# 信息收集

## 第一步 域名探测

当我们要对一个站点进行渗透测试之前，一般渗透测试人员常见方法是直接通漏洞扫描器来对指定目标站点进行渗透，当指定的目标站点无漏洞情况，渗透测试员就需要进行信息收集工作来完成后期的渗透。

目前一般域名漏洞扫描工具分为Web与系统扫描器，Web主要有：AWVS、APPSCAN、Netspark、WVSS 、WebInspect，系统扫描器有：Nmap、Nessus、天镜、明鉴、RSAS等，后面会分开给大家讲解。

## 第二步 子域名探测

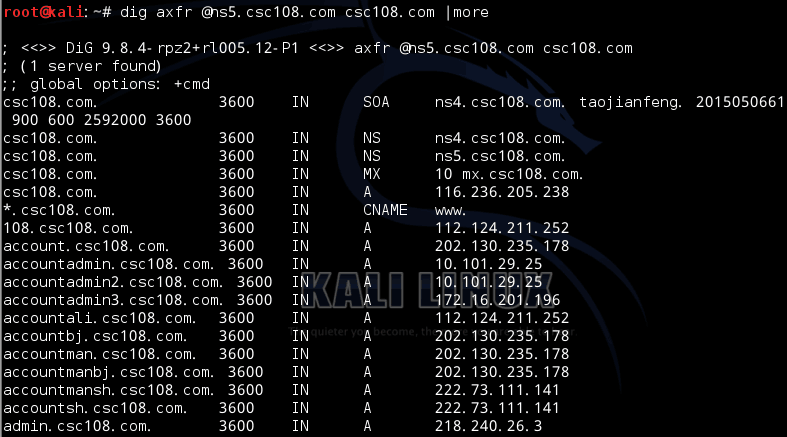
根据主域名，可以获取二级域名、三级域名、......主要姿势可以有：



**【1】DNS域传送漏洞（不得不称赞）**

       如果存在，不仅能搜集子域名，还能轻松找到一枚洞，这样子的好事百试不厌。如果SRC一级域名不多，直接在kali下 dnsenum oldboyedu.com 。





**工具说明及用法可参考如下：**

dnsenum的目的是尽可能收集一个域的信息，它能够通过谷歌或者字典文件猜测可能存在的域名，以及对一个网段进行反向查询。它可以查询网站的主机地址信息、域名服务器、mx record（函件交换记录），在域名服务器上执行axfr请求，通过谷歌脚本得到扩展域名信息（google hacking），提取自域名并查询，计算C类地址并执行whois查询，执行反向查询，把地址段写入文件。

**参数说明：**

-h 查看工具使用帮助

--dnsserver <server> 指定域名服务器

--enum 快捷选项，相当于"--threads 5 -s 15 -w"

--noreverse 跳过反向查询操作

--nocolor 无彩色输出

--private 显示并在"domain\_ips.txt"文件结尾保存私有的ips

--subfile <file> 写入所有有效的子域名到指定文件

-t, --timeout <value> tcp或者udp的连接超时时间，默认为10s（时间单位：秒）

--threads <value> 查询线程数

-v, --verbose 显示所有的进度和错误消息

-o ,--output <file> 输出选项，将输出信息保存到指定文件

-e, --exclude <regexp> 反向查询选项，从反向查询结果中排除与正则表达式相符的PTR记录，在排查无效主机上非常有用

-w, --whois 在一个C段网络地址范围提供whois查询

-f dns.txt 指定字典文件，可以换成 dns-big.txt 也可以自定义字典

**相关解析记录说明可参考：**<https://wenku.baidu.com/view/d2d597b669dc5022aaea0030.html>

**【2】备案号查询**

       这算是奇招吧，通过查询系统域名备案号，再反查备案号相关的域名，收获颇丰。

**网站备案查询地址：**[**http://www.beianbeian.com**](http://www.beianbeian.com)**、**<http://icp.bugscaner.com/>、https:*//www.tianyancha.com/、*http:*//www.beianbeian.com、*https:*//icp.aizhan.com、*http:*//cha.fute.com/index*

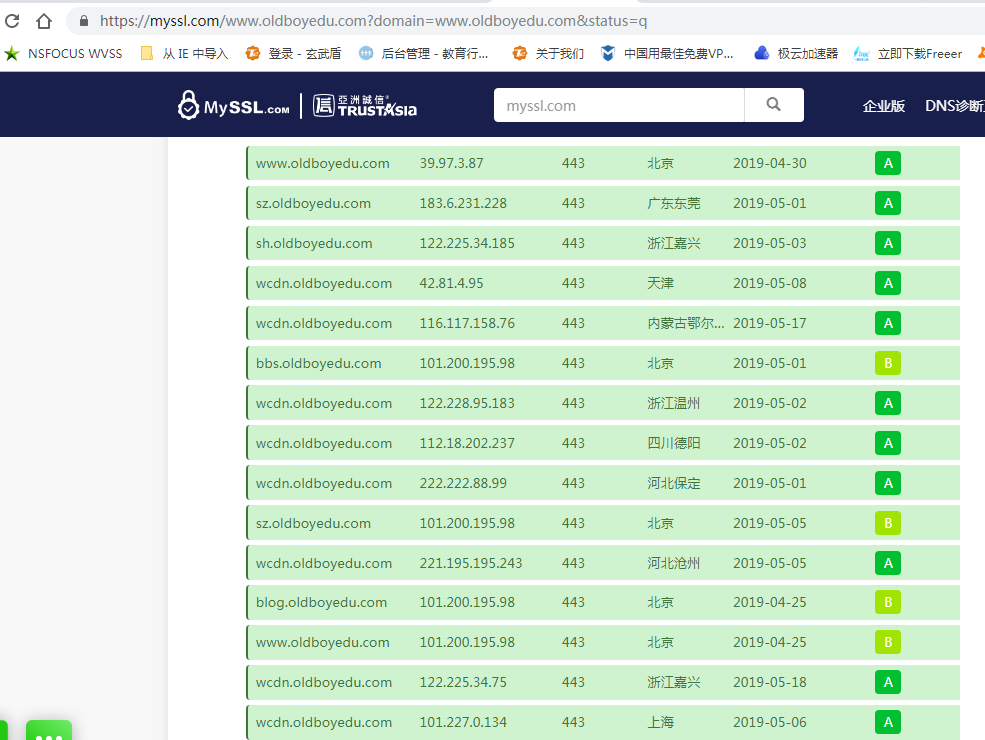
****

****

**【3】SSL证书**

       通过查询SSL证书，获取的域名存活率很高，这应该也是不错的思路。

查询网址: <https://myssl.com/ssl.html> 和<https://www.chinassl.net/ssltools/ssl-checker.html>

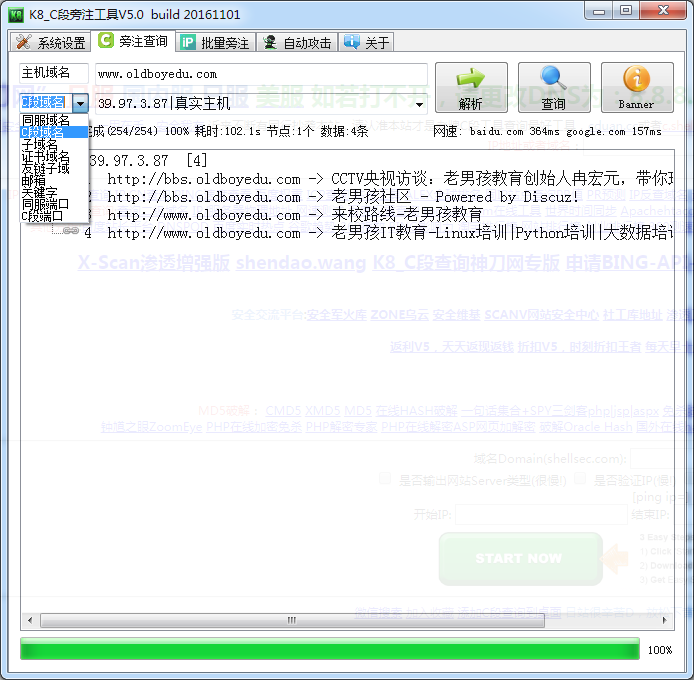


**【4】google搜索C段**

       这招用的比较少，国内没条件的就用bing或百度吧（国内站点足矣），在没什么进展的时候或许会有意外惊喜。

方法一：参考GoogleHack用法

方法二：用k8工具，前提条件记得注册bing接口

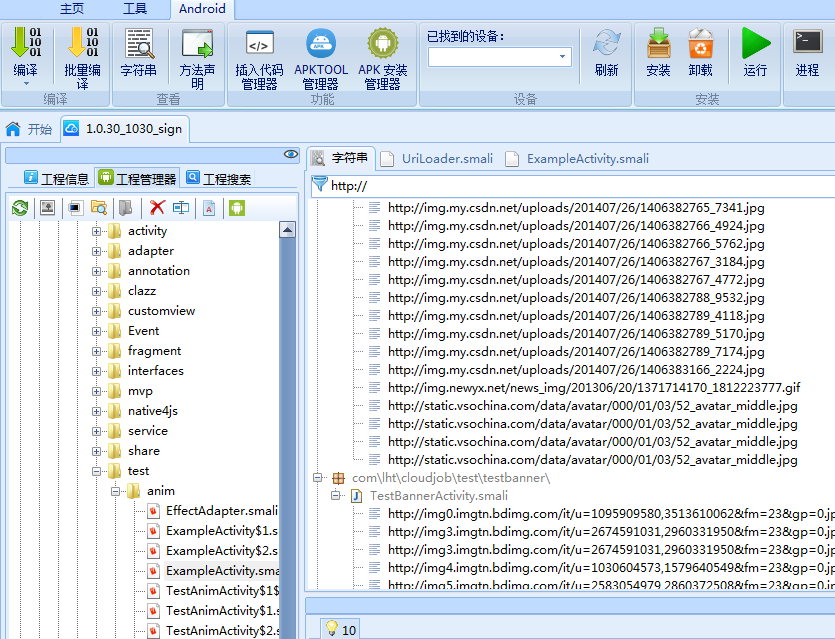


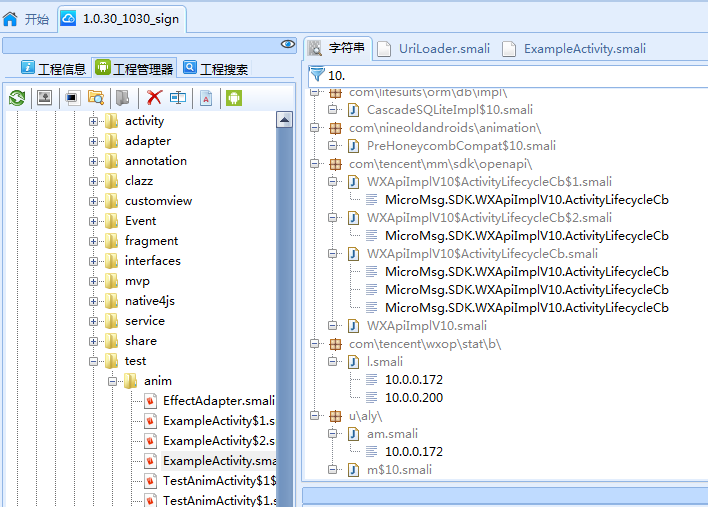
**什么是C段：**比如在：127.127.127.4 这个IP上面有一个网站 127.4 这个服务器上面有网站我们可以想想..他是一个非常大的站几乎没什么漏洞！但是在他同C段 127.127.127.1~127.127.127.255 这 1~255 上面也有服务器而且也有网站并且存在漏洞,那么我们就可以来渗透 1~255任何一个站 之后提权来嗅探得到127.4 这台服务器的密码 甚至3389连接的密码后台登录的密码 如果运气好会得到很多的密码…

10.

