

信息广度收集:

Whois信息

- 站长之家: <http://whois.chinaz.com>
 - 域名对应的邮箱;
 - 该邮箱注册的所有域名;
 - 企业CEO名称注册的域名;
- SRC: 安全应急响应中心(漏洞、情报) <https://security.alibaba.com>

一级域名

- 企查查: <https://www.qichacha.com>



- 天眼查: <https://www.tianyancha.com>



- 企业的工程师不一定比白帽子更了解企业自身的状况。

子域名

- OneForAll: <https://github.com/shmilylty/OneForAll>
- ksubdomain: <https://github.com/knownsec/ksubdomain>
- subDomainsBrute: <https://github.com/lijiejie/subDomainsBrute>
- Sublist3r: <https://github.com/aboul3la/Sublist3r>

- RappidDns: <https://rapiddns.io/subdomain> (在线)
- 查子域: <https://chaziyu.com/> (在线)
- 子域名挖掘机

旁站 (同IP网站)

一个服务器可以起多个web服务, 开不同的端口即可, 相当于一个IP映射给多个域名。

旁站的查询涉及到cdn的问题, 所以为了查询到准确的旁站信息, 我们需要找到目标的真实IP。

- 在线: <http://stool.chinaz.com/same>
- 在线: <https://site.ip138.com>

真实IP

- 全球ping: <http://tool.zhiduopc.com/ping>
- DNS检测: <https://tools.ipip.net/dns.php>
- Xcdn: <https://github.com/3xp10it/xcdn>
- 在线: <https://ipchaxun.com/>
- Ping.cn: <https://www.ping.cn/dns/>

端口+子目录

- Nmap: <https://nmap.org>
- masscan: <https://github.com/robertdavidgraham/masscan>
- Goby: <https://gobies.org/>
- 御剑: <https://github.com/foryujian/yujianportscan> 推荐在虚拟机里玩一玩

敏感信息

GoogleHack语法

<https://cn.bing.com/>

1、后台地址

- site:xxx.com 管理后台/登录/管理员/系统, 可以通过添加双引号增加精确度 sf-express.com
- site:xxx.com inurl:login/admin/system/manage

2、敏感文件

- site:xxx.com filetype:pdf/doc/xls/txt
- site:xxx.com filetype:log/sql/conf

3、测试环境

- site:xxx.com inurl:test/ceshi
- site:xxx.com intitle:后台/测试

4、邮箱/QQ/群

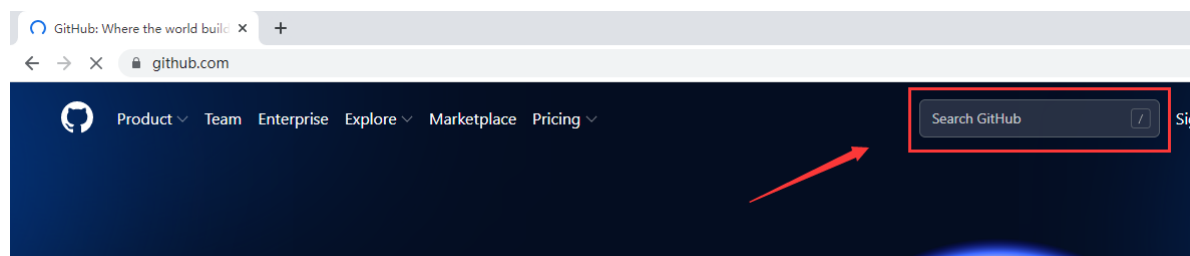
- site:xxx.com 邮件/email
- site:xxx.com qq/群/企鹅/腾讯
- site:xxx.com intitle:"Outlook Web App" 邮件服务器的web界面
- site:xxx.com intitle:"mail"
- site:xxx.com intitle:"webmail"

5、其他

- site:xxx.com inurl:api
- site:xxx.com inurl:uid=/id=
- site:xxx.com intitle:index.of "server at"

