

Kunyu(坤舆)

#0x00 介绍

工具介绍

Kunyu(坤舆)，名字取自 <坤舆万国全图>，测绘实际上是一个地理信息相关的专业学科，针对海里的、陆地的、天上的地理信息进行盘点。同样应用于网络空间，发现未知、脆弱的资产也是如此，更像是一张网络空间地图，用来全面描述和展示网络空间资产、网络空间各要素及要素之间关系，以及网络空间和现实空间的映射关系。所以我认为“坤舆”还是比较贴合的。

Kunyu(坤舆)，旨在让企业资产收集更高效，使更多安全相关从业者了解、使用网络空间测绘技术。

应用场景

对于 kunyu 的使用，应用场景可以有很多，例如：

- 企业内遗忘的，孤立的资产进行识别并加入安全管理。
- 企业外部暴露资产进行快速排查，统计。
- 红蓝对抗相关需求使用，对捕获IP进行批量搜索。
- 批量收集脆弱资产(0day) 影响内的设备、终端。
- 新型网络犯罪涉案站点信息进行快速收集，合并，进行更高效的研判、分析。
- 对互联网上受相关漏洞影响的脆弱资产，进行统计、复现。
-

0x01 安装

需要Python3以上的支持

```
git clone https://github.com/wikiz/Kunyu.git  
tar -xvf Kunyu.tar  
cd Kunyu  
pip3 install -r requirements.txt  
python3 kunyu.py
```

0x02 配置说明

在第一次运行程序时通过输入以下命令进行初始化操作，提供了其他登录方式，但是推荐使用API的方式，因为用户名/密码登录需要额外做一次请求，所以理论上API的方式会更加高效(Seebug API选填，但是不填写无法使用Seebug相关命令)。

```
python3 Kunyu.py init -apikey your <zoomeye key> --seebug <your seebug key>
```

0x03 工具使用

```
python Kunyu.py console -m module <ZoomEye>
```

A screenshot of a terminal window titled "PS C:\Users\风起\Desktop>". The window displays the Kunyu logo, which is a stylized tree or forest scene composed of purple ASCII art. Below the logo, the text "-V 1.1 Alpha" is visible. The terminal then lists global commands with their descriptions:

info	Print User info
SearchHost <query>	Basic Host search
SearchWeb <query>	Basic Web search
SearchIcon <file>/<URL>	Icon Image Search
SearchBatch <File>	Batch search Host
SearchCert <Domain>	SSL certificate Search
SearchDomain <Domain>	domain name associated/subdomain search
Sebug <Query>	Search Sebug vulnerability information
set <Option>	SET arguments values (Result)
clear	clear the console screen
help	Print Help info
exit	Exit KunYu &

At the bottom of the terminal, the text "Kunyu (ZoomEye) >" is displayed.

ZoomEye

Global commands:	
info	Print User info
SearchHost <query>	Basic Host search
Searchweb <query>	Basic Web search
SearchIcon <File>/<URL>	Icon Image Search
SearchBatch <File>	Batch search Host
SearchCert <Domain>	SSL certificate
Search	
SearchDomain <Domain>	domain name
associated/subdomain search	
Seebug <Query>	Search Seebug
vulnerability information	
set <Option>	SET arguments
values (result)	
clear	clear the console
screen	
help	Print Help info
exit	Exit KunYu &

OPTIONS

ZoomEye:
page <Number> 查询返回页数(默认查询一页, 每页20条数据)
dtype <0/1> 查询关联域名/子域名(设置0为查询关联域名, 反之为子域名)

使用案例

这里我们使用 ZoomEye 进行演示，因为相比较而言功能更加全面。

HOST 主机搜索

ID	IP	Port	Protocol	Service	ISP	City	Title	Latitude	Longitude
1	39.97.118.130	22	ssh	OpenSSH	ALIYUN	Beijing		39.938884	116.397459
2	39.97.118.130	80	http	Apache httpd	ALIYUN	Beijing		39.938884	116.397459
3	39.97.118.130	8080	http-proxy	Apache httpd	ALIYUN	Beijing		39.938884	116.397459
4	39.97.118.130	8089	http	Apache httpd	ALIYUN	Beijing		39.938884	116.397459
5	39.97.118.130	81	https	Apache	ALIYUN	Beijing		39.938884	116.397459
6	39.97.118.130	82	https	Apache httpd	ALIYUN	Beijing		39.938884	116.397459
7	39.97.118.130	3306	mysql		ALIYUN	Beijing		39.904989	116.405285

