WEB 编程安全(SQL 注入)

1. 编写一个实际的例子,实现 SQL 注入

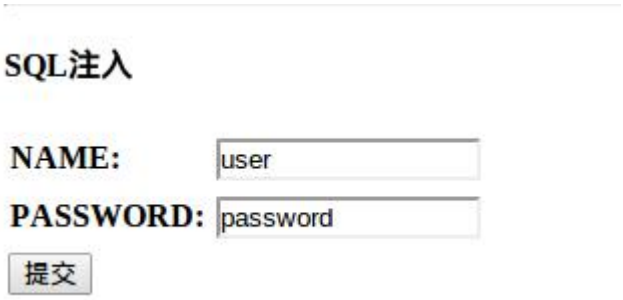
我们构造一个数据库 buggy_db，新建表 user_table

然后添加一条记录：

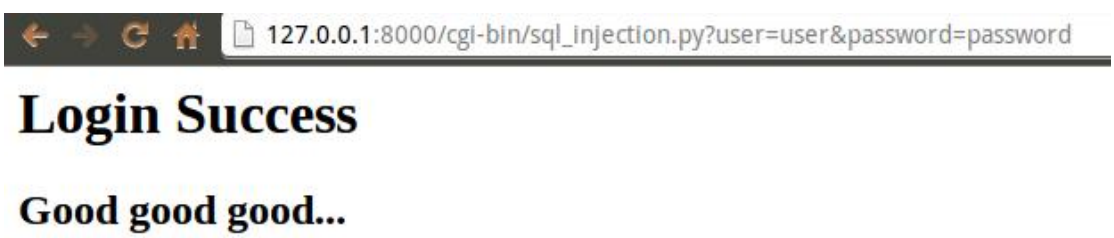
```
mysql> select * from user_table;
+----+------+----------+
| id | user | password |
+----+------+----------+
|  1 | user | password |
+----+------+----------+
1 row in set (0.00 sec)
```

我们使用 SQL 注入的方法，绕过验证

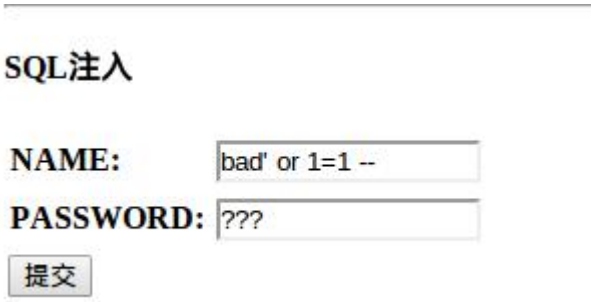
正常情况下，是这个样子的：



然后



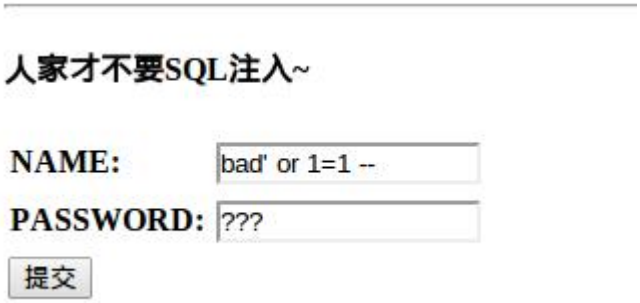
现在我们 Hack 一下 ~



然后就：

2. 编写一段代码,防范 SQL 注入

使用 MySQLdb.escape_string 对输入进行过滤，就可以在一定程度上避免 SQL 注入



3. 通过 SQL 注入可以实现数据库表的删除,怎样通过授权来防范?

在 MySQL 中，我们可以使用 GRANT PRIVILEGE 语句限定一个用户的权限。

避免在线上服务中使用 root 账户，这是非常危险的!

4. 隐藏表单具有不安全因素,可以被其他技术取代吗?

可以使用 session 和 Ajax 技术取代。

5. 编写一段代码,过滤表单提交中的所有特殊字符

6. 注释

文档里的所有代码都在 buggy_website 文件夹下 ~

G`Day~