云安全技术与应用

- 日照职业技术学院
- 电子信息工程系
- 赵娜

项目七

数据库攻击与加固技术

目录

CONTENTS

01.

SQL语言基础回顾

MySQL

SQL结构化查询语言，绝大多数关系型数据库（MySQL、Access、Oracle等）都采用SQL进行查询、管理及常用操作。

MySQL是被广泛使用的一种开源数据库，官方网站www.mysql.com。

MySQL基本操作

在MySQL中所有的语句后面都要加上“;” 表示结束。

```
select version();          #查看mysql版本

select user();             #查看当前用户

select database();         #查看当前打开的数据库

show databases;            #查看MySQL中共包含了哪些数据库

use test;                  #打开test数据库

show tables;               #显示数据库中的表
```

MySQL基——创建表、向表中添加记录

创建表：

```
mysql> create table hack
    -> (
    -> id int,
    -> username varchar(20),
    -> password varchar(30)
    -> );
```

向表中添加记录：

```
insert into hack
values(1,'admin',  ‘456');
insert into hack
values(2,'boss',  ‘123');
```

MySQL基——创建表、向表中添加记录

创建表：

```
mysql> create table hack
    -> (
    -> id int,
    -> username varchar(20),
    -> password varchar(30)
    -> );
mysql> create table news
    -> (
    -> id int,
    -> title varchar(50)
    -> );
```

向表中添加记录：

```
insert into hack
values(1,'admin',  ‘456');
insert into hack
values(2,'boss',  ‘123');

insert into news
values(1,'web');
```

MySQL基——select

```
select * from hack;                          #显示hack表中的所有记录
select * from hack where id=1;    #从hack表中查找满足条件id=1的记录
select username,password from hack where id=1;
#从hack表中查找满足条件id=1的记录，并只显示username和password字段内容
select * from hack where id=1 and username="admin";
#从hack表中查找同时满足条件id=1以及username=“admin”的记录
select * from hack where id=1 or username="boss";
#从hack表中查找同时满足条件id=1或者username=“boss”的记录
```

MySQL基——select

```
select * from news where id=1 and exists (select * from hack);
#通过exists()函数判断hack表是否存在

select * from news where id=1 and exists (select username from hack);
#通过exists()函数判断hack表中是否存在username字段

select * from hack order by id;                    #按照hack表中的id列升序排序

select username,password from hack order by 2;
#按照查询结果中的第2列（即password列）升序排序
```

MySQL基——union select联合查询

union联合查询可以一次性执行两个或多个查询，并将它们的结果组合在一起输出显示。

union联合查询的基本规则：　　所有查询中的列数必须相同

select * from news union select * from hack; #字段数不匹配，查询报错

select * from news union select username,password from hack;　　#查询正常

select * from hack union select 1,id,title from news; #查询正常

MySQL基——注释语句

注释方式

- \- \# 号注释
- \- %23 注释
- \- --+ 注释

MySQL基——常用的查询信息

常用的查询信息

- database() # 在用的[数据库]名
- user()　# 用户信息
- version() # 数据库版本信息
- @@basedir # 数据库安装路径
- @@version_compile_os # 操作系统版本

MySQL基——group_concat()

使用 group_concat() 将多行合并成一行(比较常用)
语法：group_concat([[distinct] 要连接的字段 [order by 排序字段 asc/desc] [separator '分隔符'])

```
SELECT
  T.DEPTNO,
        group_concat ( T.ENAME ORDER BY DEPTNO separator ',' )
FROM
        EMP T
WHERE
        T.DEPTNO = '20'
GROUP BY
        T.DEPTNO;
```

MySQL基——limit

limit 是 MySQL 中的一个特殊关键字，用于指定查询结果从哪条记录开始显示，一共显示多少条记录。

LIMIT 指定初始位置的基本语法格式如下：

LIMIT 初始位置，记录数

其中，“初始位置”表示从哪条记录开始显示；“记录数”表示显示记录的条数。第一条记录的位置是 0，第二条记录的位置是 1。后面的记录依次类推。

02.

