**f ofa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"](https://fofa.so/result?qbase64=aG9zdD0iLmdvdi5jbiI%3D)

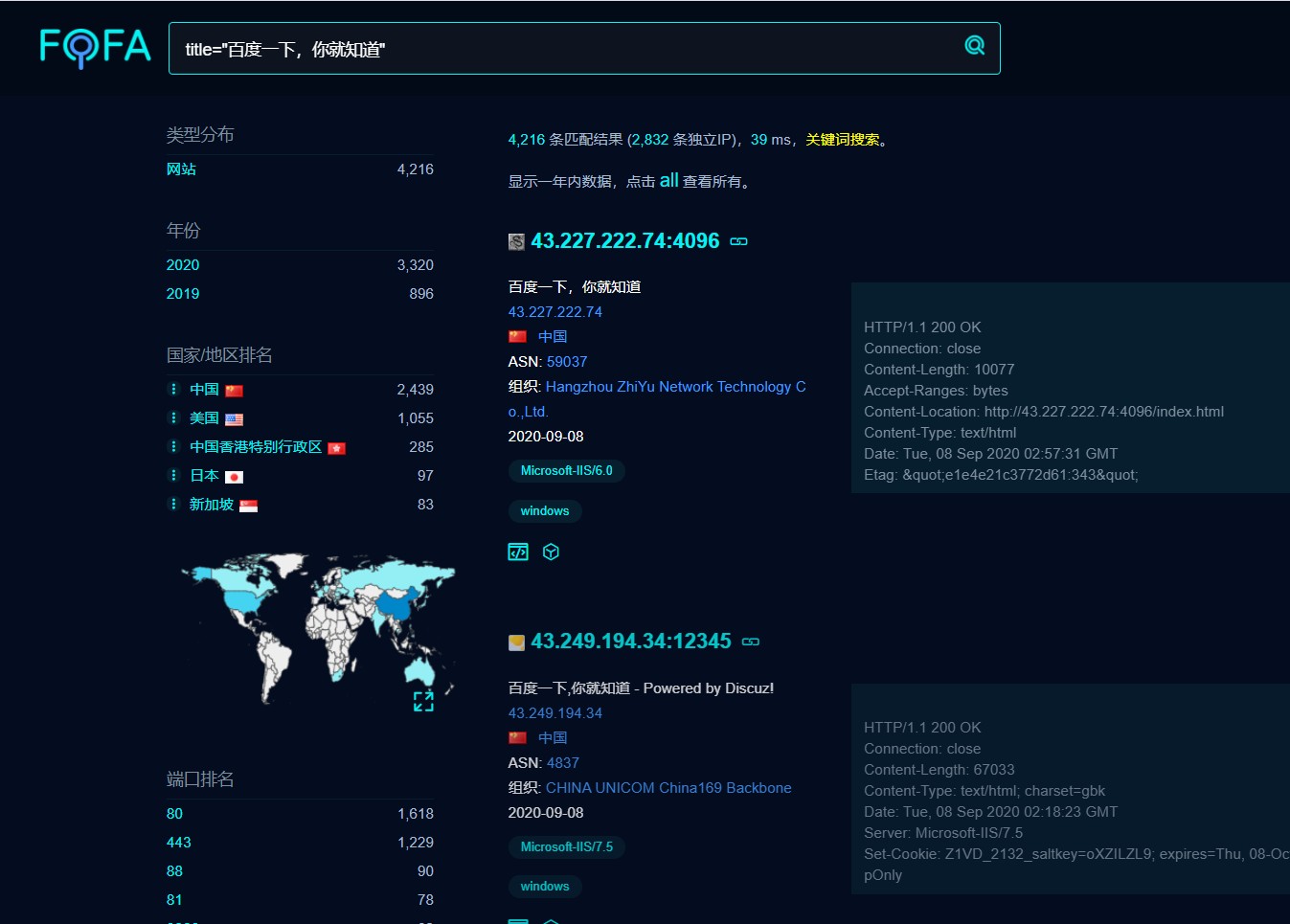
结果如图

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





