

**实 验 报 告**

**（ 2021/ 2022 学年 第 二 学期）**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 课程名称 | Web安全 | | | | | |
| 实验名称 | 文件上传攻击 | | | | | |
| 实验时间 | 2022 | 年 | 5 | 月 | 23 | 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** | | 文件上传攻击 | | | | | **指导教师** | | 陈伟 |
| **实验类型** | | 上机 | | **实验学时** | | 2 | **实验时间** | | 2022.05.23 |
| 1. **实验目的和要求**   1.针对DVWA Low和Medium级别的文件上传漏洞进行渗透；  2.使用BP实现文件上传绕过；  3.编写一句话木马并上传，使用Hackbar工具进行远程操作；  4.使用蚁剑工具进行Webshell的操作。 | | | | | | | | | |
| 二、**实验环境(实验设备)**  1.安装Windows操作系统并连接网络的一台PC机。  2. Apache+PHP+MySQL  3.DVWA  4. Firefox，Hackbar，Burp Suite，蚁剑 | | | | | | | | | |
| **三、实验内容**  1. 完成任务一步骤（7），在BP中修改content-type后，在Forwad提交前，把BP中的内容截图，截图范围和步骤（7）中类似，需要显示数据包的主要内容。  C:\Users\Claymore\Documents\Tencent Files\2833846150\FileRecv\MobileFile\Image\NM1@2V[~4DEC9K1)V%)OYKD.png    2.完成任务二步骤（4），显示phpinfo();运行的结果，截图记录。  https://127.0.0.1/DVWA/hackable/uploads/shell.php    3.完成任务三步骤（4），在DVWA的“/hackable/uploads/”目录下用自己的学号新建一个文件，例如“B18030740.txt”，并截图记录。 | | | | | | | | | |
| **四、实验小结（包括问题和解决方法、心得体会、意见与建议等）**  1.问题和解决方法  问题：AntSword连接一句话木马失败  解决方法：应该使用HTTP，而不是HTTPS  2.心得体会  通过这次实验，我理解了文件上传漏洞和一句话木马拿到webshell的原理。我发现开发网站时最好不要提供回显内容，避免暴露服务器的文件储存路径。同时不仅应该对文件名，文件格式进行检查，还要对文件内容进行审查，这样才能尽可能避免文件上传攻击。  3.意见与建议 | | | | | | | | | |
| **五、指导教师评语** | | | | | | | | | |
| **成 绩** |  | | **批阅人** | |  | | **日 期** |  | |