

2、众测挖掘方法

一、前言

二、资产收集

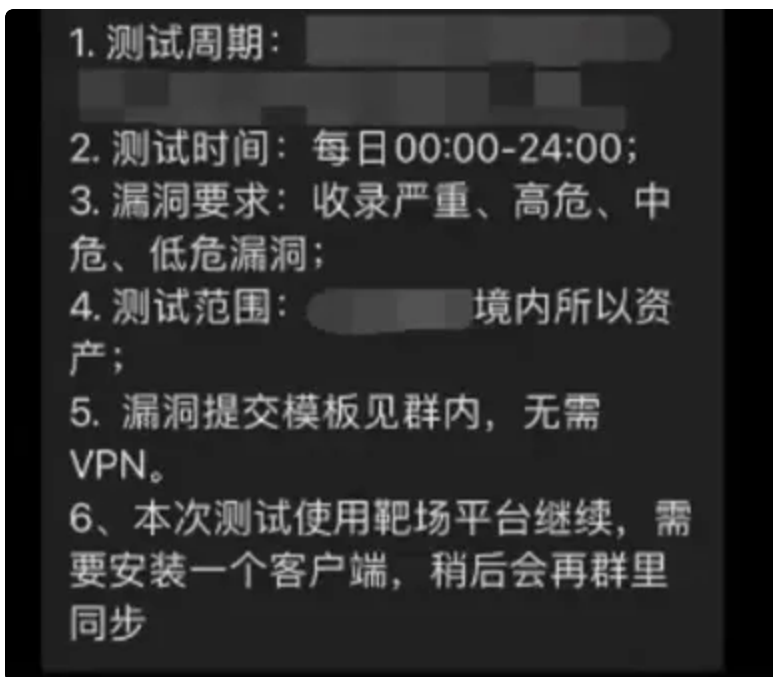
三、众测案例

国内众测得情况大多数都是一些银行和gov，还有一些私人企业，四大银行难度非常的大

一、前言

1、如何去找资产--主要就是对子域名的收集情况

从测试范围里面去排查资产信息



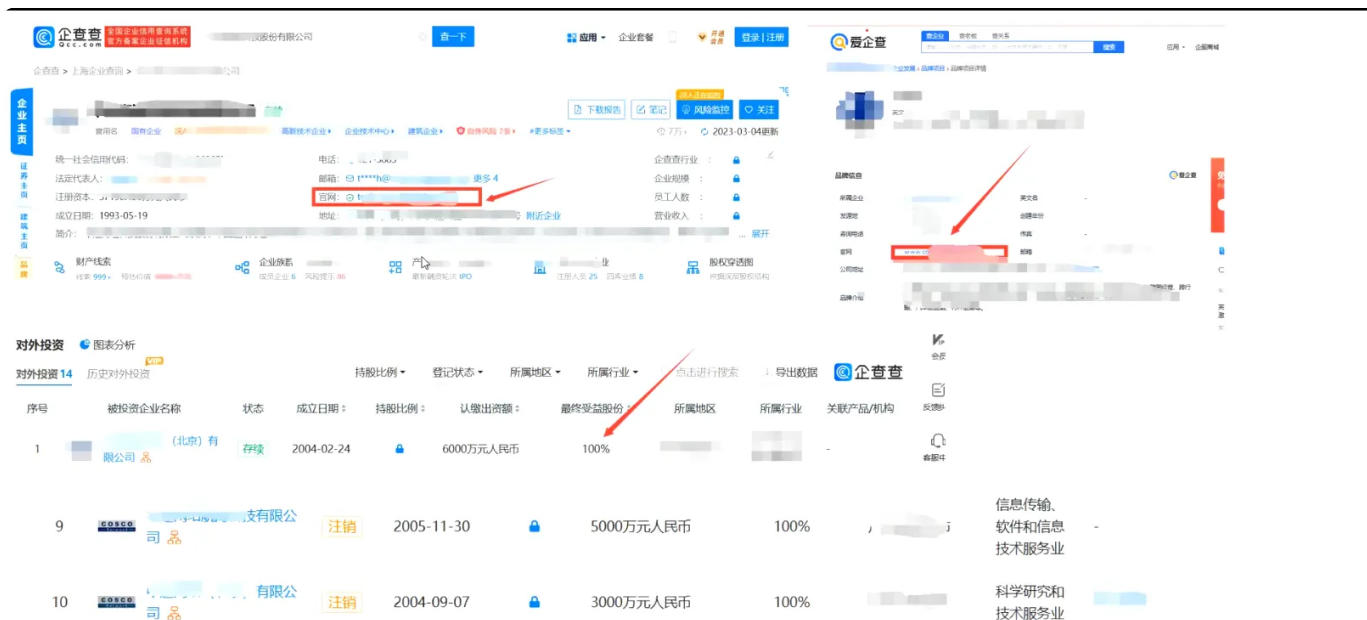
2、一般常见提交的类型

- sql报错泄漏.docx
- swagger未授权.docx
- swagger未授权2.docx
- web、小程序后台所有用户接管.docx
- xss打包.docx
- 存在接口文档泄漏.docx
- 返回包存在信息泄漏.docx
- 工号遍历.docx
- 控制主机.docx
- 控制主机2.docx
- 目录遍历.docx
- 绕过登陆.docx
- 弱口令.docx
- 弱口令1.docx
- 弱口令的副本.docx
- 上传存在跨站请求xss.docx
- 上传文件造成xss.docx
- 刷点赞收藏.docx
- 刷粉丝.docx
- 未授权.docx
- 未授权打包.docx
- 未授权打包的副本.docx
- 未授权访问 1.docx
- 未授权访问.docx
- 未授权访问的副本.docx
- 未授权访问泄漏账号密码造成登陆.docx
- 未授权组合拳.docx
- 优惠券并发.docx
- 越权修改密码.docx
- 账号密码泄漏.docx

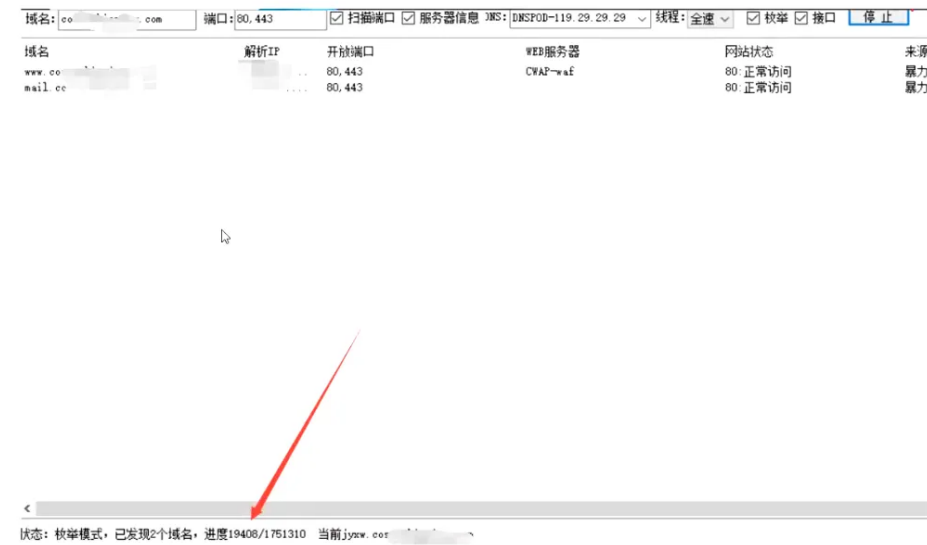
众测的话就是低危-->200 中危-->600 高危-->1800

