# 二.信息收集语法

# 信息收集语法

## Google语法

### 一：常用语法：

1、intitle：搜索网页标题中包含有特定字符的网页。例如输入“intitle: cbi”，这样网页标题中带有cbi的网页都会被搜索出来。2、inurl：搜索包含有特定字符的URL。例如输入“inurl:cbi”，则可以找到带有cbi字符的URL。3、intext:搜索网页正文内容中的指定字符，例如输入“intext:cbi”。这个语法类似我们平时在某些网站中使用的“文章内容搜索”功能。4、Filetype:搜索指定类型的文件。例如输入“filetype:cbi”，将返回所有以cbi结尾的文件URL。5、Site：找到与指定网站有联系的URL。例如输入“Site：family.chinaok.com”。所有和这个网站有联系的URL都会被显示。

### 二：常见搜索

查找后台地址：site:域名 inurl:login|admin|manage|member|admin\_login|login\_admin|system|login|user|main|cms查找文本内容：site:域名 intext:管理|后台|登陆|用户名|密码|验证码|系统|帐号|admin|login|sys|managetem|password|username查找可注入点：site:域名 inurl:aspx|jsp|php|asp查找上传漏洞：site:域名 inurl:file|load|editor|Files查找eweb编辑器：site:域名 inurl:ewebeditor|editor|uploadfile|eweb|edit存在的数据库：site:域名 filetype:mdb|asp|#查看脚本类型：site:域名 filetype:asp/aspx/php/jsp迂回策略入侵：inurl:cms/data/templates/images/index/各种敏感数据收集：inurl:phpmyadmin/main.php intitle:phpmyadminfiletype:inc inurl:config.inc hostfiletype:txt inurl:"新建文本文档.txt"密码inurl:phpinfo.php intitle:“phpinfo()”“PHP Version”+“Server API”filetype:log inurl:log mdb

### 三：实例

site:github.com intext:bilibili.com intext:rootsite:baidu.com intitle:后台/管理 搜索百度标题为后台的界面site: baidu.com intext:用户 页面包含 用户intext:administrator intext:密码 filetype:txtintext:身份证 intext:手机号 intext:女 filetype:xls

### 四：利用

[利用”inurl：“或”allinurl：“寻找有漏洞的网站或服务器]a，利用”allinurl：winnt / system32 /“查询：列出的服务器上本来应该受限制的诸如“system32”等目录，如果你运气足够好，你会发现“system32”目录里的“cmd.exe”文件，并能执行他，接下来就是提升权限并攻克了b，查询“allinurl：wwwboard / passwd.txt”将列出所有有“WWWBoard密码漏洞”漏洞的服务器，阅读更多请参见下面链接.http：//[www.securiteam.com/exploits/2BUQ4S0SAW.html](http://www.securiteam.com/exploits/2BUQ4S0SAW.html)c ，查询“inurl：.bash\_history”将列出互联网上可以看见“inurl：.bash\_history”文件的服务器。这是一个命令历史文件，这个文件包含了管理员执行的命令，有时会包含一些敏感信息比如管理员键入的密码.d，查询“inurl：config.txt”将看见网上暴露了“inurl：config.txt”文件的服务器，这个文件包含了经过哈希编码的管理员的密码和数据库存取的关键词信息.e，还有一些其他一些使用“inurl：”和“allinurl：”查询组合的例子inurl：admin filetype：txtinurl：admin filetype：dbinurl：admin filetype：cfginurl：mysql filetype：cfginurl：passwd filetype：txtinurl：“wwwroot / \*。”inurl：adpassword.txtinurl：webeditor.phpinurl：file\_upload.php

# fofa语法

FoFA（Fingerprint of Attack）是一种基于信息收集的网络安全评估工具，可以用于发现网络漏洞和风险。其语句包含一系列关键词和语法规则，用于定制化的网络攻击目标筛选。

## FOFA搜索语法

主要分为检索字段以及运算符，所有的查询语句都是由这两种元素组成的。目前支持的检索字段包括：domain，host，ip，title，server，header，body，port，cert，country，city，os，appserver，middleware，language，tags，user\_tag等等，支持的逻辑运算符包括：= ，==，!= ，&&，||

