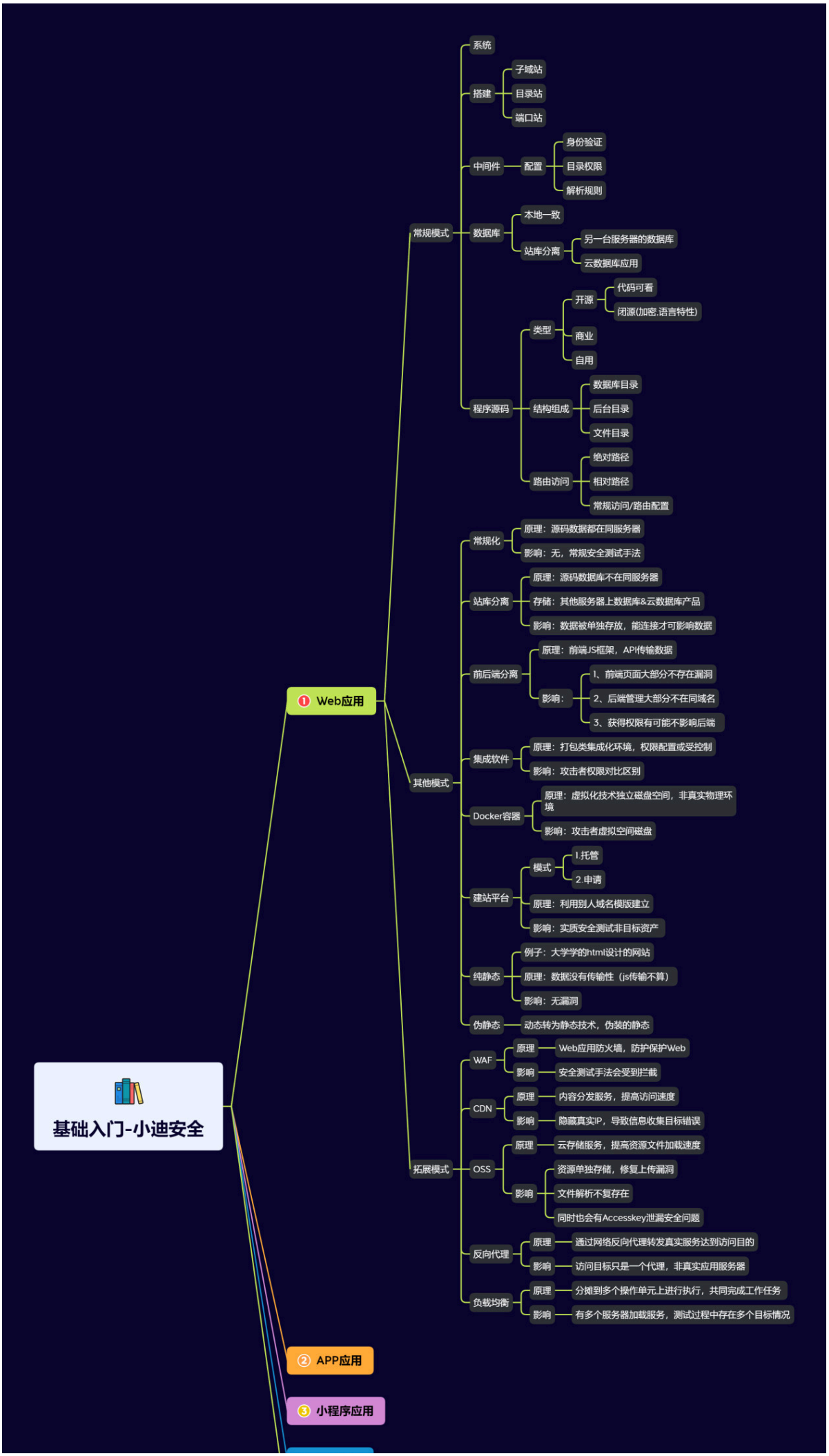
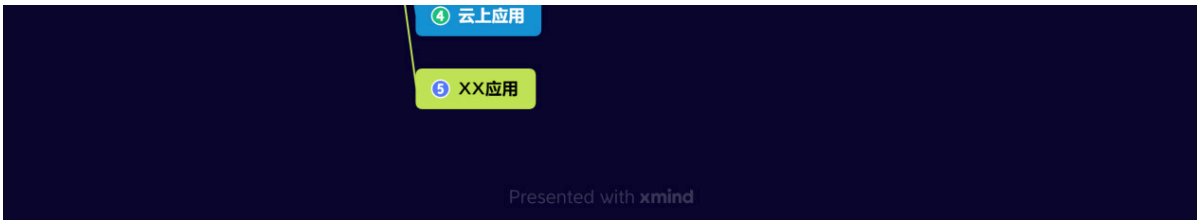
