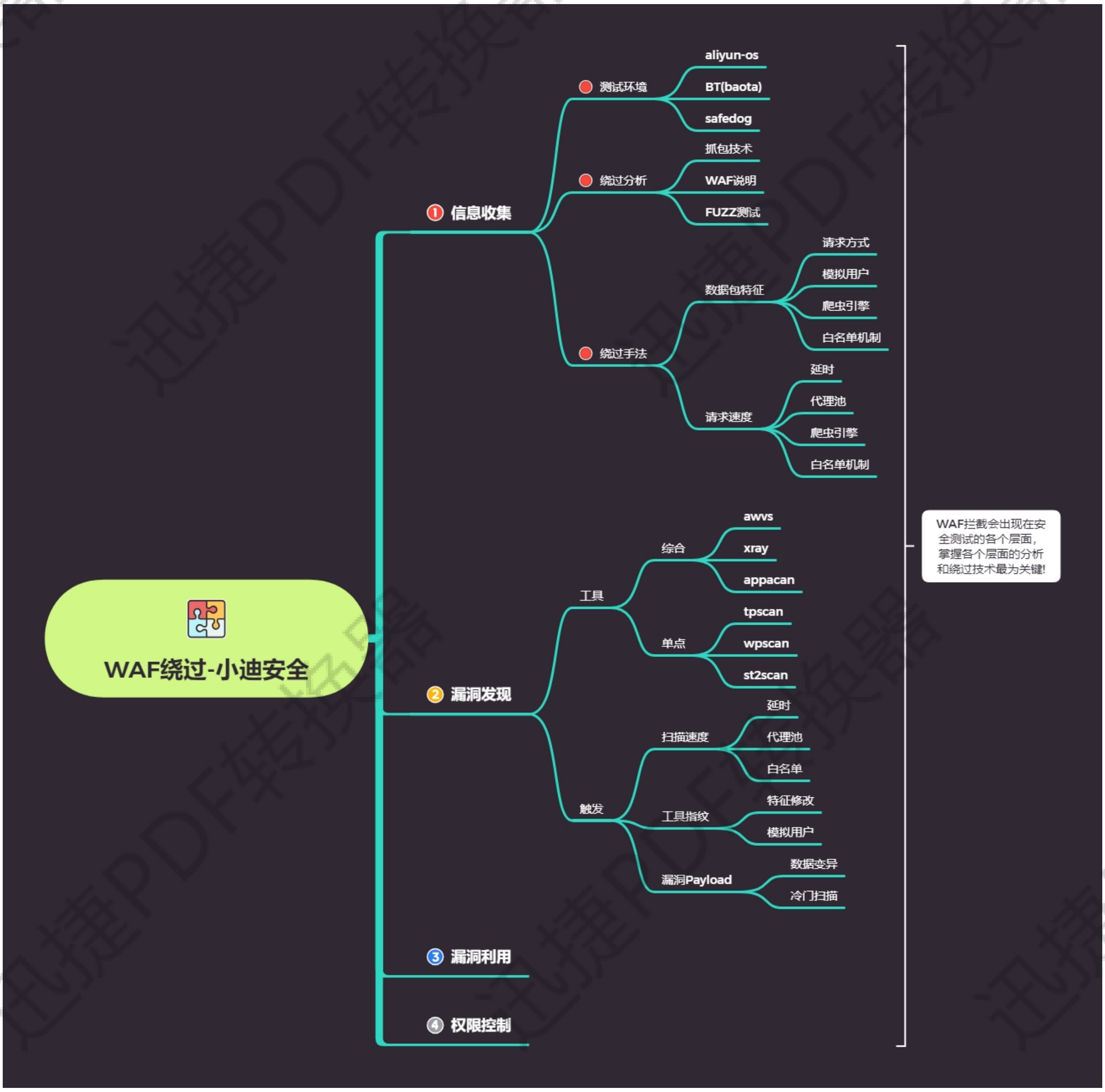
# WAF 绕过-漏洞发现之代理池指纹被动探针



WAF拦截会出现在安全测试的各个层面，掌握各个层面的分析和绕过技术最为关键!

#漏洞发现触发 WAF 点-针对 xray,awvs 等

1.扫描速度-(代理池，延迟，白名单等)

2.工具指纹-(特征修改，伪造模拟真实用户等)

3.漏洞 Payload-(数据变异，数据加密，白名单等)

案例演示：

- 代理池 Proxy_pool 项目搭建及使用解释
- 充钱代理池直接干 safedog+BT+Aliyun 探针
- Safedog-awvs 漏扫注入测试绕过-延时,白名单
- Aliyun_os-awvs 漏扫注入测试绕过-延时白名单
- BT(baota)-awvs+xray 漏扫 Payload 绕过-延时被动
- 充钱代理池直接干 Safedog+BT+AliyunOS 漏洞发现

涉及资源：

http://httpbin.org/ip

https://www.kuaidaili.com/

https://github.com/jhao104/proxy_pool

```
#配合代理池吃瓜扫描
#Author:小迪安全
#QQ471656814
import requests
import time

headers={
'Connection': 'keep-alive',
'Cache-Control': 'max-age=0',
'Upgrade-Insecure-Requests': '1',
'User-Agent': 'Mozilla/5.0 (compatible; Baiduspider-render/2.0; +http://www.baidu.com/search/spider.html)',
'Sec-Fetch-Dest': 'document',
'Accept':
'text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/si
gned-exchange;v=b3;q=0.9',
'Sec-Fetch-Site': 'none',
'Sec-Fetch-Mode': 'navigate',
'Sec-Fetch-User': '?1',
'Accept-Encoding': 'gzip, deflate, br',
'Accept-Language': 'zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7',
'Cookie': 'www.xiaodi8.com',
}

for paths in open('php_b.txt',encoding='utf-8'):
url='http://www.xiaodi8.com/'
paths=paths.replace('\n','')
urls=url+paths
proxy = {
'http': 'tps116.kdlapi.com:15818',
}
try:
code=requests.get(urls,headers=headers,proxies=proxy).status_code
print(urls+'|'+str(code))
if code==200 or code==403:
print(urls+'|'+str(code))
except Exception as err:
print('connecting error')
time.sleep(3)
```