# 一、intitle：搜索网页标题中包含有特定字符的网页。 例如： intitle:admin

二、inurl：搜索包含有特定字符的URL。例如输入“inurl:/admin\_login”，则可以找到带有admin\_login字符的URL,通常这类网址是管理员后台的登录网址。inurl：admin

目标关键字+inurl:id

英语字母及单词+inurl:id

网站域名+inurl:id

阿拉伯数字+inurl:id

inurl:Company.asp?id=

inurl:CompHonorBig.asp?id=xx

inurl:CompHonorBig.asp?id=XX

inurl:Newsx.asp?id=

inurl:show.asp?id=

inurl:.asp?id= and intitle:?????

inurl:asp?readid=

inurl:asp

三、intext:搜索网页正文内容中的指定字符，例如输入“intext:管理”。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。

四、Filetype:搜索指定类型的文件。例如输入“filetype:PDF”，将返回PDF文档。“filetype：”后可以跟以下文件格式：doc、xls、ppt、pdf、rtf、all。其中，all包含所有[文件类型](https://www.baidu.com/s?wd=%E6%96%87%E4%BB%B6%E7%B1%BB%E5%9E%8B&tn=SE_PcZhidaonwhc_ngpagmjz&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1dWP1Pbnj0YmhczuAnLm10z0ZwV5Hcvrjm3rH6sPfKWUMw85NP7gdKWyh9GuA7EUMICmdq8uLK9uvdJX6K1TL0qnfK1TL0z5HD0IgF_5y9YIZ0lQzqlpA-bmyt8mh7GuZR8mvqVQL7dugPYpyq8Q1fsP1bYnHbsr0)。

google已经可以支持13种非[html文件](https://www.baidu.com/s?wd=html%E6%96%87%E4%BB%B6&tn=SE_PcZhidaonwhc_ngpagmjz&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1dWP1Pbnj0YmhczuAnLm10z0ZwV5Hcvrjm3rH6sPfKWUMw85NP7gdKWyh9GuA7EUMICmdq8uLK9uvdJX6K1TL0qnfK1TL0z5HD0IgF_5y9YIZ0lQzqlpA-bmyt8mh7GuZR8mvqVQL7dugPYpyq8Q1fsP1bYnHbsr0)的搜索。除了[pdf文档](https://www.baidu.com/s?wd=pdf%E6%96%87%E6%A1%A3&tn=SE_PcZhidaonwhc_ngpagmjz&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1dWP1Pbnj0YmhczuAnLm10z0ZwV5Hcvrjm3rH6sPfKWUMw85NP7gdKWyh9GuA7EUMICmdq8uLK9uvdJX6K1TL0qnfK1TL0z5HD0IgF_5y9YIZ0lQzqlpA-bmyt8mh7GuZR8mvqVQL7dugPYpyq8Q1fsP1bYnHbsr0)，google现在还可以搜索microsoft office (doc, ppt, xls, rtf) 、shockwave flash (swf)、postscript (ps)和其它类型文档。新的文档类型只要与用户的搜索相关，就会自动显示在搜索结果中。例如，如果只想查找 pdf或flash文件，只需搜索“关键词 filetype:pdf” 或“关键词 filetype:swf”就可以了。flash文件百度尚未支持查询。（有些文件类型在百度上使用filetype查找可能不行）

补充：“filetype:”是一个非常强大而且实用的搜索语法。通过这个语法，能搜索一般的网页，还能对某些二进制文件进行检索。

1.Office文件搜索

微软的Office系列是应用最广泛的办公软件，因此网上的这类文档资料也是最丰富的。

假如你是一家企业的企划部负责人，老总突然要求你写一个本企业的网络营销策划方案，而你有没有这方面的资料怎么办?别慌，帮你从网上找几个现成的。

举例：搜索包含“网络营销策划方案”关键词的Office 文件。

关键词：“网络营销策划方案 filetype:doc OR filetype:ppt”。

搜索到有关网络营销策划方案的.doc、.ptt文件约有867项。如此多的资料，够参考的了。这里的每一项都是一个可下载的文件，点击之后弹出文件下载对话框，选择打开或者保存。注意，下载的 Office 文件可能含有宏病毒，请谨慎操作。

