
Google
Google
Google
Scholar
BETA
Google
SMS
BETA
Google
Groups
BETA
Google
Google
News
BETA
Google
Froogle
BETA
Google
Catalogs
BETA
Google
Book Search
BETA
Google
Alerts
Google
Local
Google
Answers
Google
Blog Search
BETA
Google
Directory
Google
Google
PhoneBook
Google
Image Search
Google
LABS
Google
Store
Google
dog
Google Search
Web
Images

کتاب راهنمای تصویری استفاده از گوگل برای هکرها

همراه با امکانات و سرویس های دیگر گوگل (نسخه ۲)

مؤلف: محمد بشیری

Site: http://bashiry.250free.com

The Google Hackers Guide

Farsi Edition

نام کتاب : راهنمای تصویری استفاده از گوگل برای هکرها

به همراه امکانات و سرویس های دیگر گوگل

نسخه ۲,۰,۰

مؤلف : محمد بشیری

پست الکترونیک: m.bashiry@gmail.com

آدرس سایت : http://bashiry.250free.com

تاریخ تالیف: ۸۴/۷/۱۱ **تاریخ پایان ویرایش دوم:** ۸۴/۱۱/۲۲

هشدار : تمامی مطالب گفته شده در این کتاب برای آشنایی شما دوستان با امکانات و خدمات گوگل و همچنین جستجو در گوگل می باشد و مسئولیت استفاده نادرست از مطالب بیان شده فقط و فقط به عهده خواننده می باشد.

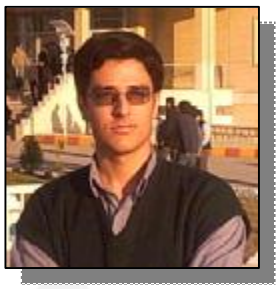
کتاب راهنمای تصویری استفاده از گوگل برای هکرها

همراه با امکانات و سرویس های دیگر گوگل (نسخه ۲)

مؤلف: محمد بشیری

Site: http://bashiry.250free.com

درباره مؤلف:



☒ محمد بشیری

☒ دانشجوی رشته کامپیوتر – نرم افزار

☒ استان همدان – شهر سامن

☒ پست الکترونیک ۱: m.bashiry@gmail.com

☒ پست الکترونیک۲: mohamad_bashiry@yahoo.com

☒ آدرس سایت: http://bashiry.250free.com

مخاطبان این کتاب تمام کسانی هستند که مایلند جستجو در گوگل را به طور حرفه ای بیاموزند.

فهرست مطالب

مقدمه ۹

فصل اول ۱۰

شروع کار با گوگل ۱۱

تکنیک های پایه جستجو ۱۷

- جستجوی عبارت در گوگل ۱۷
- جستجوی ترکیبی در گوگل ۱۸
- عملگر AND یا + ... ۱۸
- عملگر OR یا | ۱۹
- عملگر پرانتز (..... ۱۹
- عملگر NOT یا - ۲۰

فصل دوم ۲۱

عملگرهای پیشرفته در گوگل ۲۲

- جستجو در یک سایت خاص یا حوزه ۲۳
- عملگر filetype ۲۴
- عملگر link ۲۷
- عملگر cache ۲۸
- عملگر intitle ۲۹

❖ عملگر allintitle ۳۰
❖ عملگر inurl ۳۱
❖ عملگر intext ۳۲
❖ عملگر allintext ۳۲
❖ عملگر inanchor ۳۳
❖ عملگر daterange ۳۵
❖ عملگر numrange ۳۵
❖ عملگر related ۳۶
❖ عملگر info ۳۷
❖ عملگر phonebook ۳۷
❖ عملگر rphonebook ۳۹
❖ عملگر bphonebook ۳۹
❖ عملگر * ۴۰
▪ یافتن subdomain های یک سایت با استفاده از گوگل ۴۲

جستجوی حوزه ها با استفاده از عملگر Site ۴۲
یافته های googleturds با استفاده از عملگر site ۴۴
Site mapping ۴۵
توضیح درباره Google URL ۴۷

فصل سوم ۵۷

- **کار با cache در گوگل ۵۸**
  - استفاده از گوگل به عنوان سرور پروکسی ۶۵
- **لیست دایرکتوری ها (directory list) ۷۱**
  - پیدا کردن لیست های دایرکتوری از طریق گوگل ۷۱
  - بدست آوردن لیست دایرکتوری های خاص ۷۳
  - پیدا کردن فایلهای خاص ۷۳
  - بدست آوردن نسخه نرم افزار وب سرور از طریق لیست دایرکتوری ۷۴
  - تکنیک های پیمایش در لیست دایرکتوری ها (مسیرها) ۸۳
  - و ...
- **استفاده از گوگل به عنوان پویشگر CGI ۹۲**
- **استفاده از گوگل برای یافتن فایلها و مسیرهای جالب ۹۸**

