## 信息收集

-----灯塔自动化推荐

Docker 安装

docker 安装参考：https://docs.docker.com/engine/install/

shell脚本:

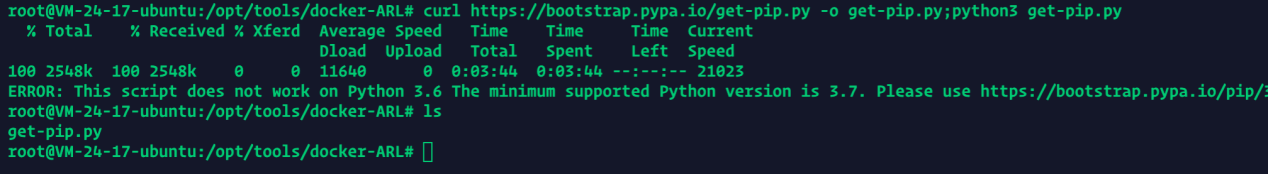
curl -fsSL https://get.docker.com -o get-docker.sh

sudo sh get-docker.sh

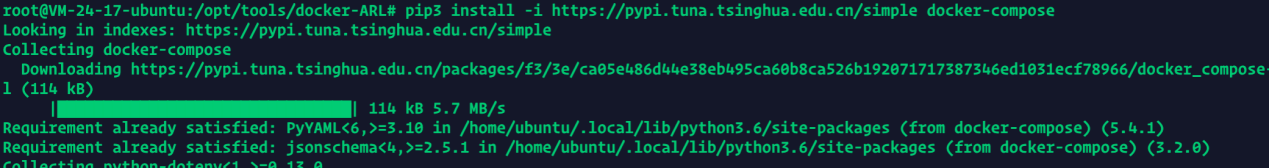
灯塔安装

mkdir docker-ARL;cd docker-ARL

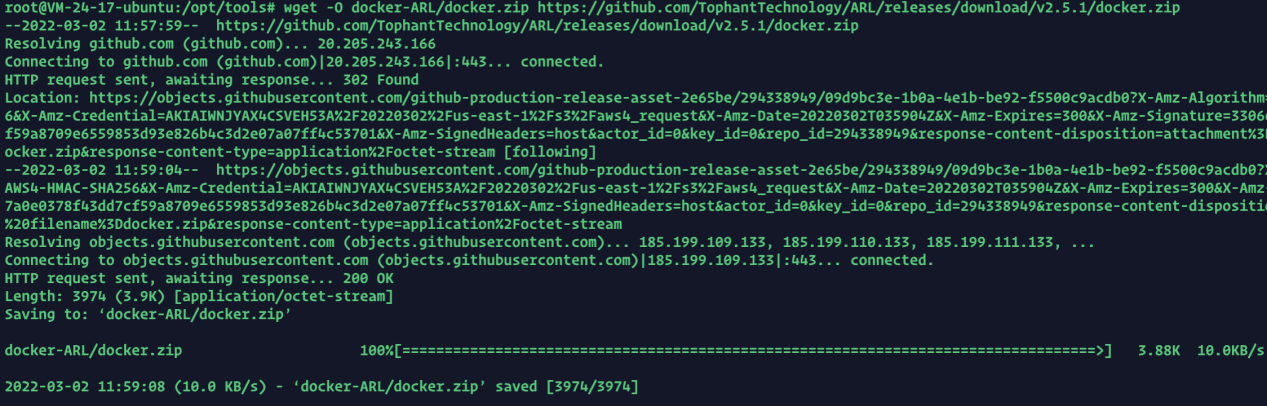
curl https://bootstrap.pypa.io/get-pip.py -o get-pip.py;python3 get-pip.py



