登录

SRC漏洞挖掘实用技巧

tinyfisher / 2019-09-02 09:05:00 / 浏览数 7907 渗透测试 渗透测试 顶(6) 踩(0)

0x01 信息收集

1、Google Hack实用语法

迅速查找信息泄露、管理后台暴露等漏洞语法，例如：

```
filetype:txt ■■
filetype:xls ■■
filetype:doc ■■
intitle:■■■■
intitle:login
intitle:■■■■  inurl:admin
intitle:index of /
```

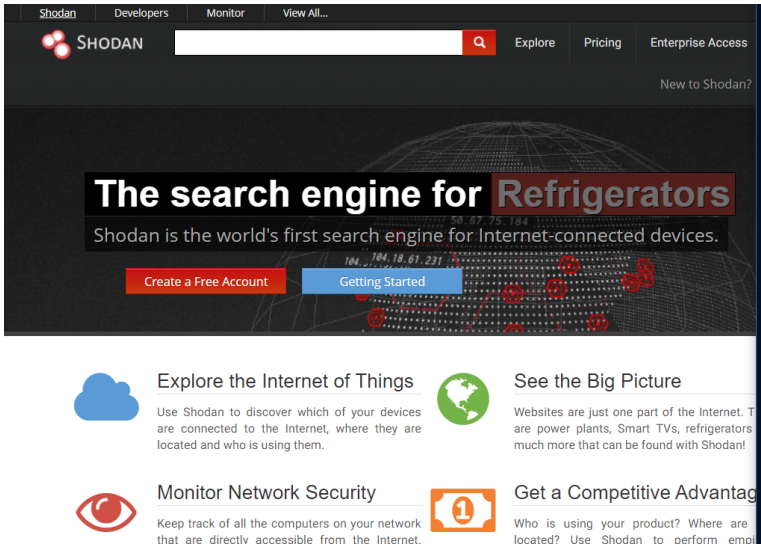
查找指定网站，再加上site:example.com，例如：

```
site:example.com filetype:txt ■■
site:example.com intitle:■■■■
site:example.com admin
site:example.com login
site:example.com system
site:example.com ■■
site:example.com ■■
site:example.com ■■
site:example.com ■■
```

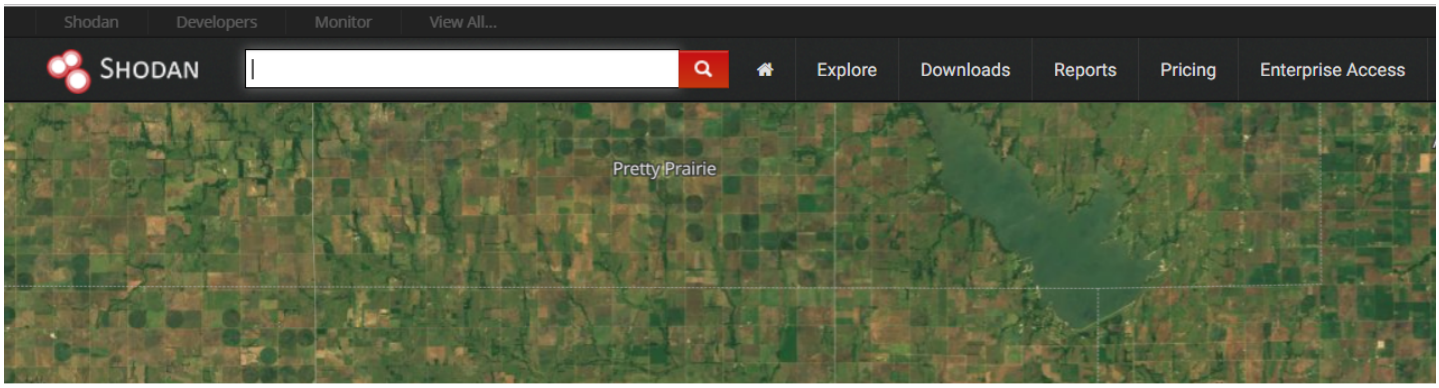
关键词可以根据实际情况进行调整，推荐Google、Bing，搜索内容如果被删除，网页快照一般仍会有记录。

