北京邮电大学网络空间安全学院
信息安全认知实习
实验报告

课程名称：信息安全认知实习

单元名称：跨站脚本攻击（XSS）实验

姓名：任子恒

学号：2017522133

班级：2017661801

专业：信息安全

指导教师：颉夏青

成绩：

日　　期：2018 年 9 月 19 日

一、 实验目的

通过对一个示例漏洞网站的攻击尝试，了解 XSS 攻击的基本概念和操作，为后续专业课学习打下基础。

了解一些基本的 javascript 语句。

二、 实验原理

XSS 是一种在 web 应用中的计算机安全漏洞，它允许恶意 web 用户将代码植入到提供给其它用户使用的页面中。利用此漏洞的攻击叫做跨站脚本攻击。

XSS 攻击可分为两种类型：持久型和非持久型。

三、 实验环境

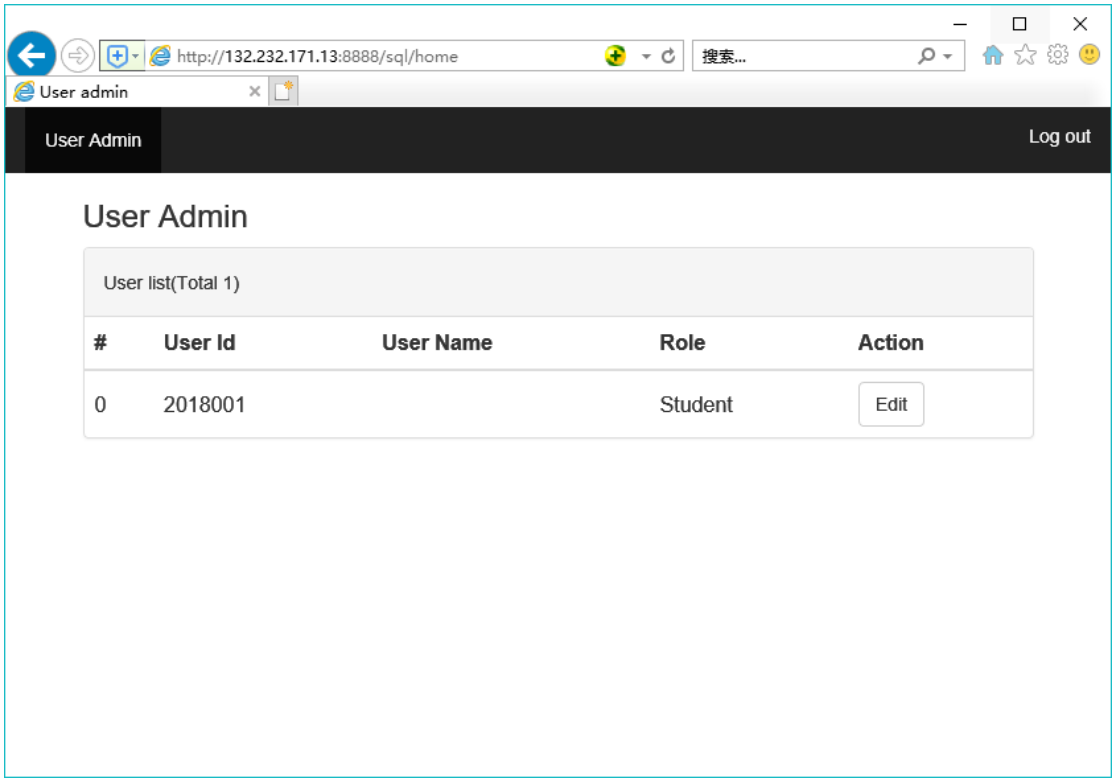
一台装有 IE 11 的 Windows10 电脑，已经通过 SQL 注入实验完成模拟漏洞网站的登录工作。