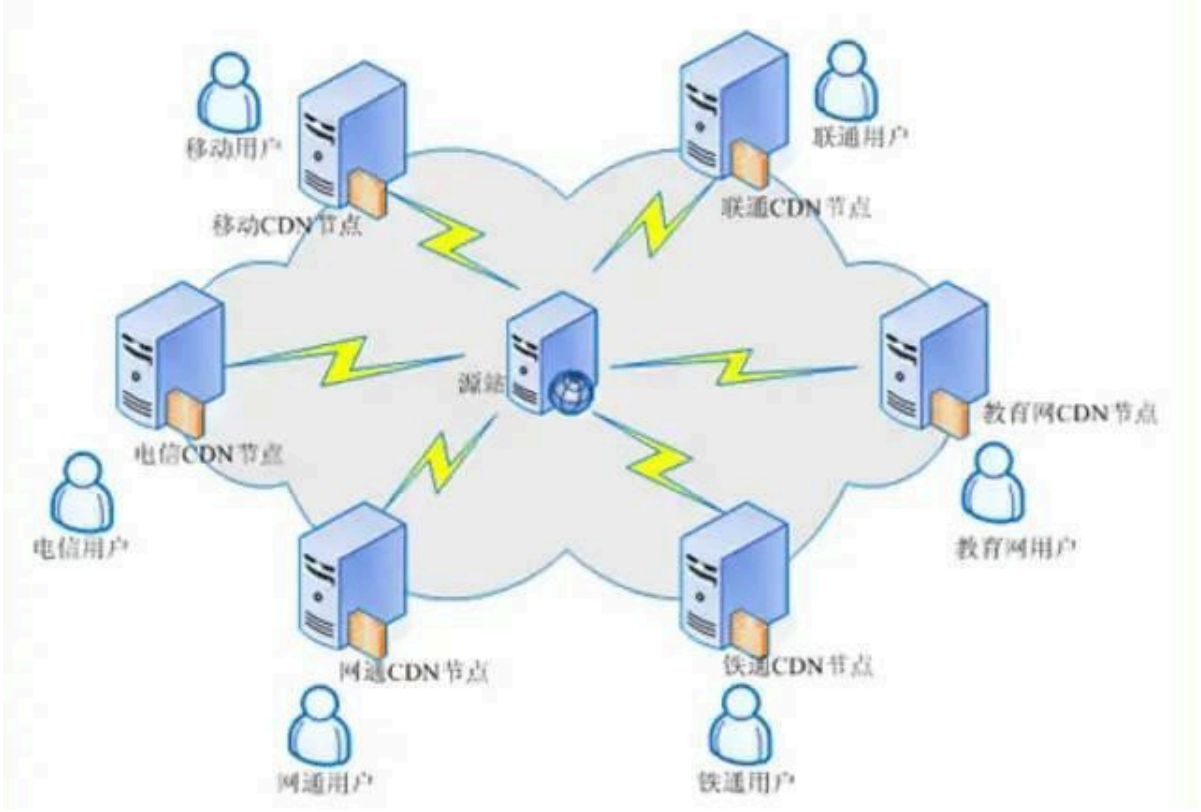
Day03　基础入门-Web架构&OSS存储&负载均衡&CDN加速&反向代理&WAF防护