2、Shodan、fofa网络资产搜索引擎

Shodan、foda等网络资产搜索引擎可以用来搜索网络空间中在线设备，功能十分强大，相当于网络安全界的google：



特别是超强搜索引擎shodan，甚至可以根据logo查询互联网资产：
比如对某IP进行信息检索，点击view raw data：



.88.123 View Raw Data

Ports

Country United States

80 443

找到data.0.http.favicon.data字段：

data.0.http.components.jQuery.categories ['JavaScript Libraries']

data.0.http.favicon.data AAABAAEAQEAAAAEAIAAoQgAAFgAAACgAAABAAA
8v////////////////////////////////
Zf//pWX//6Vl//+lZf//////////////w5
////////////////////////////////
////////////////////////////////
zP////////////////////////////////
////////////////////////////////

data.0.http.favicon.hash -1507567067

搜索相应的值即可根据企业logo查询资产：

```
http.favicon.hash:-1507567067
```

推荐安装shodan chrome 插件，方便进行查看和使用：

```
https://chrome.google.com/webstore/detail/shodan/jjalcfnidlmpjhdfepjhjbhnhkbgleap
```

fofa是国内的一款网络空间资产搜索引擎，与shodan类似，常见搜索语法：

```
title="abc" ■■■■■■abc■■■■■■■■■■■■■
header="abc" ■http■■■■abc■■■jboss■■■
body="abc" ■html■■■■■■abc■■■■■■■■Hacked by
domain="qq.com" ■■■■■■■■qq.com■■■■■■■ ■■■■■qq.com■■■
host=".gov.cn" ■url■■■■.gov.cn,■■■■■■■host■■■■■■■■ ■■■■■, ■■■■■
```

```
port="443" ■■■■443■■■■■■■■ ■■■■443■■■■■
...
```