**【5】APP提取**

       反编译APP进行提取相关IP地址，此外在APP上挖洞的时候，可以发现前面招式找不到的域名，在APP里面有大量的接口IP和内网 IP，同时可获取不少安全漏洞。





**【6】微信公众号**

       企业的另一通道，渗透相关公众号，绝对会有意外收获：不少漏洞+域名，有关Burp如何抓取微信公众号数据可参考 Burp APP抓包。

**【7】字典枚举法**

       字典枚举法是一种传统查找子域名的技术，这类工具有  DNSReconcile、Layer子域名挖掘机、DirBuster等。

**【8】公开DNS源**

1）DNS解析记录可以反查IP，比较早的解析记录有时可以查到真实IP，需要留意一下。

（2）注册人电话，注册人邮箱等社工信息可以钓鱼或者收集进字典来爆破目标办公系统。

Rapid7下Sonar项目发布的： https://scans.io/study/sonar.fdns\_v2。

DNS历史解析： https://dnsdb.io/zh-cn/

**【9】威胁情报查询**

华为安全情报 <https://isecurity.huawei.com>

<https://ti.360.cn/>

**【10】JS文件域名、ip探测**

<https://github.com/Threezh1/JSFinder>

**【11】网站在线查找**

查找目标域名信息的方法有：

（1）FOFA title="公司名称"

（2）百度 intitle=公司名称

（3）Google intitle=公司名称

（4）站长之家，直接搜索名称或者网站域名即可查看相关信息：

http:*//tool.chinaz.com/*

（5）钟馗之眼 site=域名即可

https:*//www.zoomeye.org/*

找到官网后，再收集子域名，下面推荐几种子域名收集的方法，直接输入domain即可查询

（6）子域名在线查询

https:*//phpinfo.me/domain/*

（7）子域名在线查询

https:*//www.t1h2ua.cn/tools/*

（8）Layer子域名挖掘机4.2（使用方便，界面整洁）：

https:*//www.webshell.cc/6384.html*

（9）Layer子域名挖掘机5.0（使用方便，界面整洁）：

https:*//pan.baidu.com/s/1wEP\_Ysg4qsFbm\_k1aoncpg 提取码：uk1j*

（9）SubDomainBrute

https:*//github.com/lijiejie/subDomainsBrute*

（10）Sublist3r

https:*//github.com/aboul3la/Sublist3r*

提示：以上方法为爆破子域名，由于字典比较强大，所以效率较高。

（7）IP138查询子域名

https:*//site.ip138.com/baidu.com/domain.htm*

（8）FOFA搜索子域名

https:*//fofa.so/*

语法：domain=”baidu.com”

提示：以上两种方法无需爆破，查询速度快，需要快速收集资产时可以优先使用，后面再用其他方法补充。

（9）Hackertarget查询子域名

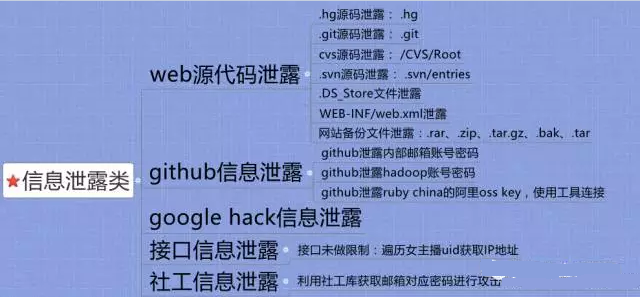
https:*//hackertarget.com/find-dns-host-records/*

注意：通过该方法查询子域名可以得到一个目标大概的ip段，接下来可以通过ip来收集信息。

## 第三步 敏感信息收集

**【1】Web源代码泄露**

通过工具暴破相关Web源代码泄露，流程如下：



最想强调的是github信息泄露了，直接去github上搜索，收获往往是大于付出。可能有人不自信认为没能力去SRC挖洞，可是肯定不敢说不会上网不会搜索。github相关的故事太多，但是给人引出的信息泄露远远不仅在这里：github.com、rubygems.org、pan.baidu.com...

QQ群备注或介绍等，甚至混入企业qq工作群...

然后说再多，也没这个好用：<https://sec.xiaomi.com/article/37> 全自动监控github

**信息泄露收集可能会用到如下地址：**

网盘搜索：http://www.pansou.com/或<https://www.lingfengyun.com/> 网盘密码破解可参考：https://www.52pojie.cn/thread-763130-1-1.html

社工信息泄露：https://www.instantcheckmate.com/、http://www.uneihan.com/

源码搜索：https://searchcode.com/、<https://gitee.com/>、gitcafe.com、code.csdn.net

钟馗之眼： https://www.zoomeye.org/

天眼查 https://www.tianyancha.com/

其它：威胁情报：微步在线、 ti.360.cn、 Virustotal

**【2】邮箱信息收集**

收集邮箱信息主要有两个作用：1.通过发现目标系统账号的命名规律，可以用来后期登入其他子系统。2.爆破登入邮箱用。

通常邮箱的账号有如下几种生成规律： 比如某公司有员工名叫做“张小三”，它的邮箱可能如下：

zhangxiaosan@xxx.com     xiaosan.zhang@xxx.com        zxiaosan@xxx.com

当我们收集几个邮箱之后，便会大致猜出对方邮箱的命名规律。除了员工的邮箱之外，通过公司会有一些共有的邮箱，比如人力的邮箱、客服的邮箱，hr@xxx.com/kefu@xxx.com,这种邮箱有时会存在弱口令，在渗透时可额外留意一下。我们可以通过手工或者工具的方式来确定搜集邮箱：

**手工的方式：**

1.可以到百度等搜索引擎上搜索邮箱信息

2.github等第三方托管平台

3.社工库

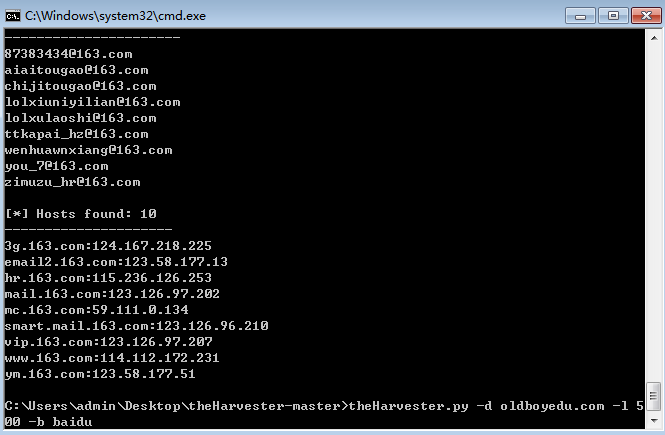
**工具方式：**

在邮箱收集领域不得不提一个经典的工具，The Harvester,The Harvester可用于搜索Google、Bing和PGP服务器的电子邮件、主机以及子域名,因此需要翻墙运行该工具。工具下载地址为：<https://github.com/laramies/theHarvester>

* **注：python -m pip install -r requirements.txt 导入相关配置，python3.6版本**

使用方式很简单：

   ./theHarvester.py -d 域名   -1 1000   -b all



**【3】历史漏洞收集**

仔细分析，大胆验证，发散思维，对企业的运维、开发习惯了解绝对是有很大的帮助。可以把漏洞保存下来，进行统计，甚至炫一点可以做成词云展示给自己看，看着看着或者就知道会有什么漏洞。

wooyun 历史漏洞库：<http://www.anquan.us/> 、<http://wooyun.2xss.cc/>

漏洞银行：<https://www.bugbank.cn/>

奇安信补天：<https://www.butian.net/>

Cnvd <https://www.cnvd.org.cn/>

漏洞盒子 https://www.vulbox.com/

教育行业漏洞报告平台（Beta）<https://src.edu-info.edu.cn/login/>

<https://www.bugcrowd.com/>

https://www.hackerone.com/

**【4】工具信息收集**

如：7kbscan、破壳Web极速扫描器等

**【5】whois查询**

**1、在线whois查询**

通过whois来对域名信息进行查询，可以查到注册商、注册人、邮箱、DNS解析服务器、注册人联系电话等，因为有些网站信息查得到，有些网站信息查不到，所以推荐以下信息比较全的查询网站，直接输入目标站点即可查询到相关信息。

（1）站长之家域名WHOIS信息查询地址

http:*//whois.chinaz.com/*

（2）爱站网域名WHOIS信息查询地址

https:*//whois.aizhan.com/*

（3）腾讯云域名WHOIS信息查询地址

https:*//whois.cloud.tencent.com/*

（4）美橙互联域名WHOIS信息查询地址

https:*//whois.cndns.com/*

（5）爱名网域名WHOIS信息查询地址

https:*//www.22.cn/domain/*

（6）易名网域名WHOIS信息查询地址

https:*//whois.ename.net/*

（7）中国万网域名WHOIS信息查询地址

https:*//whois.aliyun.com/*

（8）西部数码域名WHOIS信息查询地址

https:*//whois.west.cn/*

（9）新网域名WHOIS信息查询地址

http://whois.xinnet.com/domain/whois/index.jsp

（10）纳网域名WHOIS信息查询地址

http:*//whois.nawang.cn/*

（11）中资源域名WHOIS信息查询地址

https:*//www.zzy.cn/domain/whois.html*

（12）三五互联域名WHOIS信息查询地址

https:*//cp.35.com/chinese/whois.php*

（13）新网互联域名WHOIS信息查询地址

http://www.dns.com.cn/show/domain/whois/index.do

（14）国外WHOIS信息查询地址

https:*//who.is/*

## 第四步 指纹识别、Waf、CDN识别

在这个过程中，可以加入端口扫描、敏感文件扫描之类的操作，工具可自由选择，如：

御剑WEB指纹识别系统、whatweb、Wapplyzer等工具。

一、在线识纹识别：

**1、云悉**

http:*//www.yunsee.cn/info.html*

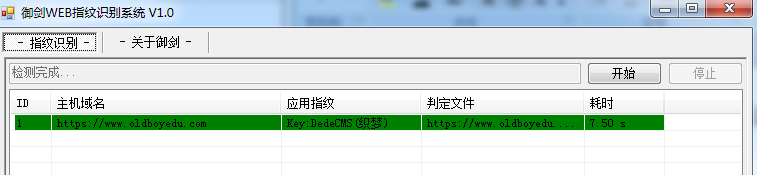
**2、潮汐指纹**

http:*//finger.tidesec.net/*

**3、CMS指纹识别**

http:*//whatweb.bugscaner.com/look/*

二、工具识别



2、Waf识别

[github.com/EnableSecurity/wafw00f](https://github.com/EnableSecurity/wafw00f)