二、资产收集

通过企查查或者爱企查找信息，因为很多众测项目他只会告诉你某某公司名字，所以就需要找官网是什么，找他的子域名信息,而且百分之百控股公司，都是属于这个公司的全域的资产，都是需要测试的范围内的资产。



1、常规的思路，打web资产，拿着子域名挖掘机去扫描，但会发现很难去挖掘漏洞，发现web没什么东西去挖掘



oneforall
fofa_view
google语法
bbot
挖掘机

1.1、推荐一个工具bbot，它是通过dns解析去找子域名信息的，爆破的子域名多一点

BBOT是一个用 Python 编写的递归模块化OSINT 框架。

它能够在单个命令中执行整个 OSINT 进程，包括子域枚举、端口扫描、网页截图（及其gowitness模块）、漏洞扫描（带有nuclei）等等。

先决条件：

- 必须安装 Python 3.9 或更新版本
- pipx推荐作为替代方案，因为pip它在自己的 Python 环境中安装了 BBOT。

▼ 安装bbot

Bash |

```
1 # 安装更新版本的python
2 sudo apt install python3.9 python3.9-venv
3 # 安装pipx
4 python3.9 -m pip install --user pipx
5 # 为pipx添加路径
6 python3.9 -m pipx ensurepath
7 # 重启
8 reboot
9 # 安装bbot
10 python3.9 -m pipx install bbot
11 # 运行bbot
12 bbot --help
```