实用查询语句：

```
body="■■■1" && country=CN&&title="■■■2"
```

可以快速定位国内想要搜索的网站信息。

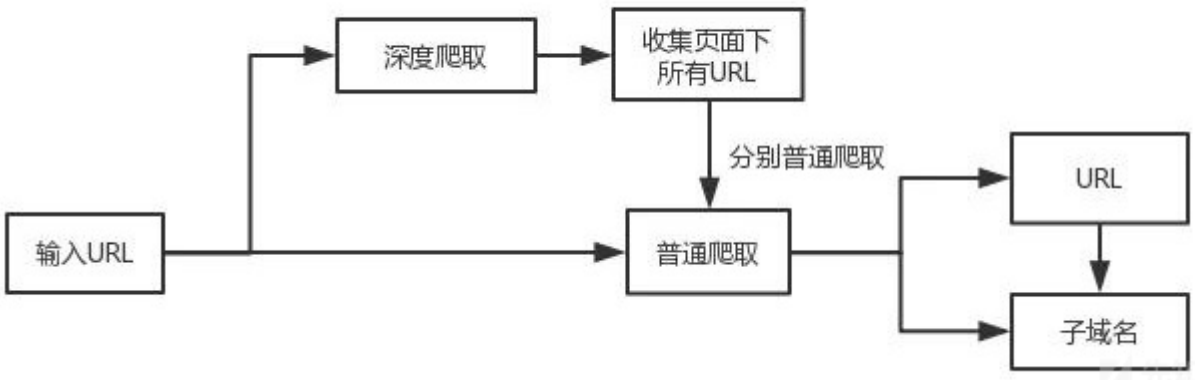
3、子域名收集

推荐几个好用的工具：

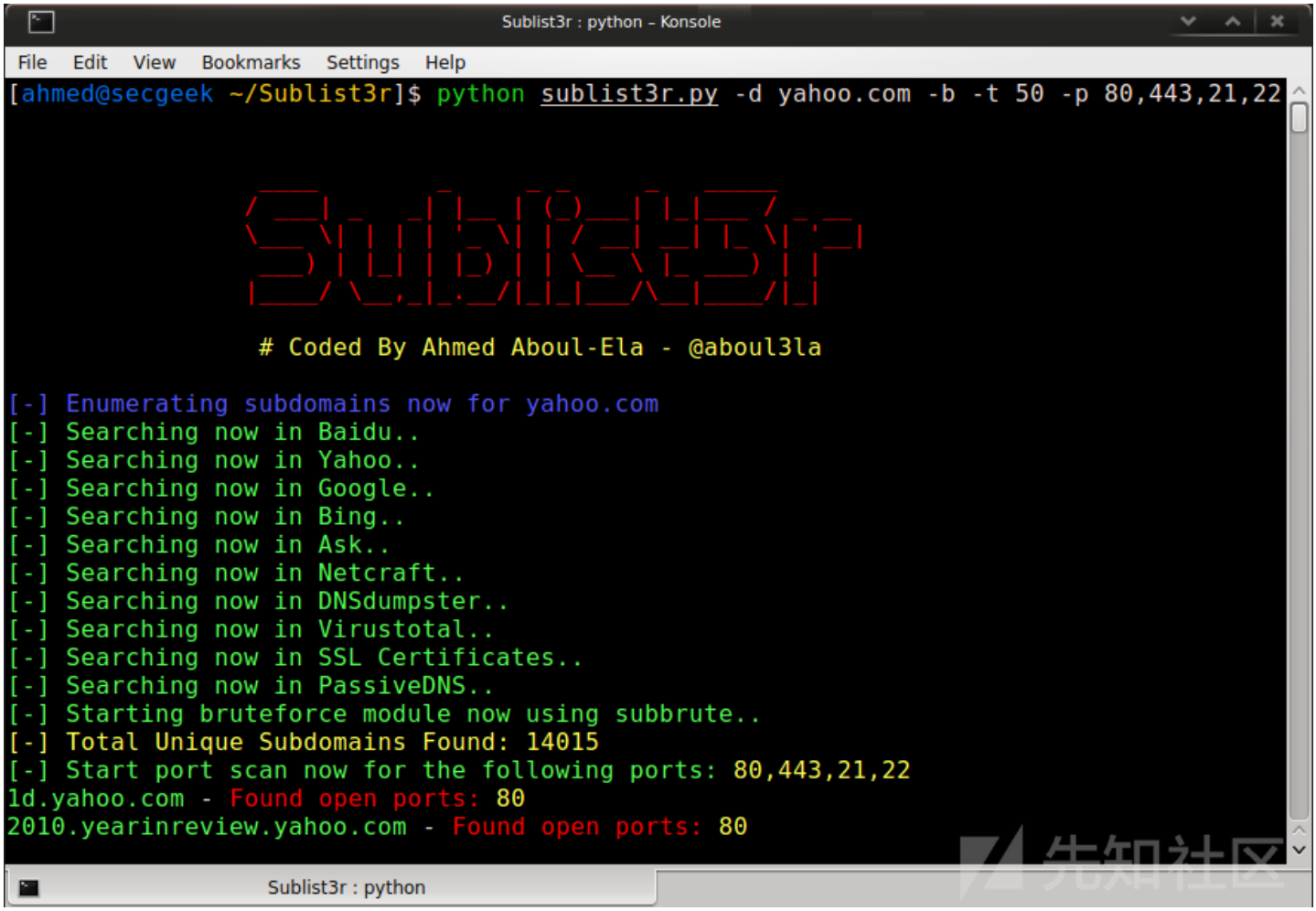
- JSFinder(https://github.com/Threezh1/JSFinder)

```
PS C:\Users\tinyfisher\Desktop\SRC\JSFinder-master> python .\JSFinder.py -h
usage: JSFinder.py [-h] [-u URL] [-f FILE] [-ou OUTPUTURL]
                   [-os OUTPUTSUBDOMAIN] [-j] [-d]

optional arguments:
  -h, --help            show this help message and exit
  -u URL, --url URL     The website
  -f FILE, --file FILE  The file contains url or js
  -ou OUTPUTURL, --outputurl OUTPUTURL
                        Output file name.
  -os OUTPUTSUBDOMAIN, --outputsubdomain OUTPUTSUBDOMAIN
                        Output file name.
  -j, --js              Find in js file
