SQL注入之获取指定数据库数据Mysql（基础篇）

潇洒哥 / 2017-03-12 08:57:40 / 浏览数 4238 安全技术 漏洞分析 顶(0) 踩(0)

前言

> 我们知道，在我们进行某网站sql注入的时候，我们有时候只可以进行简单的 union select user(),version(),@@basedir() #
>
这类简单的查询，想要获得管理员用户密码或者敏感信息的时候就很难搞，因为我们不知道他的数据库表的名字以及字段名字，这篇文章就是介绍一下如果利用Mysql数据库

1.查看information_schema数据库

information_schema这张数据库保存了MySQL服务器所有数据库的信息。如■■■■，■■■■■，■■■■■
■■■■■■■■■■■■■。再简单点，这台Mysql服务器上，到底有哪些数据库、各个数据库有哪些表，每张表的字段类型是什么，各个数据库要什么权限才能访问，等等信息

---

information_schema数据库里面的数据非常大，我们也不需要接触那么多，只需要记住几个重要的就可以了
需要记住的:

> 这些很难解释，主要是多实践就知道了

```
information_schema.schemata //Mysql■■■■■■■■■■

information_schema.tables  //Mysql■■■■■■■■■■■■

information_schema.columns //Mysql■■■■■■■■■■■■■■

schema_name                //Mysql■■■■■■information_schema.schemata■■■■■■■■

table_name                 //Mysql■■■■■■information_schema.tables■■■■■■■■

column_name                ////Mysql■■■■■■information_columns.column■■■■■■■■
```

1. SCHEMATA表

SCHEMATA表提供了当前mysql实例中所有数据库的信息。是show databases的结果取之此表。

1. TABLES表

TABLES表提供了关于数据库中的表的信息（包括视图）。详细表述了某个表属于哪个schema，表类型，表引擎，创建时间，等等信息。是show tables from schemaname的结果取之此表。

1. COLUMNS表

COLUMNS表提供了表中的列信息。详细表述了某张表的所有列以及每个列的信息。是show columns from schemaname.tablename的结果取之此表。

2.查询例子

1. 查询所有数据库

```
select schmea_name from information_schema.schemata
```

2. 查询指定数据库下的表名

> 这里我们以'test'数据库为例子，并且要注意的是：查询指定数据库下面的表名必须要用WHERE选择你要查询的数据库名字

```
select table_name from information_schema.tables where table_schema = 'test'
```

如果过滤了=号这段语句可以变形为(用like替换=号)：

```
select table_name from information_schema.tables where table_schema like 'test'
```

如果过滤了■■■这段语句可以变形为(16■■转换)：

```
select table_name from information_schema.tables where table_schema like 0x74657374
```

3. 查询数据库下面表名的列名

```
select column_name from information_schema.columns where table_name= '■■' and table_schema= '■■■■'
select column_name from information_schema.columns where table_name= 'users' and table_schema= 'test'
```

4. 获取想要的目标数据

```
select username,password from users
```

点击收藏 | 0 关注 | 0

上一篇：opensns最新版前台getshell 下一篇：CSRF攻防汇总梳理

1. 0 条回复
   - 动动手指，沙发就是你的了！