3、CDN识别

如果目标网站使用了CDN，那么我们就需要找到它的真实ip

注意：很多时候，主站虽然是用了CDN，但子域名可能没有使用CDN，如果主站和子域名在一个ip段中，那么找到子域名的真实ip也是一种途径。

**1、多地ping确认是否使用CDN**

http:*//ping.chinaz.com/*http:*//ping.aizhan.com/*

**2、查询历史DNS解析记录**

在查询到的历史解析记录中，最早的历史解析ip很有可能记录的就是真实ip，快速查找真实IP推荐此方法，但并不是所有网站都能查到。

（1）DNSDB

https:*//dnsdb.io/zh-cn/*

（2）微步在线

https:*//x.threatbook.cn/*

（3）在线网站查找

[https:*//tools.ipip.net/cdn.php*](https://tools.ipip.net/cdn.php)

<https://raw.githubusercontent.com/3xp10it/mytools/master/xcdn.py>

**3、phpinfo**

如果目标网站存在phpinfo泄露等，可以在phpinfo中的SERVER\_ADDR或\_SERVER[“SERVER\_ADDR”]找到真实ip

**4、绕过CDN**

绕过CDN的多种方法具体可以参考

https://www.cnblogs.com/qiudabai/p/9763739.html

**5、参考fofa绕过**

参考扩展fafo

## 第五步 旁站与C段

旁站往往存在业务功能站点，建议先收集已有IP的旁站，再探测C段，确认C段目标后，再在C段的基础上再收集一次旁站。

旁站是和已知目标站点在同一服务器但不同端口的站点，通过以下方法搜索到旁站后，先访问一下确定是不是自己需要的站点信息。

**1、站长之家**

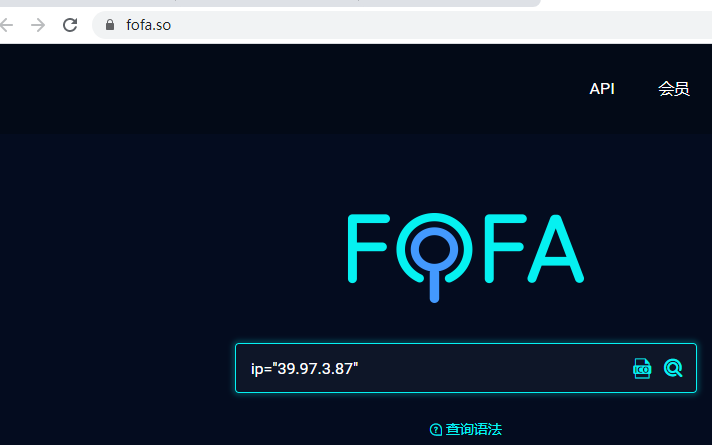
同ip网站查询

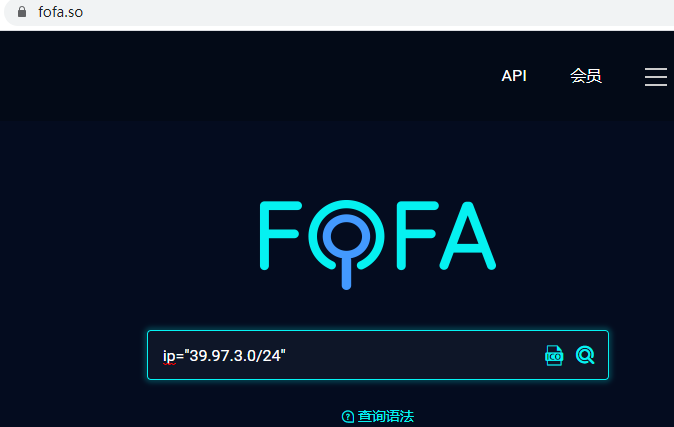
http:*//stool.chinaz.com/same*



**2、网络空间搜索引擎**

如FOFA搜索旁站和C段



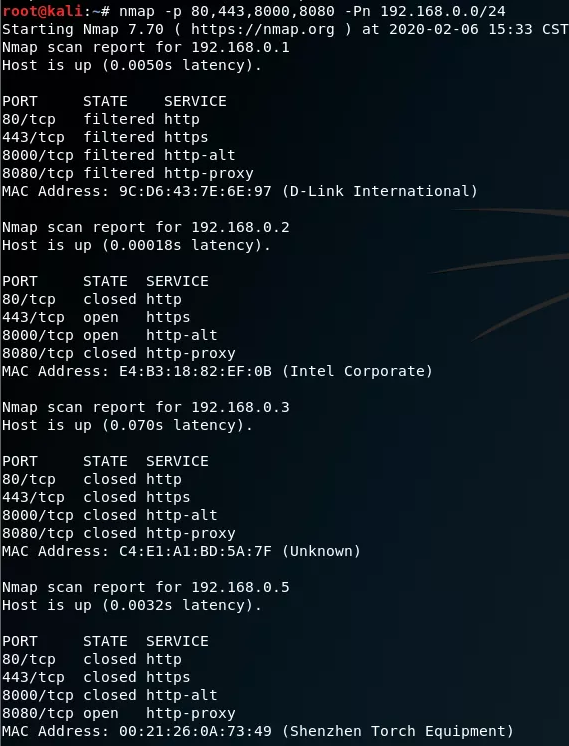


该方法效率较高，并能够直观地看到站点标题，但也有不常见端口未收录的情况，虽然这种情况很少，但之后补充资产的时候可以用下面的方法nmap扫描再收集一遍。

**3、Nmap,Msscan扫描等**

例如：

nmap -p 80,443,8000,8080 -Pn 39.97.3.0/24



**4、常见端口表**

21,22,23,80-90,161,389,443,445,873,1099,1433,1521,1900,2082,2083,2222,2601,2604,3128,3306,3311,3312,3389,4440,4848,5432,5560,5900,5901,5902,6082,6379,7001-7010,7778,8080-8090,8649,8888,9000,9200,10000,11211,27017,28017,50000,50030,50060

注意：探测C段时一定要确认ip是否归属于目标，因为一个C段中的所有ip不一定全部属于目标。

## 第六步 资产梳理

 有了庞大的域名，接下来就是帮助SRC梳理资产了。域名可以先判断存活，活着的继续进行确定IP环节。根据IP的分布，确定企业的公网网段。这其实是一项不小的工程，精准度比较难以拿捏。不过通过不断实战，肯定可以琢磨出一些东西，所以有人称白帽子可能会比企业的运维更了解资产信息。资产梳理过程中可能需要对相关资产漏洞进行查询、利用、发布等，可能会用到已下相关链接地址：

**SRC众测平台**

国际漏洞提交平台 https://www.hackerone.com/

BugX区块链漏洞平台 http://www.bugx.org/

Gsrc瓜子src https://security.guazi.com/

区块链安全响应中心 https://dvpnet.io/

CNVD国家信息安全漏洞平台 http://www.cnvd.org.cn/

漏洞银行：<https://www.bugbank.cn/>

奇安信补天：<https://www.butian.net/>

教育行业漏洞报告平台（Beta）<https://src.edu-info.edu.cn/login/>

**国内平台**

知道创宇Seebug漏洞平台 https://www.seebug.org/

工控系统行业漏洞平台 http://ivd.winicssec.com/

打造中文最大exploit库 http://www.expku.com/

为数不多的漏洞管理插件收集平台 http://www.bugscan.net/source/template/vulns/

一家管理漏洞收集的平台 http://www.0daybank.org/

**国外平台**

国际漏洞提交平台 https://www.hackerone.com/

xss poc http://xssor.io/

oday漏洞库 https://www.0day.today/

路由器漏洞库 http://routerpwn.com/

cve漏洞平台 http://cve.mitre.org/

**威胁情报**

安全数据交流平台 https://www.secsilo.com/

华为安全情报 https://isecurity.huawei.com/sec/web/intelligencePortal.do

威胁情报共享平台 https://www.threatcrowd.org/

被黑站点统计 http://www.hacked.com.cn/

**社工库**

微信伪造 http://www.jietuyun.com/

任意邮箱发送 http://tool.chacuo.net/mailanonymous和https://emkei.cz/

临时邮箱 http://www.yopmail.com/

邮箱池群 http://veryvp.com/

社工库 http://www.uneihan.com/

## GoogleHack

### 功能介绍

使用[Google](http://baike.haosou.com/doc/108804.html)等搜索引擎对某些特定的[网络](http://baike.haosou.com/doc/3663174.html)主机漏洞（通常是服务器上的脚本漏洞）进行搜索，以达到快速找到漏洞主机或特定主机的漏洞的目的。Google毫无疑问是当今世界上最强大的搜索引擎。然而，在黑客手中，它也是一个秘密武器，它能搜索到一些你意想不到的信息。

### 部署指南

1. 一台可以正常访问互联网的设备（通常为PC）
2. 一个常用浏览器（IE、Chrome等等）
3. 掌握强大的搜索关键词

### 实战

Google搜索引擎之所以强大，关键在于它详细的搜索关键词，以下是几个常用的搜索关键词：（更多详细教程，参见http://user.qzone.qq.com/568311803/main）

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: 只搜索网页部分中包含的文字(也就是忽略了标题,URL等的文字).

site: 可以限制你搜索范围的域名.

filetype: 搜索文件的后缀或者扩展名

intitle: 限制你搜索的网页标题.