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

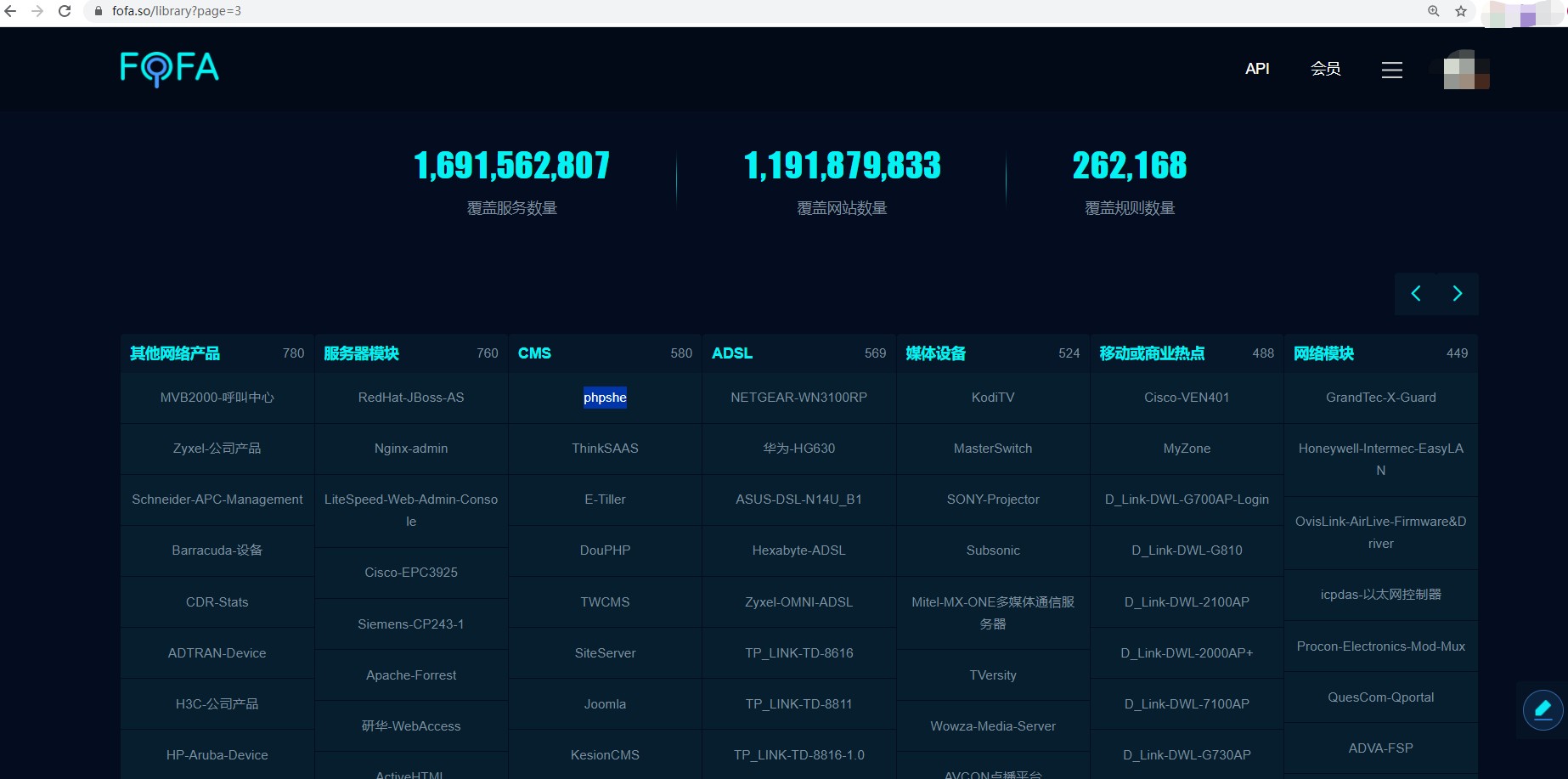
protocol=redis

**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>

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。