فصل چهارم ۱۰۰

- **یافتن نام های کاربری، کلمات عبور و اطلاعات حساس دیگر**
  - یافتن نام های کاربری یا Usernames ۱۰۲
  - جستجو برای یافتن کلمات عبور Passwords ۱۰۷
  - جستجو برای اطلاعات مالی و حسابداری ۱۱۶
  - جستجو برای اطلاعات حساس دیگر ۱۱۷
  - هک پایگاه داده ها از طریق گوگل ۱۲۲

فصل پنجم ۱۲۵

۹ نوع جستجوی امنیتی ساده

- Site ۱۲۶
- intitle:index.of ۱۲۸
- error | warning ۱۲۸
- login | logon ۱۳۰
- username | userid | employee.ID | "your username is" ۱۳۱
- password | passcode | "your password is" ۱۳۲
- admin | administrator ۱۳۲
- –ext:html –ext:htm –ext:shtml –ext:asp –ext:php ۱۳۴
- inurl:temp | inurl:tmp | inurl:backup | inurl:bak ۱۳۶

فصل ششم ۱۳۷

یافتن محل اکسپلویت ها[1] و پیدا کردن نقاط آسیب پذیری روی اهداف

- مقدمه ۱۳۸
- یافتن محل اکسپلویت ها ۱۳۸
- یافتن محل سایتهای دارای اکسپلویت های عمومی ۱۳۹
- یافتن اکسپلویت ها از طریق کدهای رشته ای رایج ۱۴۰
- یافتن محل آسیب پذیری روی اهداف ۱۴۲

[1] Exploits

فصل هفتم ۱۴۳

امکانات و سرویس های دیگر گوگل ۱۴۴
- Alerts ۱۴۸
- Local ۱۴۹
- Answers Local ۱۵۰
- Maps ۱۵۲
- Blog Search ۱۵۶
- Mobile ۱۵۸
- Book Search ۱۶۰
- News ۱۶۱
- Catalogs ۱۶۲
- Scholar ۱۶۳
- Directory ۱۶۴
- SMS ۱۶۶
- Froogle ۱۶۶
- Special Search ۱۶۷
- Groups ۱۶۹
- University Search ۱۷۰
- Images ۱۷۱
- Web Search ۱۷۱
- Labs ۱۷۲
- Video ۱۷۳

منابع و مؤاخذ ۱۷۵

تقدیر و تشکر ۱۷۶

مقدمه:

اگر تا به حال به سایت گوگل رفته باشید حتما متوجه شدید که صفحه وب بسیار بسیار ساده ای دارد و بعضی کاربران فکر می کنند که این سایت به این سادگی قدرت زیادی ندارد، ولی بر خلاف عقیده این افراد موتور جستجوگر گوگل واقعا در زمینه های مختلف قدرتمند می باشد.

آدرس اینترنتی این سایت www.google.com می باشد که دارای ابزار مختلف از قبیل: زبانهای گوناگون، ترجمه اسناد، صفحات وب، شامل تصاویر، گروه های خبری، فهرست ها ، جستجوی خبرها و جستجوی فیلم ها ... می باشد. اکثر این امکانات در فصل آخر به تفصیل بررسی شده است. اما بعضی افراد از این ابزارهای مختلف در گوگل سوء استفاده می کنند. که این افراد غالبا هکرها، مجرمان کامپیوتری، دزدان هویت ها (identity thieves) و تروریست ها می باشند. خلاصه اینکه بیشتر این افراد بد اندیش برای کارهای خود از گوگل استفاده می کنند که به این تکنیک در اصطلاح "Google hacking" گفته می شود. هدف ما از این کتاب تربیت مدیران سیستم ها در جهت بالا بردن امنیت می باشد . در تمامی این کتاب ما به بررسی روشهای مختلف جستجو در گوگل خواهیم پرداخت. در فصل اول به عملگرهای ساده جستجو در گوگل پرداخته خواهد و سپس در فصل دوم این کتاب به توضیح عملگرهای پیشرفته پرداخته می شود. در فصل سوم با cache و لیست های دایرکتوری و همچنین استفاده از گوگل به عنوان پویشگر[1] CGI پرداخته شده است. در فصل چهارم این کتاب چگونگی پیدا کردن Username ها و همچنین password ها و اطلاعات مالی حسابداری و استفاده از گوگل در هک پایگاه داده ها بررسی شده است. در فصل پنجم چندین مثال و جستجوی امنیتی ساده برای یافتن اطلاعات ار مقصد توضیح داده شده و سپس در فصل ششم استفاده از گوگل برای یافتن کدهای مخرب بررسی شده و در انتها یعنی فصل هفتم تمامی امکانات و خدمات گوگل به طور کامل آورده شده است.