allintitle: 搜索所有关键字构成标题的网页. 但是推荐不要使用

link: 可以得到一个所有包含了某个指定URL的页面列表. 例如:link:www.google.com 就可以得到所有连接到Google的页面。

**一般常见用法有：**

**site**:ooxx.com **filetype**:xls

**site:xxx.xxx admin**

**site:xxx.xxx login**

**site:xxx.xxx system**

**site:xxx.xxx 管理**

**site:xxx.xxx 登录**

**site:xxx.xxx 内部**

**site:xxx.xxx 系统**

**site:xxx.xxx 邮件**

**site:xxx.xxx email**

**site:xxx.xxx qq**

**site:xxx.xxx 群**

**site:xxx.xxx 企鹅**

**site:xxx.xxx 腾讯**

**site:ooxx.com**

**inurl:jmx-console**

实例：

1. **intext:管理**



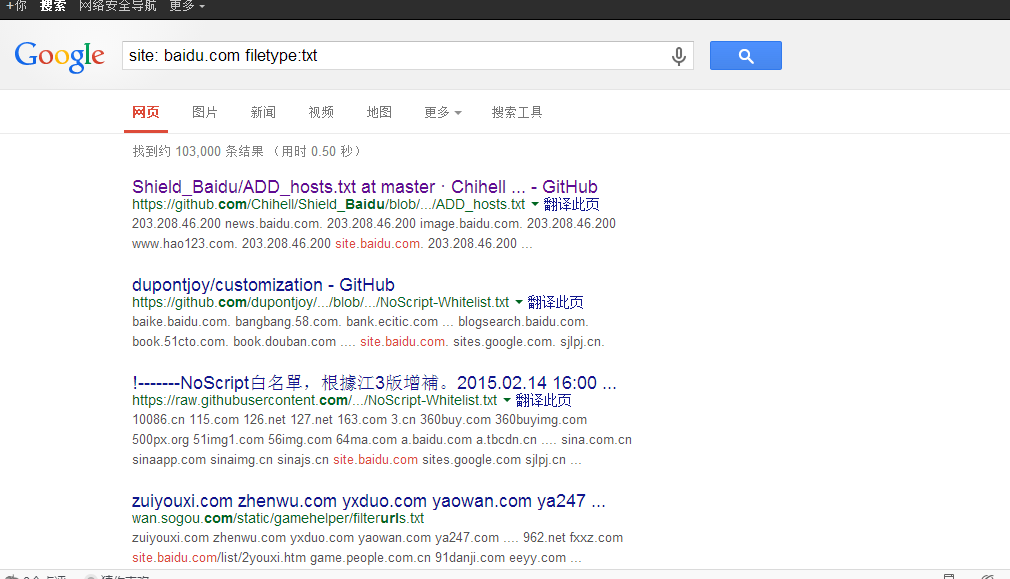
1. **filetype:mdb**



1. **inurl:file**



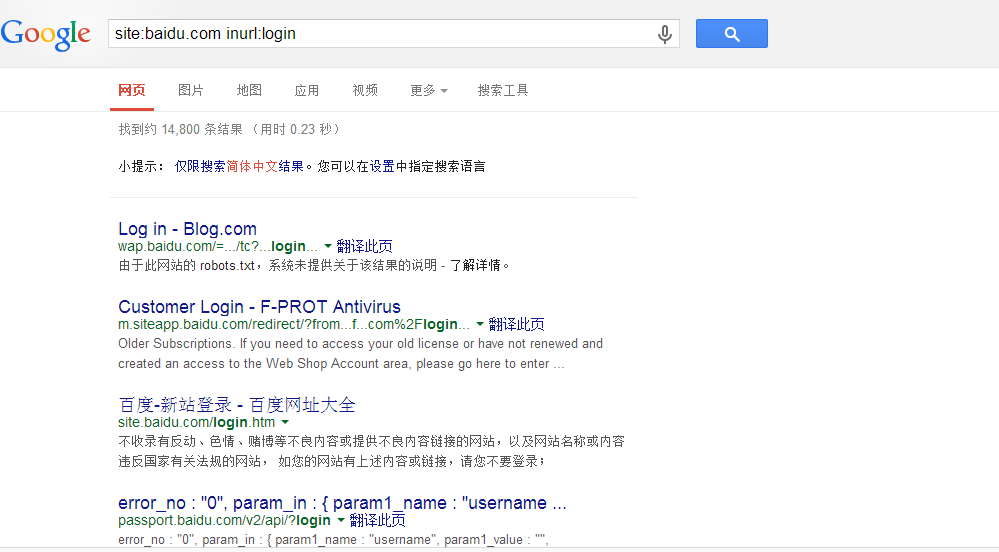
1. **site: baidu.com filetype:txt 查找TXT文件 其他的依次类推**



1. **site:baidu.com intext:管理**



1. **site:baidu.com inurl:login**

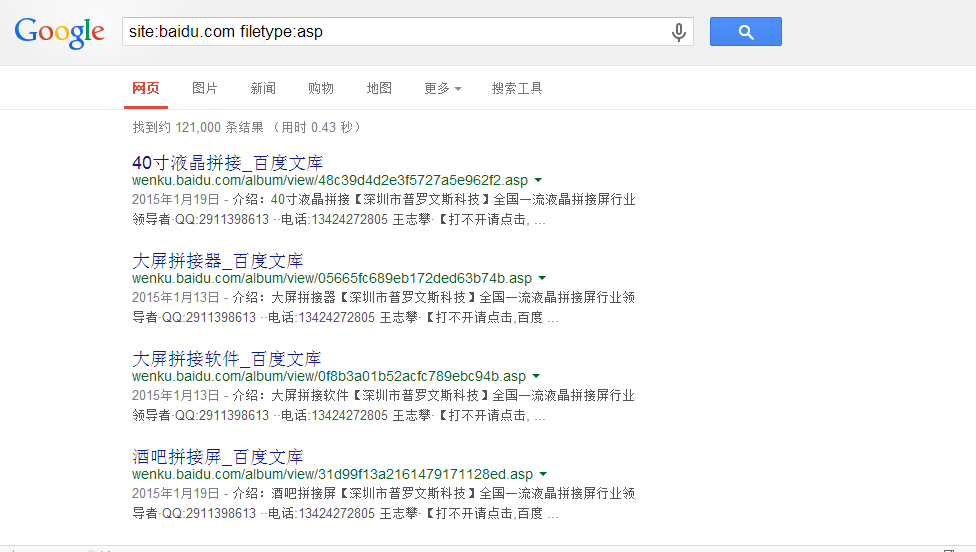


1. **site:baidu.com intitle:后台**



查看服务器使用的程序

1. **site:baidu.com filetype:asp**



1. **site:baidu.com filetype:php**



1. **site:baidu.com filetype:jsp**

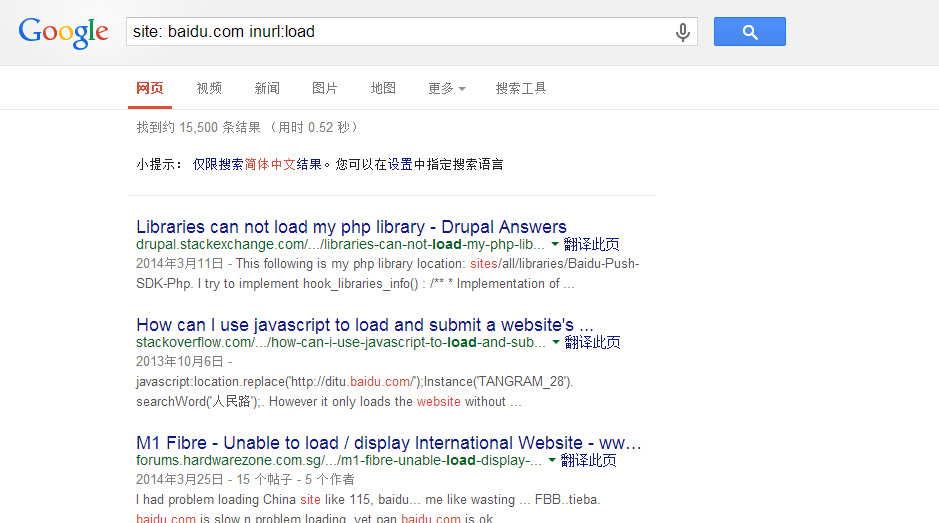


查看上传漏洞：

1. **site:baidu.com inurl:file**



1. **site: baidu.com inurl:load**



查找注射点：

1. **site:tw inurl:asp?id=**  这个是找台湾的



### Google的优劣势

优势：

* 只需一台可以访问Google的联网设备，部署简单；
* 检索资源库丰富；

劣势：

* 搜索关键词多，记忆复杂；
* GoogleHack需要借助浏览器，属于在线工具，离线不能使用；
* 国内访问Google需借助VPN等相关手段，增加了上网成本

## Nmap与在线扫描

http://blog.sina.com.cn/s/blog\_811d9fdd0101ey07.html 功能介绍

http://www.cnblogs.com/c4isr/archive/2012/12/07/2807491.html 10种扫描方式解释

由于是在win7上面使用，所以要使用兼容win7的winpcap驱动，这里我们使用最新版4.1.2版

winpcap4.1.2下载地址：http://www.onlinedown.net/soft/2685.htm

### 功能介绍

Nmap是一个网络连接端口扫描[软件](http://baike.baidu.com/view/37.htm)，用来扫描网上电脑开放的网络连接端口。确定哪些[服务](http://baike.baidu.com/view/133203.htm)运行在哪些连接端口，并且推断计算机运行哪个[操作系统](http://baike.baidu.com/view/880.htm)。它是网络管理员必用的[软件](http://baike.baidu.com/view/37.htm)之一，以及用以评估网络系统安全。

功能架构图：

### 部署指南

两种部署方式：

* Kail集成环境
* 单独安装（使用yum工具直接安装就可以）

### 实战

Nmap的参数和选项繁多，功能非常丰富。我们先来看一下Nmap的通用命令格式：（详细教程及下载方式参见：http://nmap.org/）

**Nmap*<扫描选项><扫描目标>***

1. **主机发现**

#### 主机发现原理

主机发现的原理与Ping命令类似，发送探测包到目标主机，如果收到回复，那么说明目标主机是开启的。Nmap支持十多种不同的主机探测方式，比如发送ICMP ECHO/TIMESTAMP/NETMASK报文、发送TCPSYN/ACK包、发送SCTP INIT/COOKIE-ECHO包，用户可以在不同的条件下灵活选用不同的方式来探测目标机。

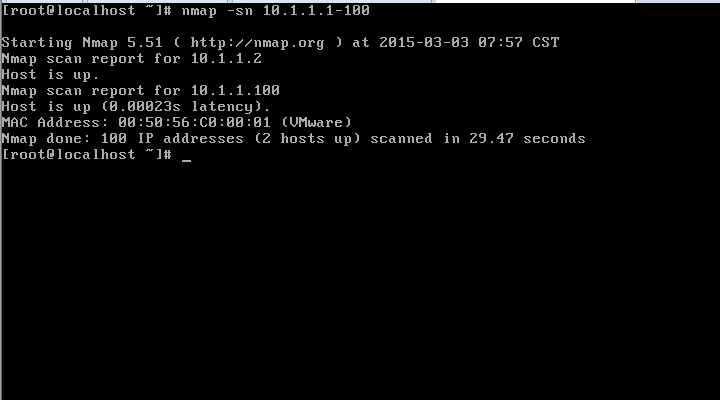
#### 主机发现的基本用法

* -sL: List Scan 列表扫描，仅将指定的目标的IP列举出来，不进行主机发现。
* -sn: Ping Scan 只进行主机发现，不进行端口扫描。
* -Pn: 将所有指定的主机视作开启的，跳过主机发现的过程。
* -PS/PA/PU/PY[portlist]: 使用TCPSYN/ACK或SCTP INIT/ECHO方式进行发现。
* -PE/PP/PM: 使用ICMP echo, timestamp, and netmask 请求包发现主机。
* -PO[protocollist]: 使用IP协议包探测对方主机是否开启。
* -n/-R: -n表示不进行DNS解析；-R表示总是进行DNS解析。
* --dns-servers <serv1[,serv2],...>: 指定DNS服务器。
* --system-dns: 指定使用系统的DNS服务器
* --traceroute: 追踪每个路由节点