[13:38:56] [gather_zoomeye.py:246] [INFO]- Search information retrieval is completed

Kunyu (ZoomEye) >

Web 主机搜索

ID	IP	URL	Title	OS	WebApp	DB	Language	Server
1	104.216.173.21	999515com.com	香港六合总论坛,香港马会平特一肖一尾	Windows	DedeCMS	MySQL	ASP	Microsoft IIS httpd
2	120.26.40.196	m.bnmylike.com	宁波美莱整形医院【美莱官网】_宁波整形医院哪家好_东莞品牌运营策划,智能分销方案,全网合一分销系统,	Windows	DedeCMS	MySQL	ASP	Microsoft IIS httpd
3	113.195.191.213	a00k0.bizyi.cn	ltygwyb.com	Windows	DedeCMS	MySQL	PHP	Nginx
4	107.187.127.186	ltgwyb.com	llygy.com	Windows	DedeCMS	MySQL	PHP	Nginx
5	154.23.21.18	m.szxfwl.com	光荣注册,光荣总代理--GOG光荣平台	Windows	DedeCMS	MySQL	PHP	Nginx
6	154.198.202.196	lyquani.com	lyquani.com	Windows	DedeCMS	MySQL	PHP	Apache httpd
7	108.187.83.104	a1709.cn	a1709.cn	Windows	DedeCMS	MySQL	PHP	Nginx
8	154.210.232.170	m56165.com	m56165.com	Windows	DedeCMS	MySQL	PHP	Nginx
9	166.88.159.134	91lp.com	91lp.com	Windows	DedeCMS	MySQL	PHP	Nginx
10	154.221.135.29	998sq.com	998sq.com	Windows	DedeCMS	MySQL	PHP	Nginx
11	156.229.160.110	9da5.com	9da5.com	Windows	DedeCMS	MySQL	PHP	Nginx
12	107.164.169.123	lzkyk.com	泸州可一可装饰,泸州家装设计,装修施工,房屋局部改	Windows	DedeCMS	MySQL	PHP	Apache httpd
13	122.114.8.167	9youcp.com	9youcp.com	Windows	DedeCMS	MySQL	PHP	Nginx
14	107.164.216.145	984x.com	984x.com	Windows	DedeCMS	MySQL	PHP	Nginx
15	107.149.169.118	9youcp.com	9youcp.com	Windows	DedeCMS	MySQL	PHP	Nginx
16	113.185.191.213	97d79.bizyi.cn	东莞市品牌运营策划,智能分销方案,全网合一分销系统,	Windows	DedeCMS	MySQL	PHP	Nginx
17	47.92.174.227	m.shuibiaojia.com	河北巨灵智能水表厂 智能水表 远传水表 ic卡预付费	Windows	DedeCMS	MySQL	PHP	Nginx
18	154.221.180.169	977404.com	977404.com	Windows	DedeCMS	MySQL	PHP	Nginx
19	59.110.61.187	m.haiko.com.cn	301 Moved Permanently	Windows	DedeCMS	MySQL	PHP	Apache httpd
20	104.164.170.153	95464867.xyz	95464867.xyz	Windows	DedeCMS	MySQL	PHP	Nginx

[13:40:56] [gather_zoomeye.py:246] [INFO]- Search information retrieval is completed

