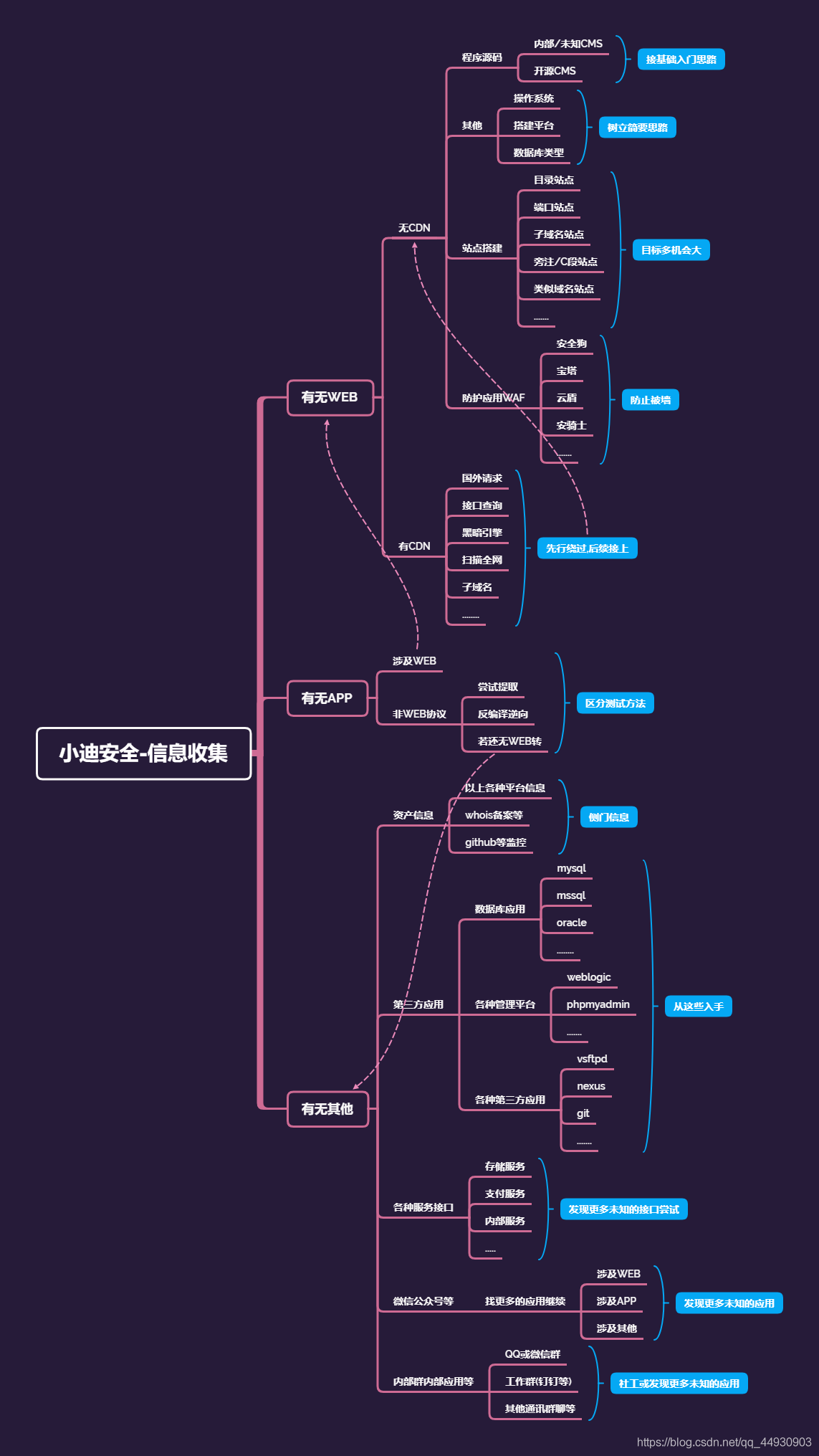
# 08 信息收集-架构,搭建,WAF等



CMS识别技术

源码获取技术

架构信息获取

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（前提条件：多个站点服务器）：同服务器不同站点，一个域名不行就尝试服务器的另一个域名）； 有一些旁注查询的第三方网站，直接搜，如 https://www.webscan.cc/；

C段：同网段不同服务器不同站点，例如一个服务器的某站点IP为192.168.1.101，那么就可以从这入手，拿到同一网段另一个服务器（站点IP假设为192.168.1.103）的权限。

搭建习惯-搭建软件特征站点

回想一下自己搭的各个网站，前后端的特征

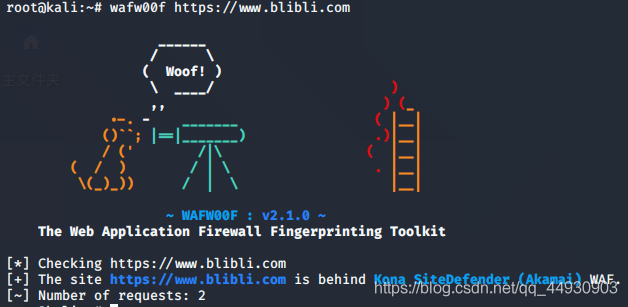
WAF防护分析

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）。利用国际上公认的一种说法：Web应用防火墙是通过执行一系列针对HTTP/HTTPS的安全策略来专门为Web应用提供保护的一款产品。

如何快速识别WAF？

https://github.com/EnableSecurity/wafw00f



如果使用kali系统，就不用安装，直接使用，如：在这里插入图片描述

还有一种办法：F12查看X-Powered-By: WAF参数

识别WAF对于安全测试的意义？

 知道站点用waf之后，可以判断产商尝试绕过，而且知道站点存在waf之后，用扫描工具的时候留意点，容易被禁ip。

演示案例：

IMG_256

如果有bbs这个目录，有多少个就可判断其有多少个目标（网站）。比如上面的sti.blcu.deu.cn和sti.blcu.deu.cn/bbs/是两个完全不同的网站。

✧ web.0516jz-8080-端口类站点分析

端口设置，不同端口对应不同应用。比如ssh默认端口是22

✧ goodlift-www.bbs-子域名两套CMS

例：





bbs.goodlift.net是用Discuz搭建的，而www.goodlift.net是用destoon b2b搭建的。

✧ jmlsd-cn.com.net等-各种常用域名后缀

很多网站都会有子域名，找到不同后缀的子域名，从这入手一般效果很不错。

✧ weipan-qqyewu-查询靶场同服务器站点

✧ weipan-phpstudy-查询特定软件中间件等

shodan搜索下面这条信息，接着查询出来站点的phpmyadmin目录，有些人搭建网站可能phpmystudy的密码没有改

Apache/2.4.23(Win32)OpenSSL/1.0.2jPHP/5.4.45

1

✧ wafw00f-shodan(X-Powered-By: WAF)

F12查看X-Powered-By: WAF参数

涉及资源：

https://www.shodan.io/

https://www.webscan.cc/

https://github.com/EnableSecurity/wafw00f