Web信息收集之搜索引擎

1. 信息收集概述

1、Web信息搜集（探测）即Web踩点，主要是掌握目标Web服务的方方面面，是实现Web渗透入侵前的准备工作
2、Web踩点内容包括操作系统、服务器类型、数据库类型、Web容器、Web语言、域名信息、网站目录....
3、Web信息搜集涉及搜索引擎、网站扫描、域名遍历、指纹识别等工作

2. 项目实验环境

目标靶机：OWASP_Broken_Web_Apps_VM_1.2
测试渗透机：win7/Kali

3. Google Hacking

3.1 site

功能： 搜索指定的域名的网页内容，可以用来搜索子域名、跟此域名相关的内容。

示例：

```
site:zhihu.com                搜索跟zhihu.com相关的网页
"web安全" site:zhihu.com       搜索zhihu.com跟web安全相关的网页
"sql注入"  site:csdn.net       在csdn.net搜索跟sql注入相关的内容

"教程" site:pan.baidu.com      在百度盘中搜索教程
```

3.2 filetype

功能： 搜索指定文件类型

示例：

```
"web安全" filetype:pdf          搜索跟安全书籍相关的pdf文件
nmap filetype:ppt               搜索跟nmap相关的ppt文件
site:csdn.net filetype:pdf      搜索csdn网站中的pdf文件
filetype:pdf site:www.51cto.com 搜索51cto的pdf文件
```

3.3 inurl

功能： 搜索url网址存在特定关键字的网页，可以用来搜寻有注入点的网站

示例：

```
inurl:.php?id=                  搜索网址中有"php?id"的网页
inurl:view.php=?                搜索网址中有"view.php="的网页
inurl:.jsp?id=                  搜索网址中有"jsp?id"的网页
inurl:.asp?id=                  搜索网址中有"asp?id"的网页
inurl: /admin/login.php         搜索网址中有"/admin/login.php"的网页
inurl:login                     搜索网址中有"login"等登录网页
```

3.4 intitle

功能： 搜索标题存在特定关键字的网页

示例：

```
intitle:后台登录                搜索网页标题是“后台登录”的相关网页
intitle:后台管理 filetype:php   搜索网页标题是“后台管理”的php页面
intitle:index of "keyword"      搜索此关键字相关的索引目录信息
intitle:index of "parent directory" 搜索根目录相关的索引目录信息
intitle:index of "password"     搜索密码相关的索引目录信息
intitle:index of "login"        搜索登录页面信息
intitle:index of "admin"        搜索后台管理页面信息
```

3.5 intext

功能： 搜索正文存在特定关键字的网页

示例：

```
intext:Powered by Discuz        搜索Discuz论坛相关的页面
intext:powered by wordpress     搜索wordpress制作的博客网址
intext:Powered by *CMS          搜索*CMS相关的页面
intext:powered by xxx inurl:login 搜索此类网址的后台登录页面
```

3.6 实例

```
搜索美女/电影等相关网站:
inurl:php?id= intitle:美剧
inurl:php?id= intitle:美女
inurl:php?id  intitle:美女图片 intext:powered by discuz
inurl:php?id  intitle:美女图片 intext:Powered by *cms

搜索用Discuz搭建的论坛:
inurl:php?id  intitle:电影 intext:powered by discuz
intext:”powered by discuz!  7.2”   inurl:faq.php  intitle:论坛

搜索使用Struts的相关网站:
intitle:"Struts Problem Report"
intitle:"Struts Problem Report" intext:"development mode is enabled."
```

3.7 符号

```
-keyword     强制结果不要出现此关键字,例如：电影 -黑客
*keyword     模糊搜索，强制结果包含此关键字,例如：电影   一个叫*决定*
"keyword"    强制搜索结果出现此关键字,例如：书籍 "web安全"
```

3.8 参考

从谷歌搜获更多

Get More Out of Google

一些提示和技巧
献给网上做调研的童鞋们

关于学生们作研究的技能，据不知道来自哪里的调查结果显示，让人意外的是有**四分之三**的学生都没能较好的利用网络搜索。在资讯丰富的互联网中，如何有效地搜索那可是攸关论文和报告能否准时搞定的关键技能啊

