SQL注入之显错注入（一）

原创

VIP文章 Mr.Huang__ 于 2021-08-10 20:05:39 发布 179 收藏 1

分类专栏： 学习笔记 文章标签： sql 渗透测试 网络安全

本文链接：https://blog.csdn.net/m0_46140380/article/details/119575201

SQL注入的原理解析

sql注入是指web应用程序对用户输入数据的合法性没有判断，导致攻击者可以构造不同的sql语句来实现对数据库的操作。

SQL注入本质

1. 谈到SQL注入前我们先谈谈什么是注入
   注入攻击的本质，是把用户输入的数据当做代码执行。
2. SQL注入的本质
   用户输入的数据当做SQL代码执行
3. SQL注入的条件,这里有两个关键条件
    1. 第一个是用户能够控制输入
    2. 第二个是原本程序要执行的代码，拼接了用户输入的数据然后进行执行

MySQL系统自带库

MySQL 中存储所有数据库名、所有表名、所有字段名的系统数据库叫 `information_schema`，这是在 MySQL 数据库初始化就存在的系统库。库里存储数据库名、表名、字段名的表分别为 `schemata`、`tables`、`columns`（原始表名为大写，但小写也能取到数据）。

表名	关键字段
schemata	schema_name [数据库名]
tables	table_schema [数据库名],table_name [表名]
columns	table_schema [数据库名],table_name [表名],column_name [列名]

SQL注入流程