#### 使用演示

扫描局域网10.1.1.1-10.1.1.100范围内哪些IP的主机是活动的。

命令如下：nmap –sn 10.1.1.1-100



由图可知：10.1.1.2、10.1.1.100两台主机处于存活状态。

1. **端口扫描**

#### 端口扫描原理

端口扫描是Nmap最基本最核心的功能，用于确定目标主机的TCP/UDP端口的开放情况。默认情况下，Nmap会扫描1000个最有可能开放的TCP端口。Nmap通过探测将端口划分为6个状态：  
open：端口是开放的。  
closed：端口是关闭的。  
filtered：端口被防火墙IDS/IPS屏蔽，无法确定其状态。  
unfiltered：端口没有被屏蔽，但是否开放需要进一步确定。  
open|filtered：端口是开放的或被屏蔽。  
closed|filtered ：端口是关闭的或被屏蔽。

端口扫描方面非常强大，提供了很多的探测方式：

* TCP SYN scanning
* TCP connect scanning
* TCP ACK scanning
* TCP FIN/Xmas/NULL scanning
* UDP scanning
* 其他方式

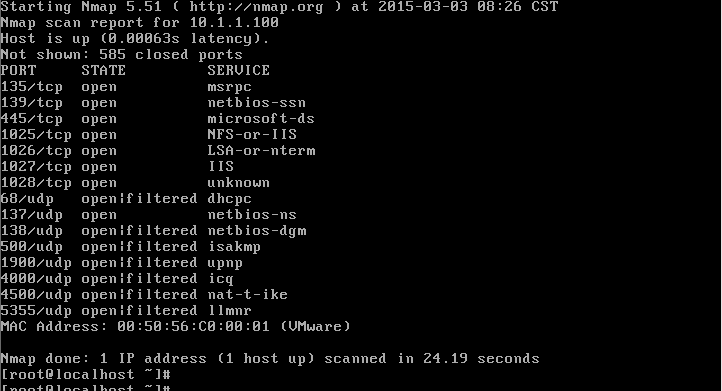
#### 端口扫描用法

* -sS/sT/sA/sW/sM:指定使用 TCP SYN/Connect()/ACK/Window/Maimon scans的方式来对目标主机进行扫描。
* -sU: 指定使用UDP扫描方式确定目标主机的UDP端口状况。
* -sN/sF/sX: 指定使用TCP Null, FIN, and Xmas scans秘密扫描方式来协助探测对方的TCP端口状态。
* --scanflags <flags>: 定制TCP包的flags。
* -sI <zombiehost[:probeport]>: 指定使用idle scan方式来扫描目标主机（前提需要找到合适的zombie host）
* -sY/sZ: 使用SCTP INIT/COOKIE-ECHO来扫描SCTP协议端口的开放的情况。
* -sO: 使用IP protocol 扫描确定目标机支持的协议类型。
* -b <FTP relay host>: 使用FTP bounce scan扫描方式

#### 使用演示

在此，我们以主机10.1.1.100为例。命令如下：nmap -sS -sU -T4 -top-ports 300 1.1.1.100

参数-sS表示使用TCP SYN方式扫描TCP端口；-sU表示扫描UDP端口；-T4表示时间级别配置4级；--top-ports 300表示扫描最有可能开放的300个端口（TCP和UDP分别有300个端口）。



1. **版本侦测**

#### 版本侦测原理

简要的介绍版本的侦测原理。版本侦测主要分为以下几个步骤：

* 首先检查open与open|filtered状态的端口是否在排除端口列表内。如果在排除列表，将该端口剔除。
* 如果是TCP端口，尝试建立TCP连接。尝试等待片刻（通常6秒或更多，具体时间可以查询文件nmap-services-probes中Probe TCP NULL q||对应的totalwaitms）。通常在等待时间内，会接收到目标机发送的“WelcomeBanner”信息。nmap将接收到的Banner与nmap-services-probes中NULL probe中的签名进行对比。查找对应应用程序的名字与版本信息。
* 如果通过“Welcome Banner”无法确定应用程序版本，那么nmap再尝试发送其他的探测包（即从nmap-services-probes中挑选合适的probe），将probe得到回复包与数据库中的签名进行对比。如果反复探测都无法得出具体应用，那么打印出应用返回报文，让用户自行进一步判定。
* 如果是UDP端口，那么直接使用nmap-services-probes中探测包进行探测匹配。根据结果对比分析出UDP应用服务类型。
* 如果探测到应用程序是SSL，那么调用openSSL进一步的侦查运行在SSL之上的具体的应用类型。
* 如果探测到应用程序是SunRPC，那么调用brute-force RPC grinder进一步探测具体服务。

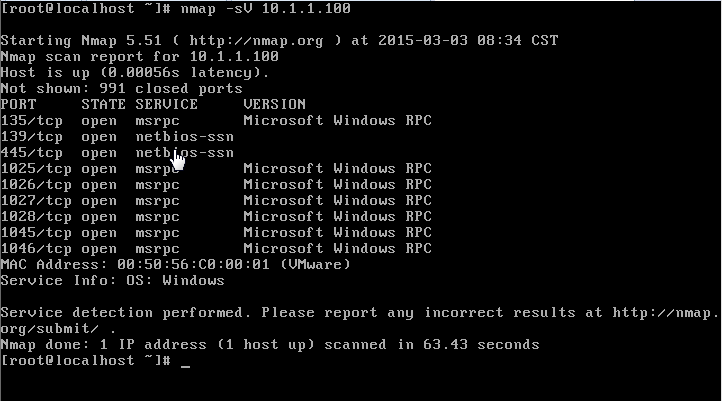
#### 版本侦测用法

* -sV: 指定让Nmap进行版本侦测
* --version-intensity <level>: 指定版本侦测强度（0-9），默认为7。数值越高，探测出的服务越准确，但是运行时间会比较长。
* --version-light: 指定使用轻量侦测方式 (intensity 2)
* --version-all: 尝试使用所有的probes进行侦测 (intensity 9)
* --version-trace: 显示出详细的版本侦测过程信息。

#### 使用演示

对主机10.1.1.100进行版本侦测。

命令如下：nmap –sV 10.1.1.100



1. **OS侦测**

#### OS侦测原理

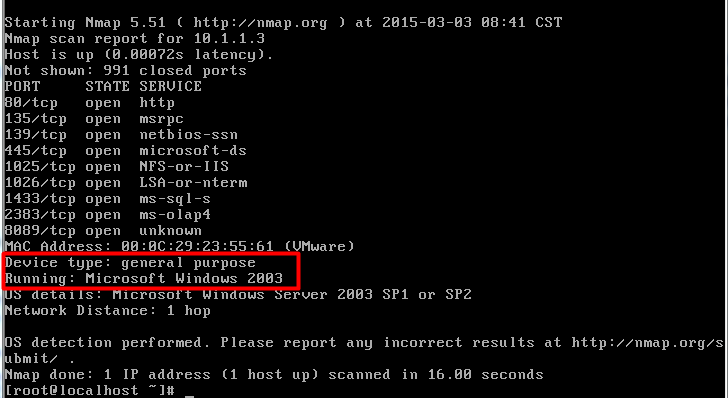
Nmap使用TCP/IP协议栈指纹来识别不同的操作系统和设备。在RFC规范中，有些地方对TCP/IP的实现并没有强制规定，由此不同的TCP/IP方案中可能都有自己的特定方式。Nmap主要是根据这些细节上的差异来判断操作系统的类型的。  
具体实现方式如下：  
Nmap内部包含了2600多已知系统的指纹特征（在文件nmap-os-db文件中）。将此指纹数据库作为进行指纹对比的样本库。分别挑选一个open和closed的端口，向其发送经过精心设计的TCP/UDP/ICMP数据包，根据返回的数据包生成一份系统指纹。将探测生成的指纹与nmap-os-db中指纹进行对比，查找匹配的系统。如果无法匹配，以概率形式列举出可能的系统。

#### OS侦测用法

* -O: 指定Nmap进行OS侦测。
* --osscan-limit: 限制Nmap只对确定的主机的进行OS探测（至少需确知该主机分别有一个open和closed的端口）。
* --osscan-guess: 大胆猜测对方的主机的系统类型。由此准确性会下降不少，但会尽可能多为用户提供潜在的操作系统。

#### 使用演示

命令：nmap -O 10.1.1.100



1. **漏洞扫描**

**扫描端口并且标记可以爆破的服务**

**nmap** 目标 --script=ftp-brute,imap-brute,smtp-brute,pop3-brute,mongodb-brute,redis-brute,ms-sql-brute,rlogin-brute,rsync-brute,mysql-brute,pgsql-brute,oracle-sid-brute,oracle-brute,rtsp-url-brute,snmp-brute,svn-brute,telnet-brute,vnc-brute,xmpp-brute

**判断常见的漏洞并扫描端口**

**nmap** 目标 --script=auth,vuln

**精确判断漏洞并扫描端口**

**nmap** 目标 --script=dns-zone-transfer,ftp-anon,ftp-proftpd-backdoor,ftp-vsftpd-backdoor,ftp-vuln-cve2010-4221,http-backup-finder,http-cisco-anyconnect,http-iis-short-name-brute,http-put,http-php-version,http-shellshock,http-robots.txt,http-svn-enum,http-webdav-scan,iis-buffer-overflow,iax2-version,memcached-info,mongodb-info,msrpc-enum,ms-sql-info,mysql-info,nrpe-enum,pptp-version,redis-info,rpcinfo,samba-vuln-cve-2012-1182,smb-vuln-ms08-067,smb-vuln-ms17-010,snmp-info,sshv1,xmpp-info,tftp-enum,teamspeak2-version