  -d, --deep            Deep find

Example: python .\JSFinder.py -u http://www.baidu.com
```

在网站的JS文件中，会存在各种对测试有帮助的内容，JSFinder可以帮助我们获取到JS中的url和子域名的信息，拓展我们的渗透范围。爬取分为普通爬取和深度爬取，深度爬



- Sublist3r(https://github.com/aboul3la/Sublist3r)
  Sublist3r是一个python版工具，其设计原理是基于通过使用搜索引擎，从而对站点子域名进行列举。Sublist3r目前支持以下搜索引擎：Google, Yahoo, Bing, 百度以及Ask，而未来将支持更多的搜索引擎。目前，Sublist3r同样也通过Netcraft以及DNSdumpster获取子域名。



- 云悉(http://www.yunsee.cn/info.html)
  云悉可以在线搜集子域名、ip段、CMS指纹等信息

4、github敏感信息泄露实时监控

GSIL(GitHub Sensitive Information Leakage)项目，地址：
https://github.com/FeeiCN/GSIL

通过配置关键词，实时监控github敏感信息泄露情况，并发送至指定邮箱：

5、网盘搜索引擎

和github类似，网盘中往往会存在企业泄露的内部信息，同样需要关注，常见的网盘搜索引擎：
盘多多：http://www.panduoduo.net/
盘搜搜：http://www.pansoso.com/
盘搜：http://www.pansou.com/
凌云风搜索：https://www.lingfengyun.com/