Kunyu (ZoomEye) >

批量 IP 搜索

ID	IP	Port	Protocol	Service	ISP	City	Title	Latitude	Longitude
1	39.97.118.130	22	ssh	OpenSSH	ALIYUN	Beijing		39.938884	116.397459
2	148.66.10.244	443	https	simcentric.com	simcentric.com			22.396428	114.189497
3	148.66.10.246	443	https	simcentric.com	simcentric.com			22.396428	114.189497
4	39.97.118.130	80	http	Apache httpd	ALIYUN	Beijing		39.938884	116.397459
5	148.66.10.244	80	http	Apache httpd	simcentric.com		400 Bad Request	22.396428	114.189497
6	39.97.118.130	8080	http-proxy	Apache httpd	ALIYUN	Beijing		39.938884	116.397459
7	39.97.118.130	8089	http	Apache httpd	ALIYUN	Beijing		39.938884	116.397459
8	148.66.10.246	80	http	simcentric.com	simcentric.com			22.396428	114.189497
9	39.97.118.130	81	https	Apache	ALIYUN	Beijing		39.938884	116.397459
10	39.97.118.130	82	https	Apache httpd	ALIYUN	Beijing		39.938884	116.397459
11	39.97.118.130	3306	mysql		ALIYUN	Beijing		39.904989	116.405285
12	148.66.10.244	8888	http	simcentric.com	simcentric.com			22.396428	114.189497
13	148.66.10.244	888	http	Apache httpd	simcentric.com			22.396428	114.189497
14	148.66.10.246	888	http	Apache httpd	simcentric.com			22.396428	114.189497
15	148.66.10.246	8888	http	simcentric.com	simcentric.com			22.396428	114.189497
16	148.66.10.244	21	ftp	Pure-FTPd	simcentric.com			22.396428	114.189497
17	148.66.10.246	111	rpcbind	Spacetnet				38	-97
18	148.66.10.244	111	rpcbind	simcentric.com				22.396428	114.189497

[13:44:52] [gather_zoomeye.py:246] [INFO]- Search information retrieval is completed