▼

Bash |

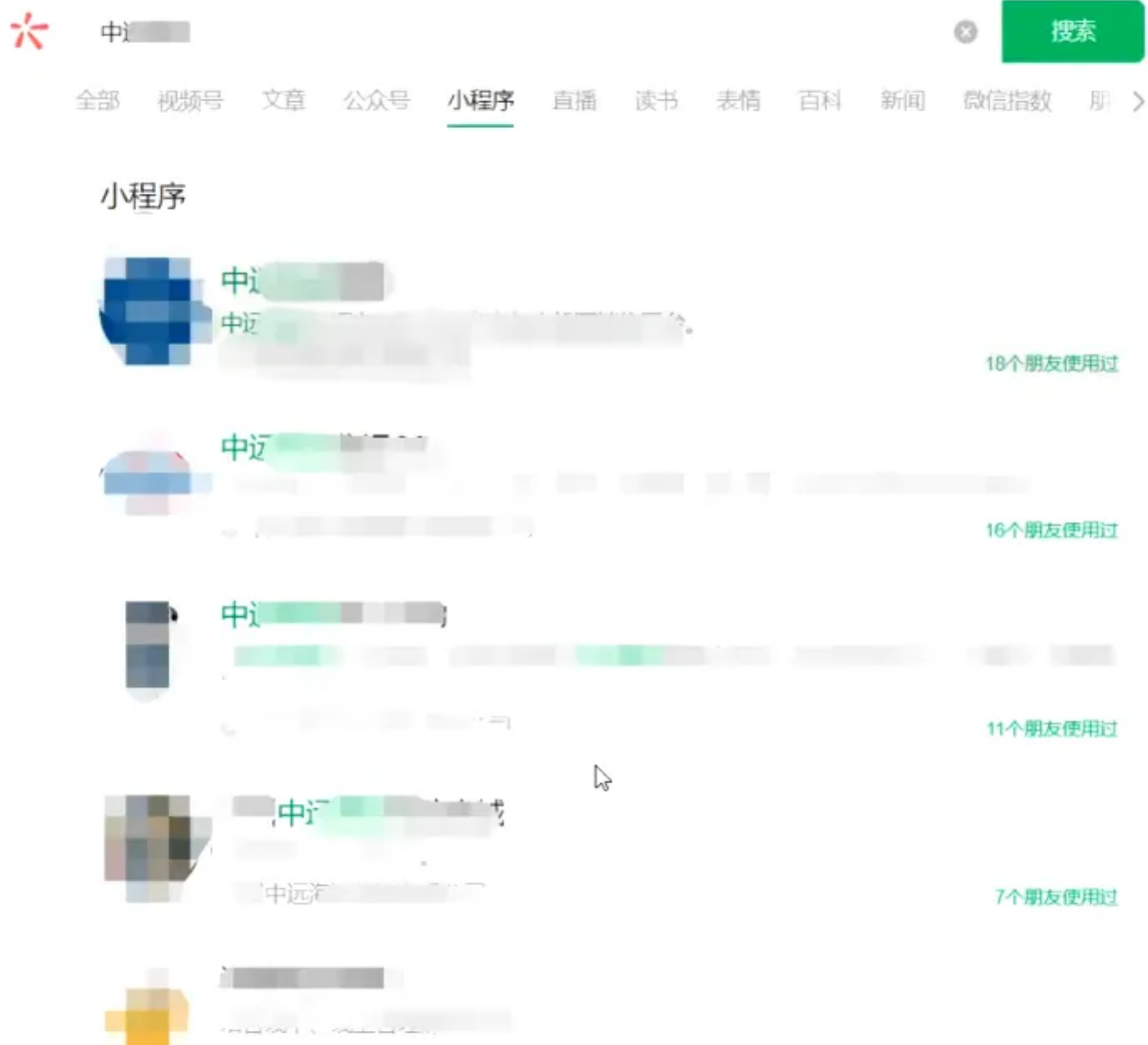
```
1 #列出模块
2 bbot -l
3
4 #子域名枚举
5 bbot --flags subdomain-enum --targets evilcorp.com
6
7 #只进行被动扫描
8 bbot --flags passive --targets evilcorp.com
9
10 #使用gowitness进行网页截图
11 bbot --modules naabu httpx gowitness --name my_scan --output-dir . --targets evilcorp.com 1.2.3.4/28 4.3.2.1 targets.txt
12
13 #Web spider(搜索电子邮件等)
14 bbot -m httpx -c web_spider_distance=2 -t www.evilcorp.com
```

