
Github

语法

限定词	案例
in:name	`in:name python` 查出仓库名中有 python 的项目（python in:name 也是一样的）
in:description	`in:name,description python` 查出仓库名或者项目描述中有 python 的项目
in:readme	`in:readme python` 查出 `readme.md` 文件里有 python 的项目
repo:owner/name	`repo:octocat/hello-world` 查出 octocat 的 hello-world 项目（指定了某个人的某个项目）
user:USERNAME	`user:1335951413 stars:<10` 查出用户 1335951413 名下 stars 少于 10 的项目
org:ORGNAME	`org:github` 查出 github 名下的项目
stars:n	`stars:>=5` 查出 star数大于等于 5 个 的项目（支持大于小于区间等）
pushed:YYYY-MM-DD	`css pushed:>2013-02-01` 查出仓库中包含 css 关键字，并且在 2013年1月 之后更新过的项目
language:LANGUAGE	`rails language:javascript` 查出仓库包含 rails 关键字，并且使用 javscript 语言的项目
created:YYYY-MM-DD	`webos created:<2011-01-01` 查出仓库中包含 webos 关键字并且是在 2011 年之前创建的项目（也支持时分秒，支持大于小于区间等）
followers:n	`followers:1000` 查出有 1000 个拥护者（followers） 的项目（支持大于小于区间等）
forks:n	`forks:5` 查出有 5 个 forks 的项目（支持大于小于区间等）
filename:n	`filename:xxx.txt` 查找xxx.txt文件
topic:TOPIC	`topic:jekyll` 查出含有 jekyll 这个 topic 的项目（项目描述下面的东西，相当于标签、分类）
topics:n	`topics:>5` 查出有 5 个以上 topic 的项目（支持大于小于区间等）
archived:true/false	`archived:true GNOME` 查出已经封存了并且含有 GNOME 关键字的项目（已经不再维护了的项目）
license:LICENSE_KEYWORD	`license:apache-2.0` 查出仓库的开源协议是 apache-2.0 的
size:n	`size:1000` 查出仓库大小等于 1MB 的项目
size:n	`size:>=30000` 查出仓库大小至少大于 30MB 的项目
size:n	`size:50..120` 查出仓库大小在 50KB 至 120KB 之间的项目
is:public/private	`is:public org:github` 查出仓库所有组织是 github 并且公开的项目

限定词	案例
is:public/private	`is:private github` 查出含有 github 关键字并且是私有的项目（私有的别人看不到，所以这个是用来搜索自己的私有项目的）

> 项目名字(name)里有 python 的

```
in:name python
```

> 名字(name)里有 python 的并且 stars 大于 3000 的

```
in:name python starts:>3000
```

> 名字(name)里有 python 的并且 stars 大于 3000 、forks 大于 200 的

```
in:name python starts:>3000 forks:>200
```

> 详情(readme)里面有 python 的并且 stars 大于 3000 的

```
in:readme python starts:>3000
```

> 描述(description)里面有 python 的并且 stars 大于 3000 的

```
in:description python starts:>3000
```

> 描述(description)里面有 python 的并且是 python 语言的

```
in:description python language:python
```

> 描述(description)里面有 python 的并且 2019-12-20 号之后有更新过的

```
in:description python pushed:>2019-12-20
```

例子

- 敏感信息

  ```
  create user identified by
  create user zabbix@'%' identified by
  各单位
  XX市XX局版权所有
  技术支持：xxxx公司
  去github上搜开发公司的客服电话
  密码
  源码
  ```

- 交流

```
内部
钉钉群
企微群
```

Google

语法

```
site：可以限制你搜索范围的域名；可用于收集子域名
inurl：用于搜索网页上包含的URL，这个语法对寻找网页上的搜索，帮助之类的很有用；
intext： 只搜索网页<body>部分中包含的文字(也就是忽略了标题、URL等的文字)；
filetype：搜索文件的后缀或者扩展名；
intitle：限制你搜索的网页标题；
```

- 包含关键字: `intitle:关键字`
- 包含多个关键字: `allintitle:关键字 关键字2`
- url中包含关键字： `inurl：关键字`
- 搜索特定类型的文件: `关键字 filetype:扩展名` ,例如 `人类简史 filetype:pdf`
- 搜索特定网站的内容: `关键字 site:网址`
- 排除不想要的结果: `关键字 -排查条件` ,例如搜索 "运动相机",但只想看 GoPro 品牌以外的产品 `运动相机 -GoPro`
- 双引号的用处:例如: `"how to write a code"` 如果没有引号,搜索的大部分结果是以 `write code` 为关键字.包含引号后,会确保将完整的字符串做为期望的检索结果提交给搜索引擎.
- 搜索缓存: `cache: 后缀` ， 如： `cache: regontool.org`