## 常用命令

逻辑连接符  
   
= 匹配，=""时，可查询不存在字段或者值为空的情况。  
== 完全匹配，==""时，可查询存在且值为空的情况。  
&& 与   
|| 或者  
!= 不匹配，!=""时，可查询值为空的情况。  
\*= 模糊匹配，使用\*或者?进行搜索，比如banner\*="mys??" (个人版及以上可用)。  
() 确认查询优先级，括号内容优先级最高。  
   
   
title="beijing" 从标题中搜索“北京”  
   
header="elastic" 从http头中搜索“elastic”  
-  
body="网络空间测绘" 从html正文中搜索“网络空间测绘”  
-  
fid="sSXXGNUO2FefBTcCLIT/2Q==" 查找相同的网站指纹  
   
domain="qq.com" 搜索根域名带有qq.com的网站  
-  
icp="京ICP证030173号" 查找备案号为“京ICP证030173号”的网站  
   
js\_name="js/jquery.js" 查找网站正文中包含js/jquery.js的资产  
   
js\_md5="82ac3f14327a8b7ba49baa208d4eaa15" 查找js源码与之匹配的资产  
-  
cname="ap21.inst.siteforce.com" 查找cname为"ap21.inst.siteforce.com"的网站  
-  
cname\_domain="siteforce.com" 查找cname包含“siteforce.com”的网站  
-  
cloud\_name="Aliyundun" 通过云服务名称搜索资产  
-  
product="NGINX" 搜索此产品的资产  
   
category="服务" 搜索此产品分类的资产  
   
icon\_hash="-247388890" 搜索使用此 icon 的资产  
   
host=".gov.cn" 从url中搜索”.gov.cn”搜索要用host作为名称  
port="6379" 查找对应“6379”端口的资产  
-  
ip="1.1.1.1" 从ip中搜索包含“1.1.1.1”的网站搜索要用ip作为名称  
ip="220.181.111.1/24" 查询IP为“220.181.111.1”的C网段资产  
-  
status\_code="402" 查询服务器状态为“402”的资产  
   
protocol="quic" 查询quic协议资产  
   
country="CN" 搜索指定国家(编码)的资产  
-  
region="Xinjiang Uyghur Autonomous Region" 搜索指定行政区的资产  
-  
city="Ürümqi" 搜索指定城市的资产  
-  
cert="baidu" 搜索证书(https或者imaps等)中带有baidu的资产  
-  
cert.subject="Oracle Corporation" 搜索证书持有者是Oracle Corporation的资产  
-  
cert.issuer="DigiCert" 搜索证书颁发者为DigiCert Inc的资产  
-  
cert.is\_valid=true 验证证书是否有效，true有效，false无效  
   
cert.is\_match=true 证书和域名是否匹配；true匹配、false不匹配  
   
cert.is\_expired=false 证书是否过期；true过期、false未过期  
   
jarm="2ad...83e81" 搜索JARM指纹  
-  
banner="users" && protocol="ftp" 搜索FTP协议中带有users文本的资产  
-  
type="service" 搜索所有协议资产，支持subdomain和service两种  
   
os="centos" 搜索CentOS资产  
-  
server=="Microsoft-IIS/10" 搜索IIS 10服务器  
-  
app="Microsoft-Exchange" 搜索Microsoft-Exchange设备  
-  
after="2017" && before="2017-10-01" 时间范围段搜索  
-  
asn="19551" 搜索指定asn的资产  
-  
org="LLC Baxet" 搜索指定org(组织)的资产  
-  
base\_protocol="udp" 搜索指定udp协议的资产  
-  
   
is\_domain=true 搜索域名的资产,只接受true和false  
is\_cloud=true 筛选使用了云服务的资产  
-  
port\_size="6" 查询开放端口数量等于"6"的资产  
   
port\_size\_gt="6" 查询开放端口数量大于"6"的资产  
   
port\_size\_lt="12" 查询开放端口数量小于"12"的资产  
   
ip\_ports="80,161" 搜索同时开放80和161端口的ip  
ip\_country="CN" 搜索中国的ip资产  
ip\_region="Zhejiang" 搜索指定行政区的ip资产(以ip为单位的资产数据)  
   
ip\_city="Hangzhou" 搜索指定城市的ip资产(以ip为单位的资产数据)  
   
ip\_after="2021-03-18" 搜索2021-03-18以后的ip资产  
ip\_before="2019-09-09" 搜索2019-09-09以前的ip资产