Kunyu (ZoomEye) >

Icon 搜索

在搜集企业资产时，我们可以使用这样的方式进行检索相同 ico 图标资产，在关联相关企业资产时，通常会有不错的效果。但是需要注意的是如果某些站点也使用这个 ico 图标，可能会关联出无关资产(但是无聊用别人 ico 图标的人总归是少数吧)。支持url或本地文件的方式搜索。

```

SearchBatch <File>
SearchCert <Domain>
SearchDomain <Domain>
Seebug <Query>
set <Option>
clear
help
exit

Batch search Host
SSL certificate Search
domain name associated/subdomain search
Search Seebug vulnerability information
SET arguments values (result)
Print Help info
Exit KunYu &

Kunyu (ZoomEye) > SearchIcon https://www.baidu.com/favicon.ico
[13:10:04] search result amount: 633
gather_zoomeye.py:244



| ID | IP              | Port | Protocol | Service           | ISP               | City        | Title     | Latitude  | Longitude   |
|----|-----------------|------|----------|-------------------|-------------------|-------------|-----------|-----------|-------------|
| 1  | 39.156.66.14    | 443  | https    | BWS               | ChinaMobile       | Beijing     | 百度一下，你就知道 | 39.938884 | 116.397459  |
| 2  | 39.156.66.92    | 443  | https    | BWS               | ChinaMobile       | Beijing     | 百度一下，你就知道 | 39.938884 | 116.397459  |
| 3  | 39.156.66.94    | 443  | https    | BWS               | ChinaMobile       | Beijing     | 百度一下，你就知道 | 39.938884 | 116.397459  |
| 4  | 39.156.66.98    | 443  | https    | BWS               | ChinaMobile       | Beijing     | 百度一下，你就知道 | 39.938884 | 116.397459  |
| 5  | 39.156.66.18    | 443  | https    | BWS               | ChinaMobile       | Beijing     | 百度一下，你就知道 | 39.938884 | 116.397459  |
| 6  | 39.156.66.93    | 443  | https    | BWS               | ChinaMobile       | Beijing     | 百度一下，你就知道 | 39.938884 | 116.397459  |
| 7  | 168.235.92.62   | 443  | https    | nginx             | ramnode.com       | Los Angeles | 百度一下，你就知道 | 34.052234 | -118.243685 |
| 8  | 194.168.90.82   | 443  | https    | nginx             | cocolcrossing.com | Los Angeles | 百度一下，你就知道 | 34.052234 | -118.243685 |
| 9  | 194.168.43.72   | 443  | https    | nginx             | cocolcrossing.com | San Jose    | 百度一下，你就知道 | 37.3386   | -121.886002 |
| 10 | 139.159.226.174 | 443  | https    | nginx             | Chinatelecom      | Guangzhou   | 百度一下，你就知道 | 23.12911  | 113.264385  |
| 11 | 139.155.242.68  | 443  | https    | nginx             | Chinatelecom      | Chengdu     | 302 Found | 30.658529 | 104.075546  |
| 12 | 119.63.197.139  | 80   | http     | BWS               | BWS               | Tokyo       | 百度一下，你就知道 | 35.709026 | 139.731993  |
| 13 | 194.168.14.75   | 443  | https    | coloccrossing.com | ChinaUnicom       | San Jose    | 百度一下，你就知道 | 37.3386   | -121.886002 |
| 14 | 119.3.249.226   | 80   | http     | nginx             | ChinaTelecom      | Beijing     | 百度一下，你就知道 | 39.938884 | 116.397459  |
| 15 | 218.91.286.10   | 443  | https    | nginx             | hostdare.com      | Nantong     | 百度一下，你就知道 | 32.20839  | 121.038918  |
| 16 | 212.103.62.186  | 443  | https    | nginx             | choopa.com        | Los Angeles | 百度一下，你就知道 | 34.052234 | -118.243685 |
| 17 | 287.246.105.2   | 443  | https    | BWS               | choopa.com        | Los Angeles | 百度一下，你就知道 | 34.052234 | -118.243685 |
| 18 | 45.77.28.249    | 80   | http     | nginx             | it7.net           | Tokyo       | 百度一下，你就知道 | 35.709026 | 139.731993  |
| 19 | 45.62.121.65    | 80   | http     | Tengine httpd     | sharktech.net     | Rotterdam   | 百度一下，你就知道 | 51.92442  | 4.477733    |
| 20 | 45.58.174.243   | 80   | http     |                   |                   | Los Angeles | 順豐淘寶集運    | 34.052234 | -118.243685 |


[13:10:04] [gather_zoomeye.py:246] [INFO]- Search information retrieval is completed
Kunyu (ZoomEye) >

