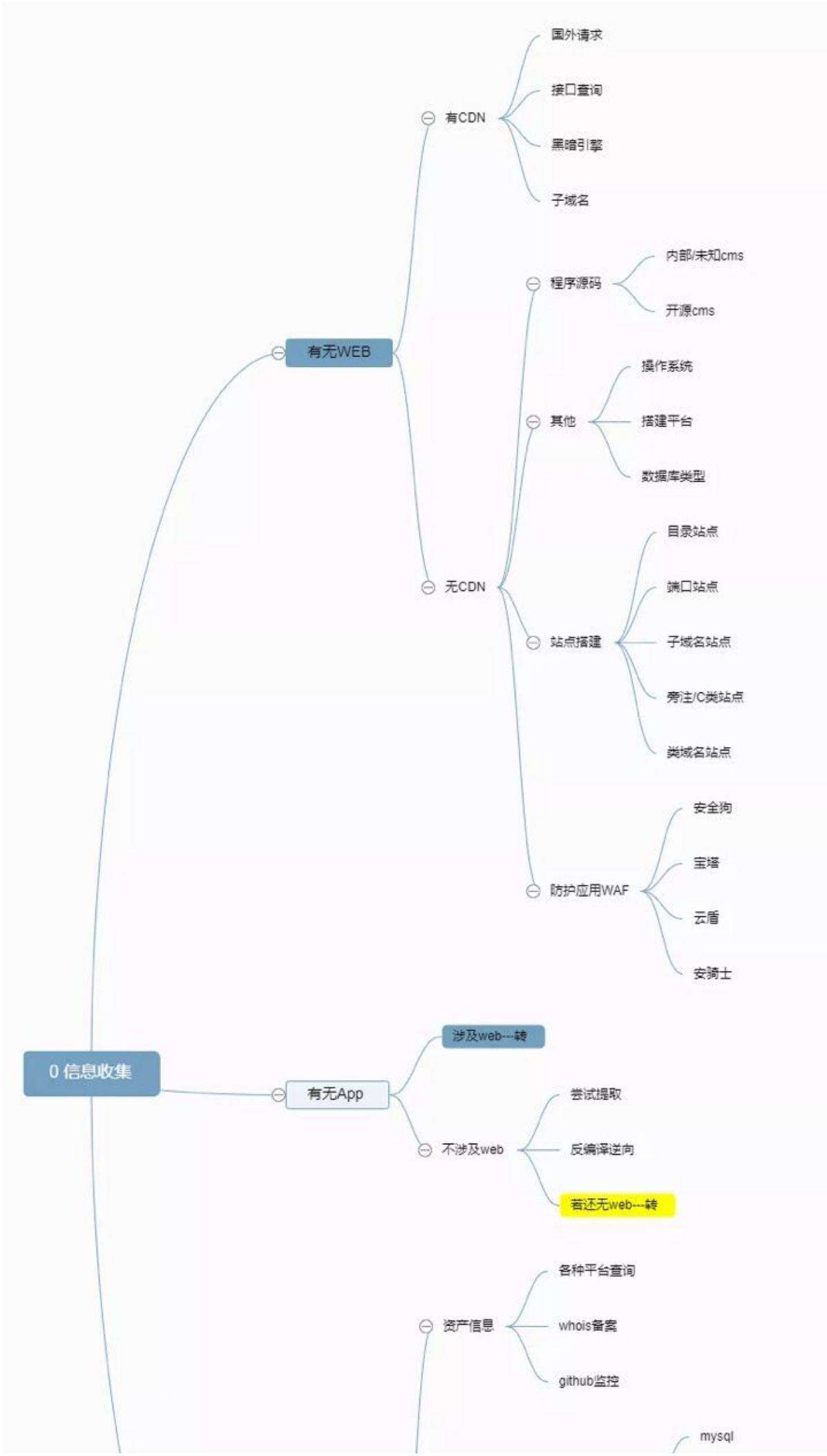
Day08　信息收集–架构,搭建,WAF等


0 信息收集
有无WEB
有CDN
国外请求
接口查询
黑暗引擎
子域名
无CDN
程序源码
内部/未知cms
开源cms
其他
操作系统
搭建平台
数据库类型
站点搭建
目录站点
端口站点
子域名站点
旁注/C类站点
类域名站点
防护应用WAF
安全狗
宝塔
云盾
安骑士
有无App
涉及web---转
不涉及web
尝试提取
反编译逆向
若还无web---转
资产信息
各种平台查询
whois备案
github监控
mysql

源码获取技术 架构信息获取

8.1 站点搭建分析

- 搭建习惯-目录型站点
- 搭建习惯-端口类站点
- 搭建习惯-子域名站点
- 搭建习惯-类似域名站点
- 搭建习惯-旁注, c段站点

旁注：同服务器不同站点（192.168.1.100[www.a.com;www.b.com]）

C段：同网段不同服务器不同站点(192.168.1.100[www.a.com;www.b.com])(192.168.1.101[www.c.com;www.d.com])

- 搭建习惯-搭建软件特征站点

8.2 WAF防护分析

- 什么是WAF应用?

Web应用防护系统（也称为：网站应用级入侵防御系统。英文：Web Application Firewall，简称：WAF）。

- 如何快速识别WAF?

1.手工识别或者使用WAFW00F。

2.查看数据包的指纹头(X-Powered-By:WAF)

- 识别WAF对于安全测试的意义?

如果不识别WAF，当网站安装WAF时，黑客攻击行为会被WAF识别，从而屏蔽本机IP，造成无法访问该网站的现象。

资源

```
https://www.shodan.io/
https://www.webscan.cc/
https://github.com/EnableSecurity/wafw00f
```