语法合集

- Google Hacking Database
- K0rz3n/GoogleHacking-Page
- BullsEye0/google_dork_list

dork工具

- dwisiswant0/go-dork - Go 语言编写的快速 Dork 扫描仪。

例子

常用

```
site:*.site.com -www
site:*.*.site.com -www
site:*.*.*.site.com -www

inurl:tw
inurl:jp

inurl:editor/db/
inurl:eWebEditor/db/
inurl:bbs/data/
inurl:databackup/
inurl:blog/data/
inurl:\boke\data
```

```
inurl:bbs/database/
inurl:conn.asp
inc/conn.asp
Server.mapPath(".mdb")
allinurl:bbs data
filetype:mdb inurl:database
filetype:inc conn
inurl:data filetype:mdb
intitle:"index of" data

intitle:"index of" etc
intitle:"Index of" .sh_history
intitle:"Index of" .bash_history
intitle:"index of" passwd
intitle:"index of" people.lst
intitle:"index of" pwd.db
intitle:"index of" etc/shadow
intitle:"index of" spwd
intitle:"index of" master.passwd
intitle:"index of" htpasswd
inurl:service.pwd
```

漏洞

```
目录遍历漏洞
    site:xxx.com intitle:index.of
    site:xxx.com intitle:转到父目录

配置文件泄露
    site:xxx.com ext:xml | ext:conf | ext:cnf | ext:reg | ext:inf | ext:rdp |
ext:cfg | ext:txt | extra | ext:ini

数据库文件泄露
    site:xxx.com ext:sql | ext:dbf | ext:mdb

日志文件泄露
    site:xxx.com ext:log

备份和历史文件
    site:xxx.com ext:bkf | ext:bkp | ext:bak | extld | ext:backup

SQL错误
    site:xxx.com intext:"sql syntax near" | intext:"syntax error has occurred" |
intext:"incorrect syntax near" | intext:"unexpected end of SQL command" |
intext:"Warning: mysql_connect()" | intext:"Warning: mysql_query()" |
intext:"Warning: pg_connect()"

公开文件信息
    site:xxx.com ext:doc | ext:docx | extdt | ext:pdf | ext:rtf | ext:sxw |
ext:psw | ext:ppt | ext:pptx | ext:pps | ext:csv

phpinfo()
    site:xxx.com ext:php intitle:phpinfo "published by the PHP Group"

JIRA
    配置错误的 JIRA 设置  inurl:/UserPickerBrowser.jspa -intitle:Login -intitle:Log
```

```
    此查询列出了其 URI 中具有"UserPickerBrowser"的所有 URL,以查找公开而且不需要经过身份验证的所有配置错误的 JIRA 用户选择器功能.

    inurl:/ManageFilters.jspa?filterView=popular AND ( intext:All users OR intext:Shared with the public OR intext:Public )
    此查询列出了所有在其 URI 中具有"Managefilters"并且文本为"Public"的 URL,以便找到所有公开暴露且未经过身份验证的错误配置的 JIRA 过滤器.

    inurl:/ConfigurePortalPages!default.jspa?view=popular
    此查询列出其 URI 中具有"ConfigurePortalPages"的所有 URL,以查找公开公开的所有 JIRA 仪表板.
```

搜参数/接口

```
inurl:.php?id=xx 公司
inurl:.asp?id=xx 公司
inurl:.jsp?id=xx 公司
inurl:.php?id=xx 公司 陕西
（可以用来找sql注入漏洞）
```

找文章

```
inurl:csdn.net CVE-2019-3403
inurl:51cto.com VRRP
inurl:habr.com powershell
inurl:exploit-db.com docker
```

Shodan

语法

官网

- https://www.shodan.io

搜索语法合集

- Shodan Pentesting Guide

- jakejarvis/awesome-shodan-queries
- Shodan的http.favicon.hash语法详解与使用技巧

常用语法

```
hostname:搜索指定的主机或域名,例如 hostname:"google"
port:搜索指定的端口或服务,例如 port:"21"
country:搜索指定的国家,例如 country:"CN"
city:搜索指定的城市,例如 city:"Hefei"
org:搜索指定的组织或公司,例如 org:"google"
isp:搜索指定的 ISP 供应商,例如 isp:"China Telecom"
product:搜索指定的操作系统/软件/平台,例如 product:"Apache httpd"
version:搜索指定的软件版本,例如 version:"1.6.2"
geo:搜索指定的地理位置,参数为经纬度,例如 geo:"31.8639, 117.2808"
before/after:搜索指定收录时间前后的数据,格式为 dd-mm-yy,例如 before:"11-11-15"
net:搜索指定的 IP 地址或子网,例如 net:"210.45.240.0/24"
```