```

SSL证书搜索

通过 SSL 证书的序列号进行查询，这样关联出来的资产较为精准，能搜索出使用相同证书的服务。碰到https站点时，可以通过这样的方式。

```

Kunyu (ZoomEye) > SearchCert www.ccccltd.cn
[13:19:41] search result amount: 37
gather_zoomeye.py:244



| ID | IP              | Port | Protocol | Service            | ISP            | City      | Title         | Latitude   | Longitude  |
|----|-----------------|------|----------|--------------------|----------------|-----------|---------------|------------|------------|
| 1  | 218.85.125.72   | 443  | https    | nginx              | ChinaTelecom   | Xiamen    | 中交邮件系统        | 24.602301  | 118.011002 |
| 2  | 218.85.125.80   | 443  | https    | Apache httpd       | ChinaTelecom   | Xiamen    | 302 Found     | 24.602301  | 118.011002 |
| 3  | 162.14.2.130    | 443  | https    | nginx              | ChinaTelecom   | Beijing   | 交建通           | 39.938884  | 116.397459 |
| 4  | 58.23.4.165     | 993  | imap     | Coremail mail      | ChinaUnicom    | Xiamen    | 24.602301     | 118.011002 |            |
| 5  | 39.96.8.8       | 443  | https    | Apache httpd       | ALIYUN         | Beijing   | 404 Not Found | 39.938884  | 116.397459 |
| 6  | 18.156.25.189   | 443  | https    | Apache httpd       | amazon.com     | Frankfurt | 50.11208      | 8.68341    |            |
| 7  | 62.234.4.195    | 443  | https    | nginx              | ChinaTelecom   | Beijing   | 专家库用户PC端      | 39.938884  | 116.397459 |
| 8  | 58.23.4.165     | 443  | https    | HAProxy http proxy | ChinaUnicom    | Xiamen    | 24.602301     | 118.011002 |            |
| 9  | 59.110.144.216  | 443  | https    | nginx              | ALIYUN         | Beijing   | 39.938884     | 116.397459 |            |
| 10 | 140.143.120.184 | 443  | https    | nginx              | ChinaTelecom   | Beijing   | 惠创新创新平台       | 39.938884  | 116.397459 |
| 11 | 220.160.194.243 | 443  | https    | nginx              | ChinaTelecom   | Xiamen    | 中交邮件系统        | 24.602301  | 118.011002 |
| 12 | 220.160.194.241 | 443  | https    | Apache httpd       | ChinaTelecom   | Xiamen    | 302 Found     | 24.602301  | 118.011002 |
| 13 | 220.160.194.240 | 443  | https    | Apache httpd       | ChinaTelecom   | Xiamen    | 302 Found     | 24.602301  | 118.011002 |
| 14 | 114.255.239.249 | 443  | https    | Apache httpd       | ChinaUnicom    | Beijing   | Error Page    | 39.938884  | 116.397459 |
| 15 | 58.87.171.52    | 443  | https    | nginx              | ChinaTelecom   | Beijing   | 交建通           | 39.938884  | 116.397459 |
| 16 | 122.155.237.91  | 443  | https    | Apache httpd       | cattelecom.com | Xiamen    | 15.391327     | 100.974161 |            |
| 17 | 58.23.4.161     | 443  | https    | Apache httpd       | ChinaUnicom    | Xiamen    | 中交门户登录页面      | 24.602301  | 118.011002 |
| 18 | 220.242.160.123 | 443  | https    | Apache httpd       | wangs.com      |           | 37.553674     | 126.991138 |            |
| 19 | 183.220.199.189 | 443  | https    | Apache httpd       | ChinaMobile    | Chengdu   | 30.658529     | 104.075546 |            |
| 20 | 58.23.4.136     | 443  | https    | Apache httpd       | ChinaUnicom    | Xiamen    | 中交注销页面        | 24.602301  | 118.011002 |


[13:19:41] [gather_zoomeye.py:246] [INFO]- Search information retrieval is completed
Kunyu (ZoomEye) >

```

关联域名/子域名搜索

对关联域名以及子域名进行搜索，默认查询关联域名，可以通过设置 dtype 参数设置两种模式。

Kunyu (ZoomEye) > SearchDomain ccccltd.cn
[13:26:10] search result amount: 44

gather_zoomeye.py:244

ID	Domain	IP	TimeStamp
1	zcps.ccccltd.cn	220.160.104.241	2021-06-27
2	ys.ccccltd.cn	58.23.4.162	2021-06-27
3	xmdnscte.ccccltd.cn	222.76.205.102	2021-06-27
4	www.uat.jjt.nimbleform.ccccltd.cn	58.87.90.15	2021-06-27
5	www.ccccltd.cn.lpzyxr.cn	47.91.170.222	2021-06-27
6	www.ccccltd.cn.ayxxn.com	164.155.119.111	2021-06-27
7	uat.jjt.nimbleform.ccccltd.cn	58.87.90.15	2021-06-27
8	tunnel.ccccltd.cn	220.160.104.241	2021-06-27
9	templates.uat.jjt.nimbleform.ccccltd.cn	58.87.90.15	2021-06-27
10	sso.ccccltd.cn	220.160.104.240	2021-06-27
11	portal.ccccltd.cn.cdn20.com	157.185.175.151	2021-06-26
12	pdaa.ccccltd.cn.cdn20.com	157.185.175.151	2021-06-26
13	newvnp.ccccltd.cn.cdn20.com	157.185.161.78	2021-06-26
14	mx-ccccltd-cn.icoremail.net	52.246.167.191	2021-06-26
15	mx-ccccltd-cn.icoremail.net	40.76.198.186	2021-06-26
16	msag.ccccltd.cn	220.160.104.241	2021-06-26
17	mail.eyou.ccccltd.cn	118.26.10.254	2021-06-26
18	lzb.ccccltd.cn.ogslb.com	220.160.104.241	2021-06-25
19	live.jjt.ccccltd.cn	58.87.99.95	2021-06-25
20	jjt.nimbleform.ccccltd.cn	140.143.153.163	2021-06-25
21	jjt.ccccltd.cn	140.143.179.47	2021-06-25
22	jjt.collegetest.ccccltd.cn	58.87.101.209	2021-06-25
23	hseq.ccccltd.cn	220.160.104.241	2021-06-25
24	hr.ccccltd.cn	220.160.104.241	2021-06-25
25	empm.ccccltd.cn	220.160.104.241	2021-06-25
26	ecp.ccccltd.cn	220.160.104.241	2021-06-25
27	dnscte.ccccltd.cn	219.141.246.126	2021-06-25
28	dnsncn.ccccltd.cn	114.255.239.106	2021-06-25
29	cwglkjxt.ccccltd.cn.ogslb.com	220.160.104.241	2021-06-25
30	cxtj.ccccltd.cn	10.1.11.36	2021-06-25

