

# 红队技术 第二关 信息收集

---

**任务目标：**任选一个自己感兴趣的目标，在对其进行攻击之前，了解企业基本信息是第一步。

**收集信息包括：**

- 1、组织架构：董事长、CEO、CFO、CMO、CTO、COO 等
- 2、员工信息：姓名、地址、电话、邮箱等
- 3、三方合作公司：供应商、子公司
- 4、办公公司地址
- 5、企业业务范围

**涉及工具：**搜索引擎，推荐谷歌、必应、github、网盘等

**报告要求：**

- 1、任选一个目标，对目标进行信息收集，主要关注企业经营范围、公司组织结构、员工名单、内部邮箱后缀、公司一级域名、合作公司或者子公司信息
- 2、通过搜索引擎获取该企业无意泄漏的隐私数据，包括代码泄漏、员工花名册、内部使用的文档、vpn和邮箱等公用系统的类型等
- 3、将信息收集的过程进行记录，梳理常见信息收集方式和方法，尽可能多的对目标企业进行了解和信息梳理

## 前言

---

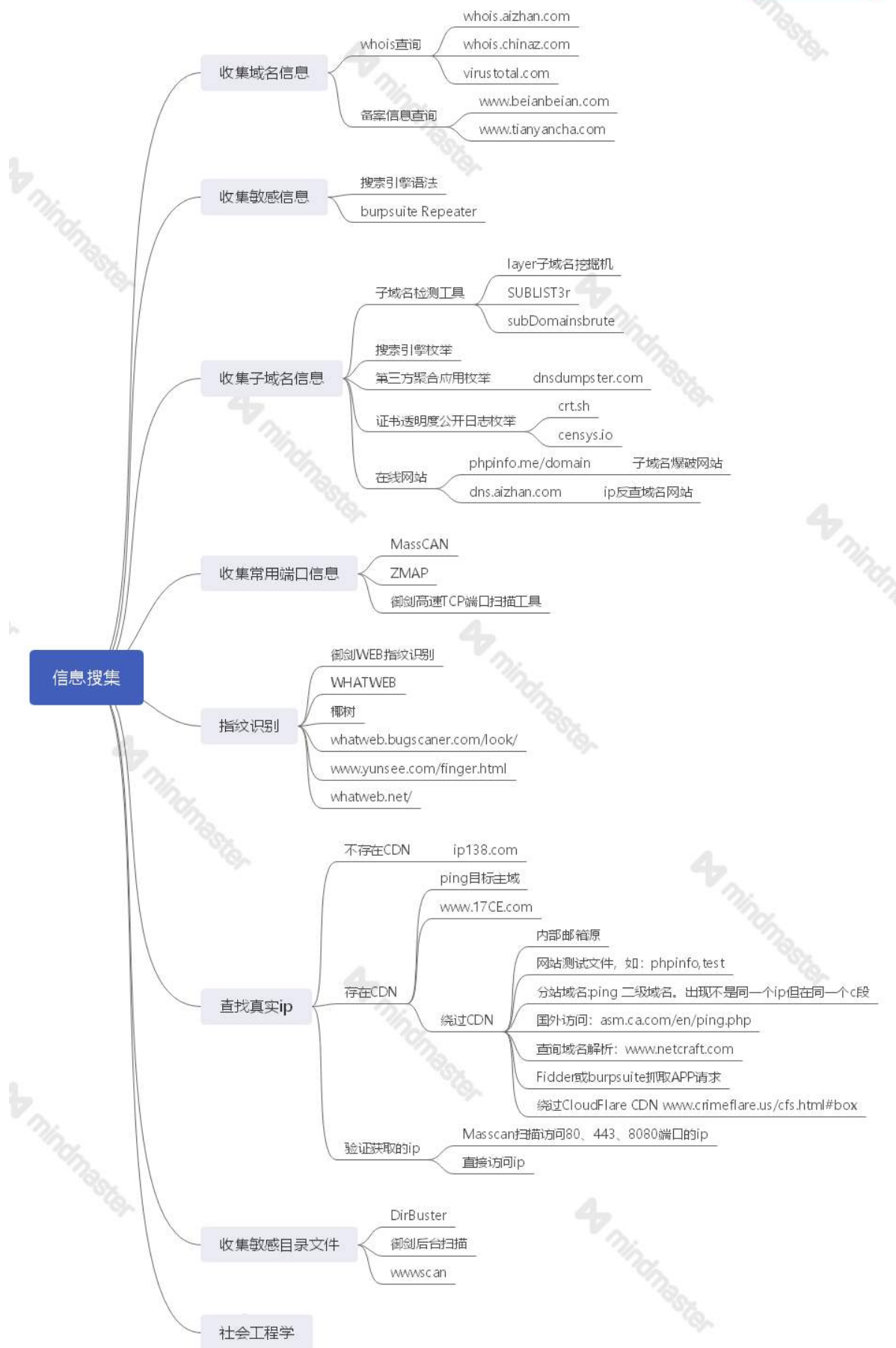
信息搜集作为渗透测试的第一步，具有重大的意义。信息搜集全面与否直接影响着渗透测试的效果，因此，必须仔细学习信息收集。

本报告选择的信息搜集实验公司为：**同程网络科技股份有限公司**

## 背景知识

---

根据《WEB安全攻防-渗透测试实战指南》一书，整理了一下信息收集的基本流程和所需工具



## 同程基本信息收集

对同程网络科技股份有限公司进行信息搜集，首先要收集它的企业信息。企业信息包括：

## 公司主要领导人



子公司情况

## 收集域名信息

whois查询

域名	www.ly.com
注册商	Xiamen 35.Com Technology Co., Ltd.
参照页	-
创建时间	1995-08-17
更新时间	2020-08-25
过期时间	2022-08-16
域名服务器	whois.verisign-grs.com
域名服务器	whois.35.com
DNS服务器	ns3.dnsv4.com - 61.129.8.140
DNS服务器	ns4.dnsv4.com - 61.151.180.50
域名状态	运营商设置了禁止转移保护 <a href="https://icann.org/epp">https://icann.org/epp</a>

## 查询网站备案

### 网站备案信息查询

主办单位名称	同程网络科技股份有限公司
主办单位性质	企业
网站备案/许可证号	苏ICP备09033604号
网站名称	同程旅行
网站首页网址	ly.com
审核时间	2009-04-08

工具简介：

网站备案信息查询工具、网站备案信息查询、网站备案信息查询、网站备案信息查询

这里使用的是

[www.beian88.com](http://www.beian88.com)

## 收集子域名信息

### 利用搜索引擎特殊语法

site: ly.com



热招职位更多>> 产品经理 同程校园小管家(校园大使)-江苏/安徽 前端开发实习生(北京) 算法实习生(北京) Java开发工程师(实习)-北京 同业销售(上海)长招职位更多>> 产品经理 自营产品经理—周边...

job.ly.com/   保障 百度快照

[汽车票首页](#)

购票成功后,会生成取票信息并发送短信给您,请您凭该取票短信和身份证原件到发车站自助取票机或服务专窗取票。可以以亲朋好友代取票吗?可以由他人代取票,代取人需凭取票信息和乘车人身份证前往自...

bus.ly.com/   保障 百度快照

[境内游](#) [自由行](#) [跟团游](#) [自由行攻略](#) [自助游](#) [同程旅游境内游](#)

同程上海旅游网提供从上海出发到全国各地旅游线路报价,在线预订享受上海旅行社团购优惠价,低至3折起!同程旅游,快乐每一程!