6、注意公众号、服务号、小程序、APP

企业的微信号、服务号、小程序、APP会帮助我们拓展攻击面，部分应用入口web中并没有，需要从公众号、小程序、APP入手，公众号中甚至会有企业用于测试的公众号、

7、注册非普通用户（商户、企业用户等等）

商户、企业用户注册一般需要提交多个资料：营业执照、企业证件号等等，比较繁琐：

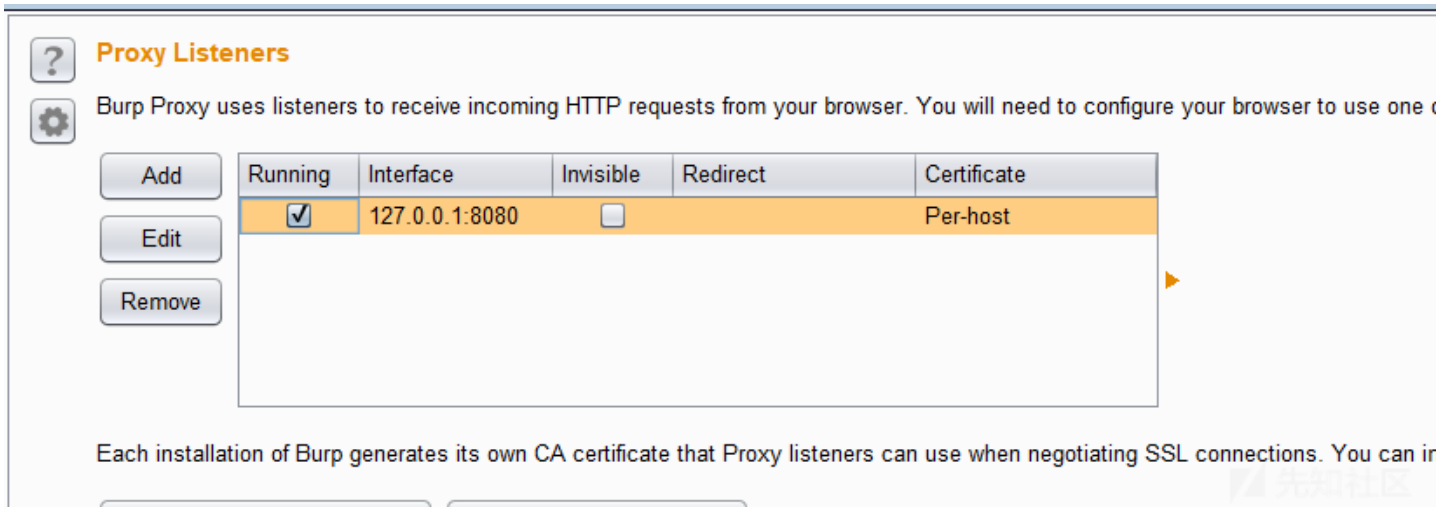
但不要因为麻烦放弃，此类用户由于注册难，意味着测试的人员少，往往漏洞比较多。部分平台审核不严，很多情况下提供资料注册即可通过或简单电话验证即可通过。