2.SWF文件搜索

喜欢看Flash动画的人有福了，通过使用“filetype:”语法，你可以搜索到能直接下载的Flash歌曲、MTV，而不必使用专门的搜索下载工具。

举例：搜索关于周杰伦的歌曲Flash MTV。

关键词：“周杰伦 filetype:swf”。

注意，要保存搜索到的Flash文件，需使用右键菜单“目标另存为”命令保存文件到一个指定位置。

【其它例子】

①chm书籍：——资料 filetype:chm

②耽美文(txt)：——耽美 filetype:txt

三、

Site：找到与指定网站有联系的URL。例如输入“Site:www.0dayhack.com”。所有和这个网站有联系的URL都会被显示。

了解了Google的基本语法后，我们来看一下黑客是如何使用这些语法进行Google Hack的，这些语法在入侵的过程中又会起到怎样的作用呢？

intitle

intitle语法通常被用来搜索网站的后台、特殊页面和文件，通过在Google中搜索“intitle:登录”、“intitle:管理”就可以找到很多网站的后台登录页面。此外，intitle语法还可以被用在搜索文件上，例如搜索“intitle:"indexof"etc/shadow”就可以找到Linux中因为配置不合理而泄露出来的用户密码文件。

inurl

Google Hack中，inurl发挥的作用的最大，主要可以分为以下两个方面:寻找网站后台登录地址，搜索特殊URL。

寻找网站后台登录地址：和intitle不同的是，inurl可以指定URL中的关键字，我们都知道网站的后台URL都是类似login.asp、admin.asp为结尾的，那么我们只要以“inurl:login.asp”、“inurl:admin.asp”为关键字进行搜索，同样可以找到很多网站的后台。此外，我们还可以搜索一下网站的数据库地址，以“inurl:data”、“inurl:db”为关键字进行搜索即可。

寻找网站的后台登录页面

搜索特殊URL：通过inurl语法搜索特殊URL，我们可以找到很多网站程序的漏洞，例如最早IIS中的Uncode目录遍历漏洞，我们可以构造“inurl:／winnt／system32／cmd exe?／c+dir”这样的关键字进行搜索，不过目前要搜索到存在这种古董漏洞的网站是比较困难的。再比如前段日子很火的上传漏洞，我们使用““inurl:upload.asp”或“inurl:upload\_soft.asp”即可找到很多上传页面，此时再用工具进行木马上传就可以完成入侵。

intext

intext的作用是搜索网页中的指定字符，这貌似在Google Hack中没有什么作用，不过在以“intext:to parent directory”为关键字进行搜索后，我们会很惊奇的发现，无数网站的目录暴露在我们眼前。我们可以在其中随意切换目录，浏览文件，就像拥有了一个简单的Webshell。形成这种现象的原因是由于IIS的配置疏忽。同样，中文IIS配置疏忽也可能出现类似的漏洞，我们用“intext:转到父目录”就可以找到很多有漏洞的中文网站。

随意浏览网站中的文件

Filetype

Filetype的作用是搜索指定文件。假如我们要搜索网站的数据库文件，那么可以以“filetype:mdb”为关键字进行搜索，很快就可以下载到不少网站的数据库文件。当然，Filetype语法的作用不仅于此，在和其他语法配合使用的时候更能显示出其强大作用。

Site

黑客使用Site，通常都是做入侵前的信息刺探。Site语法可以显示所有和目标网站有联系的页面，从中或多或少存在一些关于目标网站的资料，这对于黑客而言就是入侵的突破口，是关于目标网站的一份详尽的报告。语法组合，威力加倍虽然上文中介绍的这几个语法能各自完成入侵中的一些步骤，但是只使用一个语法进行入侵，其效率是很低下的。Google Hack的威力在于能将多个语法组合起来，这样就可以快速地找到我们需要的东西。下面我们来模拟黑客是如何使用Google语法组合来入侵一个网站的。