Github

<https://github.com/>



- @xxx.com password/secret/credentials/token/config/pass/login/ftp/ssh/pwd
- @xxx.com security_credentials/connectionstring/JDBC/ssh2_auth_password/send_keys

网盘引擎

- 盘搜搜: <http://www.pansoso.org>
- 盘多多: <http://www.panduoduo.top/>
- 大力盘: <https://dalipan.com/>

空间搜索引擎

- FOFA: <https://fofa.info/> 之前被禁用，目前已恢复，但是功能阉割严重
- Quake: <https://quake.360.cn/quake/#/index>
- ZoomEye: <https://www.zoomeye.org/>
- Shadon: <https://www.shodan.io>

基础语法: <https://blog.csdn.net/Vdieoo/article/details/109622838>

- 切记: 搜索到敏感信息之后，不要随意下载和传播，属于违法行为！应该主动进行报备。

历史漏洞

- CNVD: <https://www.cnvd.org.cn/>



- CNNVD: <http://www.cnnvd.org.cn/>



- Seebug: <https://www.seebug.org>









































[←](#)
[→](#)
[↺](#)
[🏠](#)

[🔒](#)
[🔗](#)
[https://www.seebug.org](#)

[🔍](#)
[🔖](#)

最新漏洞

More >

SSV ID	提交时间	漏洞等级	漏洞名称	漏洞状态	人气 评论
SSV-99414	2021-12-15	----	AjaxPro.NET反序列化漏洞 (CVE-2021-23758)	   	256 0
SSV-99411	2021-12-15	----	Apache Log4j 1.x JNDI 注入漏洞 (CVE-2021-4104)	   	337 0
SSV-99410	2021-12-15	----	grafana默认密码漏洞	   	223 1
SSV-99409	2021-12-15	----	ecology filedownload 目录穿越漏洞	   	148 0
SSV-99408	2021-12-15	----	泛微OA validate.jsp SQL注入漏洞	   	219 0
SSV-99406	2021-12-15	----	Apache JSPWiki Arbitrary file deletion on logout (CVE-20...	   	181 0
SSV-99405	2021-12-15	----	泛微 OA SyncUserInfo SQL 注入漏洞	   	148 0
SSV-99404	2021-12-15	----	泛微ResourceServlet任意文件下载漏洞	   	109 0
SSV-99403	2021-12-15	----	Sentry Source Code Scrapping 服务端请求伪造漏洞	   	64 0
SSV-99402	2021-12-15	----	Panabit Panalog sessiptbl.php 远程命令执行漏洞	   	89 0

- Exploit Database: <https://www.exploit-db.com>

🕷️

🔍

📄

📁

🔖

📊

📌

🎓

Exploit Database Advanced Search

Title

CVE

Type

Platform

Port

log4j

2021-1234

Content

Author

Tag

Search

☐ Verified

☐ Has App

☐ No Metasploit

🔍 Reset A

Show 15

Date	D	A	V	Title	Type	Platform	Author
2021-12-14	📄	✖		Apache Log4j2 2.14.1 - Information Disclosure	remote	Java	leonjza
2021-12-14	📄	✖		Apache Log4j 2 - Remote Code Execution (RCE)	remote	Java	kozmer

Showing 1 to 2 of 2 entries

FIRST

PREVIOUS

1

NEXT

LAST

Downloads

Certifications

Training

Professional Services

Kali Linux

OSCP

Penetration Testing with Kali Linux (PWK) (PEN-200)
All new for 2020

Penetration Testing

- [SPOITUS](#)

☐ Dark Mode



Search

☐ Title only

公众号

- 微信直接搜索
- 搜狗: <https://weixin.sogou.com>

小程序

- 微信直接搜索

信息深度收集:

指纹识别

- 火狐插件: Wappalyzer
- 云悉: <http://www.yunsee.cn>
- Nuclei: <https://github.com/projectdiscovery/nuclei>