

fofa使用

记录的比较零碎，统一起来。内容来自自己笔记与互联网搜索。侵权删倒是谈不上，自己总结的，大家能用上就看看，用不上就用不上，懂的人都懂。从fofa使用说明里面自己看的总结。免费公开，能在工作中用得上，特别是护网中能快速定位自己资产一共一条思路也是很有用的。

---by 大概没有名字

过两天再发土司哈哈哈哈

一、检索HTML源代码

0、在url中找关键字

[host=".gov.cn"](#)

结果如图



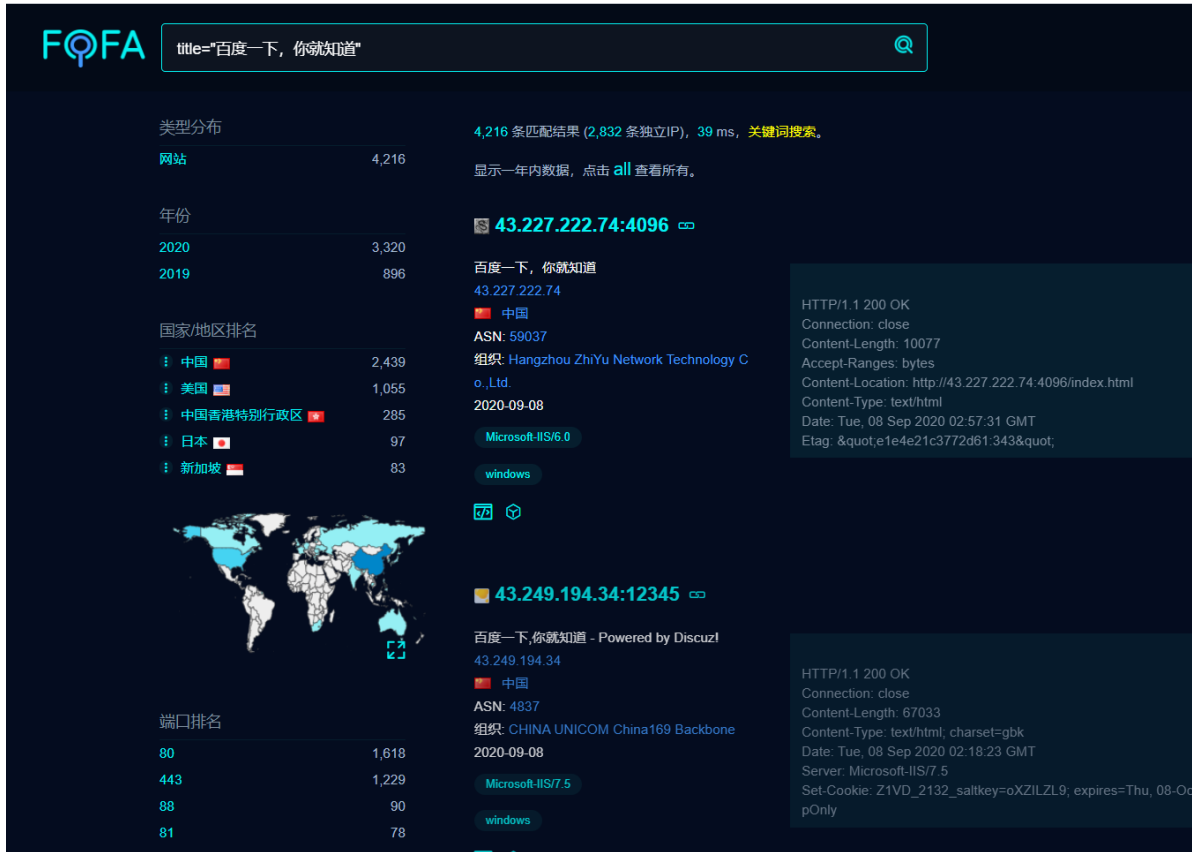
搜索的记过是url中有的，类似于google中搜索的 "inurl:index.html"