[gny.ly.com/](http://gny.ly.com/)   保障  百度快照

[同程旅行](#) [旅游](#) [旅游线路](#) [旅行](#) [出国旅游](#) [自驾游](#) [周边游](#) [旅...](#)



同程旅行(LY.COM)是一家专业的一站式旅游预订平台,提供近万家景点门票、特价机票、出国旅游、周边游、自驾游及酒店预订服务,专业旅游线路服务,让您的旅行更安心!

www.17u.com/  保障  百度快照

[ship.ly.com/](http://ship.ly.com/)

您好,请 [登录](#) [免费注册](#) [我的同程](#) [首页](#) [酒店](#) [国内酒店](#) [海外酒店](#) [机票](#) [国内机票](#) [国际机票](#) [同程商旅](#)  
[火车票](#) [汽车](#) [船票](#) [汽车票](#)[首页](#) [团队包车](#) [船票](#) [景点](#) [国内景点](#) [周边跟团游](#)...

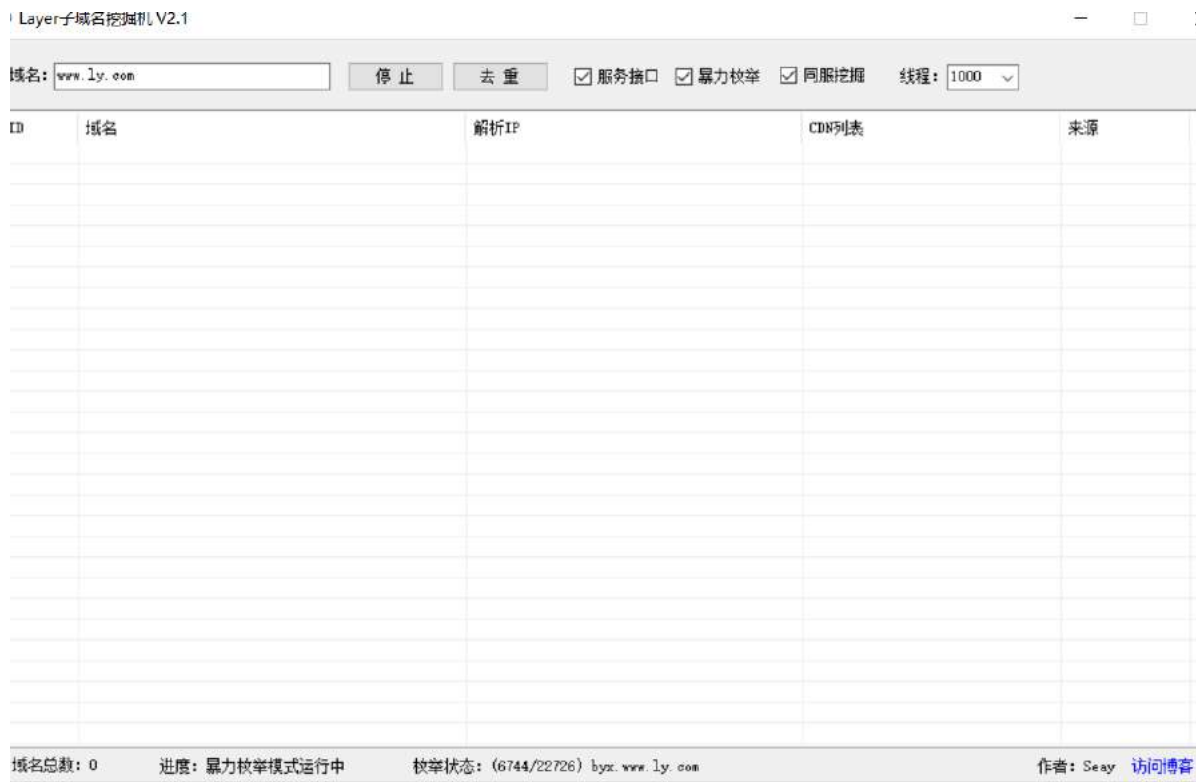
ship.ly.com/   保障 百度快照

[自由行首页](#)

[首页](#) [酒店](#) [国内酒店](#) [海外酒店](#) [机票](#) [国内机票](#) [国际机票](#) [同程商旅](#) [火车票](#) [汽车](#) [船票](#) [汽车票](#) [首页](#) [团队包车](#) [船票](#) [景点](#) [国内景点](#) [周边跟团游](#) [主题景点](#) [景点活动](#) [定制旅行](#) [迪...](#)

## layer子域名挖掘机

layer子域名挖掘机的使用方法非常简单，输入域名点击开始即可了。

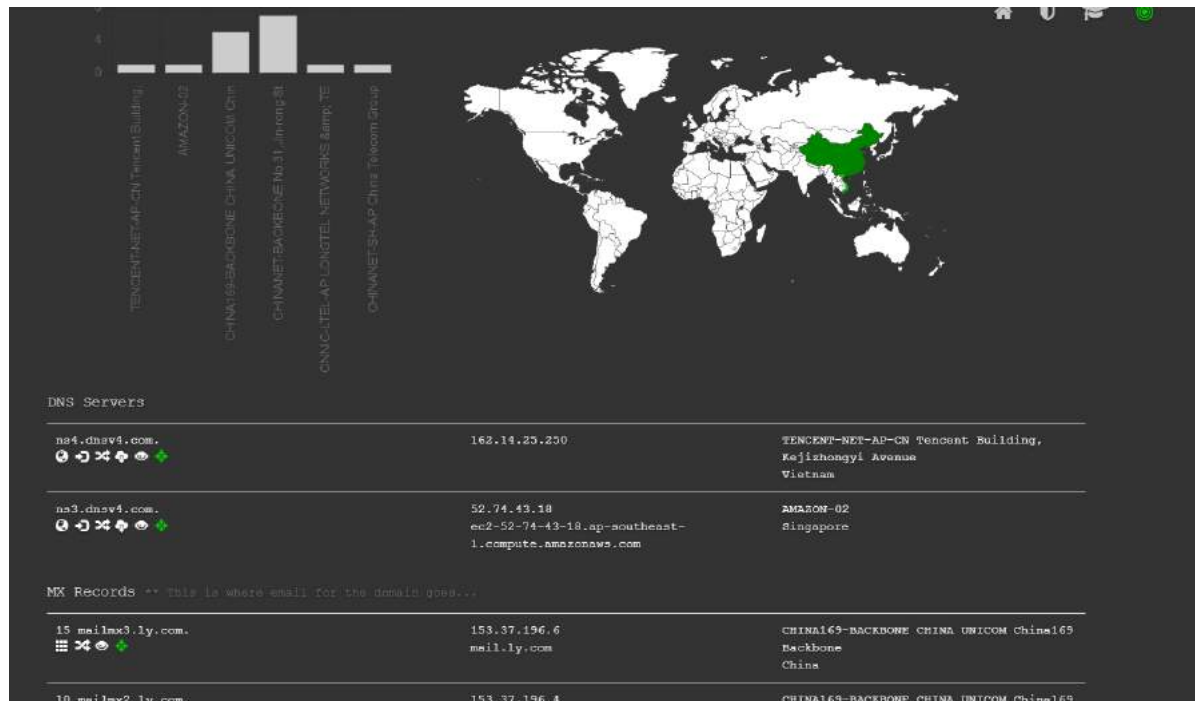


还在努力的挖掘，效率似乎不高哇。

## 在线工具

这里使用了DNSdumpster

[DNSdumpster.com](https://dnsdumpster.com) - dns recon and research, find and lookup dns records