pip3 install -i https://pypi.tuna.tsinghua.edu.cn/simple docker-compose

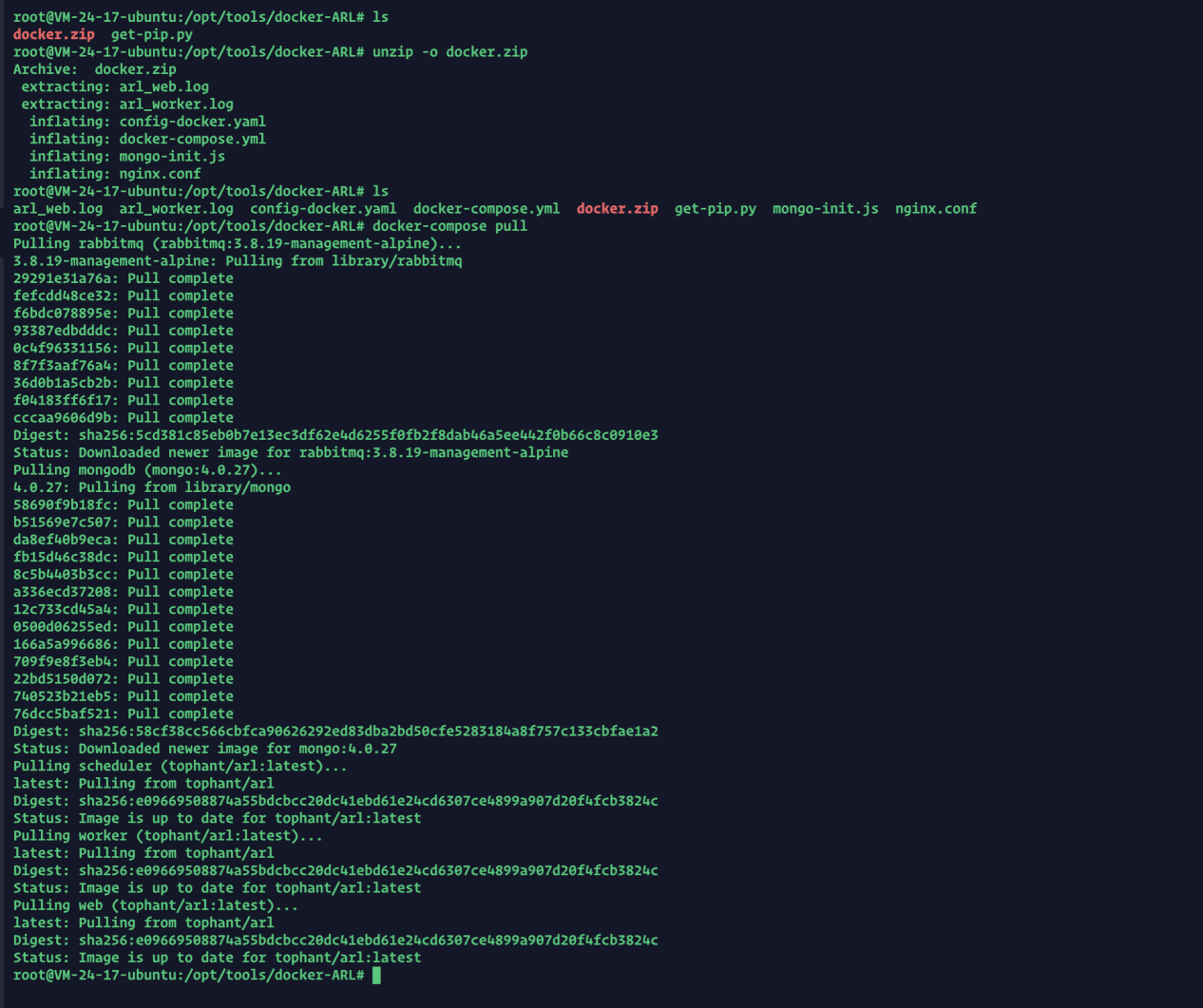


wget -O docker-ARL/docker.zip https://github.com/TophantTechnology/ARL/releases/download/v2.5.1/docker.zip