### Nmap的优劣势

优势：

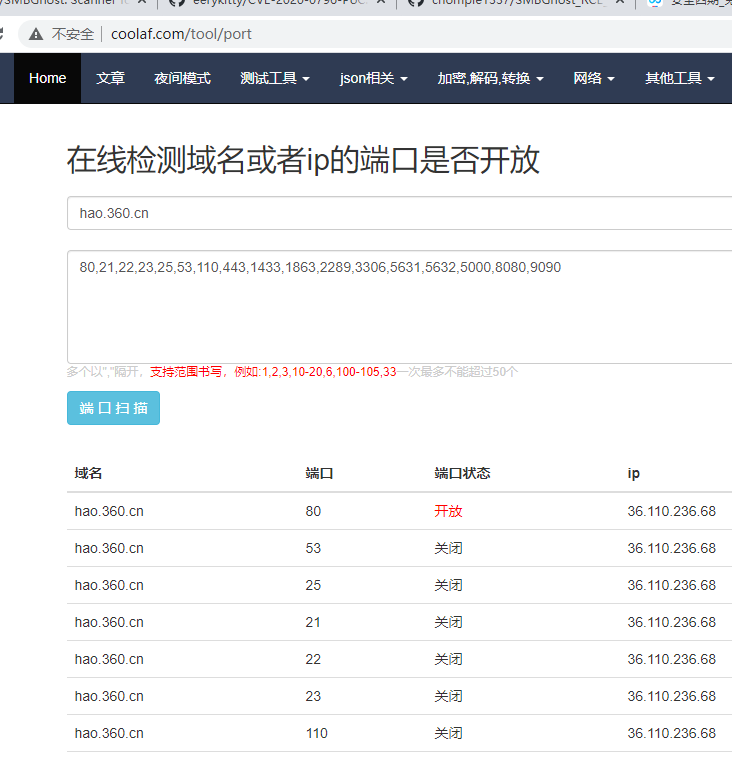
* 功能灵活强大，支持多种目标，大量计算机的同时扫描；
* 开源，相关帮助文档十分详细；
* 流行，由于其具有强大的扫描机探测功能，，已被成千上万安全专家使用。

劣势：

* Nmap参数众多，难以一一记忆；

### 在线扫描

[http:*//coolaf.com/tool/port*](http://coolaf.com/tool/port)



此方法为在线检测，虽然功能简单，但图形界面十分方便且速度快。

常见端口及对应服务和攻击方式整理如下：



## DirBuster

### 功能介绍

DirBuster是一款路径及网页暴力破解的工具,可以破解出一直没有访问过或者管理员后台的界面路径。

### 部署指南

Java运行环境+DirBuster程序包

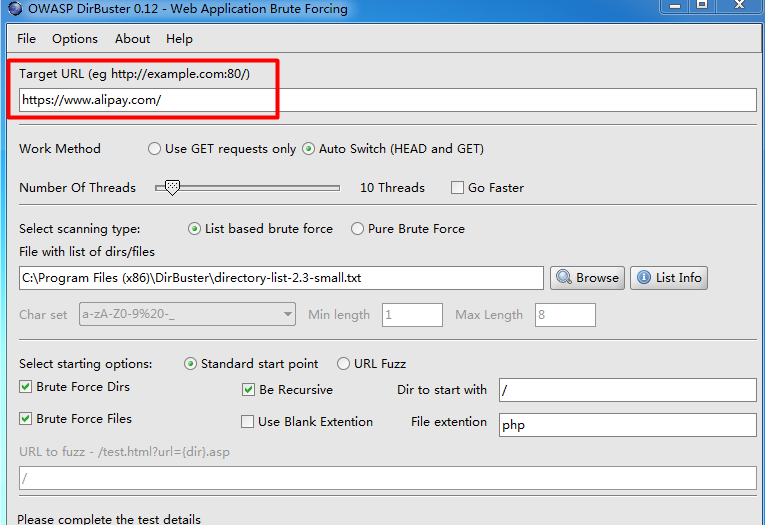
### 实战

详细教程，参见：

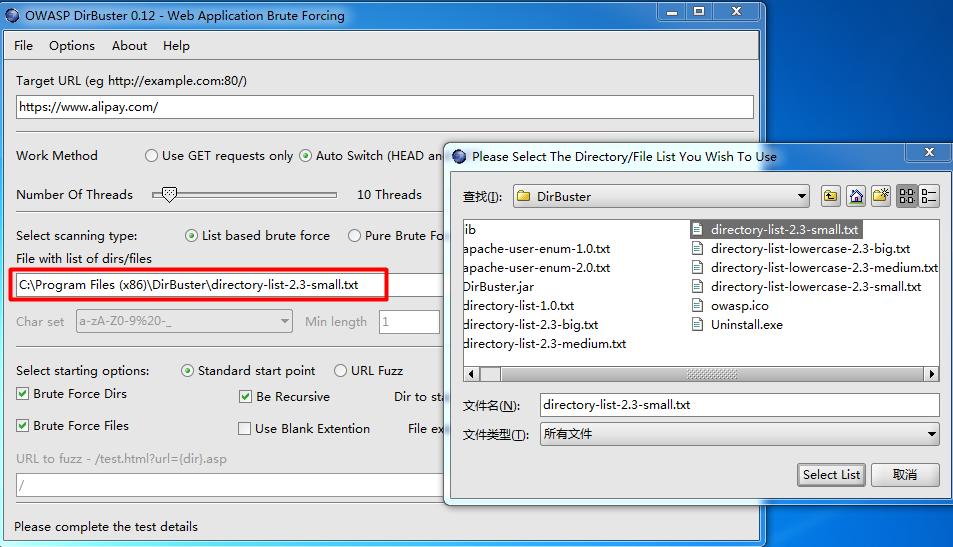
<https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project>

http://sourceforge.net/projects/dirbuster/

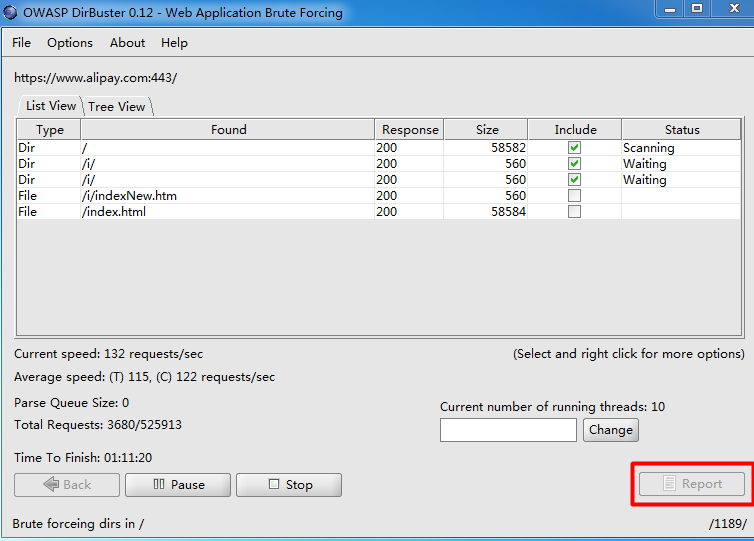
* 双击运行DirBuster.jar
* 在URL中输入目标URL或者主机IP地址



* 在file with list of dirs/files 栏后点击browse，选择破解的字典库为directory-list-2.3-small.txt



* 将File extension中填入正确的文件后缀，默认为php，如果为jsp页面，需要填入jsp
* 其他选项不变，点击右下角的start，启动目录查找



* 观察返回结果，可点击右下角的report，生成目录报告

### DirBuster优缺点

优点：

* 敏感目录发掘能力强
* OWASP安全机构极力推荐

缺点：

* 程序运行线程小
* 探测目录依赖字典文件

## 指纹识别



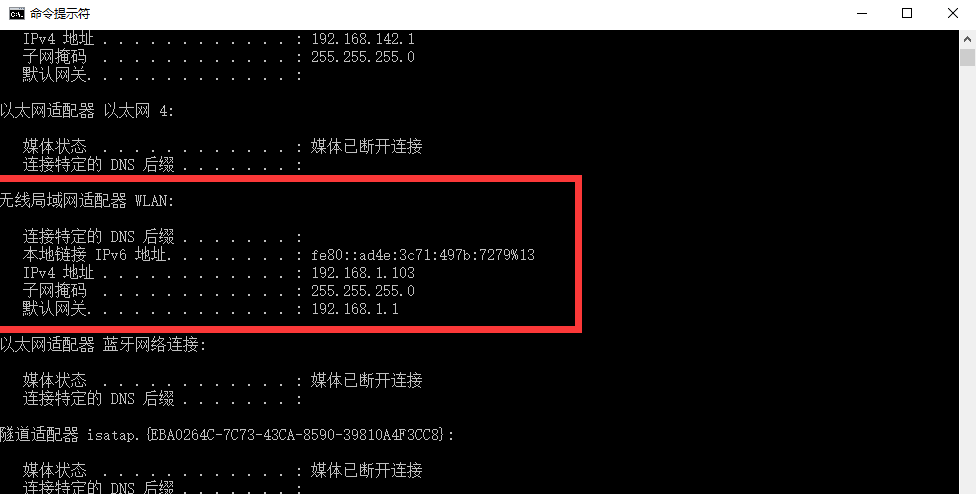
## 扩展：Burp APP抓包

**一、手机端配置**

**1.**让安卓手机和电脑连入同一个WIFI，即是在同一个无线局域网环境下。



**2.**查看电脑的本地IP地址，命令行下输入ipconfig。



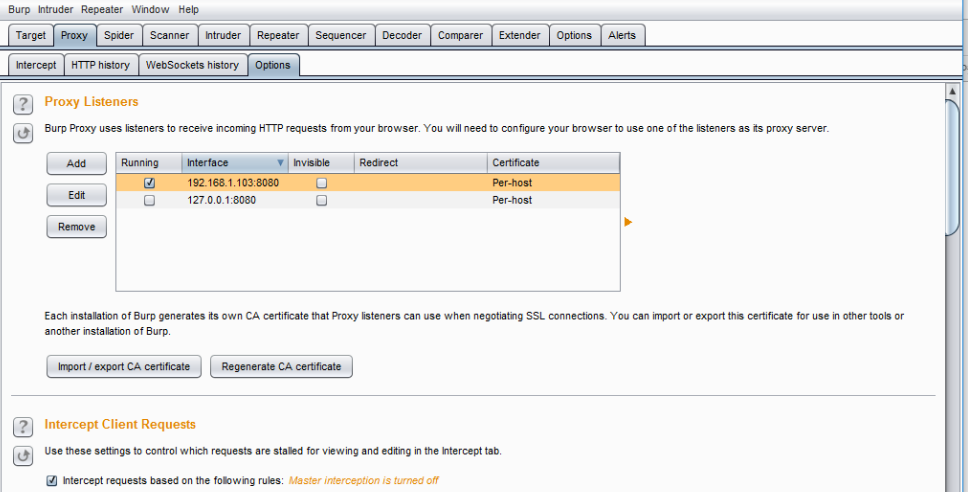
无线局域网的IP地址  
**3.**设置手机代理IP，我这里以oppo系统为例。