例子

```
# 友情提醒,请遵纪守法
misc
Server: uc-httpd 1.0.0 200 OK Country:"JP"
h3c net:"xxx.xxx.xxx.xxx/24"
country:US vuln:CVE-2014-0160
port:135,139,445 -hash:0                          # 过滤一些主文本标题为空的搜索结果
Hikvision-Webs                                    # 海康威视
title=“后台管理”
http.title:"后台管理"

database
all:"mongodb server information" all:"metrics"  # 开放 Mongodb 数据库
port:27017 -all:"partially" all:"fs.files"      # 有点存货的 Mongodb 数据库
port:"9200" all:"elastic indices"               # 开放 ElasticSearch 数据库

ftp
230 'anonymous@' login ok                         # 开放匿名ftp

vnc
port:5900 screenshot.label:loggedin               # 无认证vnc

rtsp
port:554 has_screenshot:true                      # rtsp 未授权访问

docker
port:"2375" country:"JP" Docker                   # docker-remote-api未授权

ICS
module: s7 port:102                               # S7设备
```

工具/脚本

- **Shodan cli**
  - Shodan Command-Line Interface
- **浏览器插件**
  - chrome插件
  - firefox插件
- **Metasploit**

```
use auxiliary/gather/shodan_search
```

```
set SHODAN_APIKEY ********************
set QUERY ****

use auxiliary/gather/shodan_honeyscore  # 蜜罐检测
set SHODAN_APIKEY ********************
set TARGET your_target

Recon-ng
keys add shodan_api ********************
use recon/domains-hosts/shodan_hostname
show options
set SOURCE google
set LIMIT 1
```

- **脚本**
  - random-robbie/My-Shodan-Scripts
  - woj-ciech/LeakLooker - 利用 shodan 寻找开放的数据库/服务

Censys

> Censys 搜索引擎能够扫描整个互联网，Censys 每天都会扫描 IPv4 地址空间，以搜索所有联网设备并收集相关的信息，并返回一份有关资源（如设备、网站和证书）配置和部署信息的总体报告。

官网

- https://www.censys.io

例子

```
23.0.0.0/8 or 8.8.8.0/24                    # 可以使用 and or not
80.http.get.status_code: 200                # 指定状态
80.http.get.status_code:[200 TO 300]        # 200-300之间的状态码
location.country_code: DE                   # 国家
protocols: ("23/telnet" or "21/ftp")        # 协议
tags: scada                                 # 标签
80.http.get.headers.server:nginx            # 服务器类型版本
autonomous_system.description: University   # 系统描述
```

同类搜索引擎

- Spyse - 扫描完整的数字证书数据库，获取 TLS 和 SSL 证书的相关数据。
- crt.sh - 证书搜索
- Google Transparency Report - Google监控的证书透明日志

Zoomeye

> ZoomEye 是北京知道创宇公司发布的网络空间侦测引擎，积累了丰富的网络扫描与组件识别经验。在此网络空间侦测引擎的基础上，结合“知道创宇”漏洞发现检测技术和大数据情报分析能力，研制出网络空间雷达系统，为政府、企事业及军工单位客户建设全球网络空间测绘提供技术支持及产品支撑。

官网

- https://www.zoomeye.org/

相关工具

- knownsec/ZoomEye-python

语法

```
指定搜索的组件：
    app：组件名称
    ver：组件版本
    例：搜索 apache组件版本2.4：app:apache ver:2.4
指定搜索的端口：
    port:22
指定搜索的操作系统：
    OS:Linux
指定搜索的服务：
    service：服务名称
    例：service：SSH
指定搜索的地理位置范围：
    country：国家名
    city:城市名
指定搜索的CIDR网段：
    cidr:网段
    例：CIDR：192.168.158.12/24
指定网站域名进行搜索：
    Site:网站域名
    例：site:www.baidu.com
指定主机名：
    Hostname:主机名
    例：hostname:zwl.cuit.edu.cn
指定设备名：
    device:设备名
    例：device:router
指定首页关键词：
    keyword:关键词
    例：keyword:technology
```

例子

```
city:tokyo + app:weblogic

port:102 +app:"Siemens S7 PLC"
"<title>信息中心 /</title>"
```