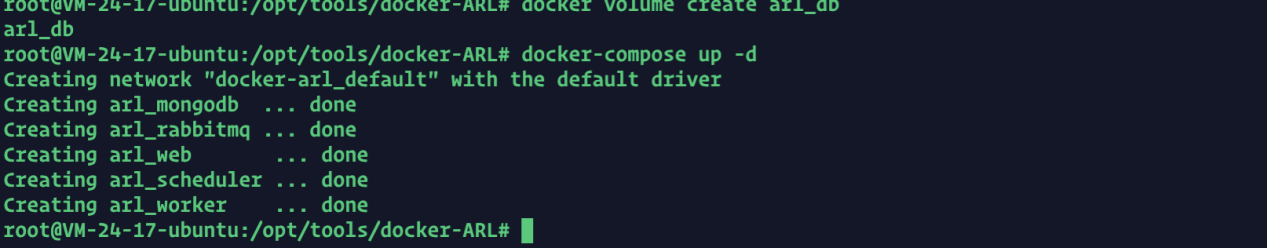
unzip -o docker.zip

docker-compose pull



docker volume create arl\_db

docker-compose up -d



dcoker-compose ps -a # 查看



修改密码

默认密码是 admin/admin

登录端口: https://IP:5003/login

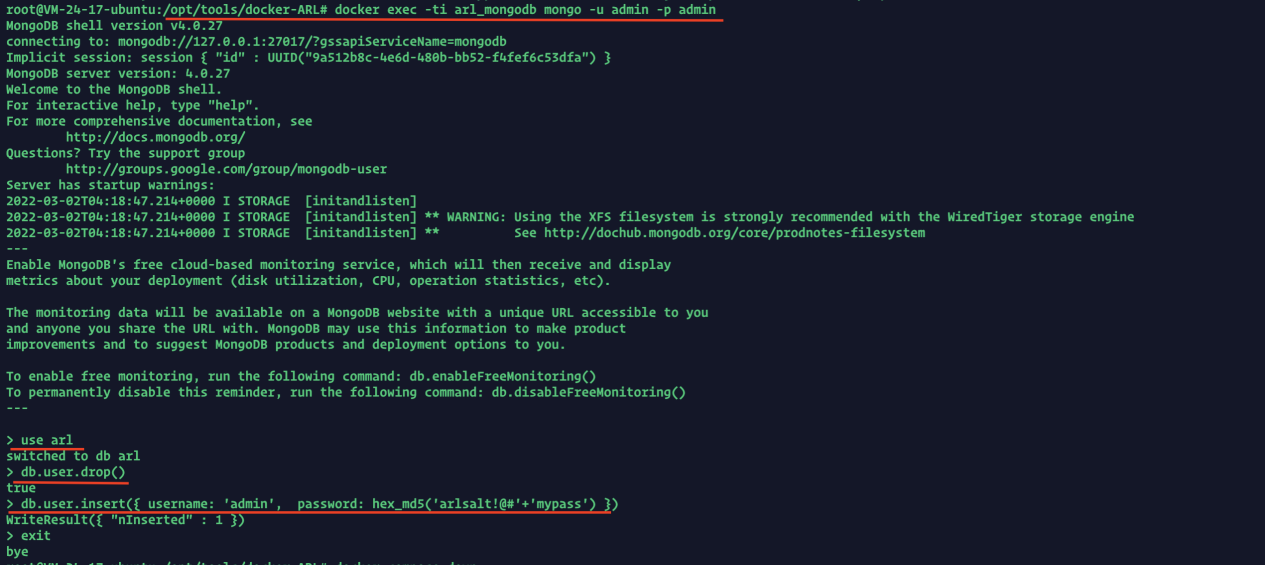
docker exec -ti arl\_mongodb mongo -u admin -p admin