以下是fofa的基本语句

<https://blog.csdn.net/weixin_44556964/article/details/130263348>

## 组合搜索语法

### 1.搜索所有暴露了RDP（远程桌面协议）的服务器。

以下是一个示例语句： protocol="rdp" && port="3389" 在这个语句中，我们使用了"protocol"关键词来筛选RDP协议，使用"port"关键词来筛选3389端口。这样可以找到所有开放了远程桌面功能的服务器，进行必要的安全评估和风险分析。

### 2、查找未授权访问漏洞：

title="401 Unauthorized" || title="403 Forbidden" || title="404 Not Found"

上述语法表示搜索所有返回“401 Unauthorized”、“403 Forbidden”或“404 Not Found”的页面，这些页面通常可能存在未授权访问漏洞。

### 3、查找弱口令漏洞：

title="401 Unauthorized" && body="input type=password" && status\_code=200  
   
方法二  
body="<input type=\"password\""

上述语法表示搜索所有返回“401 Unauthorized”的页面，并且包含HTML表单，表单中包含type=password的输入框，返回状态码为200的页面，这些页面通常可能存在弱口令漏洞。

### 4、查找文件上传漏洞：

title="Upload" && body="form enctype=multipart/form-data method=post"  
   
方法二：  
body="<form[^>]\*?enctype=\"multipart/form-data\"[^>]\*?>"

上述语法表示搜索所有包含“Upload”关键词的页面，并且包含enctype=multipart/form-data、method=post的HTML表单，这些页面通常可能存在文件上传漏洞。

### 5、查找CMS漏洞：

title="Powered by WordPress" || title="Powered by Joomla" || title="Powered by Drupal"

上述语法表示搜索所有返回“Powered by WordPress”、“Powered by Joomla”或“Powered by Drupal”的页面，这些页面通常可能存在相关CMS的漏洞。

### 6、查找Web漏洞

title="404 Not Found" || title="403 Forbidden" || title="401 Unauthorized" || title="500 Internal Server Error" || title="502 Bad Gateway" || title="503 Service Unavailable" || title="SQL Error" || title="ASP.NET Error"

上述语法表示搜索所有返回“404 Not Found”、“403 Forbidden”、“401 Unauthorized”、“500 Internal Server Error”、“502 Bad Gateway”、“503 Service Unavailable”、“SQL Error”或“ASP.NET Error”的页面，这些页面通常可能存在Web漏洞。

### 7、查找未加密的数据库：

title="phpMyAdmin" || title="MySQL" || title="phpPgAdmin" || title="PostgreSQL" || title="Microsoft SQL Server" && body="input type=password"

上述语法表示搜索所有返回“phpMyAdmin”、“MySQL”、“phpPgAdmin”、“PostgreSQL”或“Microsoft SQL Server”的页面，并且包含type=password的HTML表单，这些页面可能存在未加密的数据库。

### 8、查找存储型XSS漏洞：

body="textarea" && body="input type=text" && body="input type=password"

上述语法表示搜索所有包含HTML文本输入框和密码输入框的页面，并且包含textarea的HTML表单，这些页面可能存在存储型XSS漏洞。

### 9、查找常见漏洞指纹

title="404 Not Found" || title="403 Forbidden" || title="401 Unauthorized" || title="500 Internal Server Error" || title="502 Bad Gateway" || title="503 Service Unavailable" || title="SQL Error" || title="ASP.NET Error" || title="404" || title="Login - Powered by Discuz" || title="Login - Powered by UCenter" || title="Powered by DedeCMS" || title="Powered by PHPWind" || title="Powered by discuz" || title="Powered by phpMyAdmin" || title="Powered by phpwind" || title="Powered by vBulletin" || title="Powered by wordpress" || title="phpMyAdmin" || title="phpinfo" || title="Microsoft-IIS" || title="Joomla" || title="Drupal" || title="WordPress" || title="Apache Tomcat" || title="GlassFish Server" || title="nginx" || title="Oracle HTTP Server"

上述语法表示搜索包含常见漏洞指纹的页面，例如Web服务器和CMS名称、错误页面、phpinfo、phpMyAdmin等等。

### 10、查找远程命令执行漏洞：

body="<form method=&quot;post&quot; enctype=&quot;multipart/form-data&quot; action=&quot;\S\*/index.php&quot; name=&quot;form&quot; id=&quot;form&quot;>"

上述语法表示搜索包含特定HTML表单的页面，该表单通常存在远程命令执行漏洞。