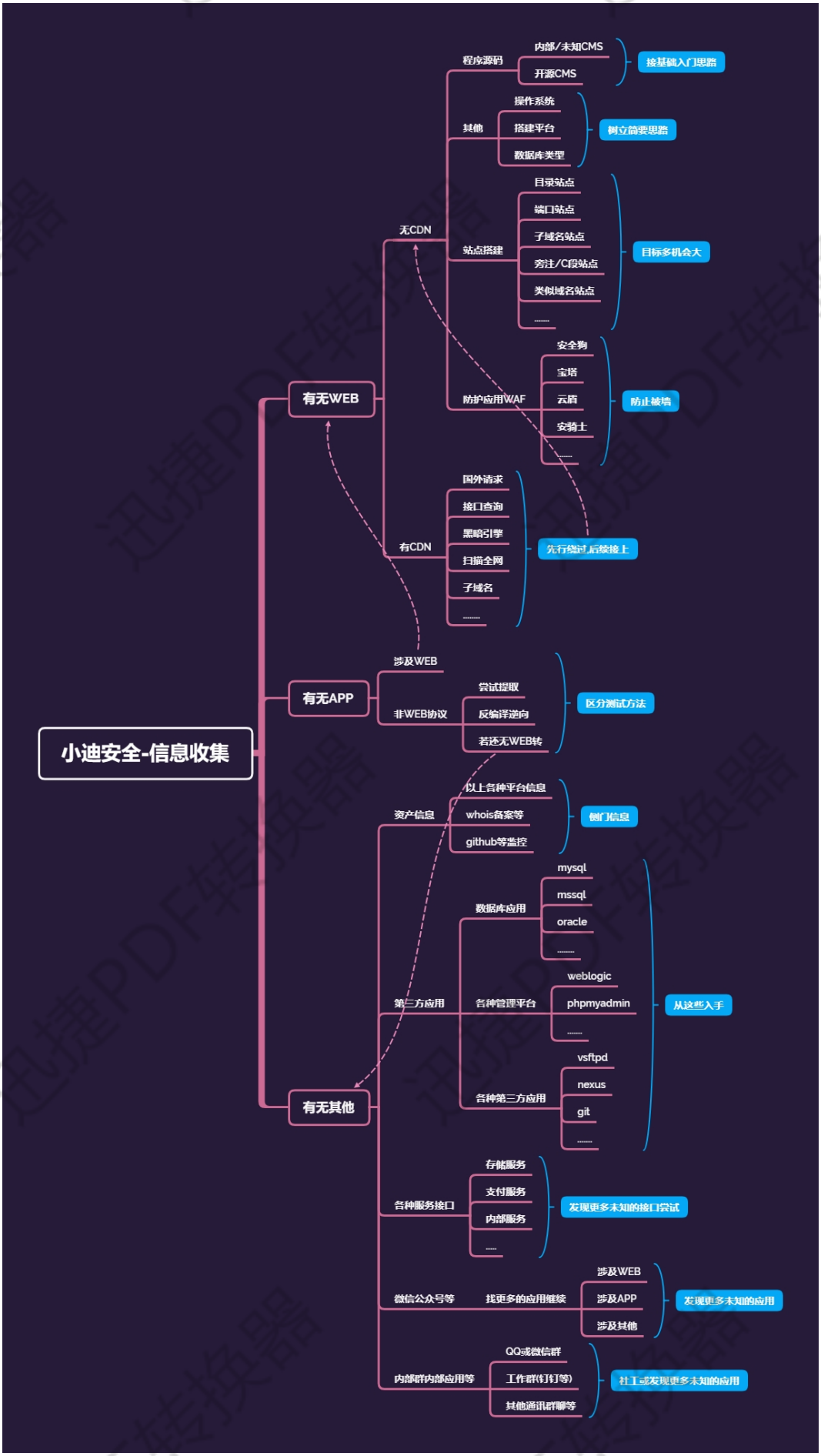
信息收集-APP 及其他资产等

在安全测试中，若 WEB 无法取得进展或无 WEB 的情况下，我们需要借助 APP 或其他资产在进行信息收集，从而开展后续渗透，那么其中的信息收集就尤为重要，这里我们用案例讲解试试如何！


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
防护应用WAF
程序源码
其他
内部/未知CMS
开源CMS
操作系统
搭建平台
数据库类型
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
.....
安全狗
宝塔
云盾
安骑士
.....
国外请求
接口查询
黑暗引擎
扫描全网
子域名
.....
接基础入门思路
树立简要思路
目标多机会大
防止被墙
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
各种管理平台
各种第三方应用
mysql
mssql
oracle
.....
weblogic
phpmyadmin
.....
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

#APP 提取一键反编译提取
#APP 抓数据包进行工具配合
#各种第三方应用相关探针技术
#各种服务接口信息相关探针技术

演示案例：

APP 提取及抓包及后续配合

某 APK 一键提取反编译
利用 burp 历史抓更多 URL

某 IP 无 WEB 框架下的第三方测试

各种端口一顿乱扫-思路
各种接口一顿乱扫-思路
接口部分一顿测试-思路

群友 WEB 授权测试下的服务测试

不管三七二十一就是扫
吃吃瓜，抽抽烟，各种干

涉及资源：

https://fofa.so/

http://tool.chinaz.com

https://www.shodan.io/

https://www.zoomeye.org/

https://nmap.org/download.html