use arl

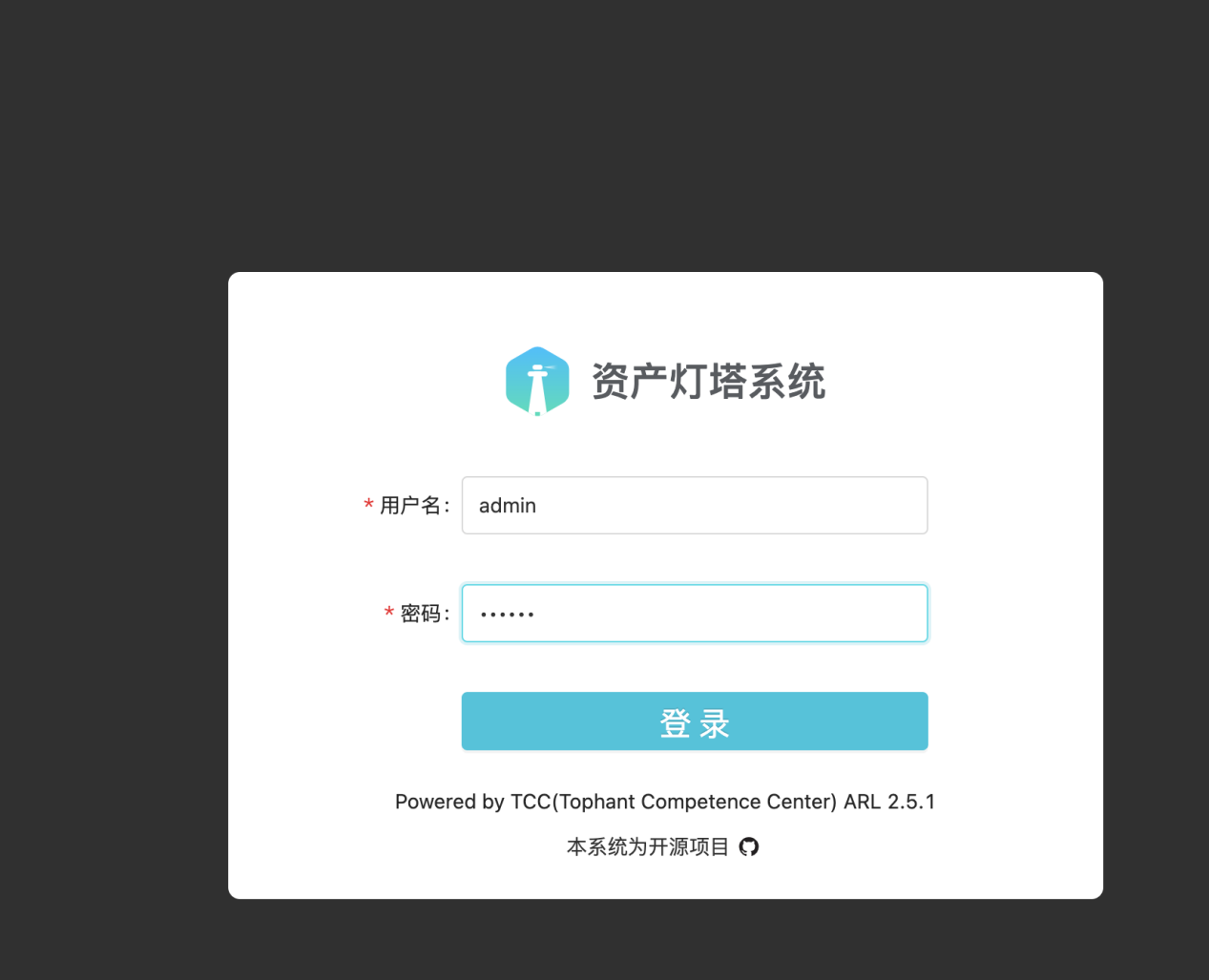
db.user.drop()

db.user.insert({ username: 'admin', password: hex\_md5('arlsalt!@#'+'你的密码') })