代理设置为“手动”，设置主机名为电脑无线局域网IP地址，端口可以随便设置，其他的设置可以默认。

**二、电脑端配置**

**1.**打开Burpsuite，设置Burp suite代理服务器，点击“Proxy”然后“Options”

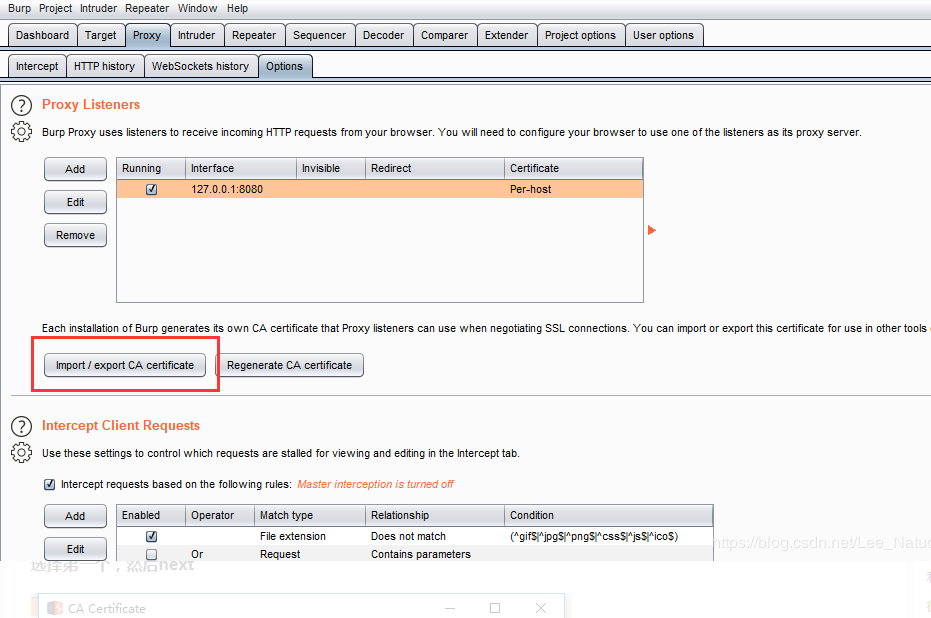


点击“add”添加和手机一样的IP地址和端口，要跟手机上设置的那个端口一致。记得勾上前面的括号。  
  
**2.**设置好了后，在“Proxy”：〉“Intercept”下开启“Intercept is on”就可以对安卓APP的网络数据进行抓包了。

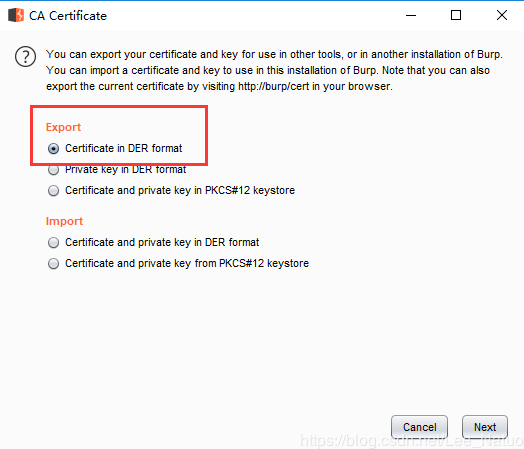
**三、证书安装**

**抓取HTTPS包需要导入Burp的证书。特别注意：一个Burp对应一个证书，就是用哪个Burp抓包就导出哪个的证书，并将该证书在手机上安装。非常重要，因为以前抓包安过证书但是用的不是同一个Burp导致抓包失败，浪费了很多时间。**

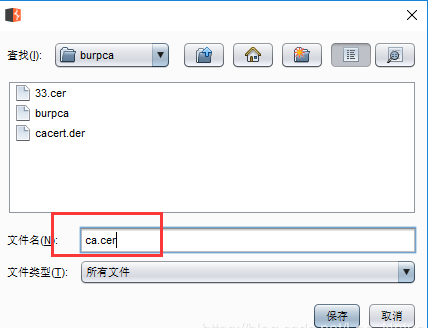
**导出Burp证书步骤为： Proxy---Options----import\export CA**



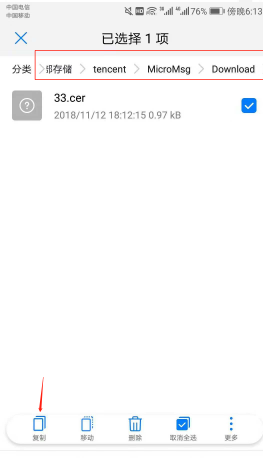
**选择第一个，然后next**



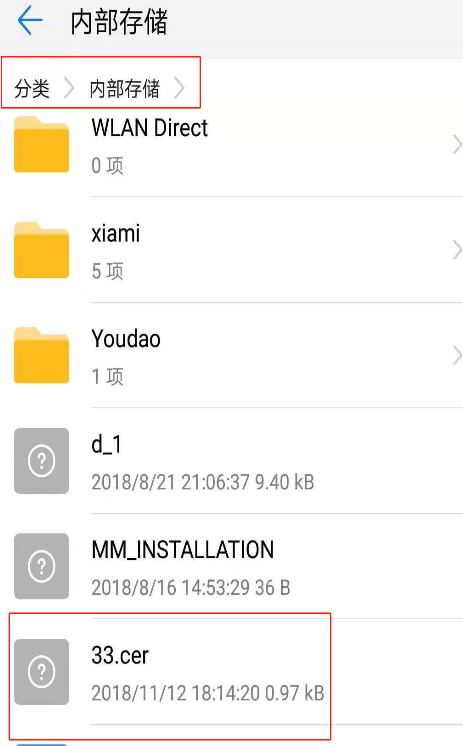
**选择保存的CA路径，文件后缀命名为.cer，非常重要，因为手机只能安装.cer的证书类型，默认的der格式是不能被识别安装的。**



**将证书发送到手机，我是直接微信发送的，然后在微信中下载，并记住下载的目录。**



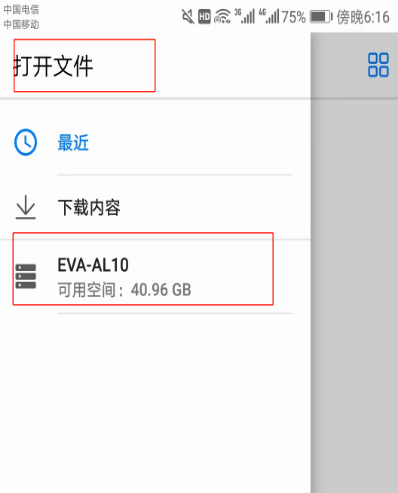
**找到下载的目录，将证书文件复制到手机存储的根目录。**

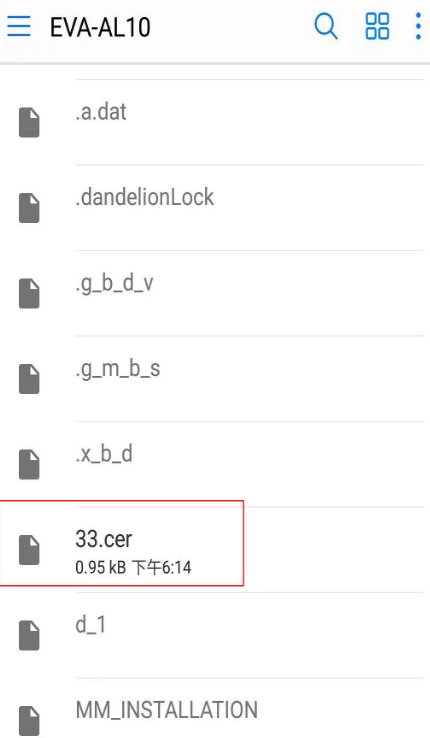


**打开手机设置--其它设置--安全和隐私--更多安全设置--从SD卡安装**



**到根目录下，找到.cer文件，安装.cer证书，重命名个名字**







**成功安装后，可以在手机----设置----安全和隐私----更多安全设置----受信任的凭据----用户----看到PortSwigger文件。**

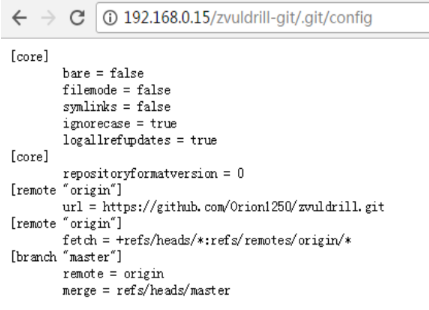


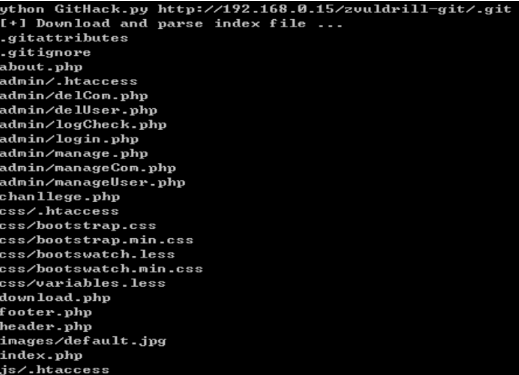


**至此，安装完成。全部工作完成，可以打开burp，准备抓包了。**

## 扩展:常见信息泄露利用方法

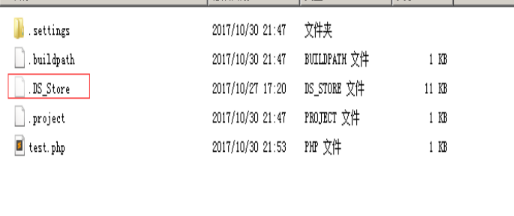
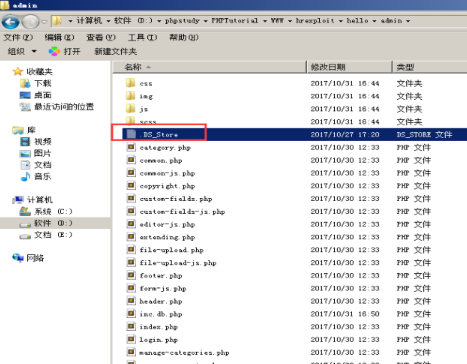
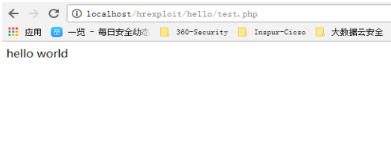
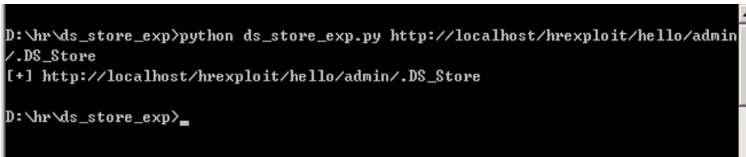
**一、Git导致文件泄露**

由于目前的 web 项目的开发采用前后端完全分离的架构:前端全部使用静态文件，和后端代码完全分离，隶属两个不同的项目。表态文件使用 git 来进行同步发布到服务器，然后使用nginx 指向到指定目录，以达到被公网访问的目的。  
 在运行git init初始化代码库的时候，会在当前目录下面产生一个.git的隐藏文件，用来记录代码的变更记录等等。在发布代码的时候，把.git这个目录没有删除，直接发布了。使用这个文件，可以用来恢复源代码  
 