这儿给你提供了一些**有效利用谷歌搜索**的提示，助你搜获撰写毕业论文所需的信息。

如何谷歌

你是否每次在Google时都只是加入空格分隔关键词呢？相对这基本的搜索功能，合理使用搜索‘操作符’，可以帮助你获得更加精确的搜索结果。

你想搜什么

纽约时报网站(nytimes.com)在2008到2010年关于大学(college)测验分数(test scores)但不是SAT入学分数的文章。

怎样谷歌呢

http://www.google.com/

你想搜什么

一份关于常见燕子飞行速度的**专业报告**。

怎样谷歌呢

不要问谷歌问题。想一下答案会有哪些词语，然后搜索这些词语（例如不要搜索：“XX的飞行速度是多少？”）

filetype:
只搜索指定类型的文档，可以用来搜索pdf，doc，jpg等类型的文档。

intitle:
只显示标题中包含指定关键词的搜索结果（例如：velocity）。

filetype:pdf air speed intitle:velocity of *swallow

*
星号用来代替任意字符（例如：‘*swallow’可以匹配‘Red Rumped swallow’和‘Lesser Striped swallow’等，意为搜索各种燕子。）

谷歌学术搜索

对于在大学里从事的多数项目，只依靠简单的谷歌搜索不能有效达到目的。使用谷歌学术搜索吧，其专门用来搜索**理论和学术著作**的，就是你会在你的论文中引用的那种。

你想搜什么

Dr. Ronald L. Green和Dr. Thomas P. Buttz.所写的关于光和作用(photosynthesis)的论文。

怎样谷歌呢

http://scholar.google.com/

author:
搜索Green发表的论文，而不是包含‘green’这个词的论文。

“ ”
想让结果更精确，你可以在引号中输入作者的全名或者是缩写。

author:green photosynthesis “tp buttz”

这里的“photosynthesis”就是一个普通的谷歌搜索，是你要找的主题关键字。

其它谷歌技巧

字词定义

快速查询字词定义。只要在你想了解的单词前面输入“define:”，例如查询angary的定义：

define:angary

数学计算

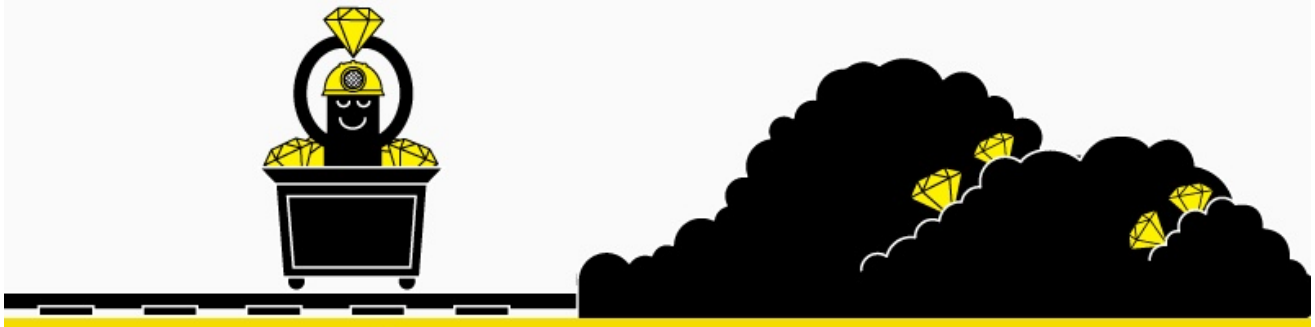
快速计算，别费力的启动你的计算器软件了。只需要直接在谷歌里输入数学算式就行了，算式可以包含+，-，*，/ 和括号这些基本的算术功能。

(2*3)/5+44-1

单位换算

方便的单位换算。只需要输入你想换算的两种单位。

54磅=？公斤



快捷键

90%的互联网用户不知道可以使用Ctrl + F在本页查找字符。如果你是这90%其中一员，这一部分内容就是为你而写。注

注：快捷键的使用在PC机和Mac机上略有不同。因为在国内大多数童鞋用的是PC机，后面的提示均默认按照PC机用户的习惯而写，如果你使用的是Mac机，多数情况用“Command”按键代替‘Ctrl’按键便可。