1、title标签检索：

在两个title标签之间的文字。支持关键字搜索。很好用

```
1 <!DOCTYPE html><!--STATUS OK-->
2
3 <html><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge, chrome=1"><meta
content="always" name="referrer"><meta name="theme-color" content="#2932e1"><meta name="description" content="全球最大的中文搜索引擎，致力于让网民更便捷地获取信
息，找到所求。百度超过千亿的中文网页数据库，可以瞬间找到相关的搜索结果。"><link rel="shortcut icon" href="/favicon.ico" type="image/x-icon" /><link rel="search"
type="application/opensearchdescription+xml" href="/content-search.xml" title="百度搜索" /><link rel="icon" sizes="any" mask
href="/www.baidu.com/img/baidu_85beaf5496f291521eb75ba38a9cd87.svg"><link rel="dns-prefetch" href="//ds0.bdstatic.com"/><link rel="dns-prefetch"
href="//dss1.bdstatic.com"/><link rel="dns-prefetch" href="//ssl.bdstatic.com"/><link rel="dns-prefetch" href="//sp0.baidu.com"/><link rel="dns-prefetch"
href="//sp1.baidu.com"/><link rel="dns-prefetch" href="//sp2.baidu.com"/><title>百度一下，你就知道</title>
4 <style index="new" type="text/css">#form_bdsug{top:39px}.bdsug{display:none;position:absolute;width:535px;background:#fff;border:1px solid
#ccc!important;overflow:hidden;box-shadow:1px 1px 3px #deded;-webkit-box-shadow:1px 1px 3px #deded;-moz-box-shadow:1px 1px 3px #deded;-o-box-shadow:1px 1px
3px #deded}.bdsug li{width:519px;color:#000;font:14px arial;line-height:25px;padding:0 8px;position:relative;cursor:default}.bdsug li.bdsug-
s{background:#f0f0f0}.bdsug-store span,.bdsug-store b{color:#7a77c8}.bdsug-store-del{font-size:12px;color:#666;text-
decoration:underline;position:absolute:right:8px;top:0;cursor:pointer;display:none}.bdsug-s .bdsug-store-del{display:inline-block}.bdsug-ala{display:inline-
block;border-bottom:1px solid #e6e6e6}.bdsug-ala h3{line-height:14px;background:url(/www.baidu.com/img/sug_bd.png?v=09816787.png) no-repeat left
center;margin:6px 0 4px;font-size:12px;font-weight:400;color:#7b7b7b;padding-left:20px}.bdsug-ala a{font-size:14px;font-weight:700;padding-left:20px}#m .bdsug
```

直接fofa搜索 title="百度一下，你就知道"
title="学院" 你懂的~~~



S

2、cert证书信息检索

cert:xxxxxx
cert="google" 搜索证书(https或者imaps等)中带有google的资产。
cert="chinamobile" 搜索证书(https或者imaps等)中带有中国移动的资产。

3、找body特征信息：

例如：

burp代理 body="welcome to Burp Suite"
找目录遍历漏洞 body="Directory"
目录遍历漏洞，这个是找美国地区ubuntu系统的 body="Directory listing" && country="US" && title="Index of /" && os="ubuntu"
body="miningcore-ui"
#在特殊的页面的特使body

4、http的header中搜索

```
从http头中搜索“jboss”  
header="jboss"
```

5、服务器状态码

```
status_code="200"
```

6、icon搜索

能够直接搜索图片。秀！

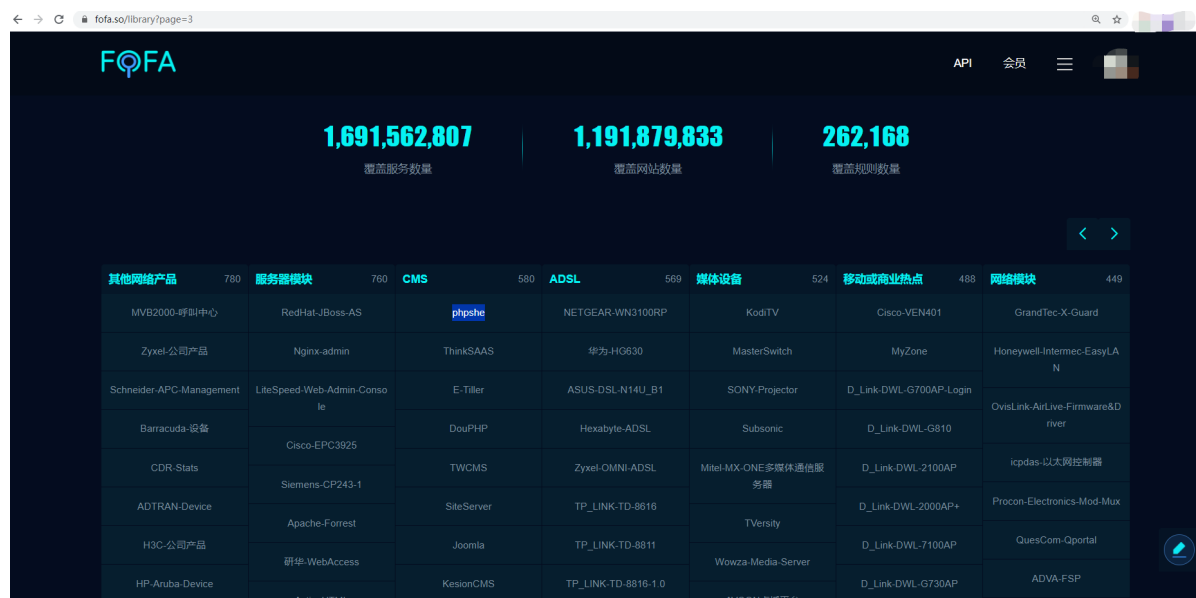
7、搜索使用的数据库

```
protocol=redis
```

8、搜索使用的中间件或者其他应用

```
app="Apache-Tomcat"  
app="RedHat-JBoss-AS"  
app="通达OA"  
server=="Microsoft-IIS/7.5"  
等等，参照链接https://fofa.so/library 有很多。
```