想办法提供各类资料注册（网上购买营业执照、公开信息收集、PS）
想办法获取到账号（撞裤、文库、QQ群、github泄漏等）
借账号/租账号/买账号

0x02 微信公众号抓包技巧

企业微信公众号可以大大拓宽我们的测试范围，公众号部分链接可以直接复制到浏览器中打开，然后按照常规的渗透测试方法进行，但是有的链接复制到浏览器后，会出现下

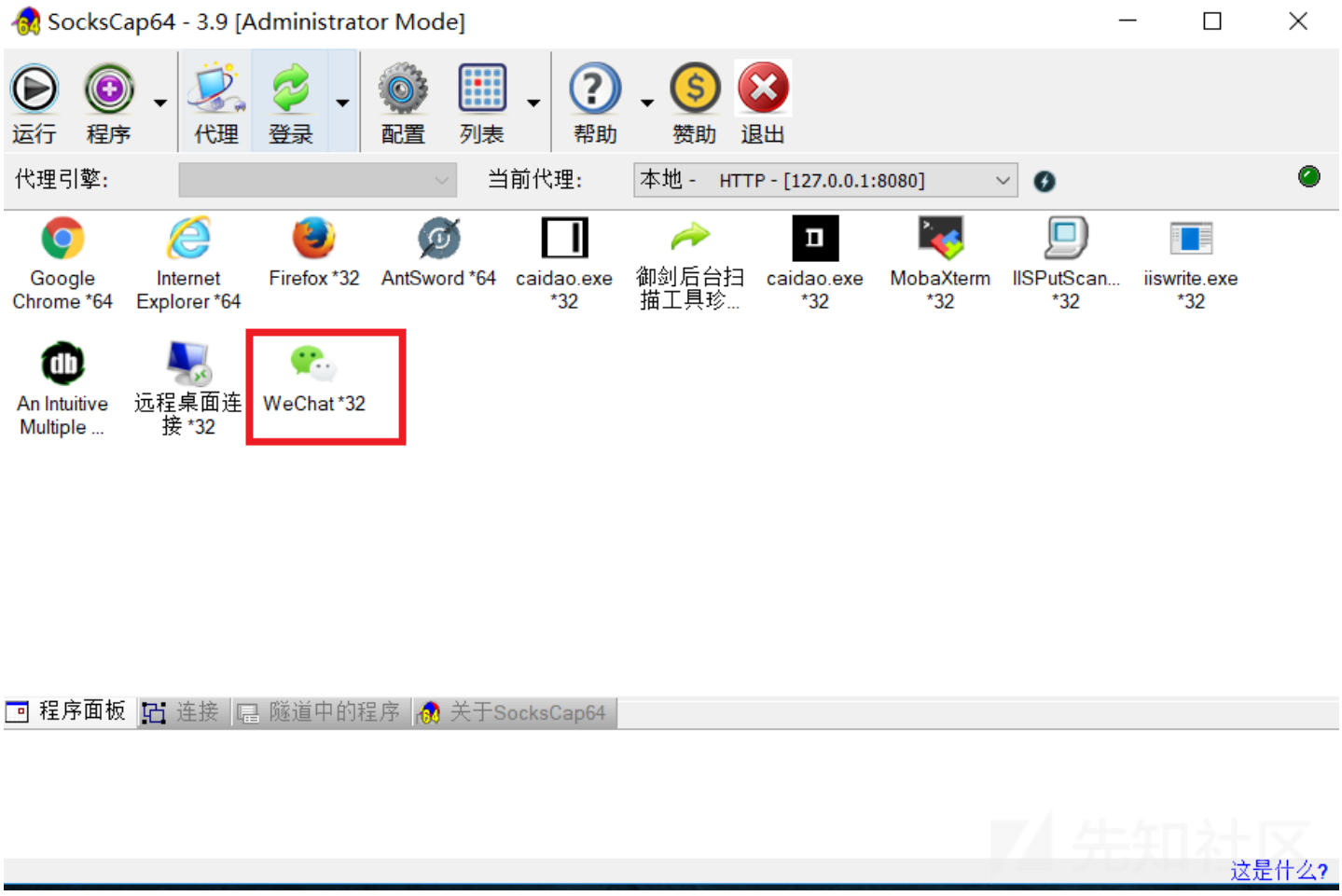
对于这种情况，可以通过安卓模拟器抓微信包、真机微信抓包的方式解决，但都相对不太方便，和大家分享通过SocksCap64直接抓微信PC端的流量方法。
SocksCap64是一款功能非常强大的代理客户端，支持http/https、socks4/5、TCP、UDP等协议，在内网渗透中经常使用，同样可以用他来代理微信PC客户端的流量，并
首先还是在burp中设置监听：



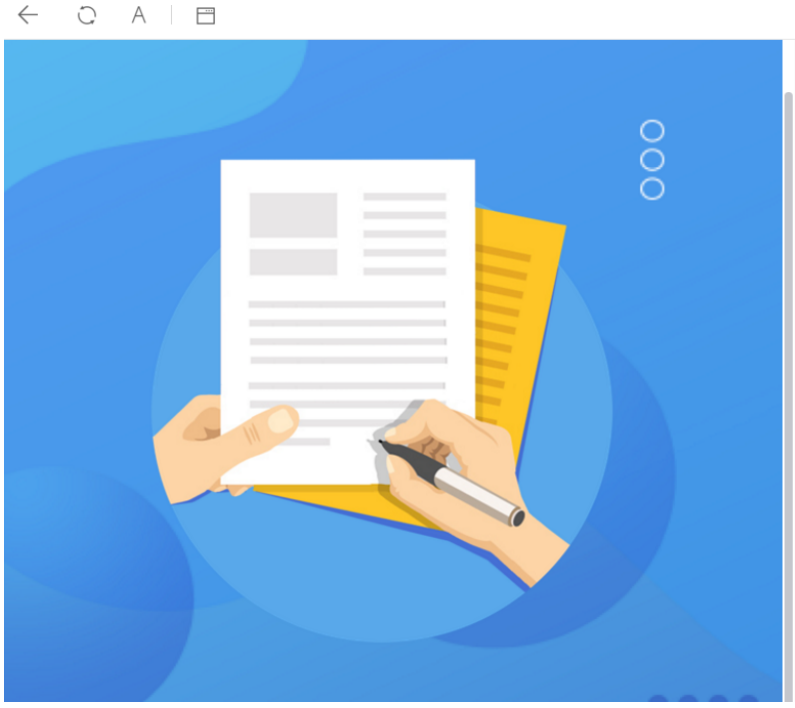
然后在SocksCap64中设置代理服务器为burp的地址和端口，代理方式HTTP：