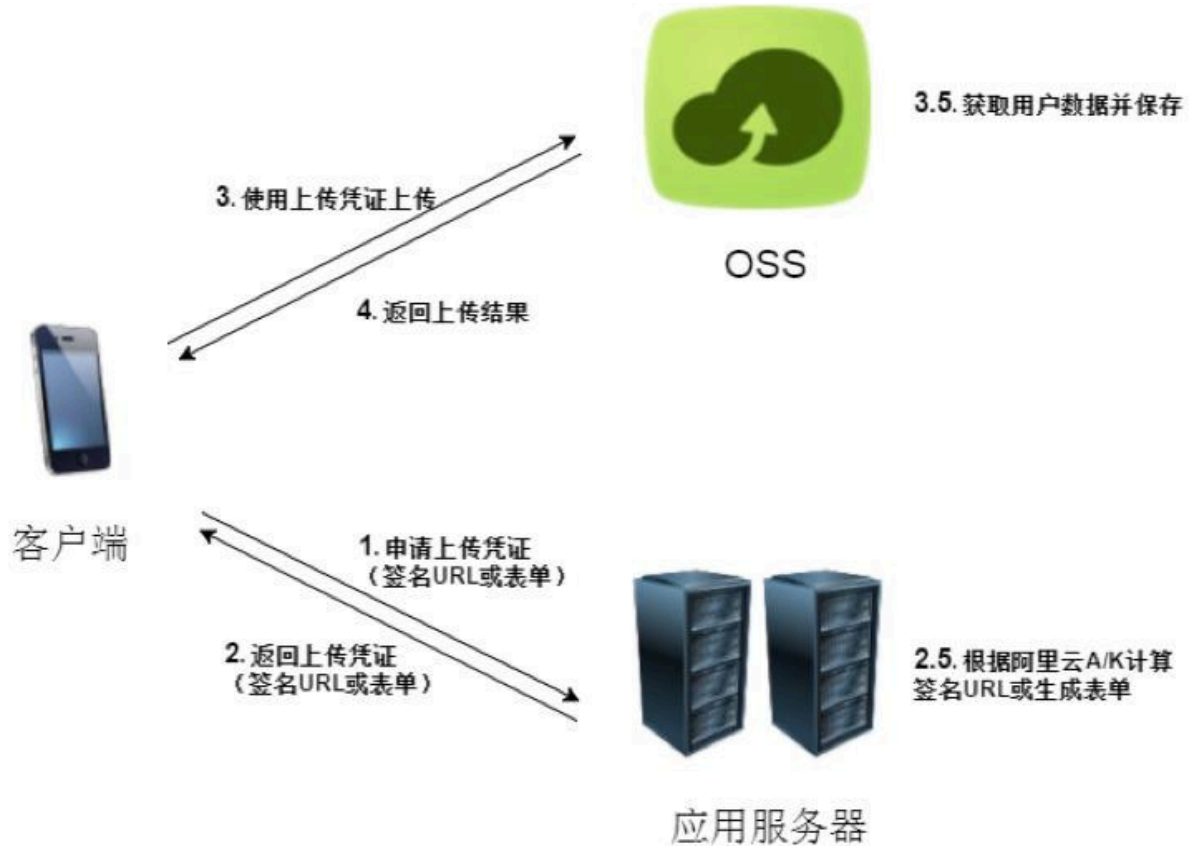

基础入门-小迪安全
① Web应用
常规模式
系统
搭建
子域站
目录站
端口站
中间件
配置
身份验证
目录权限
解析规则
数据库
本地一致
站库分离
另一台服务器的数据库
云数据库应用
程序源码
类型
开源
代码可看
闭源(加密,语言特性)
商业
自用
结构组成
数据库目录
后台目录
文件目录
路由访问
绝对路径
相对路径
常规访问/路由配置
其他模式
常规化
原理：源码数据都在同服务器
影响：无，常规安全测试手法
站库分离
原理：源码数据库不在同服务器
存储：其他服务器上数据库&云数据库产品
影响：数据被单独存放，能连接才可影响数据
前后端分离
原理：前端JS框架，API传输数据
影响：
1、前端页面大部分不存在漏洞
2、后端管理大部分不在同域名
3、获得权限有可能不影响后端
集成软件
原理：打包类集成化环境，权限配置或受控制
影响：攻击者权限对比区别
Docker容器
原理：虚拟化技术独立磁盘空间，非真实物理环境
影响：攻击者虚拟空间磁盘
建站平台
模式
1.托管
2.申请
原理：利用别人域名模版建立
影响：实质安全测试非目标资产
纯静态
例子：大学学的html设计的网站
原理：数据没有传输性（js传输不算）
影响：无漏洞
伪静态
动态转为静态技术，伪装的静态
拓展模式
WAF
原理
Web应用防火墙，防护保护Web
影响
安全测试手法会受到拦截
CDN
原理
内容分发服务，提高访问速度
影响
隐藏真实IP，导致信息收集目标错误
OSS
原理
云存储服务，提高资源文件加载速度
影响
资源单独存储，修复上传漏洞
文件解析不复存在
同时也会有Accesskey泄漏安全问题
反向代理
原理
通过网络反向代理转发真实服务达到访问目的
影响
访问目标只是一个代理，非真实应用服务器
负载均衡
原理
分摊到多个操作单元上进行执行，共同完成工作任务
影响
有多个服务器加载服务，测试过程中存在多个目标情况
② APP应用
③ 小程序应用