查询搜索参考：<https://fofa.so/library>



The screenshot shows the FOFA search engine interface. At the top, there are three large statistics: 1,691,562,807 covered services, 1,191,879,833 covered websites, and 262,168 covered rules. Below these is a table with 8 columns: 其他网络产品 (780), 服务器模块 (760), CMS (580), ADSL (569), 媒体设备 (524), 移动或商业热点 (488), and 网络模块 (449). The table lists various discovered assets such as MVB2000-呼叫中心, RedHat-JBoss-AS, ThinkSAAS, NETGEAR-WN3100RP, KodiTV, Cisco-VEN401, GrandTec-X-Guard, Zyxel-公司产品, Nginx-admin, ThinkSAAS, 华为-HG630, MasterSwitch, MyZone, Honeywell-Intermec-EasyLAN, Schneider-APC-Management, LiteSpeed-Web-Admin-Console, E-Tiller, ASUS-DSL-N14U-B1, SONY-Projector, D_Link-DWL-G700AP-Login, OvisLink-AirLive-Firmware&Driver, Barracuda-设备, Cisco-EPC3925, DouPHP, Hexabyte-ADSL, Subsonic, D_Link-DWL-G810, icpdas-以太网控制器, CDR-Stats, Siemens-CP243-1, TWCMS, Zyxel-OMNI-ADSL, Mitel-MX-ONE多媒体通信服务器, D_Link-DWL-2100AP, Procon-Electronics-Mod-Mux, ADTRAN-Device, Apache-Forrest, SiteServer, TP_LINK-TD-8816, T-Versity, D_Link-DWL-2000AP+, QuesCom-Qportal, H3C-公司产品, 研华-WebAccess, Joomla, TP_LINK-TD-8811, Wowza-Media-Server, D_Link-DWL-7100AP, ADVA-FSP, HP-Aruba-Device, KesionCMS, TP_LINK-TD-8816-1.0, and D_Link-DWL-G730AP.

其他网络产品	服务器模块	CMS	ADSL	媒体设备	移动或商业热点	网络模块
MVB2000-呼叫中心	RedHat-JBoss-AS	ThinkSAAS	NETGEAR-WN3100RP	KodiTV	Cisco-VEN401	GrandTec-X-Guard
Zyxel-公司产品	Nginx-admin	ThinkSAAS	华为-HG630	MasterSwitch	MyZone	Honeywell-Intermec-EasyLAN
Schneider-APC-Management	LiteSpeed-Web-Admin-Console	E-Tiller	ASUS-DSL-N14U-B1	SONY-Projector	D_Link-DWL-G700AP-Login	OvisLink-AirLive-Firmware&Driver
Barracuda-设备	Cisco-EPC3925	DouPHP	Hexabyte-ADSL	Subsonic	D_Link-DWL-G810	icpdas-以太网控制器
CDR-Stats	Siemens-CP243-1	TWCMS	ZyXel-OMNI-ADSL	Mitel-MX-ONE多媒体通信服务器	D_Link-DWL-2100AP	Procon-Electronics-Mod-Mux
ADTRAN-Device	Apache-Forrest	SiteServer	TP_LINK-TD-8816	T-Versity	D_Link-DWL-2000AP+	QuesCom-Qportal
H3C-公司产品	研华-WebAccess	Joomla	TP_LINK-TD-8811	Wowza-Media-Server	D_Link-DWL-7100AP	ADVA-FSP
HP-Aruba-Device	KesionCMS	TP_LINK-TD-8816-1.0	D_Link-DWL-G730AP			

```
app="通达OA" && title="2017"
```

9、搜索子域

```
domain="baidu.com"  
搜索相关的子域
```

二、资产搜索

搜索IP或者C段

```
ip="192.168.1.1"  
C段 192.168.1.1/24  B段 /16  A段 /8  
直接就能够查询开放端口
```

三、联合搜索高级用法

或

```
(title="中国移动" || title="中国联通" || title="中国电信") && body="后台" &&  
status_code=200
```

这个是搜索国内运营商的关于后台可访问的页面，后台可以更换成平台等关键词。