ZoomEye工控专题

- https://www.zoomeye.org/topic?id=ics_project

ZoomEye路由器专题

- https://www.zoomeye.org/project?id=router

其他一些专题：

https://www.zoomeye.org/topics

电力自动化专题

Git 平台专题

区块链专题

工控专题

认证专题

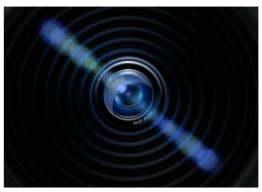
防火墙专题

路由器专题

打印机专题

WAF专题

DNS专题



摄像头专题

网络存储专题

FoFa

> FOFA 是白帽汇推出的一款网络空间搜索引擎，它通过进行网络空间测绘，能够帮助研究人员或者企业迅速进行网络资产匹配，例如进行漏洞影响范围分析、应用分布统计、应用流行度排名统计等。

相关文章

- 工具的使用 | 网络空间搜索引擎Fofa的简单使用
- 如何成为一个合格的FOFA工程师

相关工具

- FishM4n/Fofa-collect
- wgpsec/fofa_viewer

语法

```
title="abc"          # 从标题中搜索 abc.例:标题中有北京的网站.
header="abc"         # 从 http 头中搜索abc.例:jboss服务器.
body="abc"           # 从 html 正文中搜索abc.例:正文包含Hacked by.
domain="qq.com"      # 搜索根域名带有qq.com的网站.例: 根域名是qq.com的网站.
host=".gov.cn"       # 从 url 中搜索.gov.cn,注意搜索要用host作为名称.
port="443"           # 查找对应 443 端口的资产.例: 查找对应443端口的资产.
ip="1.1.1.1"         # 从ip中搜索包含 1.1.1.1 的网站,注意搜索要用ip作为名称.
protocol="https"     # 搜索制定协议类型(在开启端口扫描的情况下有效).例: 查询https协议资产.
city="Beijing"       # 搜索指定城市的资产.例: 搜索指定城市的资产.
region="Zhejiang"    # 搜索指定行政区的资产.例: 搜索指定行政区的资产.
country="CN"         # 搜索指定国家(编码)的资产.例: 搜索指定国家(编码)的资产.
cert="google.com"    # 搜索证书(https或者imaps等)中带有google.com的资产.
icon_hash="-xxxx"    # 搜索使用此icon的资产。
```

例子

```
title="powered by" && title!=discuz
title!="powered by" && body=discuz
(body="content=\"WordPress" || (header="X-Pingback" && header="/xmlrpc.php" &&
body="/wp-includes/") ) && host="gov.cn"

app="Solr" && title=="Solr Admin"   # 找 solr 服务
app="Coremail" &&  country=CN       # 查找使用 coremail 并且在中国境内的网站
title="管理后台" ||  title="登录后台"  # 查找 title 中含有管理后台或者登录后台的网站
port=”102” && protocol==”s7”        # 找 S7comm设备
```

Dnsdb

> 这是一个搜索全网络所有 DNS 服务器的搜索引擎。

官网

- https://www.dnsdb.io/

语法

```
DnsDB 查询语法结构为条件1 条件2 条件3 …., 每个条件以空格间隔, DnsDB 会把满足所有查询条件的结果返回给用户.

域名查询条件
查询语法为 `domain:.`
域名查询是指查询顶级私有域名所有的 DNS 记录,
例如查询 google.com 的所有 DNS 记录: `domain:google.com.`
域名查询可以省略 domain:.

主机查询条件
查询语法:`host:`
例如查询主机地址为 mp3.example.com 的 DNS 记录:`host:map3.example.com`
主机查询条件与域名查询查询条件的区别在于, 主机查询匹配的是 DNS 记录的 Host 值

按 DNS 记录类型查询
查询语法: `type:.`
例如只查询 A 记录: `type:a`
使用条件 : 必须存在 domain: 或者 host: 条件,才可以使用 type: 查询语法

按 IP 限制
查询语法: `ip:`
查询指定 IP: `ip:8.8.8.8` 该查询与直接输入 8.8.8.8 进行查询等效
查询指定 IP 范围: `ip:8.8.8.8-8.8.255.255`
CIDR: `ip:8.8.0.0/24`
IP 最大范围限制 65536 个
```

例子

查询 google.com 的所有 A 记录: `google.com type:a`

LeakIX

> 针对信息泄露的搜索引擎

官网

- https://leakix.net/

---

quake

> 360的空间测绘平台

- https://quake.360.cn/quake/

语法:

https://quake.360.cn/quake/#/help?id=5eb238f110d2e850d5c6aec8&title=%E6%A3%80%E7%B4%A2%E5%85%B3%E9%94%AE%E8%AF%8D

HUNTER

> 奇安信的空间测绘平台

- https://hunter.qianxin.com/

语法:

https://hunter.qianxin.com/home/helpCenter?r=2-2