在本页查找

调研中最重要的快捷键，在你正在查看的任一文档或页面，按下Ctrl+F键，弹出搜索框后，输入你想查找的字符串，立刻，所有对应的字符串都为你而高亮显示。

Ctrl + F

放大/缩小

有时候页面字体太小或者在线PDF文档勉强可以阅读，你可以使用快捷键方便的**放大或缩小页面**。

Ctrl + + / -

选中浏览器地址栏

每次使用鼠标移动到地址栏是费神又费力，只要按下Ctrl+L组合键，地址栏即刻选中。

Ctrl + L

切换标签页和程序

在电脑上做研究，随着你工作的开展，运行的应用程序和打开的窗口越来越多，烦扰着你。使用快捷键可以帮助你在不同的窗口和应用程序间切换，减轻你的烦乱。

PC机

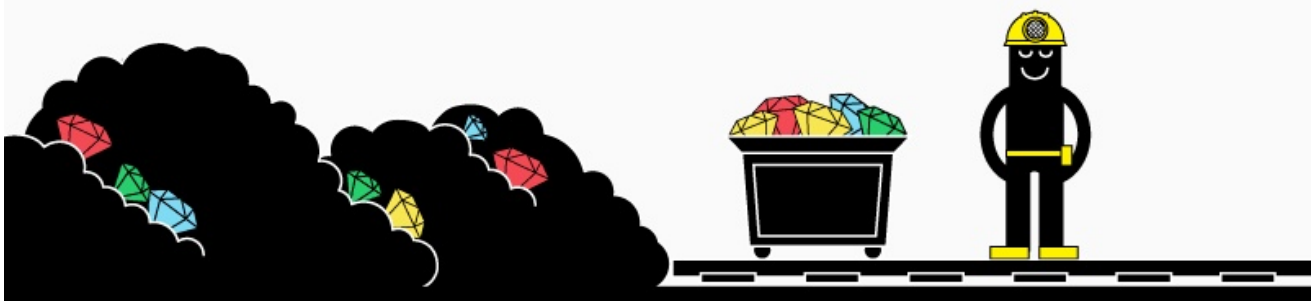
切换标签页：Ctrl + Tab

切换窗口：Alt + Tab

MAC机

切换窗口：⌘ command + ~ `

切换应用程序：⌘ command + tab



进一步提示

善用你们的图书馆网站

谷歌很给力，但决不是你做研究的唯一选择。大多数大学的图书馆网站上链接了丰富的资源任君取用。你能从中找到学术著作数据库的入口，例如超星数字图书馆。毕竟许多重要文献还是需要从专业的论文资料库里才能找到。

不要引用维基百科

面对现实吧：我们在进行研究的过程中都常会用到维基百科或者百度百科。在了解和熟悉我们论文题目的过程中，维基百科是一个很适合入门的地方，但其中很多资料缺乏来源引证。不过一个好的维基条目，底部会标明参考链接，从这里可以有助我们找到一些可靠的信息来源。

找参考文献

此段提示对于数字化或传统的调研均适用。从优质的书、论文或报告上面下手是不会错的，从文献追溯，顺藤摸瓜地探究所有相关资料，查阅每一个看起来有希望的线索。

中文版译制

作者
http://kaijuan.org/user:DramaTea
接受Bitcoin捐赠

4. Shodan Hacking

```
https://www.shodan.io
Shodan（撒旦搜索引擎）是由Web工程师John Matherly（马瑟利）编写的，被称为“最可怕的搜索引擎”，可扫描一切联网的设备。除了常见的Web服务器，还能扫描防火墙、路由器、交换机、摄像头、打印机等一切联网设备。
```


4.1 ip

```
114.114.114.114
```

4.2 service/protocol

```
http
http country:"DE"
http country:"DE" product:"Apache httpd"
http product:"Apache httpd"

ssh
ssh default password
ssh default password country:"JP"
```

4.3 keyword

```
基于关键词搜索的思路是根据banner信息（设备指纹）来搜索
"default password" country:"TH"
FTP anon successful
```

4.4 country

```
country:cn
country:us
country:jp
```

4.5 product

```
product:"Microsoft IIS httpd"
product:"nginx"
product:"Apache httpd"
product:MySQL
```

4.6 version

```
product:MySQL version:"5.1.73"
product:"Microsoft IIS httpd" version:"7.5"
```

4.7 hostname

```
hostname:.org
hostname:.edu
```


4.8 os

```
os:"Windows Server 2008 R2"
os:"Windows 7 or 8"
os:"Linux 2.6.x"
```

4.9 net

```
net:110.180.13.0/24
200 ok net:110.180.13.0/24
200 ok country:JP net:110.180.13.0/24
```