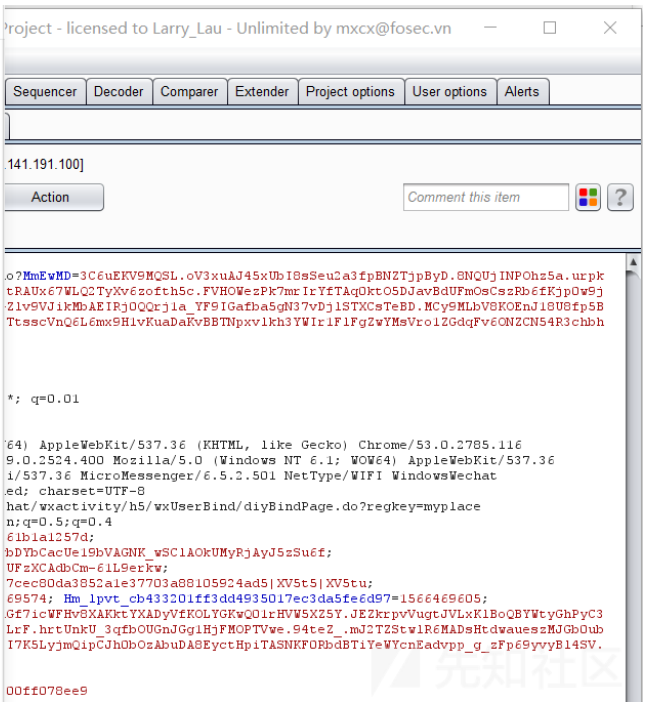
测试一下，是否成功：

然后利用SocksCap64启动微信：

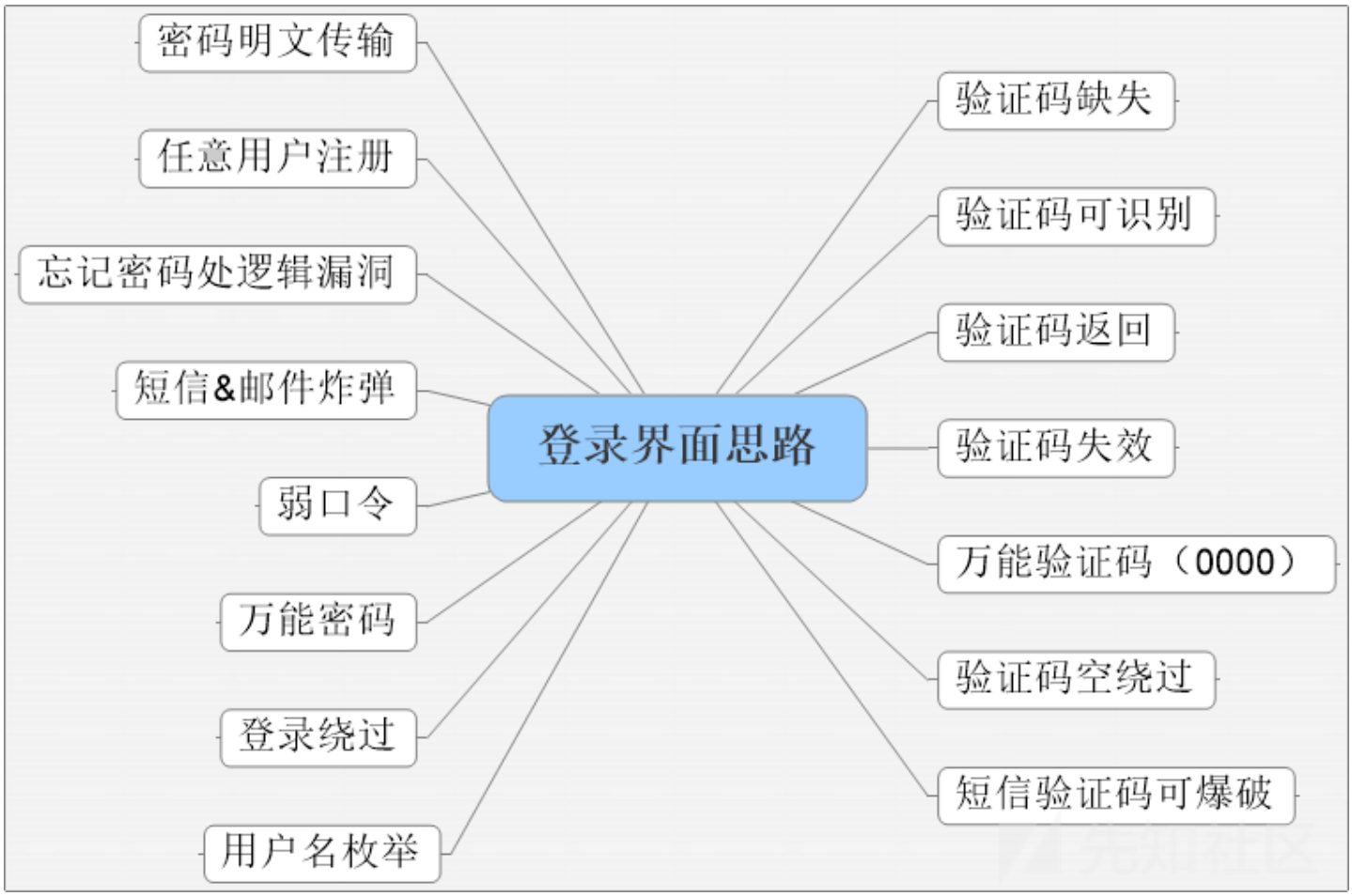


即可成功抓到微信PC端的流量：





0x03 登录界面思路



0x04 短信&邮件轰炸绕过

在网站测试的过程中，常常在用户注册登录时出现手机号/邮箱注册，这里就可能出现短信&邮件炸弹漏洞，此类漏洞测试比较方便，虽然有的站点做了防护，但也有一些绕

这里收集了部分目前较为流行的临时接收短信的网站，方便用于测试：

```
https://www.pdflibr.com/

http://www.z-sms.com/
```