## 服务器信息识别

### cms指纹识别

CMS（内容管理系统）又称为**整站系统或文章系统**，用于网站内容管理。用户只需要下载对应的CMS 软件包，就能部署搭建，并直接利用CMS。但是各种CMS都具有其独特的结构命名规则和特定的文件内容，因此可以利用这些内容来获取CMS站点的具体软件CMS与版本。在渗透测试中，对进行指纹识别是相当有必要的，**识别出相应的CMS，才能查找与其相关的漏洞**，然后才能进行相应的渗透操作。常见的CMS有Dedecms(织梦)、Discuz、PHPWEB、PHPWind、PHPCMS、ECShop、Dvbbs、SiteWeaver、ASPCMS、帝国、Z-Blog、WordPress等。

### 在线查询

好多网站都需要收费或者注册啊，qaq。这里使用了<http://whatweb.bugscaner.com/look/>查询了同程的cms信息和同ip网站信息

在线同IP网站查询工具

请输入网址比如: <http://dns.bugscaner.com> [查询一下](#)

IP地址 118.25.167.139 所在地区为: 上海市 腾讯云, 共有 2 个域名解析到该IP。

id	网址	状态码	标题	可能使用的 cms	环境探测
1	<a href="http://sh.node.toy/gaib.com">sh.node.toy/gaib.com</a>	200	正在获取中	!	!
2	<a href="http://zby.ly.com">zby.ly.com</a>	200	正在获取中	!	!

[上一页](#) [1](#) [下一页](#)



lcp备案查询:www.ly.com
whois查询:www.ly.com
address:上海市 腾讯云
JavaScript Frameworks:jQuery 1.11.3
Programming Languages:Lua
Web Servers:Nginx,OpenResty 1.15.8.2
子域名查询:www.ly.com
网站cdn服务商查询:www.ly.com

## kali whatweb 指纹查询

kali是自带whatweb工具的 因此在kali中直接运行命令:

```
whatweb www.ly.com
```

```
root@kali:~/桌面# whatweb www.ly.com
/usr/lib/ruby/vendor_ruby/target.rb:188: warning: URI.escape is obsolete
/usr/lib/ruby/vendor_ruby/target.rb:188: warning: URI.escape is obsolete
http://www.ly.com [301 Moved Permanently] Country[CHINA][CN], HTTPServer[openresty], IP[118.25.167.139], RedirectLocation[https://www.ly.com/], Title[301 Moved Permanently]
https://www.ly.com/ [200 OK] Cookies[NCName,NCid,NewProvinceId,NewProvinceName], Country[CHINA][CN], Frame, HTML5, HTTPServer[openresty/1.15.8.2], IP[118.25.167.139], JQuery[1.11.3], Meta-Author[同程旅行], Script[text/javascript], Title[同程旅行_旅游_旅游线路_旅行_出国旅游_自驾游_周边游_旅游网站], UncommonHeaders[janus-time,janus-cache,janus-configid,janus-addr], X-UA-Compatible[IE=Edge]
root@kali:~/桌面#
```

爆出了同程官网的服务器, ip地址, 位置。等都识别了出来。假如对于小的站点, 我们还能识别出他的cms。从而就可以搜索漏洞进行利用了。

假如工具无法利用, 我们还可以:

抓包分析http头 (重点关注Server、X-Powered-By、Cookie)

浏览并观察网站



# 真实ip地址识别

## 了解CDN

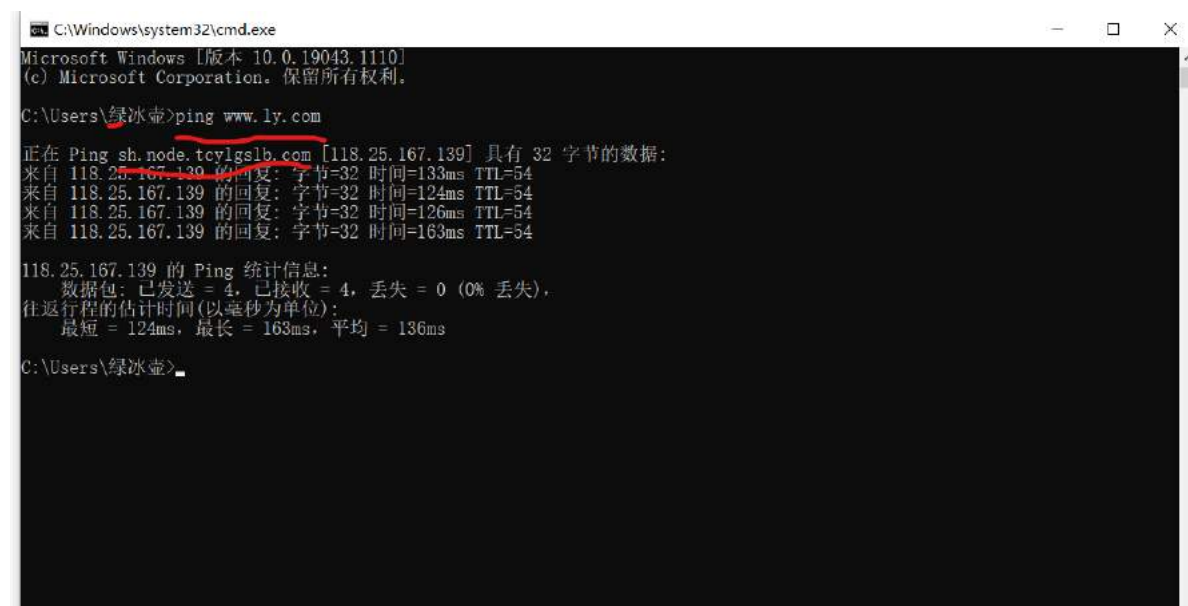
CDN的全称是Content Delivery Network 即**分发内容网络**。CDN是一种智能虚拟网络，依靠部署在各地的边缘服务器，受中心平台方的统筹规划，均衡负载，平衡调度内容分发。从而使用户就近获取所需内容，降低网络拥塞，提高用户访问响应速度和命中率。CDN的关键技术为内容存储和分发。

