国家信息安全水平考试

NATIONAL INFORMATION SECURITY TEST PROGRAM

sql注入基础知识

目录

SQL注入攻击的根源

程序命令和用户数据（即用户输入）
之间没有做到泾渭分明

注入成功的基础

1、相信用户输入的数据
2、Sql语句的拼接

注入之前必须要做三件事情

- 确定web应用程序所使用的技术
- 确定所有可能的输入方式
- 查找可以用于注入的用户输入

万能密码原理解析

- 大家经常听到网站万能密码登录，
- 输入 ‘ or 1=1 -- 发现输入任何密码都可以登录成功

注入前的准备及注入漏洞检测

- 捕捉报错信息
- 手工检测SQL注入点
  - 最常用的SQL注入点判断方法，是在网站中寻找如下形式的网页连接。
  - http:// www.*****. com/ ***.asp?id=x （ASP注入）
  - http:// www.*****. com/ ***.php?id=x （php注入）.
  - http:// www.*****. com/ ***.jsp?id=x （jsp注入）
  - http:// www.*****. com/ ***.aspx?id=x （aspx注入）
  - http:// www.****.com/index/new/id/8伪静态。
  - http:// www.*****.com/index/new/php-8.html伪静态

注入前的准备及注入漏洞检测

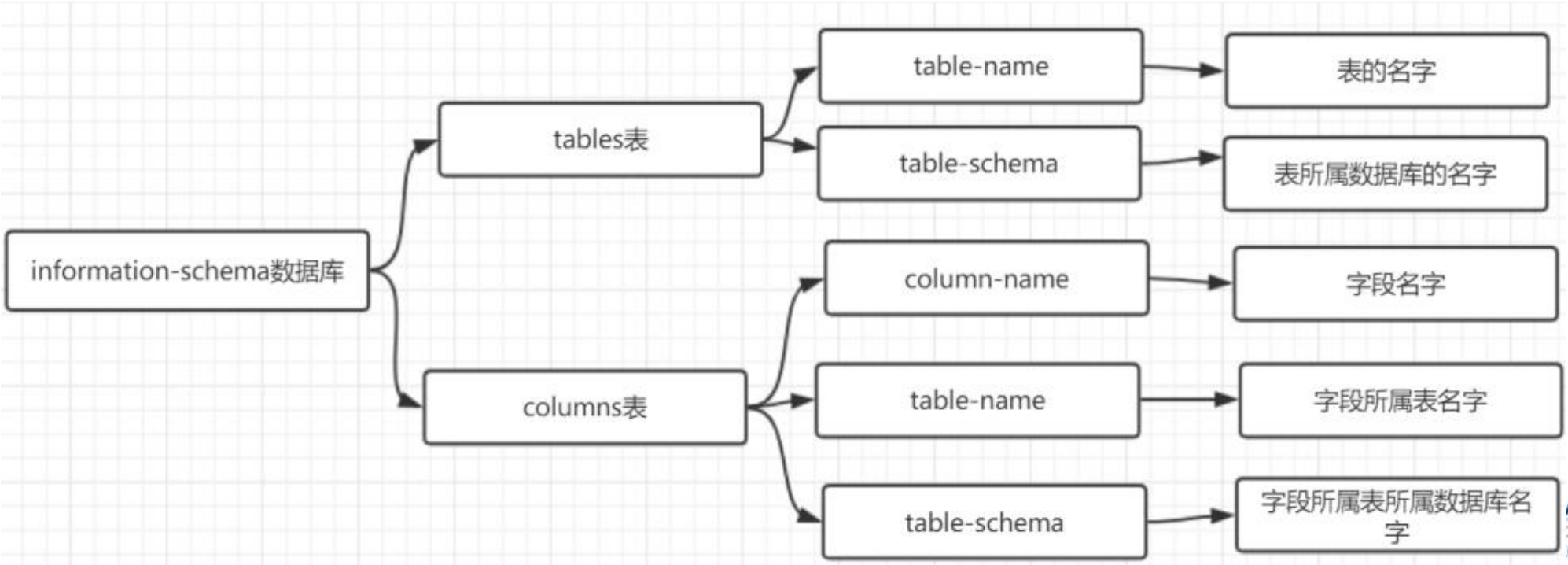
- 检测方法
- 1.“单引号”法
- 2. and 1=1和1=2法
- 3. 通过页面返回的报错信息，一般情况下页面报错会显示是什么数据库类型

SQL注入的分类

- 按照注入的网页功能类型分类
  - 1、登录注入
  - 2、cms注入
- 按照注入点值的属性分类
  - 1、数值型
  - 2、字符串型
- 基于从服务器返回的内容
  - 1、有回显
  - 2、无回显
- 按照注入的程度和顺序
  - 1、一阶注入
  - 2、二阶注入
- 其他业务场景
- Update注入
- Insert注入
- Delete注入
- Like注入
- Order by注入
- 宽字节注入
- http头注入

Mysql注入知识复习

- 在Mysql 5.0以上的版本中，为了方便管理，默认定义了information_schema数据库，用来存储数据库元信息。其中具有表schemata(数据库名)、tables(表名)、columns(列名或字段名)。



Mysql注入知识复习

- user();查看当前Mysql登录用户名
- database():查看当前使用Mysql数据库名
- version():查看当前Mysql版本
- @@version
- @@basedir
- length() 字符串长度
- substring()截取字符串
- ord 返回ASCII码值
- concat 连接字符串
- sleep(4) 睡眠指定描述
- group_concat() 查询结果放同一行
- limit m,n 从m行开始，到m+n行。
- mid()需要截取的字符串

Mysql注入知识复习

- 注释：
- #
- --空格（%20）
- /**/
- 内联注释:/*!SQL语句*只有Mysql可以识别，常用来绕过WAF
- 例如:select * from articles where id = id
- 使用内联注释注入:select *from articles where id =-1 /*!union*//*!select*/

总结

SQL注入攻击的根源
注入之前必须要做三件事情
万能密码原理解析
注入前的准备及注入漏洞检测
SQL注入的分类
Mysql注入知识复习