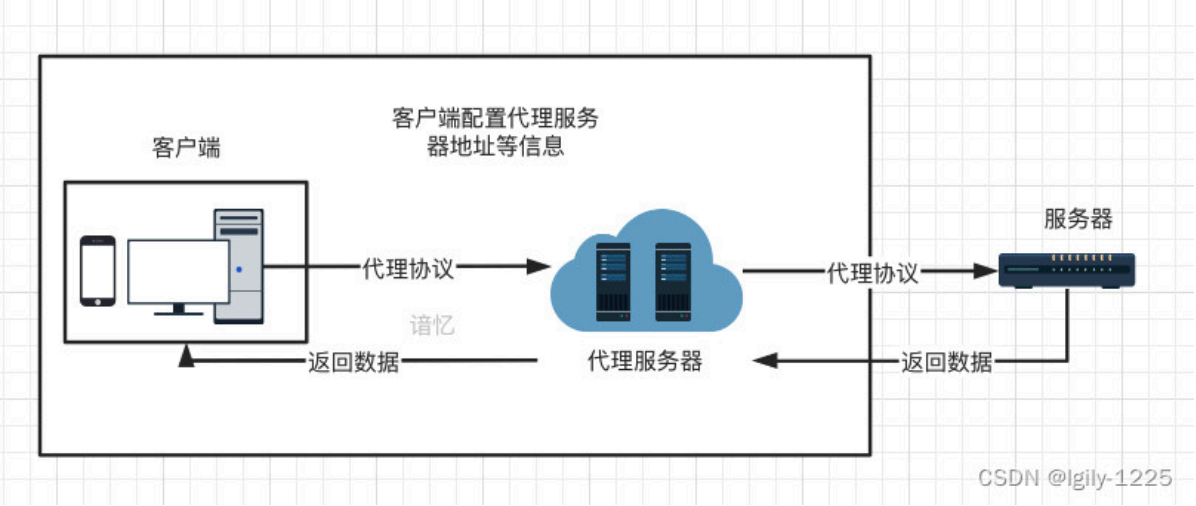


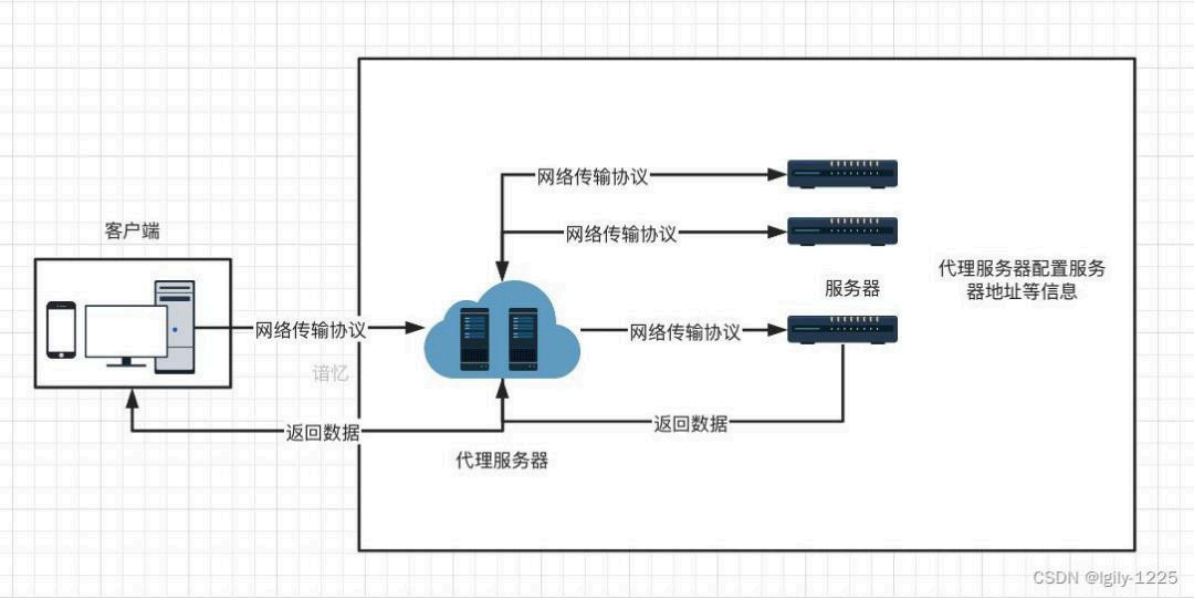
1.知识点

- 1、Web常规-系统&中间件&数据库&源码等
- 2、Web其他-前后端&软件&Docker&分配站等
- 3、Web拓展-CDN&WAF&OSS&反向&负载均衡等




3.5. 获取用户数据并保存
OSS
3. 使用上传凭证上传
4. 返回上传结果
客户端
1. 申请上传凭证
（签名URL或表单）
2. 返回上传凭证
（签名URL或表单）
2.5. 根据阿里云A/K计算
签名URL或生成表单
应用服务器


