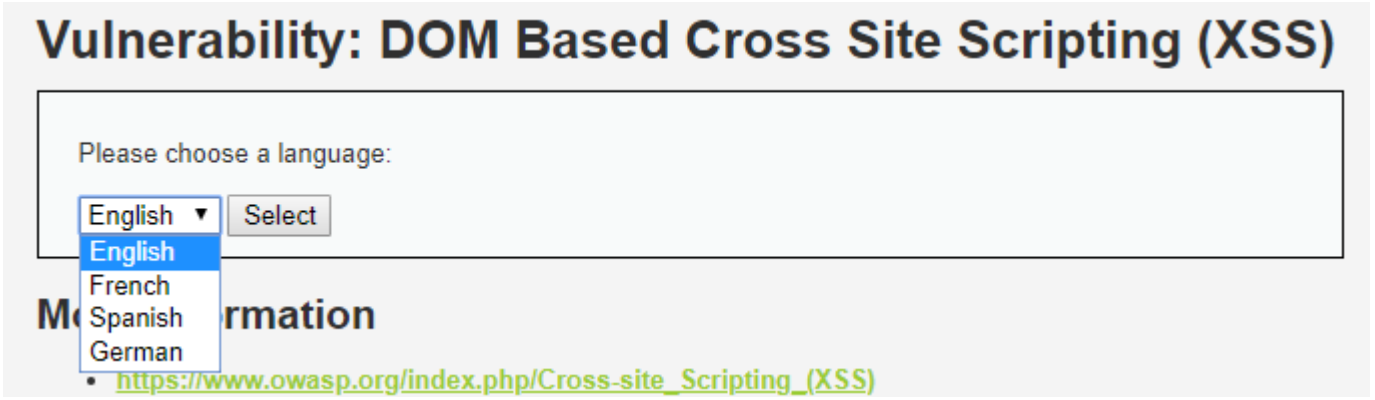
◆ DOM-base型 XSS

DOM型XSS攻击其实是一种特殊的反射型XSS， 它利用DOM基于HTML解析过程中的安全漏洞进行的跨站攻击。DOM型XSS攻击不涉及服务器的参与，完全基于客户端的机制，攻击者通过在客户端篡改网页中的DOM元素和属性，注入恶意代码进而达到攻击目的。**能够躲避WAF的监控。**



实验原理

◆ DOM型XSS示例



实验原理

◆ 防御XSS的措施CSP

- CSP（Content Security Policy）是内容安全策略，通过使用Content-Security-Policy HTTP头部，网站可以控制用户代理如何执行页面的特定部分，显著减少XSS攻击的风险。
- CSP是防XSS的利器，可以把其理解为白名单，开发者通过设置CSP的内容，来规定浏览器可以加载的资源。攻击者即使发现了漏洞，也没法注入脚本。
- CSP的一些常见指令包括：

•default-src， “self” “cdn.guangzhul.com”， 默认加载策略
•script-src， “self” “js.guangzhul.com”， 对javascript的加载策略
•style-src， “self” “css.guangzhul.com”， 对样式的加载策略
•img-src， “self” “img.guangzhul.com”， 对图片的加载策略
•content-src， “self”， 对ajax，websocket请求的加载策略。不允许的情况下浏览器会模拟一个状态为400的相应
•font-src， “font.cdn.guangzhul.com”， 针对webFont的加载策略
•object-src， “self”， 指针或标签引入flash等插件的加载策略

实验步骤

1、发布恶意消息以显示警告窗口；

2、发布恶意消息以显示Cookies；

3、窃取受害者的Cookies；

4、自动成为受害者的朋友；

5、修改受害者的个人资料；

6、编写自我传播的跨站脚本蠕虫病毒；

7、使用CSP（内容安全策略）抵御XSS攻击。

注意实验室环境要先删除 XSS下的Labsetup文件夹后重新解压

作业要求

提交内容：实验报告（有模板）

截止时间：

实验课后一周内提交至HITsz Grader 作业提交平台，具体截止日期参考平台发布。

- 登录网址：： http://grader.tery.top:8000/#/login
- 推荐浏览器： Chrome
- 初始用户名、密码均为学号，登录后请修改

注意

上传后可自行下载以确认是否正确提交

同学们
请开始实验吧！