本实验对于操作系统需求不是很大

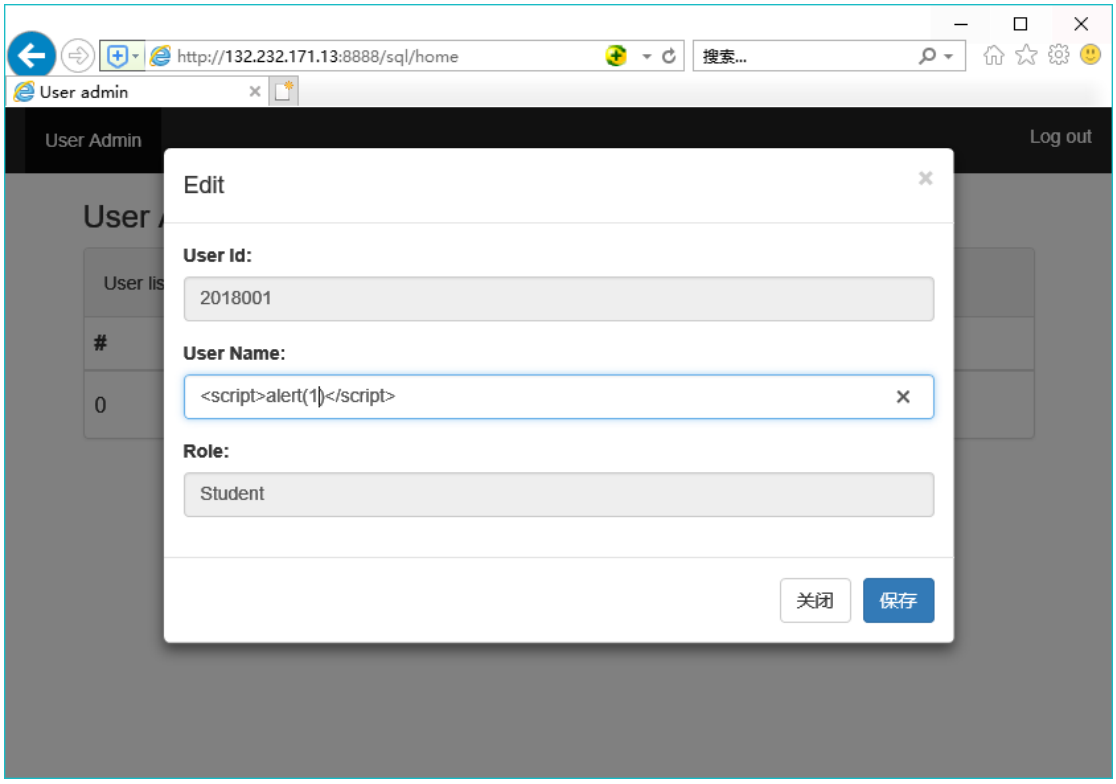
四、 实验过程及遇到的问题分析

4.1 实验过程

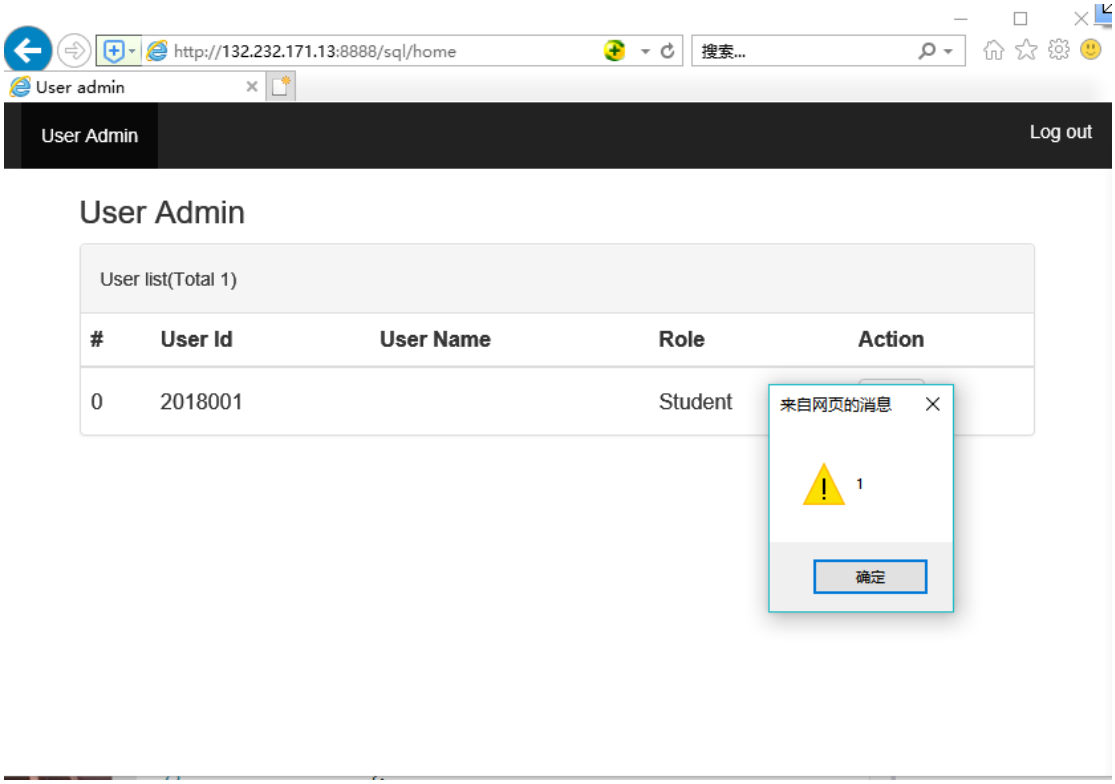
1. 已进入了漏洞模拟网站的用户界面



2. 在 username 中输入 javascript 代码，测试网站是否有 xss 漏洞。