https://www.receive-sms-online.info/

[■■] http://www.smszk.com/

[■■] http://receive-sms-online.com/

[■■] https://smsnumbersonline.com/

[■■] https://www.freeonlinephone.org/

[■■] https://sms-online.co/receive-free-sms

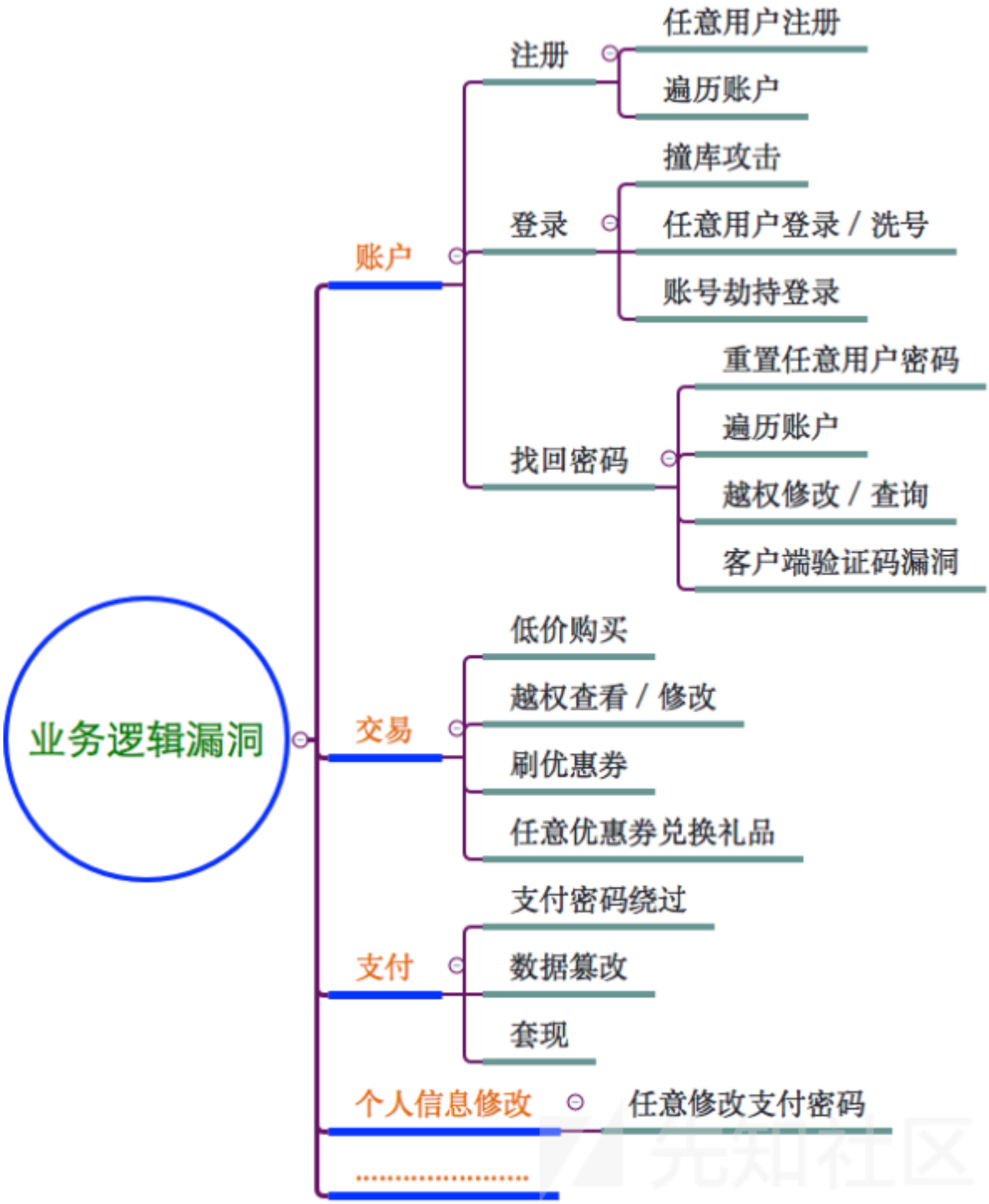
在应用手机号/邮箱和验证码作为用户登录凭证时，一般涉及到的网站功能点主要包括：

- 账号注册
- 首次设置密码时用户身份校验
- 账号登录
- 重置密码
- 绑定手机/邮箱
- 修改绑定手机/邮箱
- 免费试用/活动领取/反馈处
- ...

常见的测试和绕过手段：

0x05 逻辑漏洞

随着开发人员安全意识的日益加强，IPS/IDS、WAF、全流量检测等防护设备的不断部署，传统的SQL注入漏洞、命令执行等漏洞正变得越来越少，或者越来越难挖（需要绕



1、修改返回包的越权

场景1：修改手机号

一般的修改逻辑为：认证原手机号 -> 填写新手机号 -> 提交修改

如果在进行下一步操作时，没有校验上一步的认证是否成功时，就会存在逻辑缺陷绕过。
比如在第一步认证原手机号时，随意输入验证码，将response包中的相关字段进行修改，比如0改成1，false改成true，即可绕过第一步验证，进入填写新手机号界面，如果

乌云案例：http://www.anquan.us/static/bugs/wooyun-2015-0120951.html

场景2：登录绕过

部分网站的身份验证放在了前端，因此只需要将response包中的相关字段进行修改，比如0改成1，false改成true，就可以登录任意用户账号。

乌云案例：http://www.anquan.us/static/bugs/wooyun-2015-0151201.html

2、水平越权

场景1：遍历ID
在一些请求中，GET或POST中有明显的id数字参数（手机号、员工号、账单号、银行卡号、订单号等等），可以尝试进行遍历，如果程序没有对当前权限进行判断，就会存

乌云案例：http://www.anquan.us/static/bugs/wooyun-2016-0204958.html

场景2：ID替换
如果程序对用户标识进行了hash或者加密，而又无法破解用的什么加密方式的话，就无法通过遍历ID来获取其他用户信息了。此时可以尝试注册两个账号，通过替换两个ID

3、垂直越权

观察cookie中的session字段，猜测修改，发现：
level=1： admin
level=2： vip user
level=3： normal user

Cookie: SESSION=USER-334dsf9ref8esg8erg390g
Cookie: SESSION=USER-3dfg34768jh4h234g5h5jk
Cookie: SESSION=USER-304jkh6g9090ertk45g0s9

Cookie: SESSION=USER-2dfg34768jh4h234g5h5jk
Cookie: SESSION=USER-1dfg34768jh4h234g5h5jk

说明，本教程文章仅限用于学习和研究目的，请勿用于非法用途。漏洞挖掘中应遵守SRC中的相关规则。

上一篇：一款漏洞验证框架的构思 下一篇：pwn堆入门系列教程2
1. 5 条回复


al0an****@outloo 2019-09-02 11:51:28

师傅方便加个微信交流下吗

0 回复Ta

mochazz 2019-09-03 01:19:03

文章写的很清晰，赞！

0 回复Ta


getshell1993 2019-09-09 14:27:34

看到我PPT里的几张图 0.0

0 回复Ta


tinyfisher 2019-09-16 12:36:13

@getshell1993 原来是大佬的ppt，我也是从其他论坛中看到的，受益匪浅

0 回复Ta


tinyfisher 2019-09-16 12:36:30

@al0an****@outloo 私聊

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板