exit

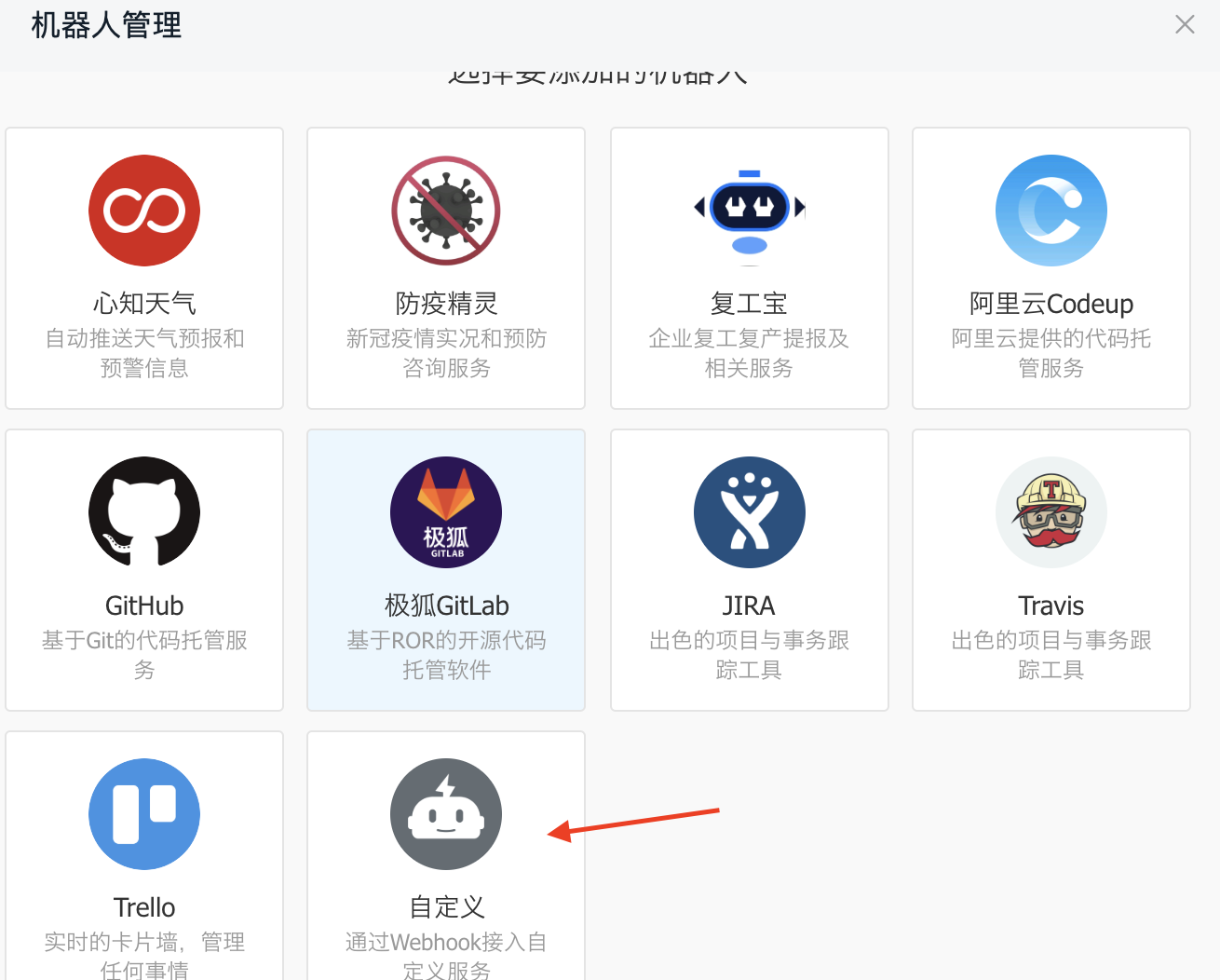


登录



1. 配置钉钉机器人

首先自己先创建个群聊，【群聊】-【群设置】-【智能群助手】-【添加更多】-【添加机器人】-【自定义】-【添加】





以下两个对应填入 config-docker.yaml中的 SECRET，ACCESS\_TOKEN





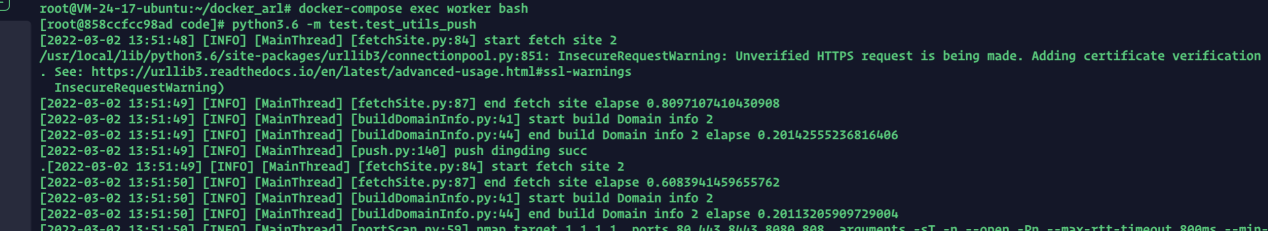
配置文件: docker-ARL/config-docker.yaml



测试是否配置成功

docker-compose exec worker bash

python3.6 -m test.test\_utils\_push





监控



上述是灯塔的安装，这个是自动检查的资产的好帮手，当你要挖掘的src有新的资产上线的时候，就自动发送到你的钉钉上，这时候，你就可以提前去挖掘，运气好就捡到高危险漏洞。