客户端
客户端配置代理服务
器地址等信息
服务器
代理协议
代理协议
返回数据
代理服务器
返回数据
CSDN @lgily-1225

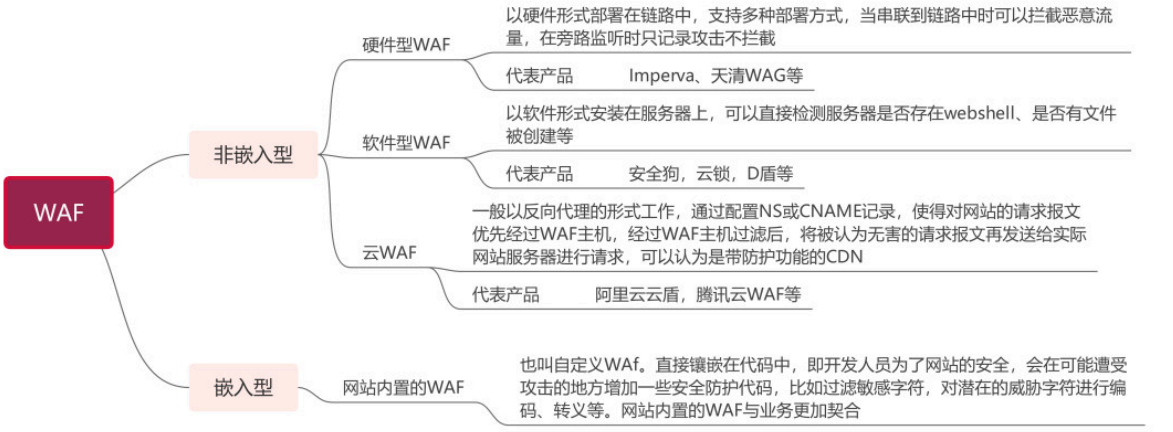

网络传输协议
网络传输协议
客户端
服务器
代理服务器配置服务
器地址等信息
网络传输协议
网络传输协议
返回数据
返回数据
代理服务器
CSDN @lgily-1225

2.演示案例

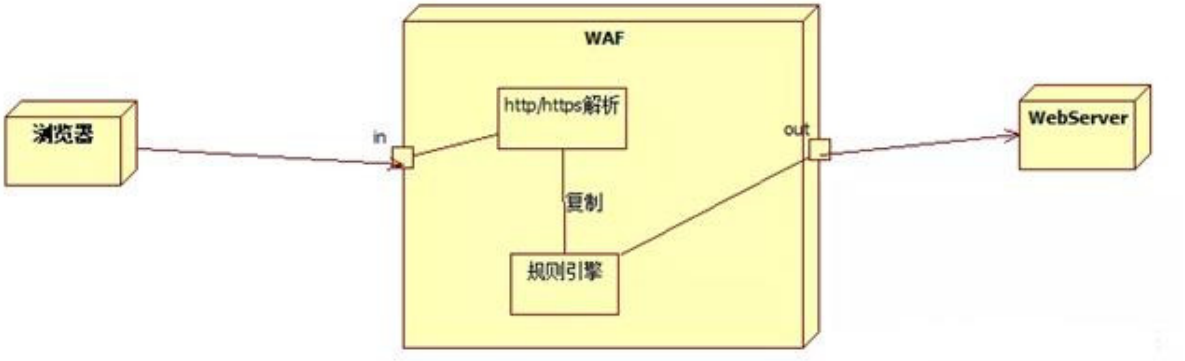
2.1 架构1-WAF防护-拦截安全攻击

```
1  原理：Web应用防火墙，旨在提供保护
2  影响：常规Web安全测试手段会受到拦截
3  演示：免费D盾防护软件
4  Windows2012 + IIS +D盾
```