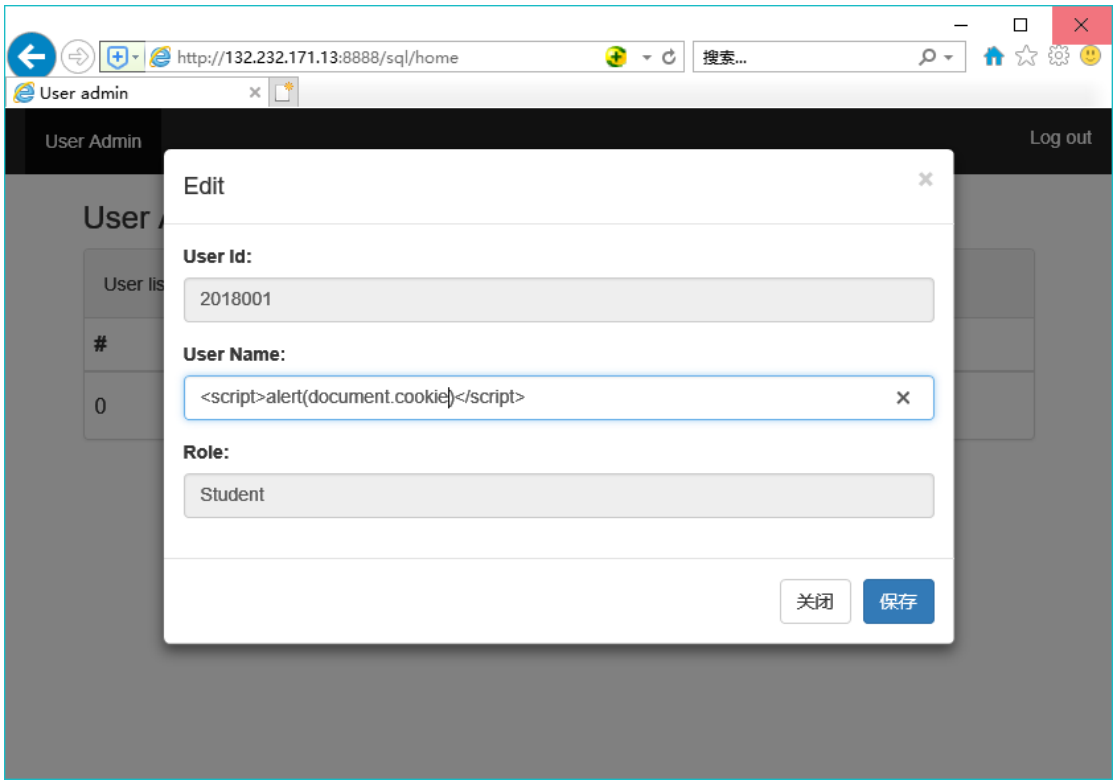


3. 保存后，网站刷新，然后弹出了写有 1 的窗口。

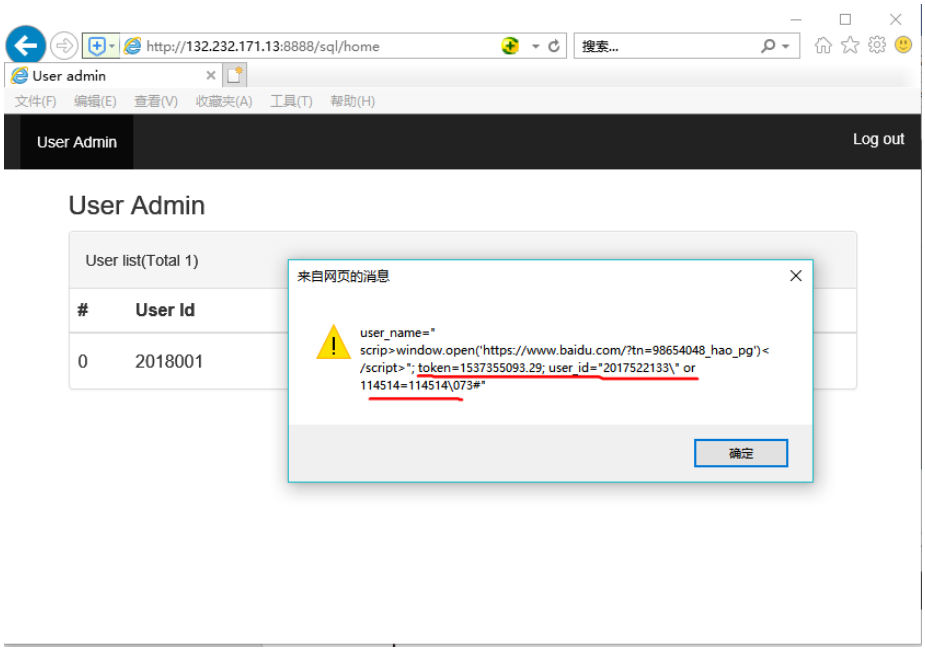


4. 现在试着获得当前用户的 cookie，在 username 栏中输入

<script>alert(document.cookie)</script>



然后弹出了一个对话框，显示了当前用户的 cookie 信息



