

**实 验 报 告**

**（ 2021/ 2022 学年 第 二 学期）**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 课程名称 | Web安全 | | | | | |
| 实验名称 | SQL注入攻击 | | | | | |
| 实验时间 | 2022 | 年 | 5 | 月 | 3 | 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** | | SQL注入攻击 | | | | | **指导教师** | | 陈伟 |
| **实验类型** | | 上机 | | **实验学时** | | 2 | **实验时间** | | 2022.5.3 |
| 1. **实验目的和要求**   1.针对DVWA Low级别的SQL注入漏洞，进行手动注入实验；  2.使用SQLMap进行自动注入实验； | | | | | | | | | |
| 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 | | | | | | | | | |
| **三、实验内容**  1. 完成任务一步骤（6），把获得的所有用户名和密码的哈希值截图记录。    2. 完成任务二步骤（9），打开SQLMap拖下来的数据文件，并截图记录。    3.如果完成任务三中部分内容，可以截图记录其中重要的心得体会  High级别的查询提交页面与查询结果显示页面不是同一个，也没有执行302跳转，这样做的目的是为了防止常规的sqlmap扫描注入测试，因为sqlmap在注入过程中，无法在查询提交页面上获取查询的结果，没有了反馈，也就没办法进一步注入；但是并不代表High级别不能用sqlmap进行注入测试，此时需要利用其非常规的命令联合操作，如：–second-order=“xxxurl”（设置二阶响应的结果显示页面的url）  新的cookie如下    Sqlmap命令  Python sqlmap.py -u "http://127.0.0.1/DVWA/vulnerabilities/sqli/session-input.php#" --data="id=1&Submit=Submit" --second-url="http://127.0.0.1/DVWA/vulnerabilities/sqli/" --cookie="security=high; PHPSESSID=omk12q5t1kscfros68f93h1g9i" –T “users” –dump | | | | | | | | | |
| **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：如何快速查看当前页面的cookie  解决办法：F12，在浏览器控制台中输入document.cookie  2.心得体会  通过这次实验，我学会了使用手动和脚本的方式进行sql注入。对于网站来说，要想防止sql注入攻击，可以采用预编译技术，预编译技术中SQL语句的语义不会是不会发生改变的，在创建的时候就已经将指定的SQL语句发送给了DBMS，完成了解析，检查，编译等工作，所以攻击者无法改变SQL语句的结构，只是把值赋给SQL语句的指定位置。此外，还可以通过严格控制数据类型，对特殊的字符进行转义等方法减少被攻击可能。  ，  3.意见与建议  无 | | | | | | | | | |
| **五、指导教师评语** | | | | | | | | | |
| **成 绩** |  | | **批阅人** | |  | | **日 期** |  | |