CDN将用户经常访问的静态数据资源**直接缓存到节点服务器上**，当用户再次请求时，会**直接分发到在离用户近的节点服务器上**响应给用户，当用户**有实际数据交互时才会从远程Web服务器上响应**，这样可以大大提高网站的响应速度及用户体验。

因此，如果目标服务器使用了CDN服务，那么我们直接查询到的IP并不是真正的目标服务器的IP，而是一台离你最近的目标节点的CDN服务器，这就导致了没法直接得到目标服务器的真实IP。

## 如何判断是否使用了cdn

使用ping 命令



```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 10.0.19043.1110]
(c) Microsoft Corporation. 保留所有权利。

C:\Users\绿冰壶>ping www.ly.com

正在 Ping sh.node.tcylgslb.com [118.25.167.139] 具有 32 字节的数据:
来自 118.25.167.139 的回复: 字节=32 时间=133ms TTL=54
来自 118.25.167.139 的回复: 字节=32 时间=124ms TTL=54
来自 118.25.167.139 的回复: 字节=32 时间=126ms TTL=54
来自 118.25.167.139 的回复: 字节=32 时间=163ms TTL=54

118.25.167.139 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 124ms, 最长 = 163ms, 平均 = 136ms

C:\Users\绿冰壶>
```

显而易见同程是使用了cdn的

我们也可以**设置代理或者通过在线ping网站来在不同地区进行ping测试**，然后对比每个地区ping出的IP结果，查看这些IP是否一致，一致，则极有可能不存在CDN。根据CDN的工作原理，如果网站使用了CDN，那么从全国各地访问网站的IP地址是各个CDN节点的IP地址，那么如果ping出来的IP大多不太一样或者规律性很强，可以尝试查询这些IP的归属地，判断是否存在CDN。有以下网站可以进行ping测试：

- <http://ping.chinaz.com/>
- <https://www.wepcc.com>
- <https://www.17ce.com>

以wepcc.com为例

www.ly.com						查询
全部 电信 联通 移动 多线 港澳台 海外						
节点名称	解析IP	IP归属地	响应时间	TTL	赞助商	
广东-东莞 (电信)	111.230.162.155	中国广东广州 tencent.com 电信/联通/移动	4.64 ms	46	快快网络	
福建-厦门 (电信)	118.25.167.139	中国上海 tencent.com 电信/联通/移动	19.81 ms	47	快快网络	
福建-泉州 (电信)	118.25.167.139	中国上海 tencent.com 电信/联通/移动	21.16 ms	47	快快网络	
山东-济南 (联通)	118.25.167.139	中国上海 tencent.com 电信/联通/移动	15.93 ms	49	快快网络	
北京 (移动)	140.143.217.31	中国北京 tencent.com 电信/联通/移动	7.72 ms	52	移动云	
北京 (多线)	140.143.217.31	中国北京 tencent.com 电信/联通/移动	4.37 ms	52	快快网络	
广东-深圳 (多线)	111.230.162.155	中国广东广州 tencent.com 电信/联通/移动	6.26 ms	48	快快网络	
江苏-扬州 (多线)	118.25.167.139	中国上海 tencent.com 电信/联通/移动	8.86 ms	45	快快网络	
浙江-宁波 (多线)	118.25.167.139	中国上海 tencent.com 电信/联通/移动	11.58 ms	44	快快网络	
浙江-杭州 (多线)	118.25.167.139	中国上海 tencent.com 电信/联通/移动	13.66 ms	52	快快网络	
贵州-贵阳 (多线)	140.143.84.81	中国四川成都 tencent.com 电信/联通/移动	14.46 ms	45	快快云	
中国-香港 (港澳台)	119.28.165.56	中国香港 tencent.com	1.66 ms	55	阿里云国际版	
中国-香港 (港澳台)	119.28.165.55	中国香港 tencent.com	0.41 ms	57	快快网络	
日本 (海外)	43.132.83.43	日本 wide.ad.jp	8.85 ms	51	阿里云	
泰国-曼谷 (海外)	150.109.190.111	泰国曼谷 tencent.com	5.15 ms	47	快快网络	

发现在各地ping出的ip有不同的情况说明其使用了cdn

## 绕过cdn查询真实ip

### 1利用子域名。

一般来说很多站长可能只会对主站或者流量较大的分站使用CDN，但是一些流量比较小的分站可能没有挂CDN，这些分站和主站虽然不是同一个IP但是都在同一个C段下面的情况，所以我们可以通过ping二级域名获取分站IP，从而能判断出目标的真实IP段。

利用baidu hacking 搜索引擎语法找一些同程子站

[同程旅行](#) [旅游](#) [旅游线路](#) [旅行](#) [出国旅游](#) [自驾游](#) [周边游](#) [旅...](#)

同程旅行(LY.COM)是一家专业的一站式旅游预订平台,提供近万家景点门票、特价机票、出国旅游、周边游、自驾游及酒店预订服务;专业旅游线路服务、让您的旅行更安心!

www.17u.com/ 百度快照

[船票首页](#)

同程旅行网为您提供船票查询 船票网上订票 官网信息 船票预订 船票查询时刻表 热门航线 江门香港船票 鹿回头到凤凰岛船票 威海到刘公岛船票 珠海到深圳船票 苏梅岛到曼谷船票 ...

ship.ly.com/ 百度快照

[自由行首页](#)

首页 酒店 国内酒店 海外酒店 机票 国内机票 国际机票 同程商旅 火车票 汽车 船票 汽车票首页 团队包车 船票 景点 国内景点 周边跟团游 主题景点 景点活动 定制旅行 通...

zby.ly.com/ 百度快照

[同程旅行](#) [旅游](#) [旅游线路](#) [旅行](#) [出国旅游](#) [自驾游](#) [周边游](#) [旅...](#)

同程旅行(LY.COM)是一家专业的一站式旅游预订平台,提供近万家景点门票、特价机票、出国旅游、周边游、自驾游及酒店预订服务;专业旅游线路服务、让您的旅行更安心!

www.ly.com/ 百度快照

[境内游](#) [自由行](#) [跟团游](#) [自由行攻略](#) [自助游](#) [同程旅游境内游](#)

同程上海旅游网提供从上海出发到全国各地旅游线路报价,在线预订享受上海旅行社团购优惠价,低至3折起!同程旅游,快乐每一程!

gny.ly.com/ 百度快照

为您推荐: [境内自由行](#) [境内跟团游](#) [凤阳旅游网](#) [新手旅游攻略怎么做](#)

- 南京疫情已蔓延至15省份267
- 河南强降雨已致99人遇难
- 陈梦4-2孙颖莎乒乓球女单夺
- 官方:暂不要来张家界市旅游
- #郎平没想到朱婷伤这么重
- #伊藤美诚夺乒乓球女单铜牌#