谷歌语法: site baidu.com -www 可以搜集子域名, 找到一些信息泄露笔记好找到一点

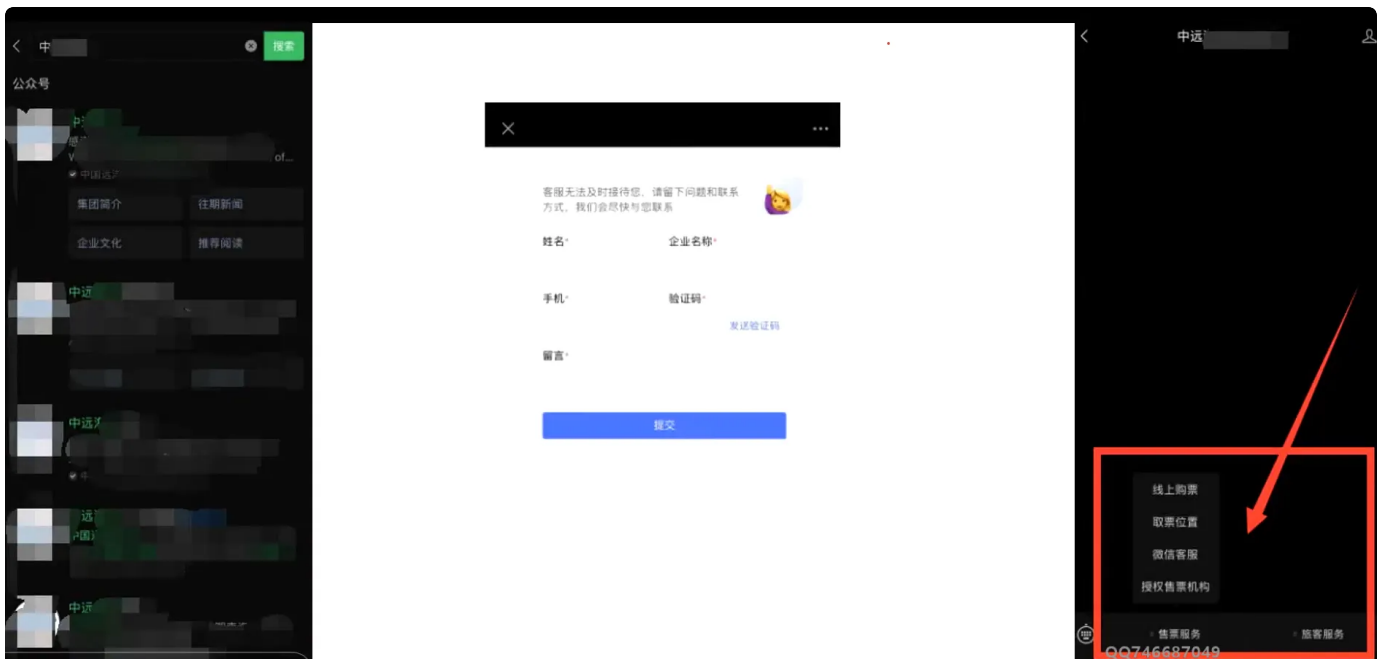
2、一定要去学会信息清理, 这个就是将你收集到的所有信息做个规整, 将能访问到的网站规整起来, 可以使用python对数据进行处理, 并返回来截图信息, 功能类似于灯塔的操作, 这样更方便更高效去挖掘漏洞。

3、比较推荐小蓝本这个搜集工具, 它会将APP资产, 网站资产全部列举过来

一般比较大的企业在众测项目中很长时间, 他的web方面挖掘漏洞会很难, 所有推荐从APP和小程序去入手, 小程序, 公众号是一个突破的一个点



给个这样的页面，会想到测试什么漏洞，如果一个存在的话，对应的子公司公众号都是存在这个漏洞的



三、众测案例

1、商城页面，每一个都是一个功能点，都可以进行测试

优惠券测试---> 并发



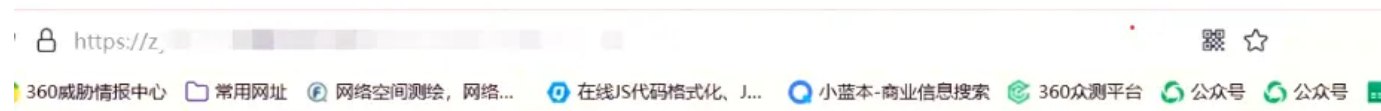
优惠券，领券中心----->并发，是否能重复使用，面额是否可以修改，是否能遍历优惠券id-找到隐藏的优惠券,越权漏洞测试

在线客服----->可以放xss语句

2、登录页面



- 1、可以去爆破，账号密码去爆破
- 2、去将小程序反编译一下，看信息
- 3、把小程序得域名放到web上看

A screenshot of a login form for a service named '海运' (Shipping). The form has a title '海运' followed by a blurred subtitle. It contains three input fields: '请输入用户名' (Please enter username), '请输入密码' (Please enter password) with an eye icon for toggling visibility, and '验证码' (Captcha) next to a green box displaying the characters 'A316'. A blue button labeled '确定' (Confirm) is at the bottom.