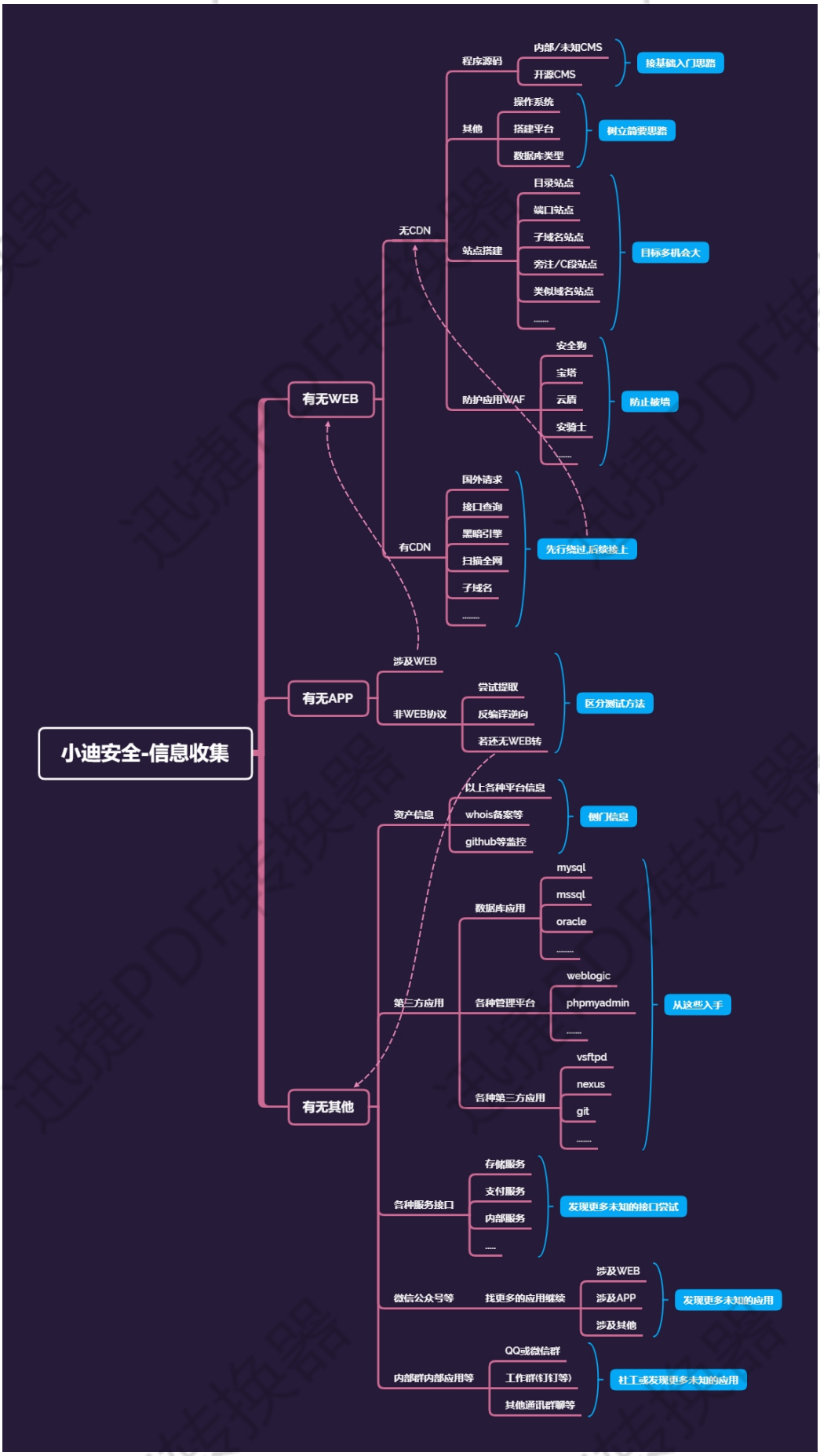
信息收集-架构,搭建,WAF 等

在安全测试中，信息收集是非常重要的一个环节，此环节的信息将影响到后续的成功几率，掌握信息的多少将决定发现漏洞机会大小，换言之决定着是否能完成目标的测试任务。也可以很直接的跟大家说：渗透测试的思路就是从信息收集这里开始，你与大牛的差距也是从这里开始的！


小迪安全-信息收集
有无WEB
有无APP
有无其他
无CDN
有CDN
站点搭建
目录站点
端口站点
子域名站点
旁注/C段站点
类似域名站点
.....
目标多机会大
防护应用WAF
安全狗
宝塔
云盾
安骑士
.....
防止被墙
程序源码
内部/未知CMS
开源CMS
接基础入门思路
其他
操作系统
搭建平台
数据库类型
树立简要思路
国外请求
接口查询
黑暗引擎
扫描全网
子域名
.....
先行绕过,后续接上
涉及WEB
非WEB协议
尝试提取
反编译逆向
若还无WEB转
区分测试方法
资产信息
以上各种平台信息
whois备案等
github等监控
侧门信息
第三方应用
数据库应用
mysql
mssql
oracle
.....
各种管理平台
weblogic
phpmyadmin
.....
各种第三方应用
vsftpd
nexus
git
.....
从这些入手
各种服务接口
存储服务
支付服务
内部服务
.....
发现更多未知的接口尝试
微信公众号等
找更多的应用继续
涉及WEB
涉及APP
涉及其他
发现更多未知的应用
内部群内部应用等
QQ或微信群
工作群(钉钉等)
其他通讯群聊等
社工或发现更多未知的应用

#申明：涉及的网络真实目标只做技术分析，不做非法操作！

#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
搭建习惯-搭建软件特征站点

#WAF 防护分析
什么是 WAF 应用?
如何快速识别 WAF?
识别 WAF 对于安全测试的意义?

演示案例:

- ✧ sti.blcu-bbs-目录型站点分析
- ✧ web.0516jz-8080-端口类站点分析
- ✧ goodlift-www.bbs-子域名两套 CMS
- ✧ jmlsd-cn.com.net 等-各种常用域名后缀
- ✧ weipan-qqyewu-查询靶场同服务器站点
- ✧ weipan-phpstudy-查询特定软件中间件等
- ✧ wafw00f-shodan(X-Powered-By: WAF)-147.92.47.120

涉及资源:

https://www.shodan.io/

https://www.webscan.cc/

https://github.com/EnableSecurity/wafw00f