全球Ping测试

<https://gny.ly.com> 查询

全部 电信 联通 移动 多线 港澳台 海外

节点名称	解析IP	IP归属地	响应时间	TTL	赞助商
广东-东莞 (电信)	111.230.162.155	中国广东广州 tencent.com 电信/联通/移动	4.71 ms	46	快快网络
福建-厦门 (电信)	118.25.167.139	中国上海 tencent.com 电信/联通/移动	19.66 ms	47	快快网络
福建-泉州 (电信)	118.25.167.139	中国上海 tencent.com 电信/联通/移动	21.17 ms	47	快快网络
山东-济南 (联通)	118.25.167.139	中国上海 tencent.com 电信/联通/移动	15.97 ms	49	快快网络
北京 (移动)	140.143.217.31	中国北京 tencent.com 电信/联通/移动	4.92 ms	52	移动云
北京 (多线)	140.143.217.31	中国北京 tencent.com 电信/联通/移动	4.37 ms	52	快快网络
广东-深圳 (多线)	111.230.162.155	中国广东广州 tencent.com 电信/联通/移动	6.28 ms	48	快快网络
江苏-扬州 (多线)	118.25.167.139	中国上海 tencent.com 电信/联通/移动	8.75 ms	45	快快网络
浙江-宁波 (多线)	118.25.167.139	中国上海 tencent.com 电信/联通/移动	11.64 ms	44	快快网络
浙江-杭州 (多线)	118.25.167.139	中国上海 tencent.com 电信/联通/移动	13.71 ms	52	快快网络
贵州-贵阳 (多线)	140.143.84.81	中国四川成都 tencent.com 电信/联通/移动	14.47 ms	45	快快云
中国-香港 (港澳台)	118.25.167.139	中国上海 tencent.com 电信/联通/移动	310.24 ms	46	阿里云国际版
中国-香港 (港澳台)	118.25.167.139	中国上海 tencent.com 电信/联通/移动	30.39 ms	46	快快网络

里输入你要搜索的内容

用在线工具ping 以下 好像不太好使呢。

## 2 查询主域

使用CDN有一个约定俗成的习惯，只让www域名使用cdn 秃域名不使用。所以我们可以尝试把www去掉 再ping以下看一看ip是不是变了。

```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 10.0.19043.1110]
(c) Microsoft Corporation. 保留所有权利。

C:\Users\绿冰壶>ping www.ly.com

正在 Ping sh.node.tcylgslb.com [118.25.167.139] 具有 32 字节的数据:
来自 118.25.167.139 的回复: 字节=32 时间=133ms TTL=54
来自 118.25.167.139 的回复: 字节=32 时间=124ms TTL=54
来自 118.25.167.139 的回复: 字节=32 时间=126ms TTL=54
来自 118.25.167.139 的回复: 字节=32 时间=163ms TTL=54

118.25.167.139 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 124ms, 最长 = 163ms, 平均 = 136ms

C:\Users\绿冰壶>ping ly.com

正在 Ping ly.com [61.177.22.232] 具有 32 字节的数据:
来自 61.177.22.232 的回复: 字节=32 时间=128ms TTL=50
来自 61.177.22.232 的回复: 字节=32 时间=137ms TTL=50
来自 61.177.22.232 的回复: 字节=32 时间=59ms TTL=50
来自 61.177.22.232 的回复: 字节=32 时间=55ms TTL=50

61.177.22.232 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 55ms, 最长 = 137ms, 平均 = 94ms

C:\Users\绿冰壶>
```

## 3扫描网站敏感文件

如phpinfo.php等，从而找到目标的真实IP。

## 4从国外访问

国内很多CDN厂商因为各种原因只做了国内的线路，而针对国外的线路可能几乎没有，此时我们使用国外的主机直接访问可能就能获取到真实IP。我们可以通过国外在线代理网站访问，可能会得到真实的IP地址，外国在线代理网站：

<https://asm.ca.com/en/ping.php>

Ping a server or web site using our network of over 60 monitoring stations worldwide

www. .com (e.g. www.yahoo.com) Start

Ping to: www.freebuf.com

Checkpoint	Result	min. rtt	avg. rtt	max. rtt	IP
India - Bangalore (inbr01)	Packets lost (100%)				123. 29.169
Bulgaria - Sofia (bgso03)	Packets lost (100%)				123. 29.169
Australia - Brisbane (aubr03)	Packets lost (100%)				123. 29.169
United States - Council Bluffs (uscb01)	Packets lost (100%)				123. 29.169
India - Chennai (inche01)	Packets lost (100%)				123. 29.169
United Kingdom - Cardiff (gbcar01)	Packets lost (100%)				123. 29.169
United States - Cheyenne (usche01)	Packets lost (100%)				123. 29.169
United States - Charleston (uscho02)	Packets lost (100%)				123. 29.169
United States - Charleston (uscho01)	Packets lost (100%)				123. 29.169
Canada - Toronto (cator03)	Packets lost (100%)				123. 29.169
Czech Republic - Prague (czprg02)	Packets lost (100%)				123. 29.169
Germany - Berlin (deber01)	Packets lost (100%)				123. 29.169
Germany - Frankfurt (defra05)	Packets lost (100%)				123. 29.169
Ireland - Dublin (iedub03)	Packets lost (100%)				123. 29.169
Austria - Vienna (atvie02)	Packets lost (100%)				123. 29.169
Netherlands - Eindhoven (nieem01)	Packets lost (100%)				123. 29.169
France - Paris (frpar05)	Packets lost (100%)				123. 29.169
United Kingdom - London (gblon03)	Packets lost (100%)				123. 29.169
United Kingdom - Edinburgh (gbedi01)	Packets lost (100%)				123. 29.169
Greece - Athens (grath02)	Packets lost (100%)				123. 29.169
China - Hong Kong (hkkg03)	Packets lost (100%)				123. 29.169
Finland - Helsinki (finhm01)	Packets lost (100%)				123. 29.169
Hungary - Budapest (hubud02)	Packets lost (100%)				123. 29.169
Italy - Milan (itmil01)	Packets lost (100%)				123. 29.169
Indonesia - Jakarta (idjak02)	Packets lost (100%)				123. 29.169
India - Mumbai (inbm03)	Packets lost (100%)				123. 29.169
London - Tel Aviv (telav01)	Packets lost (100%)				123. 29.169

Help

## 5通过邮件服务器。

一般的邮件系统都在内部，没有经过CDN的解析，通过目标网站用户注册或者RSS订阅功能，查看邮件，寻找邮件头中的邮件服务器域名IP，ping这个邮件服务器的域名，由于这个邮件服务器的有可能跟目标Web在一个段上，我们直接一个一个扫，看返回的HTML源代码是否跟web的对的上，就可以获得目标的真实IP(必须是目标自己内部的邮件服务器，第三方或者公共邮件服务器是没有用的)。

## 6查看域名历史解析记录。

也许目标很久之前没有使用CDN，所以可能会存在使用CDN前的记录。所以可以通过<https://www.netcraft.com>、<https://viewdns.info/>等网站来观察域名的IP历史记录。