4.10 port

```
port:3389
port:445
port:22
port:80
port:443
```

4.11 综合示例

```
搜索日本区开启80端口的设备:
country:jp port:"80"
country:jp port:"80" product:"Apache httpd"
country:jp port:"80" product:"Apache httpd" city:"Tokyo"
country:jp port:"80" product:"Apache httpd" city:"Tokyo" os:"Linux 3.x"

搜索日本区使用Linux2.6.x系统的设备:
country:jp os:"Linux 2.6.x"
country:jp os:"Linux 2.6.x" port:"80"
country:jp os:"Linux 2.6.x" port:"80" product:"Apache httpd"

搜索日本区使用Windows Server 系统的设备:
country:jp os:"Windows Server 2008 R2"
country:jp os:"Windows Server 2003" port:"445"
country:jp os:"Windows Server 2003" port:"80"

搜索日本区使用Microsoft IIS的设备:
country:jp product:"Microsoft IIS httpd" version:"7.5"
```

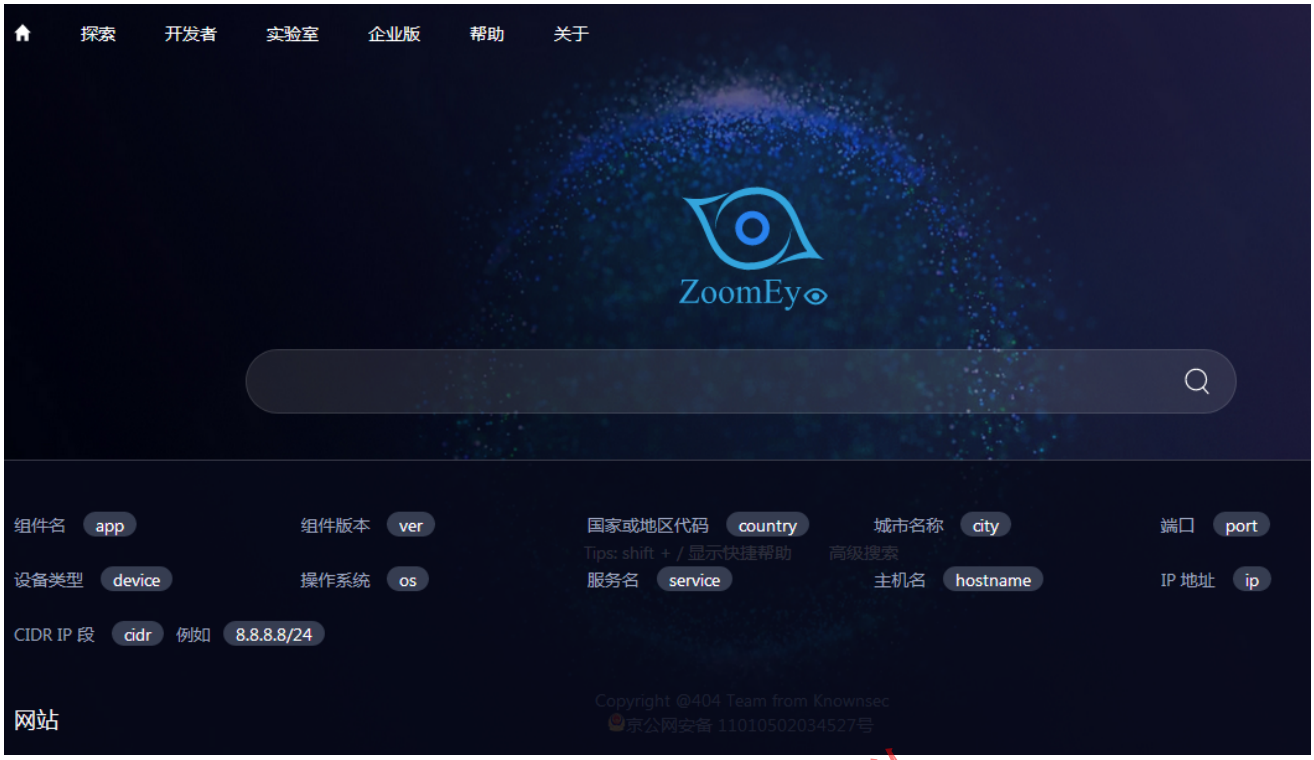

5. Zoomeye Hacking

5.1 概述

```
https://www.zoomeye.org
ZoomEye（钟馗之眼） 是一个面向网络空间的搜索引擎,"国产的Shodan"，由知道创宇出品。

ip
os
app
service
port
product
country
ver
cidr
hostname
site
title
header
keywords
desc

用户手册：https://www.zoomeye.org/help
```



5.2 示例

```
site:zhihu.com
title:电影
wordpress
wordpress product:"Apache httpd"
wordpress product:"Apache httpd" port:443
wordpress product:"Apache httpd" port:443 country:Japan
discuz product:"Microsoft IIS httpd"
```