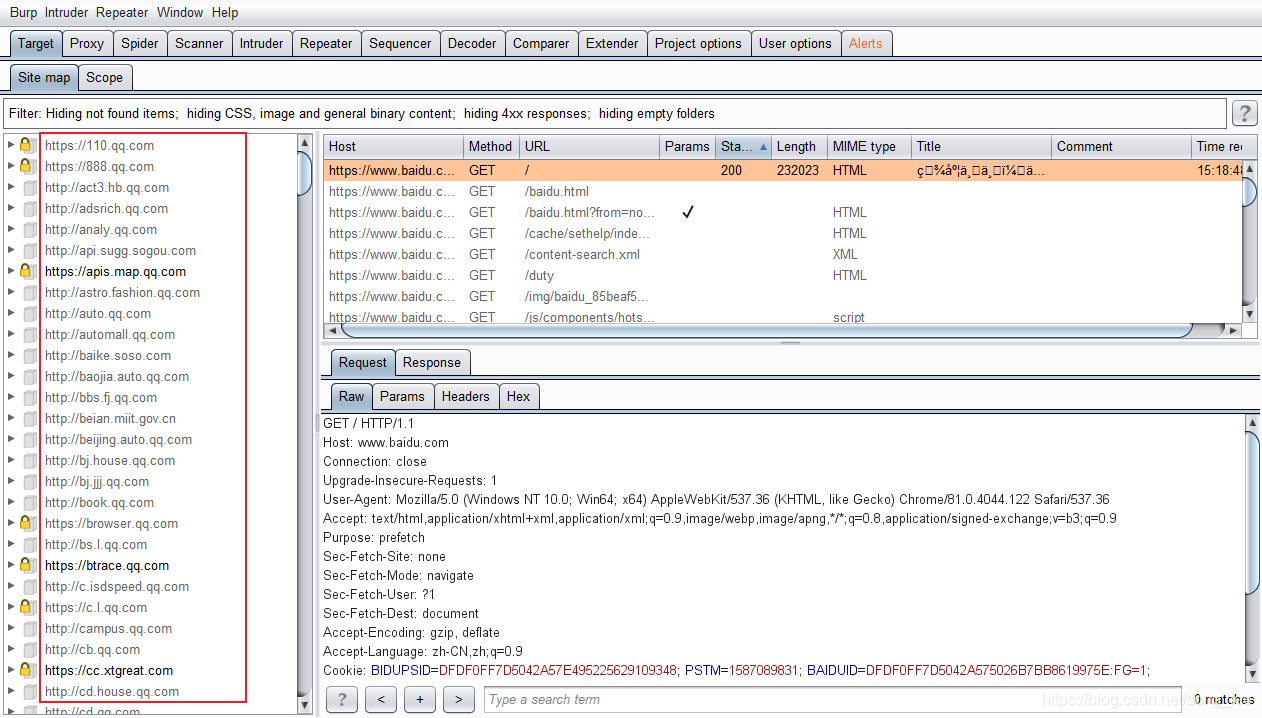
## 0x01 常用工具挖掘

还有一种信息收集收集方式就是直接子域名挖掘，然后一个站点一个站点的查看：

常用工具：[Maltego CE](https://www.paterva.com/downloads.php),[wydomain](https://github.com/ring04h/wydomain),[subDomainBrute](https://github.com/lijiejie/subDomainsBrute),[dnsmaper](http://www.pudn.com/Download/item/id/3836028.html),[Layer子域名挖掘机](http://521.li/post/544.html) oneforall子域名收集工具