## 验证获得的真实IP地址

通过上面的方法获取了很多的IP地址,此时我们需要确定哪一个才是真正的IP地址，如果是Web，最简单的验证方法是**直接尝试用IP访问**，看看响应的页面是不是和访问域名返回的一样即可。

## 收集常用端口信息

在渗透的过程中，收集端口信息是一个十分重要的过程，通过扫描目标服务器开放的端口可以从该端口判断服务器运行的服务。并且针对不同端口有不同攻击方法，获取端口信息有助于我们对症下药，渗透服务器。

## nmap工具

kali里集成了nmap工具，利用nmap扫描端口的口令如下

```
nmap -A -T4 -O -Sv 目标域名
```



```
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)

Completed Ping Scan at 21:46, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:46
Completed Parallel DNS resolution of 1 host. at 21:46, 0.08s elapsed
Initiating SYN Stealth Scan at 21:46
Scanning ly.com (61.177.22.232) [1000 ports]
Discovered open port 53/tcp on 61.177.22.232
Discovered open port 443/tcp on 61.177.22.232
Discovered open port 80/tcp on 61.177.22.232
Completed SYN Stealth Scan at 21:46, 5.03s elapsed (1000 total ports)
Initiating Service scan at 21:46
Scanning 3 services on ly.com (61.177.22.232)
Completed Service scan at 21:46, 5.01s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against ly.com (61.177.22.232)
Initiating Traceroute at 21:46
Completed Traceroute at 21:46, 9.08s elapsed
NSE: Script scanning 61.177.22.232.
Initiating NSE at 21:46
Completed NSE at 21:47, 24.08s elapsed
Initiating NSE at 21:47
Completed NSE at 21:47, 0.62s elapsed
Initiating NSE at 21:47
Completed NSE at 21:47, 0.00s elapsed
Nmap scan report for ly.com (61.177.22.232)
```

## masscan

masscan号称最快的互联网端口扫描器，最快可以在6分钟扫遍互联网。他的扫描结果与nmap类似，而且更加灵活，允许自定义任意地址和端口范围。

使用命令

```
masscan 118.25.167.139 -p0-65535 --rate=10000
```

```
root@kali:~# masscan 118.25.167.139 -p0-65535 --rate=10000

Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2021-07-29 13:54:32 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [65536 ports/host]

root@kali:~#
```

## 在线探测

工具虽好，通常会在目标网站留下痕迹，这时候在线网站就是一种不错的替代选择。

- 在线网站: <http://tool.chinaz.com/port/>
- ThreatScan在线网站（网站基础信息收集）: <https://scan.top15.cn/>
- Shodan: <https://www.shodan.io/>

这里以ThreatScan为例，但是看样子网站查询的准确度有限

## 查询结果

域名	www.ly.com
源IP	118.25.167.139 (物理地址: China,Beijing,Haidian,AS45090 Shenzhen Tencent Computer Systems Company Limited) 118.25.167.139 (物理地址: China,Beijing,Haidian,AS45090 Shenzhen Tencent Computer Systems Company Limited) 118.25.167.139 (物理地址: China,Beijing,Haidian,AS45090 Shenzhen Tencent Computer Systems Company Limited)
CDN	无CDN
语言	nothing
WAF	不存在WAF
操作系统	Linux
指纹框架	OpenResty, Lua, jQuery, aspx, Nginx, Server 【openresty/1.15.8.2】
Web容器	openresty/1.15.8.2
网站权重	获取数据失败, 稍后再试
域名信息	***** <a href="#">点击查看</a>



微信搜一搜

## 敏感目录/文件扫描

也就是对网站做个目录扫描，从中可以获取网站的后台管理页面，文件上传界面，robots.txt，甚至可能扫描出备份文件从而得到网站的源码。

常见的网站目录的扫描工具主要有：

御剑后台扫描工具

dirbuster扫描工具

dirsearch扫描工具

dirb

wwwscan

Spinder.py

## 御剑后台扫描

新手入门必备工具，使用非常简单，输入url点开始扫描即可





## dirsearch

下载地址: <https://github.com/maurosoria/dirsearch>

一款非常全面、高效的工具，在ctf比赛中常用。

使用语法很简单

```
python3 dirsearch.py -u <URL> -e <EXTENSION>
```

像我一样的懒虫可以写个txt放桌面上备着，改改url直接复制粘贴进cmd就ok啦



一天一个偷懒小技巧~

```
C:\windows\system32\cmd.exe - python dirsearch.py -u https://www.ly.com/ -e --timeout=0.5 -t 1 -x 400,403,404,500,503,429
Target: https://www.ly.com/
Output File: D:\CTF\SDPC tool bag\Web\目录扫描\dirsearch-master\reports\www.ly.com\_21-07-29_18-01-57.txt

[18:01:57] Starting:
[18:02:01] 302 - 150B - /aspx -> https://www.ly.com/404.html
[18:02:15] 302 - 165B - /.ashx -> https://www.ly.com/404.html?aspxerrorpath=/.ashx
[18:02:15] 302 - 165B - /.asmx -> https://www.ly.com/404.html?aspxerrorpath=/.asmx
[18:02:16] 302 - 165B - /.aspx -> https://www.ly.com/404.html?aspxerrorpath=/.aspx
[18:03:40] 301 - 166B - /11 -> http://m.ly.com/dujia/baoji_northad.html?wvc2=1&wvc1=1
[18:03:50] 301 - 166B - /404 -> http://www.ly.com/404.html
[18:03:50] 301 - 166B - /404.php -> https://www.ly.com/public/404.html
[18:03:50] 301 - 166B - /404.inc.php -> https://www.ly.com/public/404.html
[18:03:50] 301 - 166B - /404.jsp -> https://www.ly.com/public/404.html
[18:03:50] 301 - 166B - /404.jsf -> https://www.ly.com/public/404.html
[18:03:51] 301 - 166B - /404.asp -> https://www.ly.com/public/404.html
[18:03:51] 200 - 30KB - /404.aspx -> https://www.ly.com/public/404.html
[18:03:51] 301 - 166B - /404.do -> https://www.ly.com/public/404.html
[18:03:51] 301 - 166B - /404.action -> https://www.ly.com/public/404.html
[18:03:51] 301 - 166B - /404.cgi -> https://www.ly.com/public/404.html
[18:03:51] 301 - 166B - /404.pl -> https://www.ly.com/public/404.html
[18:03:51] 200 - 30KB - /404.html -> https://www.ly.com/public/404.html
[18:03:51] 200 - 30KB - /404.htm -> https://www.ly.com/public/404.html
[18:03:51] 301 - 166B - /404.js -> https://www.ly.com/public/404.html
[18:03:51] 301 - 166B - /404.css -> https://www.ly.com/public/404.html
[18:03:51] 301 - 166B - /404.json -> https://www.ly.com/public/404.html
[18:03:51] 301 - 166B - /404.txt -> https://www.ly.com/public/404.html
[18:03:51] 301 - 166B - /404.tar.gz -> https://www.ly.com/public/404.html
[18:03:51] 301 - 166B - /404.tgz -> https://www.ly.com/public/404.html
12.76% - Errors: 1 - Last request to: META-INF/app-config.xml
```