SQL注入的原理分析

什么是SQL注入？

SQL注入的核心思想：

黑客在正常的需要调用数据库数据的URL后面构造一段数据库查询代码，然后根据返回的结果，从而获得想要的某些数据。

SQL注入漏洞（SQL injection）是Web层面最高危的漏洞之一，曾连续3年在OWASP年度十大漏洞中排名第一。

准备实验环境

✓实验平台　　PHPstudy

✓目标网站　　sqlilabs

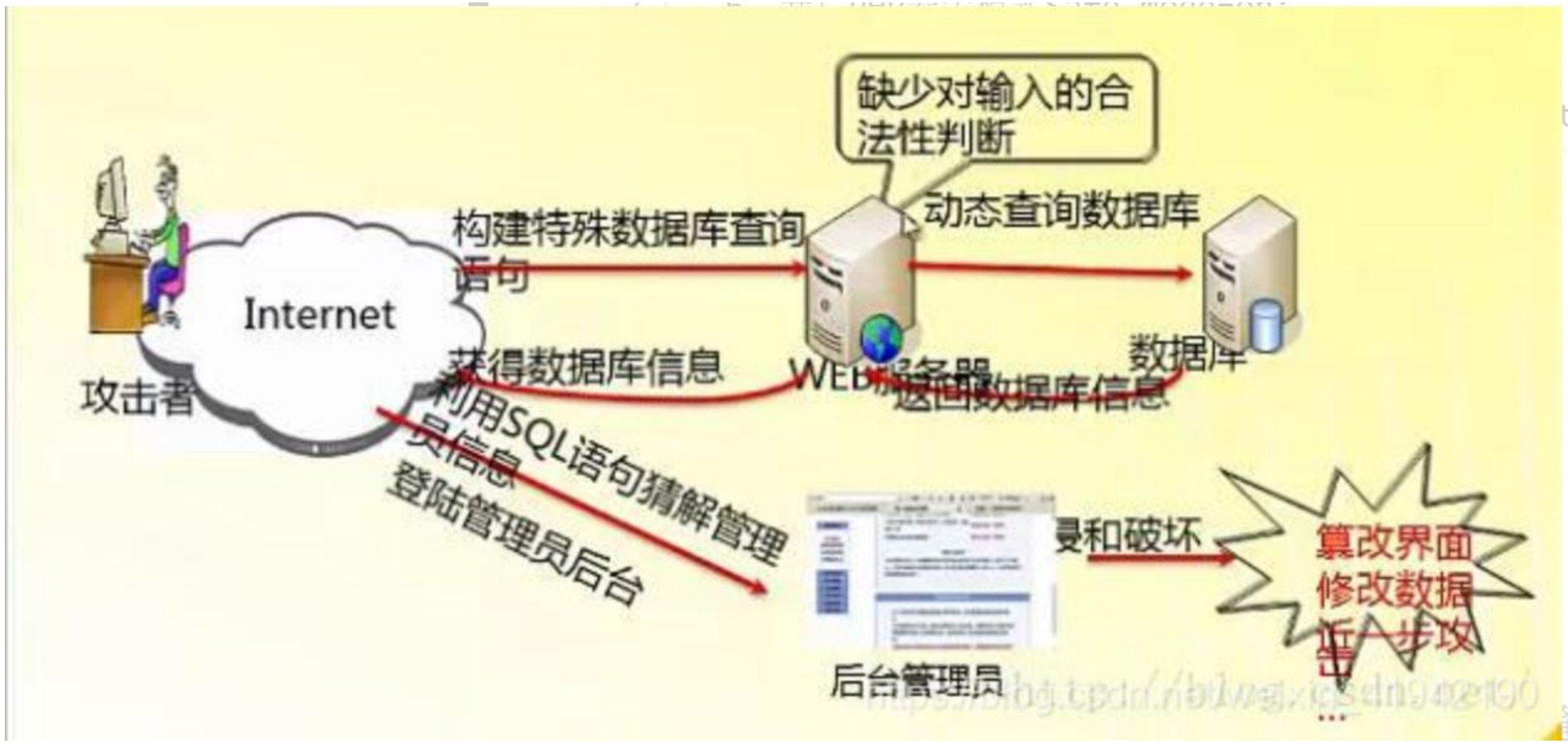
✓涉及资源：1. https://github.com/Audi-1/sqli-labs

2.墨者学院

知识点

- 1. 在Mysql5.0以上版本，mysql存在一个自带数据库名为information_schema，它是一个存储记录所有数据库名，表名，列名的数据库，也相当于可以通过查询它获取指定数据库下面的表名或列名信息。
- 2. 数据库中符号. 代表下一级，如xiaodi.user 表示xiao数据库下的user表名。
- information_schema.tables; 记录所有表名信息的表
- information_schema.columns; 记录所有列名信息的表
- table_name 表名
- column_name 列名
- table_schema 数据库名

注入原理


缺少对输入的合法性判断
构建特殊数据库查询语句
动态查询数据库
Internet
攻击者
获得数据库信息
数据库
返回数据库信息
利用SQL语句猜解管理员信息
登陆管理员后台
后台管理员
篡改界面
修改数据

SQL注入威胁表现形式可以体现为以下几点：

- 绕过认证，获得非法权限
- 猜解后台数据库全部的信息
- 注入可以借助数据库的存储过程进行提权等操作

SQL注入攻击的典型手段：

- 判断应用程序是否存在注入漏洞
- 收集信息、并判断数据库类型
- 根据注入参数类型，重构SQL语句的原貌
- 猜解表名、字段名
- 获取账户信息、攻击web或为下一步攻击做准备

SQL注入判断注入点的方法：

SQL注入漏洞的几种判断方法：

正确链接： http://www.heetian.com/showtail.asp?id=40

①http://www.heetian.com/showtail.asp?id=40'

②http://www.heetian.com/showtail.asp?id=40 and 1=1

③http://www.heetian.com/showtail.asp?id=40 and 1=2

如果执行①后，页面上提示报错或者提示数据库错误的话，说明是存在注入漏洞的。

如果执行②后，页面正常显示，而执行③后，页面报错，那么说明这个页面是存在注入漏洞的。

SQL注入判断注入点的方法：

SQL注入漏洞的几种判断方法：

因为正确的链接：http://www.heetian.com/showtail.asp?id=40 没有问题，如果如果执行①后，页面上提示报错或者提示数据库错误的话说明是不满足条件，说明查询的条件不满足，是有一个查询语句的，说明是存在注入漏洞，如果执行②后，页面正常显示，而执行③后，页面报错，那么说明这个页面是存在注入漏洞的。

实战：墨者靶机真实mysql注入演示

SQL注入之
简单SQL注入

Sqlilabs注入靶场搭建简要使用

https://blog.csdn.net/ssjjtt1997/article/details/117233500

- ✓ SQLi-Labs 是一个专业的 SQL 注入练习平台，它适用于 GET 和 POST 等多场景的注入。
- ✓ SQLi-Labs 注入场景（基于错误的注入、基于误差的注入、盲注入、更新查询注入、插入查询注入、Header 头部注入、二阶注入，也可叫二次注入、绕过 WAF、堆叠注入……）
- ✓ SQLi-Labs 下载（确定PHP版本）
- ✓ SQLi-Labs 安装

03.

sqlmap注入工具的使用

04.

数据库加固

05.

实战：Mysql数据库加固练习