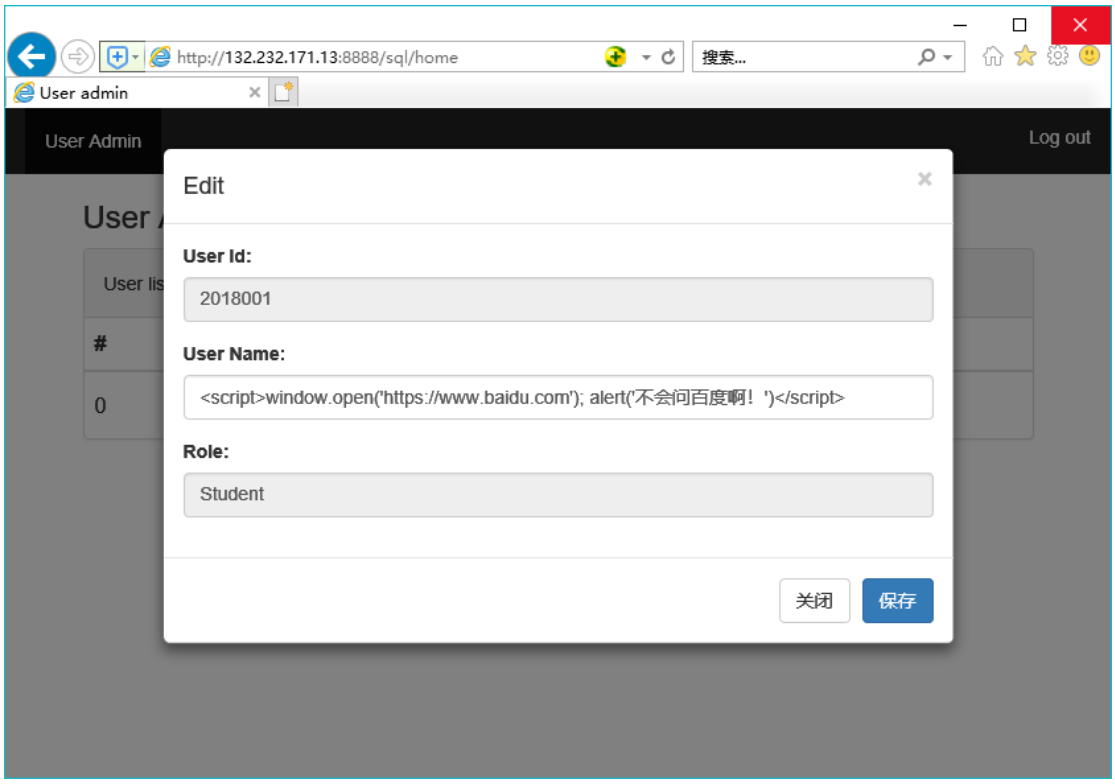
5. 尝试其它的代码。在 username 中输入

<script>

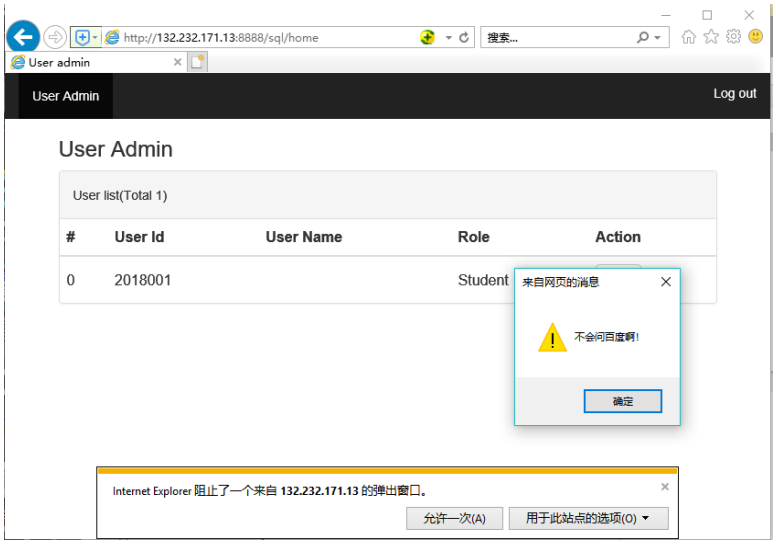
window.open(‘https://www.baidu.com’);

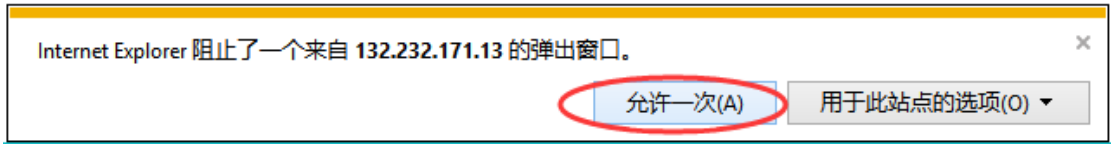
alert(‘不会问百度啊！’)

</script> 点击保存。



6. 运行效果。先弹出了一个对话框，显示了 alert 的内容，再弹出了一个窗口，内容为百度网页首页。





4.2 问题分析

网站管理员应如何防御 XSS 攻击？

1. 控制用户输入，拒绝非法字符。

2.提高对恶意代码的检测，多多留意网页代码中带有<script></script>的部分。禁止 javascript 代码自动执行。