扫出来好多。。。不愧是高效工具。

## dirbuster

DirBuster是Owasp(开放Web软件安全项目)开发的一款专门用于探测Web服务器的目录和隐藏文件的软件

1. 首先在Target URL输入框中输入要扫描的网址并将扫描过程中的请求方法设置为“Auto Switch(HEAD and GET)”。
2. 自行设置线程（太大了容易造成系统死机哦）
3. 选择扫描类型，如果使用个人字典扫描，则选择“List based bruteforce”选项。
4. 单击“Browse”加载字典。
5. 单机“URL Fuzz”，选择URL模糊测试（不选择该选项则使用标准模式）
6. 在URL to fuzz里输入“/{dir}”。这里的{dir}是一个变量，用来代表字典中的每一行，运行时{dir}会被字典中的目录替换掉。
7. 点击“start”开始扫描

## Waf识别

Web应用防护系统（也称为：网站应用级入侵防御系统。英文：Web Application Firewall 简称（WAF） 俗称 防火墙。利用国际上公认的一种说法，Web应用防火墙是通过执行一系列针对HTTP/HTTPS的安全策略来专门为Web应用提供保护的一款产品

wafw00f是一个Web应用防火墙（WAF）指纹识别的工具。

下载地址：<https://github.com/EnableSecurity/wafw00f>

工作原理：

1. 发送正常的HTTP请求，然后分析响应，这可以识别出很多WAF。
2. 如果不成功，它会发送一些（可能是恶意的）HTTP请求，使用简单的逻辑推断是哪一个WAF。
3. 如果这也不成功，它会分析之前返回的响应，使用其它简单的算法猜测是否有某个WAF或者安全 解决方案响应了我们的攻击

同时 kali上内置了该工具

使用方法很简单



哇看到了好多好多dalao公司，大公司的网站他就是不一样

## 敏感信息收集

有时候，针对某些安全做得很好的目标，直接通过技术层面是无法完成渗透测试的。此时，便可以利用搜索引擎搜索目标暴露在互联网上的关联信息。例如：**数据库文件、SQL注入、服务配置信息，甚至是通过Git找到站点泄露源代码，以及Redis等未授权访问、Robots.txt等敏感信息，从而达到渗透目的。**

## 拓展：google的艺术

搜索引擎伴随我们的互联网生活发展至今，我们各种稀奇古怪的问题，在google上几乎都能找到答案。但其实这只是google功能的冰山一角，google可以用来发现远远超过我们认知的信息，利用google，我们可以找到敏感文件、网站漏洞，甚至找到密码，数据库，邮箱内容。

Google hacking是利用google搜索功能的强大，来在浩瀚的互联网中获取我们所需要的信息。

轻量级的搜索可以找到一些遗留后门，网站后台入口，sql注入等网络漏洞。中量级的搜索出一些用户信息，源码泄露，未授权访问等等。重量级的还有mdb文件下载，CMS未被锁定install页面，网站配置密码，php远程文件包含漏洞等重要信息。

要学习google hacking 首先要学习google的一些特殊语法，同时这些语法在其他搜索引擎如：百度，必应其实大多也是适用的。

## 拓展：google引擎语法

## 关键字类

`intext:` 寻找正文中含有关键字的网页

`intitle:` 寻找标题中含有关键字的网页

`allintitle:` 用法和`intitle`类似，不过可以指定多个词

`inurl:` 寻找url中含有关键字的网页

`allinurl:` 同样的用法类似，可以指定多个词。

## 指定类

`site:`指定访问站点

`filetype:`指定文件类型

`link:`指定链接网页

## 其他类

`related:`搜索相似类型的网页

`info:`返回站点的指定信息

`phonebook:`电话簿查询美国街道地址和电话号码信息

`Index of:` 利用`Index of`语法可以发现允许目录浏览的web网站。

## 拓展google hacking0 实战常用语法

### 查找网站后台

`intext:`后台登录：将只返回正文中包含“后台登录”的网页

`intitle:`后台登录：将只返回标题中包含“后台登录”的网页



intext:后台登录



全部 图片 新闻 视频 更多

工具

找到约 76,100,000 条结果 (用时 0.33 秒)

https://admin.aillinet.com

登录--后台管理

后台登录: 登录, 记住密码, 忘记密码, 信息, 账号:demo 密码:123456, 确定.

用户还搜索了

LOGIN 后台 登录 inurl /admin/login.php 学校  
intitle:后台 登陆 inurl admin login php 学校  
Intext 后台 登录 Site 后台

http://demo.ejucms.com > login

后台登录 - 易居房产系统

易居房产系统后台管理 登录.

http://cms.dlszyht.com

登录管理后台

用户 登录, 子管理员 登录, 点击, 换一张! 忘记密码? 登录.

https://www.chenweiliang.com > WordPress

如何登陆WordPress后台? WP后台登录地址\_陈为亮博客

2018年7月15日 — 我们用WordPress建站, 登录后台的默认地址, 都是网站域名+后台登录地址。WordPress登录后台网址1) WordPress程序中哪个文件, 负责登录和验证账号?

## 查找指定网站后台

site:xx.com intext:管理

site:xx.com inurl:login

site:xx.com intitle:后台



site:ly.com intext:管理



全部 图片 新闻 视频 更多

工具

找到约 34,600 条结果 (用时 0.42 秒)

https://tmc.ly.com

同程商旅\_商旅卡\_商旅管理\_出差费用管理\_企业差旅报销服务\_...

同程商旅,为公司企业及员工节约差旅费用成本。解决差旅过程中票据不统一,灰色损耗讲不清,核销出差费用浪费人力问题。同程商旅网严格执行差旅政策规范财务凭证,...

https://tmc.ly.com > mice

同程商旅\_商旅卡\_商旅管理\_出差费用管理\_企业差旅报销服务\_...

同程商旅\_商旅卡\_商旅管理\_出差费用管理\_企业差旅报销服务\_流程审批-同程旅游.

https://tmc.ly.com > business-cooperation

同程商旅\_商旅卡\_商旅管理\_出差费用管理\_企业差旅报销服务\_...

您有什么商旅需求吗? 填写简单信息, 我们将第一时间与您联系. 获取验证码 获取验证码. 万/年. 提交. 商务合作. 173-1260-4320. tctmc@ly.com. 关于我们.

https://www.ly.com > BookSceneryTicket\_230667

山东慈铭健康体检管理有限公司济南历下门诊部门票预订\_山东慈铭

...

