3.2-SQL注入漏洞-上

无涯老师

上一节内容回顾

1、漏洞定义与漏洞扫描
2、漏洞分类与分级
3、《网络产品安全漏洞管理规定》
4、漏洞内容规划

课程大纲

1、Web网站基本架构
2、如何构建可以执行的语句
3、SQL注入的完整流程

01 Web网站基本架构

SQL注入

什么是SQL注入?

SQL的历史

- Structured Query Language
- System R
- ANSI SQL92

e.g.

```
SELECT * FROM tbl_name WHERE a= xxx AND ...
UPDATE tbl_name set col_1 = 'xx' where ...
INSERT INTO tbl_name ...
DELETE FROM tbl_name ...
```

SQL的类型

- DQL： Query，select
- DML： Manual，insert update delete
- DDL： Define，create drop alter
- DCL： Control，grant revoke commit rollback
- 函数：字符串函数、数字函数、日期函数
- 运算符：算术运算符、比较运算符、逻辑运算符、位运算符

IPv4地址

192.168.1.110

1100 0000 1010 1000 0000 0001 0110 1110

端口 Port

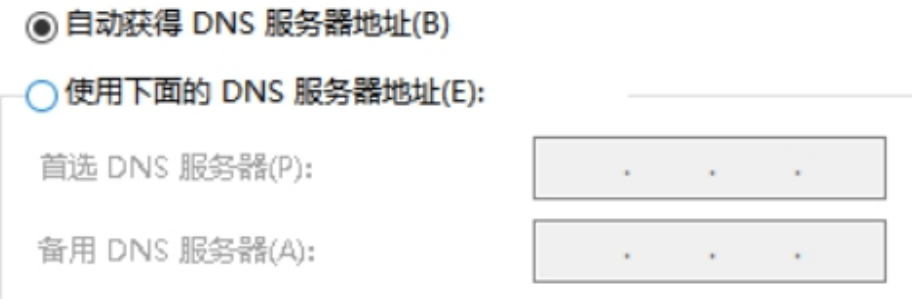
- FTP 21
- SSH 22
- Tomcat 8080
- MySQL 3306
- Redis 6379

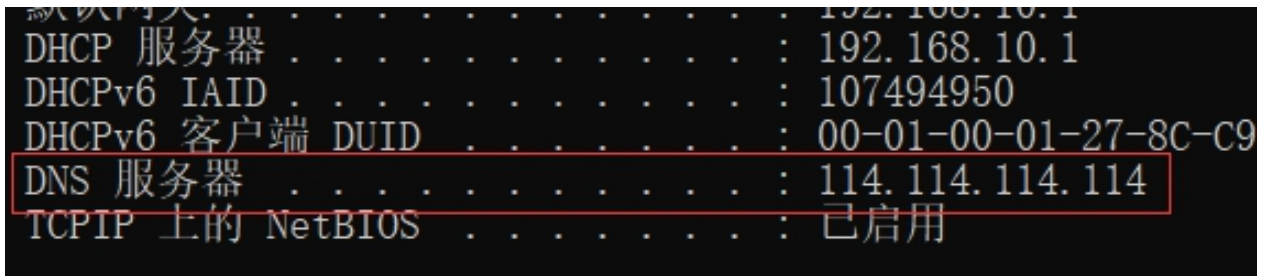
域名(Domain Name)

- 顶级域名 .com .net .org ...
- 国别/地区域名 .cn（中国） .us（美国） .jp（日本）...