信息刺探

黑客想入侵一个网站，通常第一步都是对目标网站进行信息刺探。这时可以使用“Site:目标网站”来获取相关网页，从中提取有用的资料。

搜索相关页面

下载网站的数据库。搜索“Site:目标网站 Filetype:mdb”就可以寻找目标网站的数据库，其中的Site语法限定搜索范围，Filetype决定搜索目标。用这种方法有一个缺点，就是下载到数据库的成功率较低。在这里我们还可以采用另一种语法组合，前提是目标网站存在IIS配置缺陷，即可以随意浏览站点文件夹，我们搜索“Site:目标网站 intext:to parent directory”来确定其是否存在此漏洞。在确定漏洞存在后，可以使用“Site:目标网站 intext:to parent directory+intext:mdb”进行数据库的搜索。

例子：直接下载复旦大学官网的数据库

intext:to parent directory+intext:mdb site:fudan.edu.cn//时间过了这么久，漏洞可能已经打上补丁，只是说方法

找到网站数据库

登录后台管理

下载到数据库后，我们就可以从中找到网站的管理员帐户和密码，并登录网站的后台。对于网站后台的查找，可以使用语法组合“Site:

目标网站 intitle:管理”或者“Site:目标网站 inurl:login.asp”进行搜索，当然我们可以在这里进行联想，以不同的字符进行搜索，这样就有很大的

概率可以找到网站的后台管理地址。接下去黑客就可以在后台上传Webshll，进一步提升权限，在此不再阐述。

利用其他漏洞

如果下载数据库不成功，我们还可以尝试其他的入侵方法。例如寻找上传漏洞，搜索“Site:目标网站 inurl:upload.asp”。此外，我们还可以根据一些程序漏洞的特征，定制出Google Hack的语句。

Google Hack可以灵活地组合法语，合理的语法组合将使入侵显得易如反掌，再加入自己的搜索字符，Google完全可以成为你独一无二的黑客工具。

合理设置，防范Google Hack

合理设置网站Google Hack貌似无孔不入，实则无非是利用了我们配置网站时的疏忽。例如上文中搜索“intext:to parent

directory”即可找到很多可以浏览目录文件的网站，这都是由于没有设置好网站权限所造成的。在IIS中，设置用户访问网站权限时有一个选项，叫做“目录浏览”，如果你不小心选中了该项，那么其结果就如上文所述，可以让黑客肆意浏览你网站中的文件。

这种漏洞的防范方法十分简单，在设置用户权限时不要选中“目录浏览”选项即可。

不要选中该项

编写robots.txt文件robot.txt是专门针对搜索引擎机器人robot编写的一个纯文本文件。我们可以在这个文件中说明网站中不想被robot访问的部分，这样，我们网站的部分或全部内容就可以不被搜索

引擎收录了，或者让搜索引擎只收录指定的内容。因此我们可以利用robots.txt让Google的机器人访问不了我们网站上的重要文件，Google

Hack的威胁也就不存在了。

编写的robots.txt文件内容如下：<User-agent: \*Disallow: /data/Disallow:

其中“Disallow”参数后面的是禁止robot收录部分的路径，例如我们要让robot禁止收录网站目录下的“data”文件夹，只需要在Disallow参数后面加上“/data/”即可。如果想增加其他目录，只需按此格式继续添加。文件编写完成后将其上传到网站的根目录，就可以让网站远离Google Hack了

合理设置，防范Google Hack。合理设置网站Google Hack貌似无孔不入，实则无非是利用了我们配置网站时的疏忽。例如上文中搜索“intext:to parent directory”即可找到很多可以浏览目录文件的网站，这都是由于没有设置好网站权限所造成的。在IIS中，设置用户访问网站权限时有一个选项，叫做“目录浏览”，如果你不小心选中了该项，那么其结果就如上文所述，可以让黑客肆意浏览你网站中的文件。这种漏洞的防范方法十分简单，在设置用户权限时不要选中“目录浏览”选项即可。