[13:26:10] [gather_zoomeye.py:246] [INFO]- Search information retrieval is completed

Kunyu (ZoomEye) >

Seebug漏洞查询

这里就比较简单了，通过输入想要查找的框架、设备等信息，查询历史相关漏洞，这里后期会进行改进，升级。

Kunyu (ZoomEye) > Seebug thinkphp
Number of relevant vulnerabilities: 35

[ThinkPHP Ubb标签 读取任意内容] - [89437]
[ThinkPHP web框架 php代码任意执行漏洞] - [60054]
[ThinkPHP v3.1-3.2 Driver.class.php SQL注入漏洞] - [90846]
[ThinkPHP 模板常量__SELF__ XSS漏洞] - [91097]
[ThinkPHP 某处缺陷可造成sql注射] - [95693]
[ThinkPHP 设计缺陷导致逻辑漏洞造成密码找回绕过等问题] - [95094]
[看我如何调查放置后门之Thinkphp] - [95095]
[ThinkPHP 默认配置导致验证码暴力破解] - [95096]
[thinkphp 3.0 爆路径] - [95097]
[ThinkPHP最新版3.0RC1存在XSS漏洞] - [95098]
[ThinkPHP某处设计缺陷可导致getshell] - [95099]
[ThinkPHP一处过滤不当造成SQL注入漏洞] - [95100]
[ThinkPHP一处XSS漏洞 (需要特定环境触发)] - [95101]
[从ThinkPHP谈基于框架开发程序的安全性二 (有开源程序实例)] - [95102]
[从ThinkPHP谈某干框架开发程序的安全性 (从SQL注入到代码执行)] - [95103]
[ThinkPHP架构设计不合理导致SQL注入] - [95104]
[ThinkPHP框架架构上存在SQL注入] - [95105]
[ThinkPHP补丁修复不当导致SQL注入] - [95106]
[OneThink内容管理框架网存储型XSS攻击] - [95107]
[ThinkPHP官网存储型XSS] - [95108]
[ThinkPHP3.2模版对字符过滤不严格造成框架崩溃 (远程拒绝服务)] - [95109]
[ThinkPHP远程代码执行隐患 (需满足特定条件)] - [95110]
[ThinkPHP官网xss和csrf漏洞 (删除指定文章)] - [95111]
[ThinkPHP存储型XSS漏洞一枚] - [95112]
[Thinkphp官方网站存储型XSS漏洞一枚] - [95113]
[ThinkPHP官网XSS漏洞] - [95114]
[ThinkPHP5.0.10-3.2.3缓存函数设计缺陷可导致Getshell] - [96340]
[ThinkPHP框架特性引发的SQL注入漏洞] - [95115]
[ThinkPHP3.2.3最新版update注入漏洞] - [97234]
[ThinkPHP3.2 框架sql注入漏洞] - [97511]
[ThinkPHP 3.X/X order by注入漏洞] - [97512]
[Thinkphp5控制器名过滤不严导致getshell] - [97715]
[Thinkphp 5.0.x 远程代码执行漏洞] - [97767]
[thinkphp6任意文件创建与删除漏洞] - [98124]
[ThinkPHP5 SQL注入漏洞 && 敏感信息泄露] - [98289]