子域名：
www.baidu.com
tieba.baidu.com
12345.qzone.qq.com

DNS（Domain Name System）





IP和域名关系

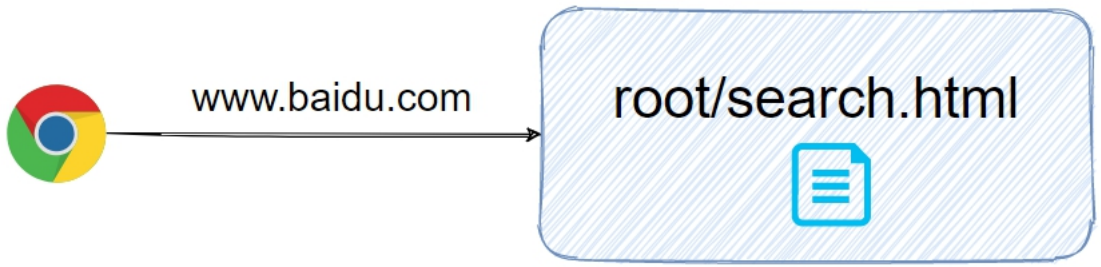
1、一个域名可以对应到多个IP吗？怎么实现？

2、多个域名可以对应到一个IP吗？怎么实现？

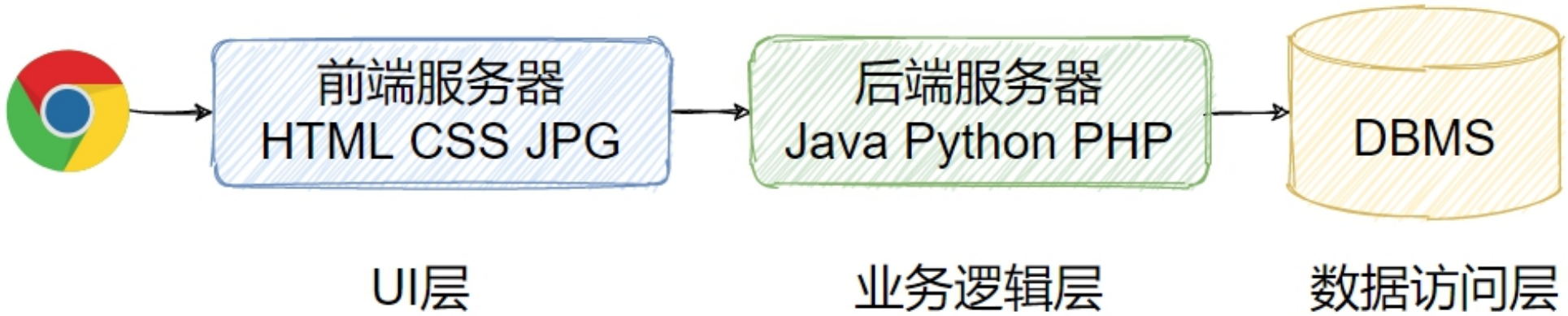
端口和文件

www.baidu.com

www.baidu.com/root/search.html

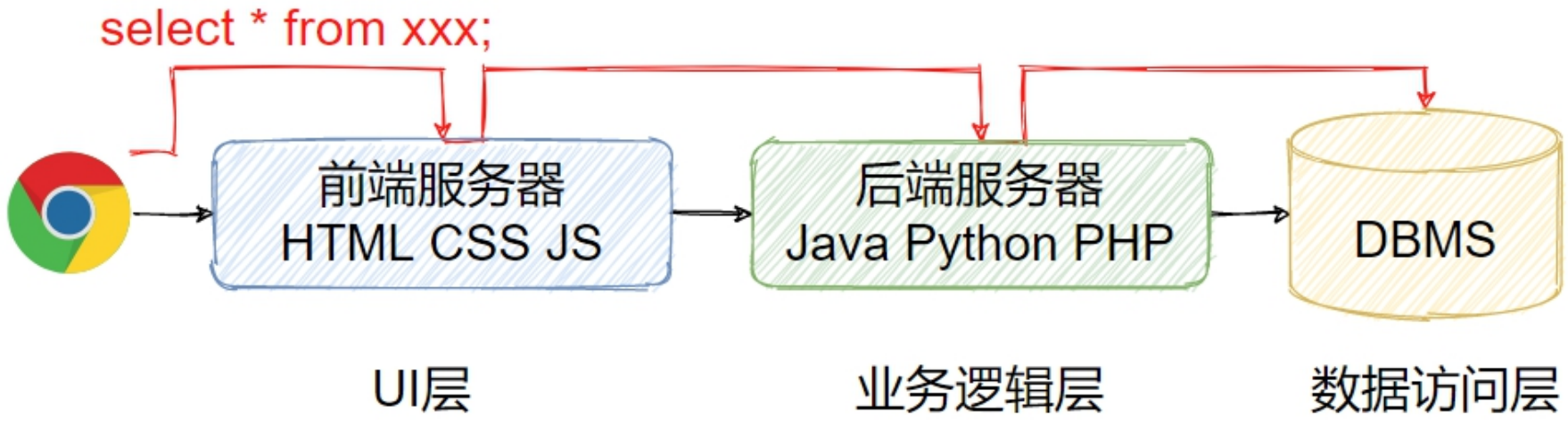


项目架构


前端服务器
HTML CSS JPG
后端服务器
Java Python PHP
DBMS
UI层
业务逻辑层
数据访问层

02 如何构建可以执行的语句

SQL注入的发生


select * from xxx;
前端服务器
HTML CSS JS
后端服务器
Java Python PHP
DBMS
UI层
业务逻辑层
数据访问层

如何获取数据库信息

- show命令
- select +函数
- 系统库

MySQL系统库（5.7）

系统库	描述
information_schema	mysql服务器所有数据库的信息
mysql	基存储数据库的用户、权限设置、关键字等
performance_schema	主要用于收集数据库服务器性能参数
sys	数据来自performance_schema

参数会如何处理?

```
user=admin&password=123456

"select * from test where user = " + user
    +  " and password = " + password
```

怎么传入SQL?

- 如何结束一个SQL?
- 如何忽略后续语句?
- 什么语句可以包含两个以上的select?

03 SQL注入的完整流程

SQL注入的完整流程

- 判断是否可以注入
- 获得数据库名
- 获得表名
- 获取列名
- 获得数据

Thank you for watching

无涯老师