

# **Day05 基础入门-资产架构 &端口&应用&CDN&WAF& 站库分离&负载均衡**

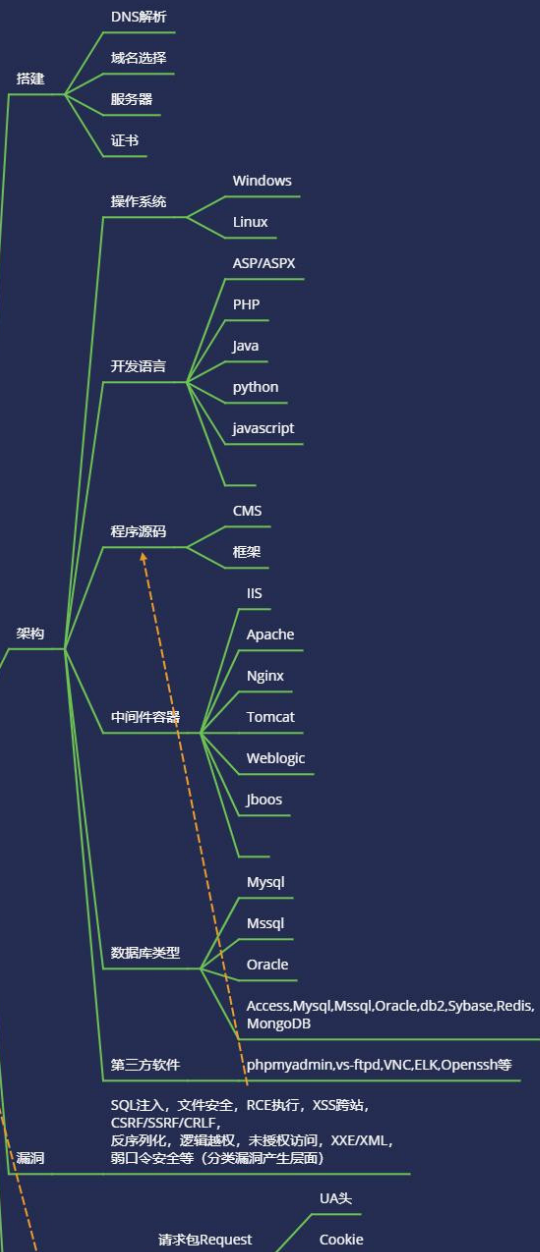
## 专业名词

前后端, POC/EXP, Payload/Shellcode, 后门/Webshell, 木马/病毒, 反弹, 回显, 跳板, 黑白盒测试, 暴力破解, 社会工程学, 拖库, ATT&CK等

## 操作系统



## Web应用



# 1.知识点

- 资产架构-端口&目录&插件接口&多站点&多应用
- 番外安全-域名&服务器本身&服务厂商&管理人员
- 考虑阻碍-站库分离&CDN&WAF&负载均衡&主机防护

## 基础入门-小迪安全

### 1.1 资产架构



- 1 WEB 单个源码指向安全
- 2 WEB 多个目录源码安全
- 3 WEB 多个端口源码安全
- 4 服务器架设多个站点安全
- 5 架设第三方插件接口安全
- 6 服务器架设多个应用安全

### 1.2 番外安全

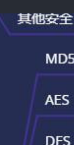


- 1 基于域名解析安全
- 2 基于服务器本身安全
- 3 基于服务商信息安全
- 4 基于管理个人的安全

### 1.3 考虑阻碍




- 1 阻碍-站库分离
- 2 阻碍-CDN 加速服务
- 3 阻碍-负载均衡服务
- 4 阻碍-WAF 应用防火墙
- 5 阻碍-主机防护防火墙



## 2.案例演示

### 2.1 资产架构-BT 搭建&多站点&多插件&多应用等

多站点:

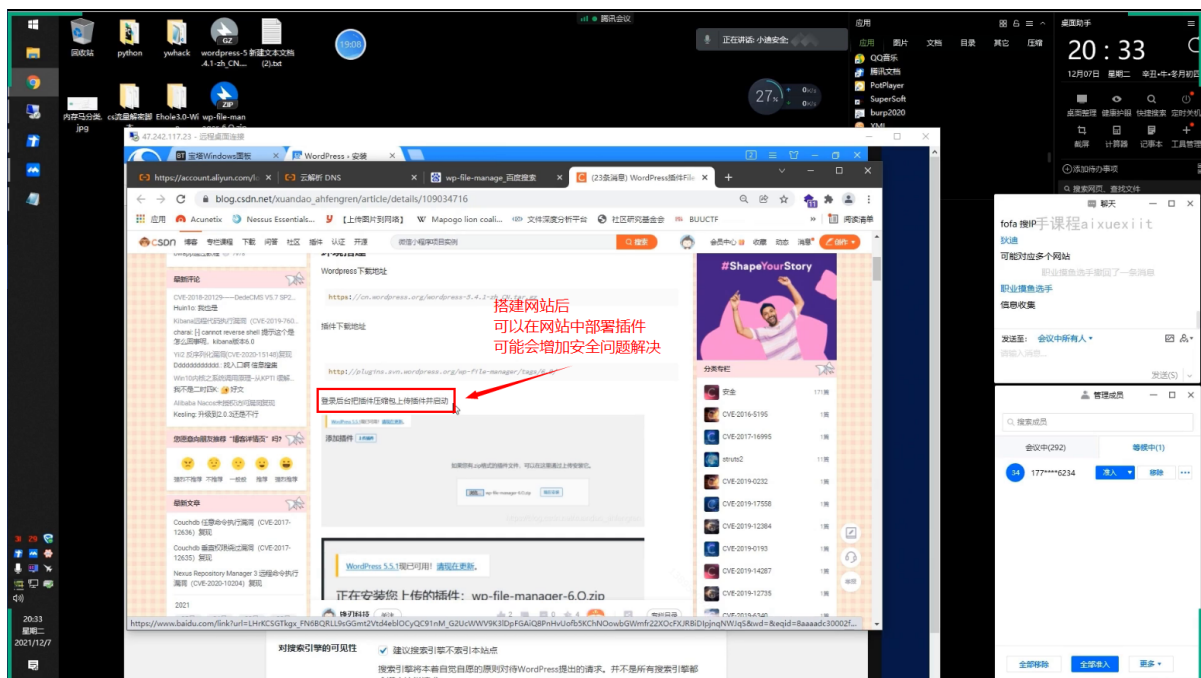


```

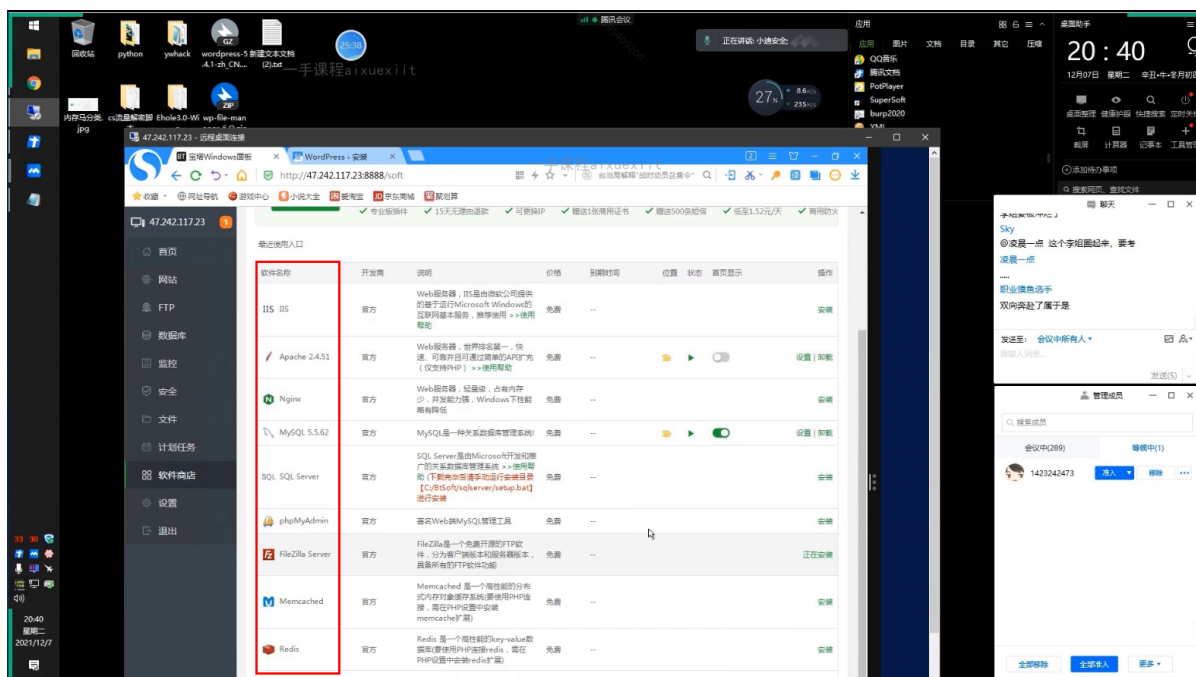
graph LR
    A[资产架构] --- B[资产]
    A --- C[系统]
    A --- D[番外]
    B --- B1[站点插件]
    B --- B2[服务应用]
    B --- B3[本身安全]
    C --- C1[中过漏洞]
    D --- D1[服务器厂商]
    D --- D2[管理人员安全]
    D --- D3[阻碍-站库分离]
  
```

- 1 edu.xiaodi8.com 47.242.117.23
- 2 bbs.xiaodi8.com 47.242.117.23
- 3 如果测试目标为bbs.xiaodi8.com, 可以对edu.xiaodi8.com 做测试

多插件.



多应用:



## 2.2 番外安全-Aliyun&域名解析&云服务器&个人等

### 域名解析：



- 1 查询域名购买厂商，获取用户个人信息，尝试爆破，修改域名信息

### 云服务器：



- 1 远程攻击者获得远程登录服务器的账号密码，直接登录云服务器

### 个人：



- 1 跟目标用户处朋友，向他发送恶意程序，使目标上当，拿下服务器

## 2.3 考虑阻碍-站库分离&部署防护&负载均衡&CDN 等

### 站库分离：



- 1 站点和数据库分离

### 部署防护：



## 1 部署安全产品

### 负载均衡：



- 1 负载均衡（**Load Balance**）其意思就是分摊到多个操作单元上进行执行，例如**web**服务器、**FTP**服务器、企业关键应用服务器和其它关键任务服务器等，从而共同完成工作任务。

### CDN：



- 1 **CDN**系统能够实时地根据网络流量和各节点的连接、负载状况以及到用户的距离和响应时间等综合信息将用户的请求重新导向离用户最近的服务节点上。其目的是使用户可就近取得所需内容，解决**Internet**网络拥挤的状况，提高用户访问网站的响应速度。