**二、DS\_store导致文件泄露**

.DS\_Store是Mac下Finder用来保存如何展示文件//文件夹的数据文件，每个文件夹下对应一个。由于开发/设计人员在发布代码时未删除文件夹中隐藏的.DS\_store，可能造成文件目录结构泄漏、源代码文件等敏感信息的泄露。  
我们可以模仿一个环境，利用phpstudy搭建PHP环境，把.DS\_store文件上传到相关目录。

  
然后利用工具进行相关检测  
  
工具下载地址：<https://github.com/lijiejie/ds_store_exp>  
为了让实验更真实，我们在本地搭建环境，然后建立一个文件夹为admin和一个hello文件夹，利用该工具运行完以后，查看工具文件夹查看有什么结果。  
   
此文件和我们在一个文件夹内，如果是苹果用户，把文件copy到相关服务器目录以后，都会默认带一个文件.DS\_Store。首先访问test.php文件，查看环境是否成功。  
   
环境搭建成功 我们利用工具进行测试，运行完如上图，运行完以后我们可以到工具目录进行查看  
 这是一个.DS\_Store文件泄漏利用脚本，它解析.DS\_Store文件并递归地下载文件到本地。

**三、SVN导致文件泄露**

Subversion，简称SVN，是一个开放源代码的版本控制系统，相对于的RCS、CVS，采用了分支管理系统，它的设计目标就是取代CVS。互联网上越来越多的控制服务从CVS转移到Subversion。  
 Subversion使用服务端—客户端的结构，当然服务端与客户端可以都运行在同一台服务器上。在服务端是存放着所有受控制数据的Subversion仓库，另一端是Subversion的客户端程序，管理着受控数据的一部分在本地的映射（称为“工作副本”）。在这两端之间，是通过各种仓库存取层（Repository Access，简称RA）的多条通道进行访问的。这些通道中，可以通过不同的网络协议，例如HTTP、SSH等，或本地文件的方式来对仓库进行操作。  
SVN漏洞在实际渗透测试过程中，利用到也比较多，由于一些开发管理员疏忽造成，原理类似DS\_Store漏洞。我们这里不再进行搭建环境，给大家推荐工具，利用方法如下：

1) 漏洞利用工具： Seay SVN漏洞利用工具  
2) 添加网站url  
在被利用的网址后面加 /.svn/entries，列出网站目录，甚至下载整站  
  
下载地址：<https://pan.baidu.com/s/1jGA98jG>

**四、WEB-INF/web.xml泄露**

WEB-INF是Java的WEB应用的安全目录。如果想在页面中直接访问其中的文件，必须通过web.xml文件对要访问的文件进行相应映射才能访问。

WEB-INF主要包含一下文件或目录：

/WEB-INF/web.xml：Web应用程序配置文件，描述了 servlet 和其他的应用组件配置及命名规则。

/WEB-INF/classes/：含了站点所有用的 **class** 文件，包括 **servlet** **class** 和非**servlet** **class**，他们不能包含在 .**jar**文件中

/WEB-INF/lib/：存放web应用需要的各种JAR文件，放置仅在这个应用中要求使用的jar文件,如数据库驱动jar文件

/WEB-INF/src/：源码目录，按照包名结构放置各个java文件。

/WEB-INF/database.properties：数据库配置文件

原因：  
通常一些web应用我们会使用多个web服务器搭配使用，解决其中的一个web服务器的性能缺陷以及做均衡负载的优点和完成一些分层结构的安全策略等。在使用这种架构的时候，由于对静态资源的目录或文件的映射配置不当，可能会引发一些的安全问题，导致web.xml等文件能够被读取

## 扩展: ZoomEye hack

ZoomEye 支持公网设备指纹检索和 Web指纹检索的网站，指纹检索包括应用名称、版本、前端框架、后端框架、服务端语言、服务器操作系统、网站容器、内容管理系统和数据库等。  
设备指纹包括应用名、版本、开放端口、操作系统、服务名、地理位置等。

**1、实战搜索**

我们今天主要讲下如何使用他的语法规则去高级搜索，搜索有用信息。

* **主机设备搜索组件名称**  
  app: 组件名  
  ver: 组件版本  
  例1：搜索使用iis6.0主机：app:"Microsoft-IIS" ver"6.0"，可以看到0.6秒搜索到41，781,210左右的使用iis6.0的主机。

例2：搜索使weblogic主机：app:"weblogic httpd" port:7001，可以看到0.078秒搜索到42万左右的使用weblogic的主机。

例3：查询开放3389端口的主机：port:3389

例4：查询操作系统为Linux系统的服务器，os:linux

例5：查询公网摄像头：service:”routersetup”

例6：搜索美国的 Apache 服务器：app:Apache country:US 后面还可以接city: 城市名称

例7：搜索指定ip信息，ip:121.42.173.26

例8：查询有关taobao.com域名的信息，site:taobao.com

例9：搜索标题中包含该字符的网站，title:weblogic

例10：keywords:Nginx

## 扩展: fofa hack

domain=""||ip=""||host=""||title=""||header=""  
protocol="https"，搜索指定协议类型

app="phpinfo"搜索某些组件相关系统

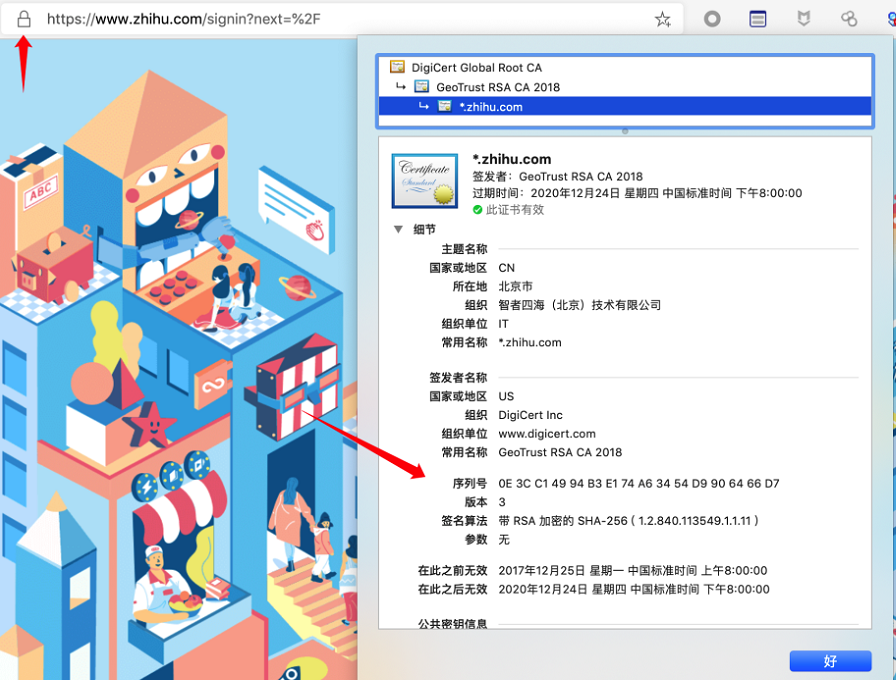
host="oldboyedu.com/"搜索包含有特定字符的URL

title="powered by" && os==windows搜索网页标题中包含有特定字符并且系统是windows的网页

详细请看官方详细文档; <https://fofa.info/help>

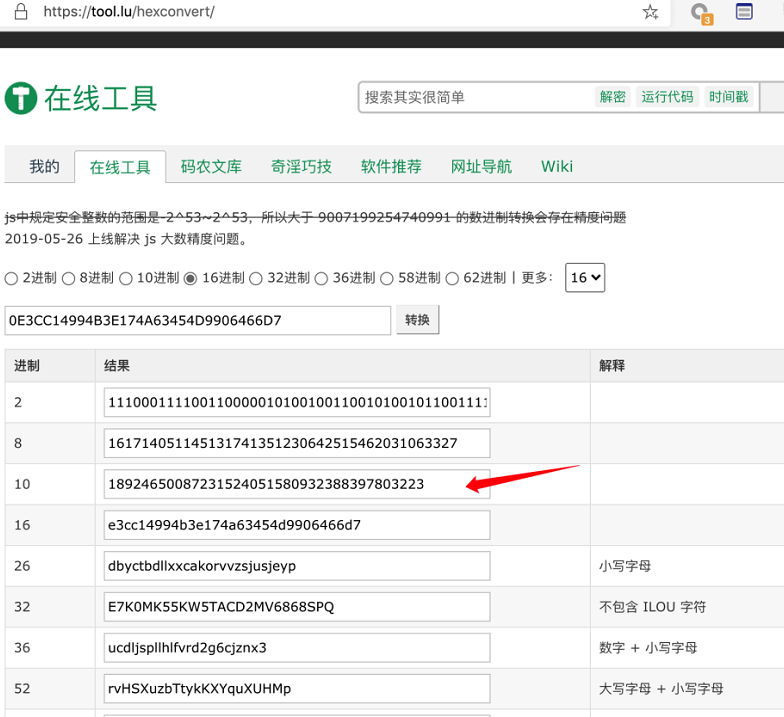
案例一：找知乎的真实ip，可以打开知乎网站右击查看源代码，找到Title=”关键字”，直接fofa里面输入：title="知乎.有问题,上知乎"

案例二：还是以知乎为例吧，知乎网站使用的是https，我们看一下其证书序列号



一串16进制字符，我们需要将其调整为10进制来满足知乎的搜索结果

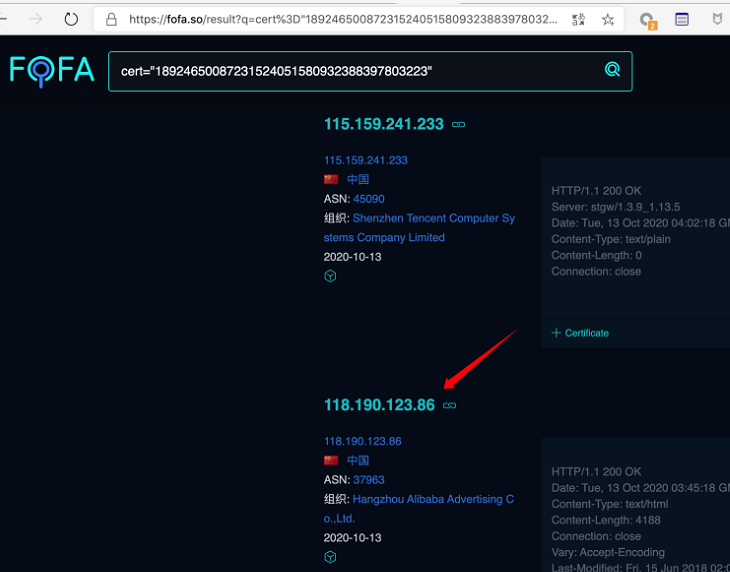
https://tool.lu/hexconvert



转成10进制为

18924650087231524051580932388397803223

重点来了，我们在fofa中使用cert 语法进行查询



<https://github.com/Threezh1/JSFinder>

## 政府网站信息收集

http:*//114.55.181.28/databaseInfo/index*