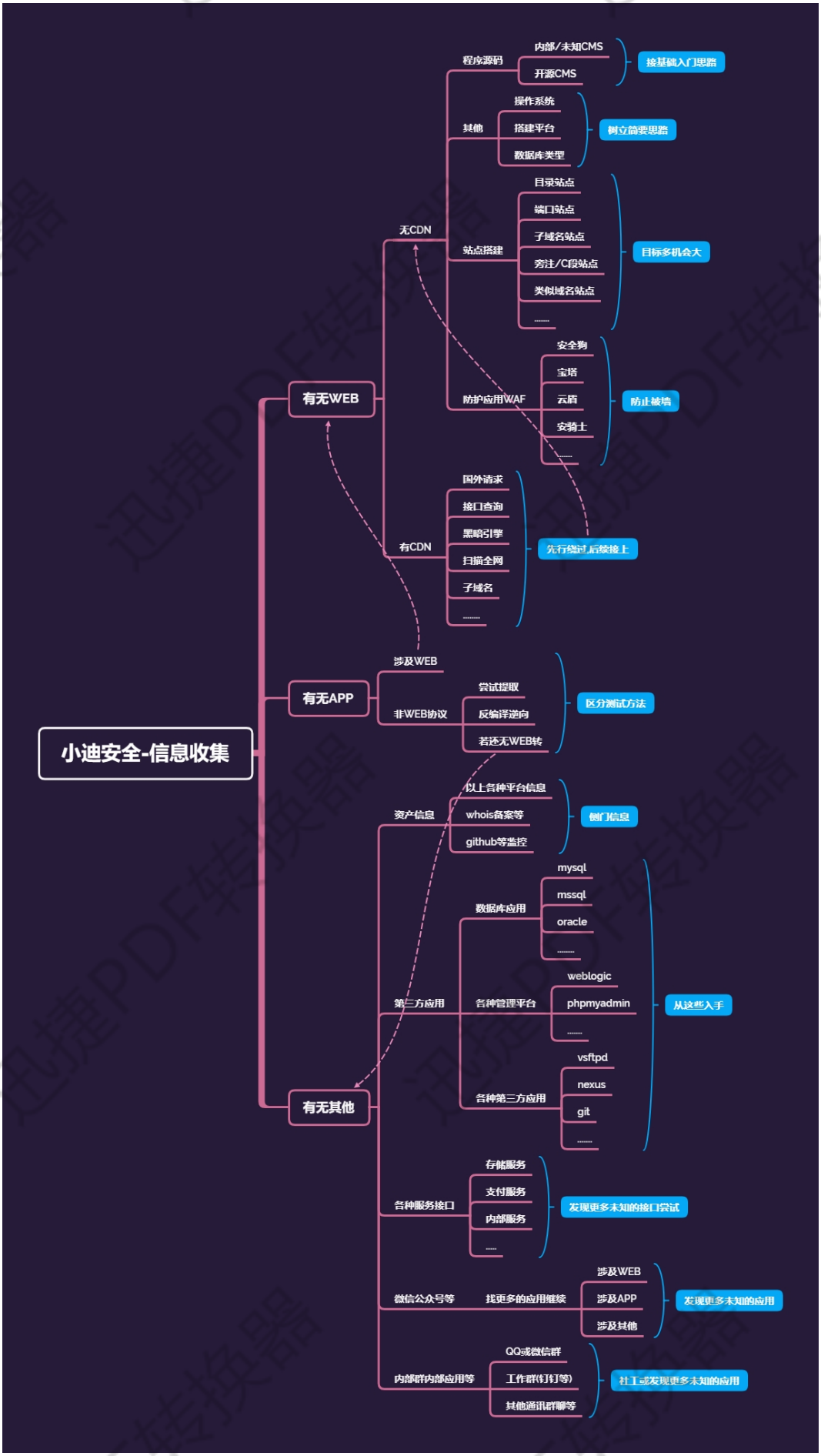
# 信息收集-资产监控拓展


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

#Github 监控
便于收集整理最新 exp 或 poc
便于发现相关测试目标的资产

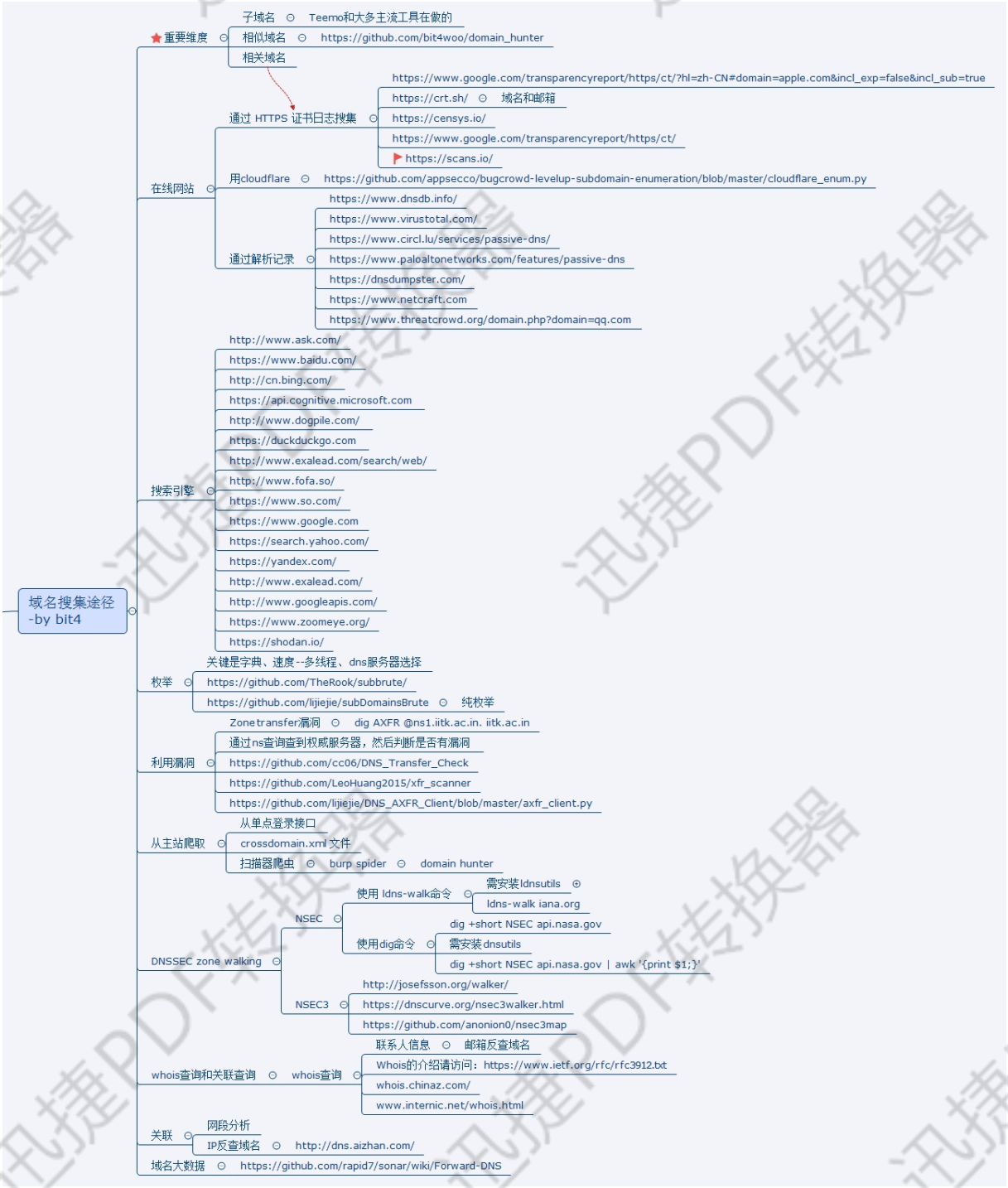
#各种子域名查询
#DNS,备案,证书
#全球节点请求 cdn
枚举爆破或解析子域名对应
便于发现管理员相关的注册信息

#黑暗引擎相关搜索
fofa，shodan，zoomeye

#微信公众号接口获取

#内部群内部应用内部接口

---




## 演示案例：

## ✧ 监控最新的 EXP 发布及其他

# Title: wechat push CVE-2020
# Date: 2020-5-9
# Exploit Author: weixiao9188
# Version: 4.0
# Tested on: Linux,windows

```
# cd /root/sh/git/ && nohup python3 /root/sh/git/git.py &
# coding:UTF-8
import requests
import json
import time
import os
import pandas as pd
time_sleep = 60 #每隔 20 秒爬取一次
while(True):
headers1 = {
"User-Agent": "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.25 Safari/537.36 Core/1.70.3741.400 QQBrowser/10.5.3863.400"}
#判断文件是否存在
datas = []
response1=None
response2=None
if os.path.exists("olddata.csv"):
#如果文件存在则每次爬取 10 个
df = pd.read_csv("olddata.csv", header=None)
datas = df.where(df.notnull(),None).values.tolist()#将提取出来的数据中的 nan 转化为 None
requests.packages.urllib3.disable_warnings()
response1 = requests.get(url="https://api.github.com/search/repositories?q=CVE-2020&sort=updated&per_page=10",headers=headers1,verify=False)
response2 = requests.get(url="https://api.github.com/search/repositories?q=RCE&ssort=updated&per_page=10",headers=headers1,verify=False)

else:
#不存在爬取全部
datas = []
requests.packages.urllib3.disable_warnings()
response1 = requests.get(url="https://api.github.com/search/repositories?q=CVE-2020&sort=updated&order=desc",headers=headers1,verify=False)
response2 = requests.get(url="https://api.github.com/search/repositories?q=RCE&ssort=updated&order=desc",headers=headers1,verify=False)

data1 = json.loads(response1.text)
data2 = json.loads(response2.text)
for j in [data1["items"],data2["items"]]:
for i in j:
s = {"name":i['name'],"html":i['html_url'],"description":i['description']}
s1 =[i['name'],i['html_url'],i['description']]
if s1 not in datas:
#print(s1)
```