2.1.1 WAF分类

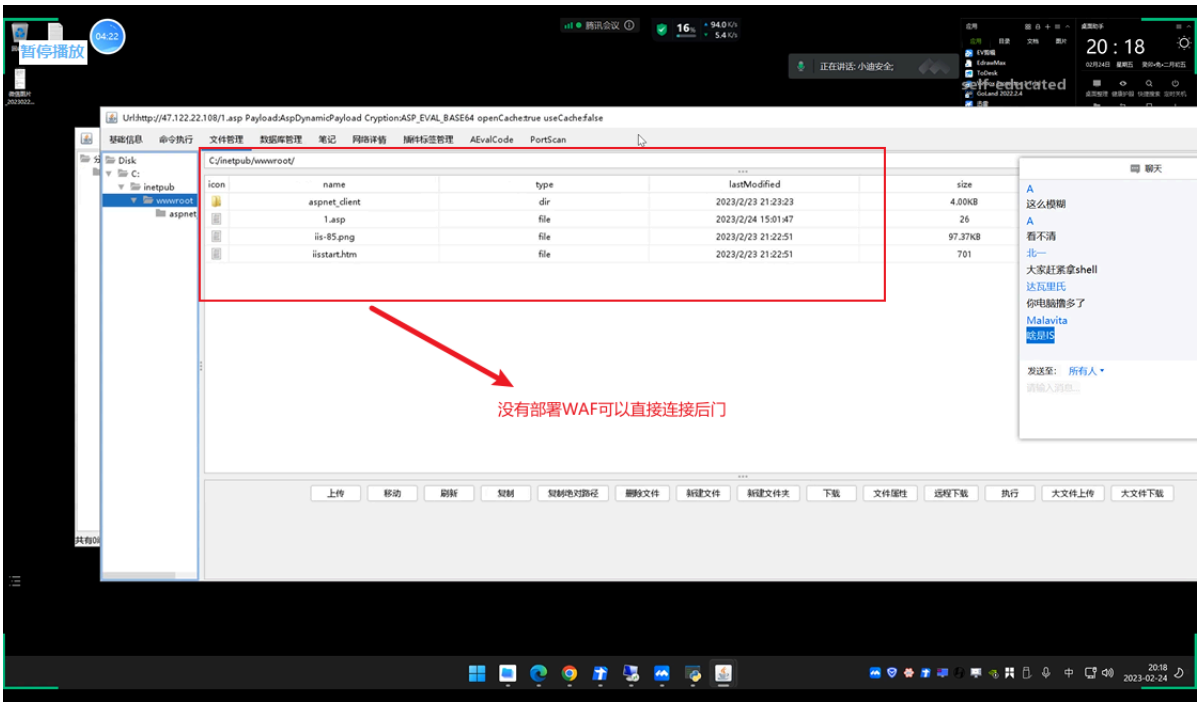


2.1.2 工作原理

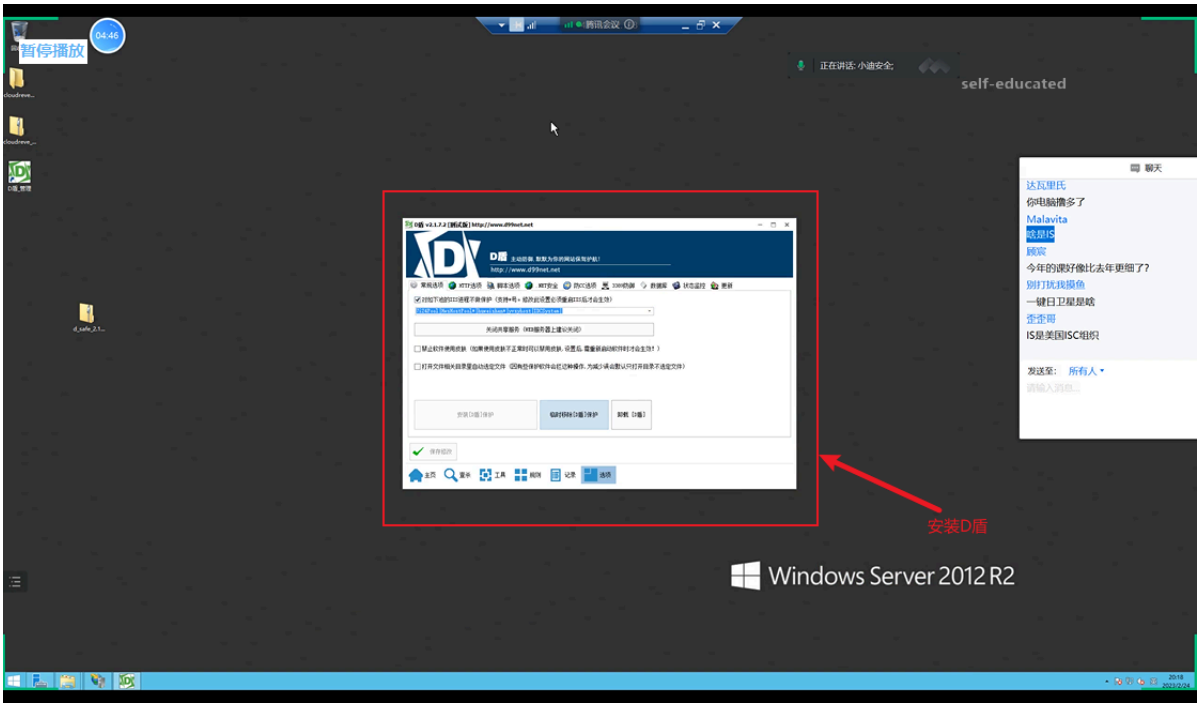


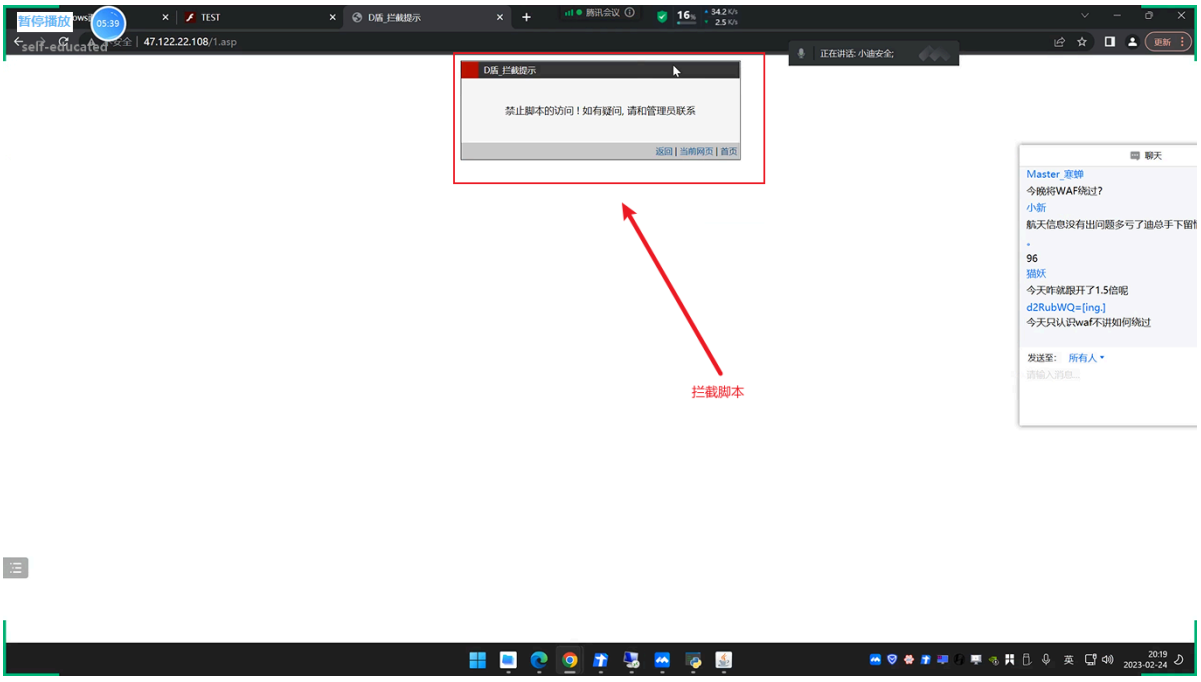
2.1.3 示例

（1）如果部署了WAF，后门可以正常连接：



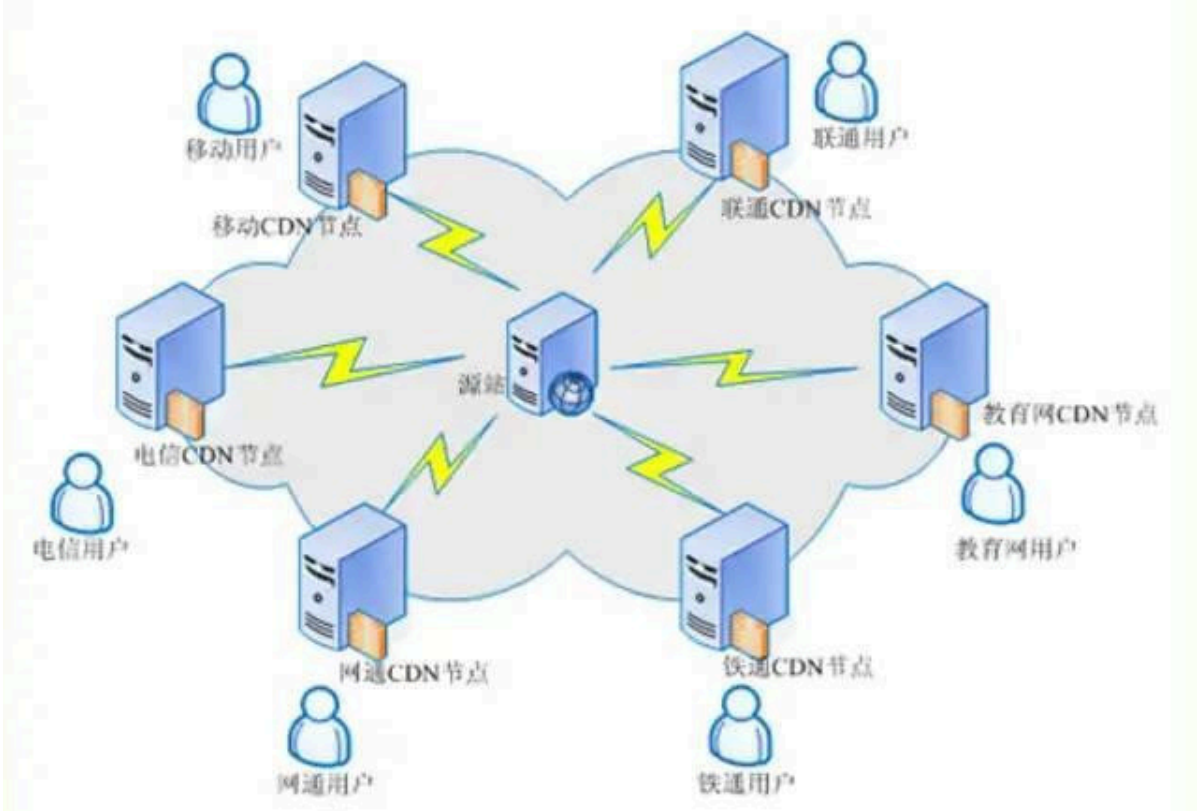
（2）如果开启了WAF防护，则无法连接后门：



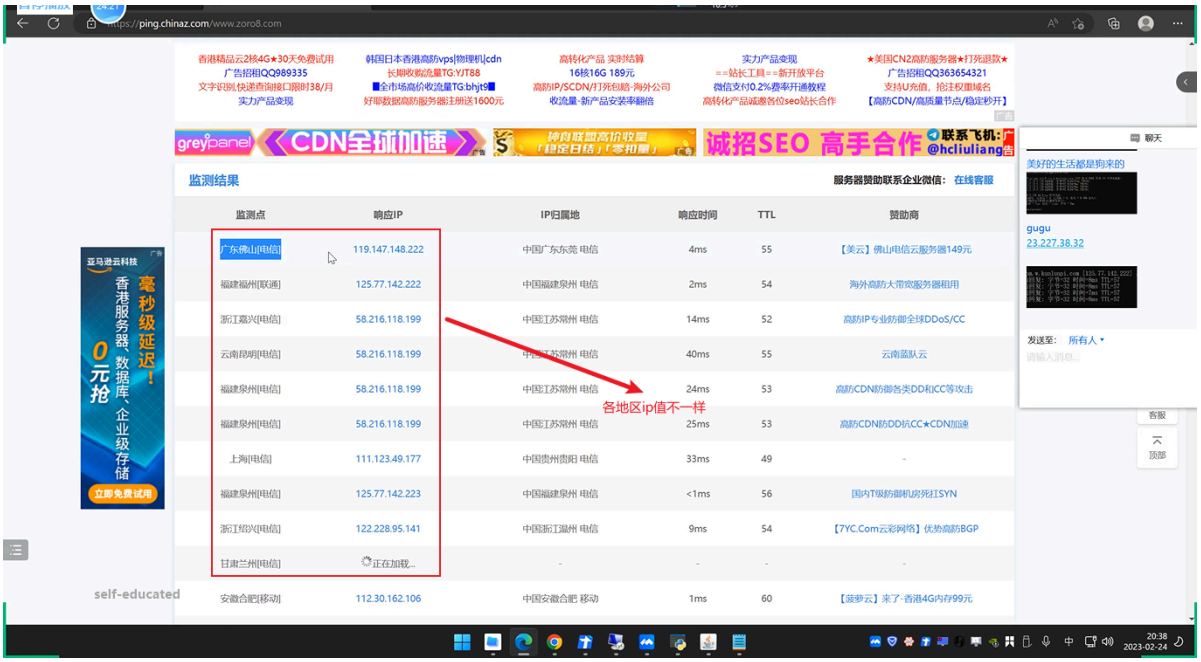


2.2 架构2-CDN节点-隐藏真实源IP

1 原理：内容分发服务，旨在提高访问速度
2 影响：隐藏真实源IP，导致对目标测试错误
3 演示：阿里云备案域名全局CDN加速服务
4 Windows2012 + BT宝塔面板 + CDN服务



（1）如果开了CDN，则ping域名会展示如下信息：



2.3 架构3-OSS存储-独立资源文件