[13:32:19] [gather_zoomeye.py:308] [INFO]- Seebug Search retrieval is completed

Kunyu (ZoomEye) >

数据结果

大家可能好奇查询的数据呢？都保存在项目下 OUTPUT 目录里啦，根据时间戳创建目录，单次启动的所有查询结果都在一个目录下。

A	B	C	D	E	F	G	H	I	
1	ID	IP	URL	Title	OS	WebApp	DB	Language	Server
2	1	104.216.173.21	999515.com.com	合总论坛_香港马会平特一	Windows	DedeCMS	MySQL	ASP	Microsoft IIS httpd
3	2	120.26.40.146	m.nbmylike.com	宁波整形医院嘲	Windows	DedeCMS	MySQL	ASP	Microsoft IIS httpd
4	3	113.105.191.213	a06k0.bizvi.cn	全网合一-分销系统,品	Windows	DedeCMS	MySQL	PHP	Nginx
5	4	107.187.127.186	ltqwyb.com	ltqwyb.com	Windows	DedeCMS	MySQL	PHP	Nginx
6	5	154.23.21.18	lylygy.com	lylygy.com	Windows	DedeCMS	MySQL	PHP	Nginx
7	6	154.198.202.196	m.szxfw.com	册,光荣总代理-GOG光	Windows	DedeCMS	MySQL	PHP	Apache httpd
8	7	108.187.83.104	lyquanxi.com	lyquanxi.com	Windows	DedeCMS	MySQL	PHP	Nginx
9	8	154.210.232.170	a1709.cn	a1709.cn	Windows	DedeCMS	MySQL	PHP	Nginx
10	9	166.88.150.134	m56165.com	m56165.com	Windows	DedeCMS	MySQL	PHP	Nginx
11	10	154.221.135.29	91ip.com	91ip.com	Windows	DedeCMS	MySQL	PHP	Nginx
12	11	156.229.160.110	998sq.com	998sq.com	Windows	DedeCMS	MySQL	PHP	Nginx
13	12	107.149.86.123	9da5.com	9da5.com	Windows	DedeCMS	MySQL	PHP	Nginx
14	13	122.114.8.167	lzykk.com	设计,装修施工,房屋局	Windows	DedeCMS	MySQL	PHP	Apache httpd
15	14	107.164.246.145	984x.com	984x.com	Windows	DedeCMS	MySQL	PHP	Nginx
16	15	107.149.169.118	9youcp.com	9youcp.com	Windows	DedeCMS	MySQL	PHP	Nginx
17	16	113.105.191.213	97d79.bizyi.cn	素,全网合一-分销系统,品	Windows	DedeCMS	MySQL	PHP	Nginx
18	17	47.92.174.227	m.shuibiaoji.com	厂_智能手表 远传水表 j	Windows	DedeCMS	MySQL	PHP	Nginx
19	18	154.221.180.169	977404.com	977404.com	Windows	DedeCMS	MySQL	PHP	Nginx
20	19	59.110.61.187	m.haiko.com.cn	301 Moved Permanently	Windows	DedeCMS	MySQL	PHP	Apache httpd
21	20	104.164.170.153	95464867.xyz	95464867.xyz	Windows	DedeCMS	MySQL	PHP	Nginx
22									
23									
24									
25									
26									
27									
28									
29									
30									

后记

其实还有很多的思路，但是作为 Alpha 版本先这样，后期会不断进行完善的，希望 Kunyu (坤舆)能够让更多安全从业者所知，谢谢各位的支持。

工具框架有参考昆仑镜、Pocsuite3，都是非常棒的作品。

感谢 Knowsec 404 Team 的全体小伙伴。