山东慈铭健康体检管理有限公司是慈铭健康体检集团股份有限公司在华东地区成立的一家旗舰店, 是集疾病检测、健康促进、健康管理为一体的专业体检机构。

https://www.ly.com > public > dtg

大唐商旅 - 同程旅行



## 查找文件上传漏洞

```
site:xx.com inurl:file
```

```
site:xx.com inurl:load
```

## 利用Index of 可以发现允许目录浏览的web站

```
index of /admin
```

```
index of /passwd
```

```
index of /password
```












```
index of /mail
```

```
"index of /" +passwd
```

```
"index of /" +password.txt
```

```
"index of /config"
```

## Index of /admin

	<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
	<a href="#">Parent Directory</a>		-	
	<a href="#">LICENSE.txt</a>	2017-03-08 09:09	1.1K	
	<a href="#">bower.json</a>	2017-03-08 09:09	2.6K	
	<a href="#">build/</a>	2017-06-19 13:36	-	
	<a href="#">changelog.md</a>	2017-03-08 09:09	870	
	<a href="#">documentation/</a>	2017-03-08 09:09	-	
	<a href="#">gulpfile.js</a>	2017-03-08 09:09	1.6K	
	<a href="#">index123.php</a>	2017-05-24 08:13	49	
	<a href="#">map/</a>	2017-06-19 13:36	-	
	<a href="#">package.json</a>	2017-03-08 09:09	963	
	<a href="#">production/</a>	2017-08-24 11:09	-	
	<a href="#">src/</a>	2017-06-19 13:36	-	
	<a href="#">vendors/</a>	2017-11-23 13:19	-	



## 备份文件泄露

```
intitle:index.of index.php.bak
```

```
inurl:index.php.bak
```

```
intitle:index.of www.zip
```

```
1: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
2: <html lang="en"> <head>
3: <meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
4: <meta name="description" content="LDAP Sample Files">
5: <meta name="author" content="Wayne Pollock">
6: <link rel="contents" href="../../index.htm">
7: <link rel="previous" href="../../index.htm">
8: <link rel="stylesheet" href="../../Styles.css" type="text/css">
9: <script type="text/JavaScript" src="../../Common.js"> </script>
10:
11: <title> LDAP Sample Files </title>
12:
13: </head>
14: <body>
15: <div class="Center">
16: <h1> <abbr>LDAP</abbr> Sample Configuration and Data Files </h1>
17: <h2 class="hide">&nbsp;</h2>
18: </div>
19:
20: <div class="Indent">
21: <?php
22:     // Script to produce a list of links for all files in this directory.
23:     // Written 11/2009 by Wayne Pollock, Tampa Florida USA. All Rights Reserved.
24:     // Updated 11/2013 to include "nodir" option to lister.php.
25:
26:     function endsWith($whole, $end)
27:     {
28:         return (strpos($whole, $end, strlen($whole) - strlen($end)) !== false);
```

## 查找sql注入

```
inurl:?id=1
```

```
inurl:php?id=
```

gle inurl:asp?id=3 X 语音 搜索

全部 图片 视频 新闻 更多 工具

找到约 419,000 条结果 (用时 0.74 秒)

<https://www.imperva.com/download?id=3> 翻译此页

<https://www.imperva.com/download.asp?id=3>

没有此网页的信息。  
了解原因

<http://kim.wits.ac.za/usrfiles/Comment.asp?id=3> 翻译此页

**Index of /usrfiles/users/9826090203/Comment.asp?id=3 - Wits**

blogconfig.yaml, 11-Jul-2013 02:55, 260. Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.12 with Suhosin-Patch Server at kim.wits.ac.za Port 80.

<http://www.kklabel.cn/shownews?id=3>

**中山仲冠纸塑制品股份有限公司**

上一篇: 公司全体成员欢聚一堂 欢乐盛宴 下一篇: 五一国际劳动节烧烤晚会 相关信息 · 2019 春茗晚宴 感恩有你, 共赢未来! 五一国际劳动节烧烤晚会 · 运动会 ...

<http://www.haochenbaon.com/wap/show>

**<a href="/list.asp?id=3">公司新闻</a> - 河北浩辰保安服务有限 ...**

保安是因应工商社会发展下的新兴服务业名称, 在中国称为保安, 日本称之为“警备会社”, 中国古代称为近身士卫。保安是指保卫治安, 防止在生产过程中发生人身事故。

随便点了一个（不在此页面中）and 1=1 1=2 测试了一波报错了 应该是存在注入点的

```

22:20:53 [INFO] testing 'MySQL >= 5.0 boolean-based blind - Parameter replace'
22:20:54 [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
22:20:55 [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
22:20:57 [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
22:20:58 [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
22:21:00 [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
22:21:00 [INFO] testing 'MySQL inline queries'
22:21:01 [INFO] testing 'PostgreSQL inline queries'
22:21:01 [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
22:21:01 [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
22:21:03 [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
22:21:04 [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
22:21:05 [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
22:21:07 [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
22:21:09 [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IP)'
22:21:11 [INFO] testing 'Oracle AND time-based blind'
22:21:14 [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
22:21:14 [WARNING] using unescaped version of the test because of zero knowledge of the back-end DBMS. You can try to
explicitly set it with option '--dbms'
22:21:36 [WARNING] GET parameter 'id' does not seem to be injectable
22:21:36 [CRITICAL] all tested parameters appear to be not injectable. Try to increase '--level'/'--risk' values to
perform more tests. Please retry with the switch '--text-only' (along with --technique=BU) as this case looks like a per
fect candidate (low textual content along with inability of comparison engine to detect at least one dynamic parameter).
so, you can try to rerun by providing either a valid value for option '--string' (or '--regexp'). If you suspect that
there is some kind of protection mechanism involved (e.g. WAF) maybe you could retry with an option '--tamper' (e.g. '-
tamper=space2comment')
22:21:36 [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 158 times

```

sqlmap跑了一下，好吧无法注入溜了。

## Github信息泄露

github作为开源代码平台，给程序员提供了很多便利，但如果使用不当，比如上传了包含账号密码，密钥等敏感信息的文件的代码，就是一个github敏感信息泄露漏洞。开发人员在开发时，常常会将源码提交到GitHub，然后再从远程托管网站把源码pull到服务器的web目录下，如果忘记删除git文件，就会造成此漏洞。

不少开发者由于安全意识不足会把相关配置文件信息也放到github上，所以如果使用以下google hacking 技巧，就能把这些敏感信息找出来。

```

site:Github.com smtp

site:Github.com smtp @qq.com

site:Github.com smtp @126.com

site:Github.com smtp @163.com

site:Github.com smtp @sina.com.cn

```

数据库信息泄露：

```

site:Github.com sa password

site:Github.com root password

```

## 社会工程学

一门博大精深的学科，嘿嘿嘿。

同时也是一门较为敏感的学科，期待以后能够深入了解

记下两本推荐书籍：《黑客心理学》、《欺骗的艺术》

## 后记

学习信息收集的过程比我想象的累多了，没有想到原来看似简单的信息收集竟有如此多的**窍门与技巧**，没有想到看似基础的信息收集原来很大程度上决定了渗透测试的成败。通过编写本报告，我对信息收集的手段极其目的有了初步的了解，也很清晰的感知到自己对于信息收集在实战中的应用还是**有些迷茫**，希望在接下来的学习中，能够不断深化对其的认识。毕竟我相信，实践是最好的老师。