```
原理：云存储服务，旨在提高访问速度
影响：上传的文件或解析的文件均来自于OSS资源，无法解析，单独存储
演示：https://cloudreve.org/
Windows2012 + cloudreve + 阿里云OSS
https://github.com/cloudreve/Cloudreve/releases/tag/3.7.1
1、启动应用
2、登录管理
3、配置存储信息
4、更改用户组存储属性

阿里云OSS:
开OSS
2、新建Bucket
3、配置Bucket属性
4、配置Access访问

原理：
```

```
为什么要使用第三方存储？
1）静态文件会占用大量带宽
2）加载速度
3）存储空间
影响：
上传的文件或解析的文件均来自于OSS资源，无法解析，单独存储
1、修复上传安全
2、文件解析不一样
3、但Accesskey隐患
```

2.4 架构4-反向代理-内网应用转发

```
正代理：为客户端服务,客户端主动建立代理访问目标（不代理不可达）
反向代理：为服务端服务,服务端主动转发数据给可访问地址（不主动不可达）
原理：通过网络反向代理转发真实服务达到访问目的
影响：访问目标只是一个代理，非真实应用服务器
注意：正向代理和反向代理都是解决访问不可达的问题，但由于反向代理中多出一个可以重定向解析的功能操作，导致反代理出的站点指向和真实应用毫无关系！
演示：Nginx反向代理配置
Windows2012 + BT宝塔面板 + Nginx
```

2.5 架构5-负载均衡-多台机器服务

```
原理：分摊到多个操作单元上进行执行，共同完成工作任务
影响：有多个服务器加载服务，测试过程中存在多个目标情况
演示：Nginx负载均衡配置
Windows2012 + BT宝塔面板 + Nginx
#定义负载设置
upstream fzjh{
    server 47.94.236.117:80 weight=2;
    server 47.122.22.195:80 weight=1;
}
#定义访问路径 访问策略
location / {
    proxy_pass http://fzjh/;
}
```