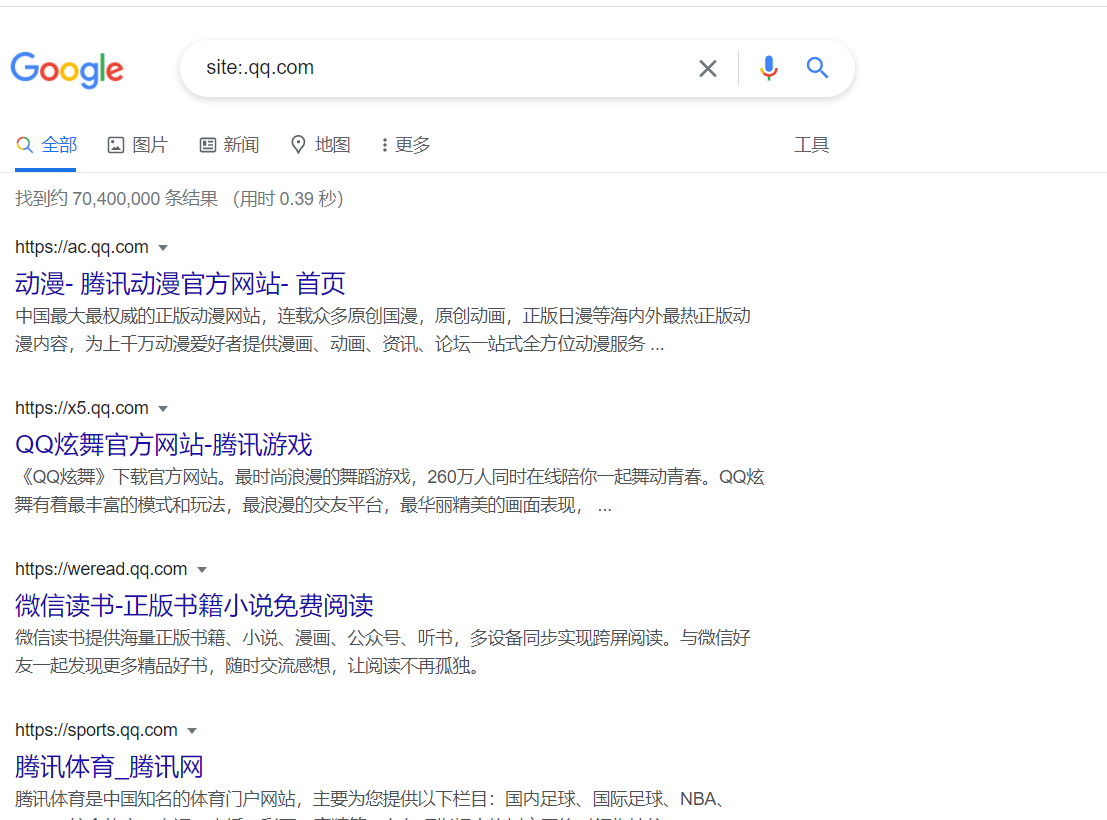
通过这些工具将相关域名的资产全部找出来，然后慢慢挖掘即可。

## 0x02 爬虫提取子域名

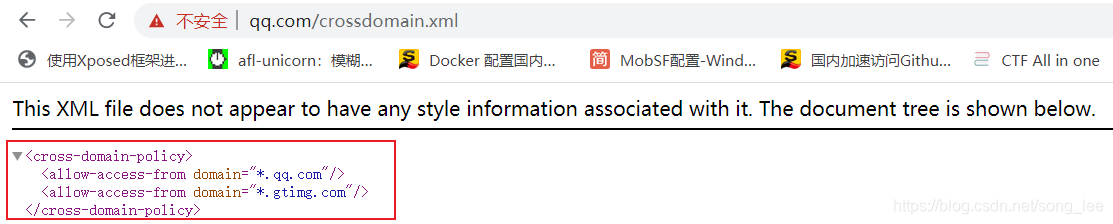
这类工具有很多，例如 burpsuite、appscan、awvs 都有爬虫的功能  


## 0x03 搜索引擎

搜索引擎提供了一些高级搜索指令，site 就可以查询相关的域名，其实搜索引起收录的网页也是通过爬虫来爬取的。



## 0x04 站点配置文件

crossdomain.xml，跨域策略配置文件  


robots.txt，反爬虫配置文件，Robots 协议用来告知搜索引擎哪些页面能被抓取，哪些页面不能被抓取  
