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](http://www.hetianlab.com/expc.do?ec=11b931ee-3b45-42d6-a208-09980befcb81) |
| 指导教师： | 刘亚维 |
| 学生姓名： | 郑民采 |
| 组 号： | 5班的2组 |
| 实验日期： | 2019-6-9 |
| 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

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。

二、实验环境

<http://www.hetianlab.com/expc.do?ce=e0052d03-6550-4810-a813-72c863841e73>的实验工具。

展览器用google chrome。

实验环境为两台互相连网Windows主机。

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，我们称为实验机（客户机）；另一台主机不可见，但从实验机可以访问，这台主机即为本次实验任务的攻击目标，我们称为目标机。

2. 实验机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的演练平台（留言系统），供本次实验使用。

三、实验内容与实验要求

**Cross Site Scripting攻击**

在网络留言板或邮件等处插入了Script,让不正常的页面看到,妨碍用户或偷盗cookie及其他个人信息的攻击.

这种攻击靠防火墙很难对付,目标又不是攻击那个网站,而且不是病毒难以探测

**Cookie sniffing**

如果使用者如果实行特定的Script, 在hacker网站运行时会留下Cookie信息, hacker可以使用那个饼干进行任何处理,但是,这样给其他人信息露的Cookie就不是问题。  
但该内容中,包含信息可以成为安全的内容时发生损失。

**显示虚假页面**

hacker可以打出想要的Script来显示虚假网页

用<script>....</script>这样的script。

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。

**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>

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。

**使用跨站漏洞加载恶意网页**

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。

2、隐藏恶意网页。增加留言，内容包含以下语句：<iframe src=http://www.baidu.com width="0" height="0"></iframe>，观察返回状态，网页被执行，但未在留言系统界面中显示。这样如果是攻击脚本就可以用此方法隐藏自己。

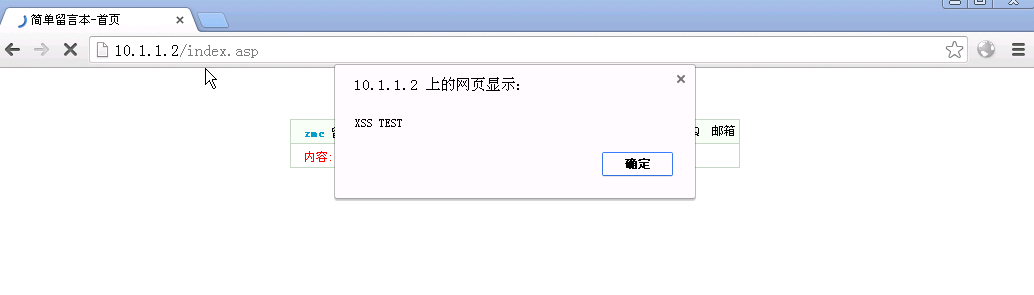
**利用存储式跨站漏洞窃取用户cookie**

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

2、继续添加留言，包含以下内容：

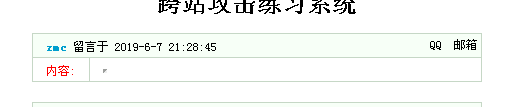
      <script>alert(document.cookie)</script>，

四、实验过程与分析



输入恶意的script显示这个alert

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



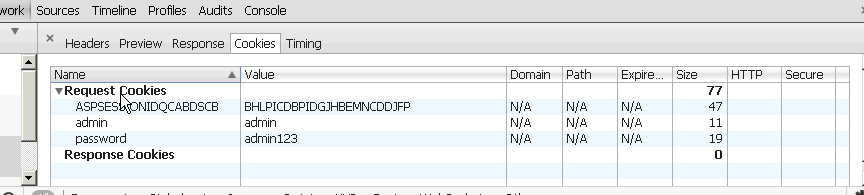
输入显示恶意的页面的script

<iframe src=http://www.baidu.com width="0" height="0"></iframe>

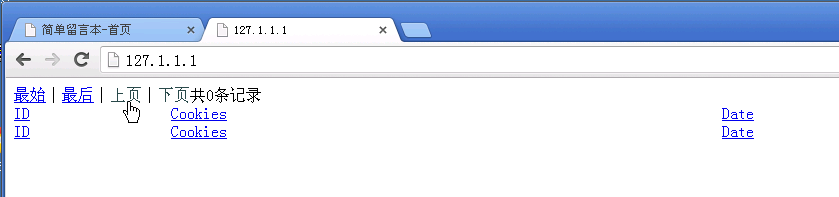


以此留下cookie记录

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

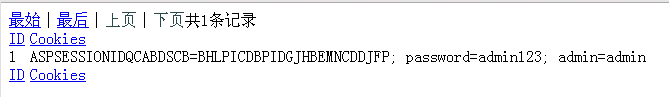


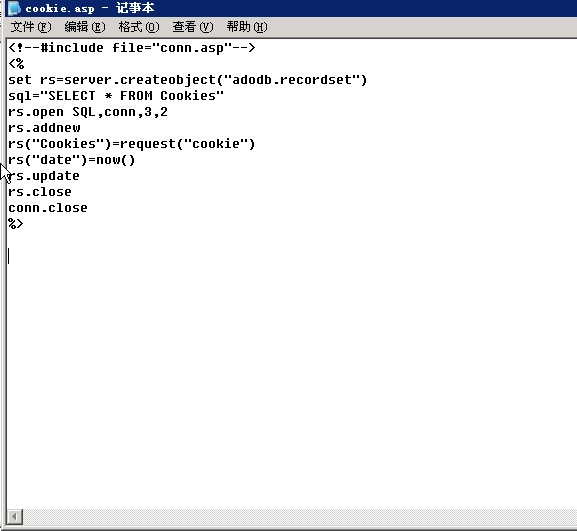
从这里可以看到cookie的记录

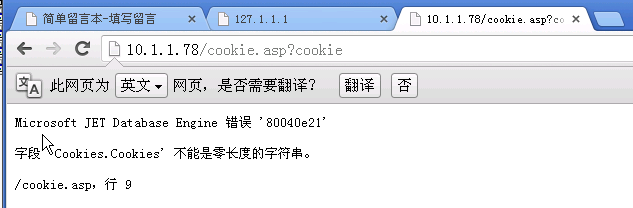




这句里面有个document.cookie,这是script的，所以必须有  <script>  </script>标签包围着







然后这些是结果

五、实验结果总结

xss就是前端漏洞的攻击 它的核心是js，是由于Web应用程序对用户的输入过滤不足所造成的

我们通过本次实验知道了xss攻击能获取cookie，按照代码能获取更多的信息。 我们掌握了用Html缺点的这个攻击的基础

这种攻击对于初级开发者来说是可以忽略的, 其实通常这种缺陷是很简单的, 使用代码时,应对方法有很多种, 还有关于那个的程序。 努力制作的程序, 更应该努力, 免得受到这样的攻击