[1] Scanner

مؤلف: محمد بشیری

Site: http://bashiry.250free.com

فصل اول

مقدمات کار با گوگل و جستجوی ساده در آن

- تکنیک های جستجو در گوگل
- تکنیک های پایه جستجو
  - جستجوی عبارت در گوگل
  - جستجوی ترکیبی در گوگل
  - عملگر AND یا +
  - عملگر OR یا |
  - عملگر پرانتز
  - عملگر NOT یا -

در این فصل ما جستجوی مقدماتی و ساده در گوگل را فرا خواهیم گرفت.

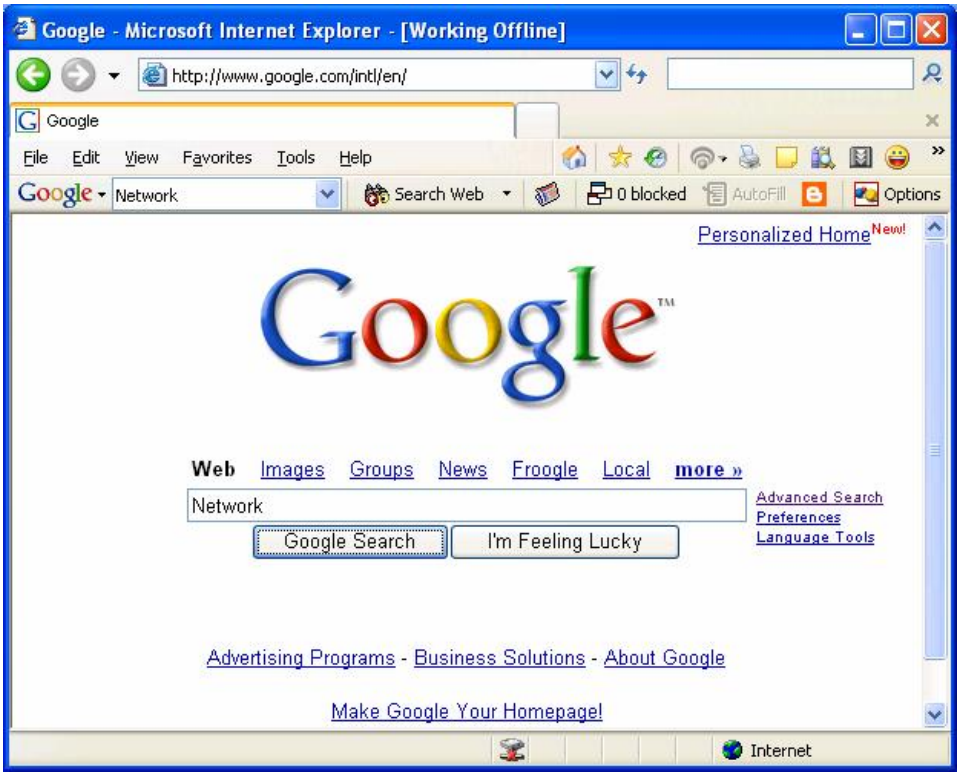
قبل از شروع کار با گوگل به چند نکته مهم باید توجه داشته باشید:

عبارات جستجو به حروف کوچک و بزرگ حساس نیست. مثلا کلمات با حروف کوچک (hackers) و حروف بزرگ (HACKERS) و یا (HaCkEr) و همچنین (hacker) برای گوگل تفاوتی ندارد.

شروع کار با گوگل

در گوگل دو نوع جستجو داریم:

- اولین نوع جستجو در گوگل این است که به دنبال یک کلمه خاص بگردیم برای این کار به سادگی آن را در گوگل نوشته و آن را مورد جستجو قرار می دهیم.
- دسته دوم آنهایی هستند که به دنبال بیش از یک کلمه به طور همزمان می گردند در این نوع جستجو از کلیدهای ترکیبی AND و OR استفاده می شود. اگر بین دو کلمه از کلید واژه AND استفاده نماییم هر دو کلمه باید در سایت پیدا شده وجود داشته باشد. OR (|) برعکس AND می باشد به این صورت که سایت پیدا شده حاوی یکی از این کلمات است.



تصویر شماره۱- صفحه اصلی موتور جستجوگر گوگل

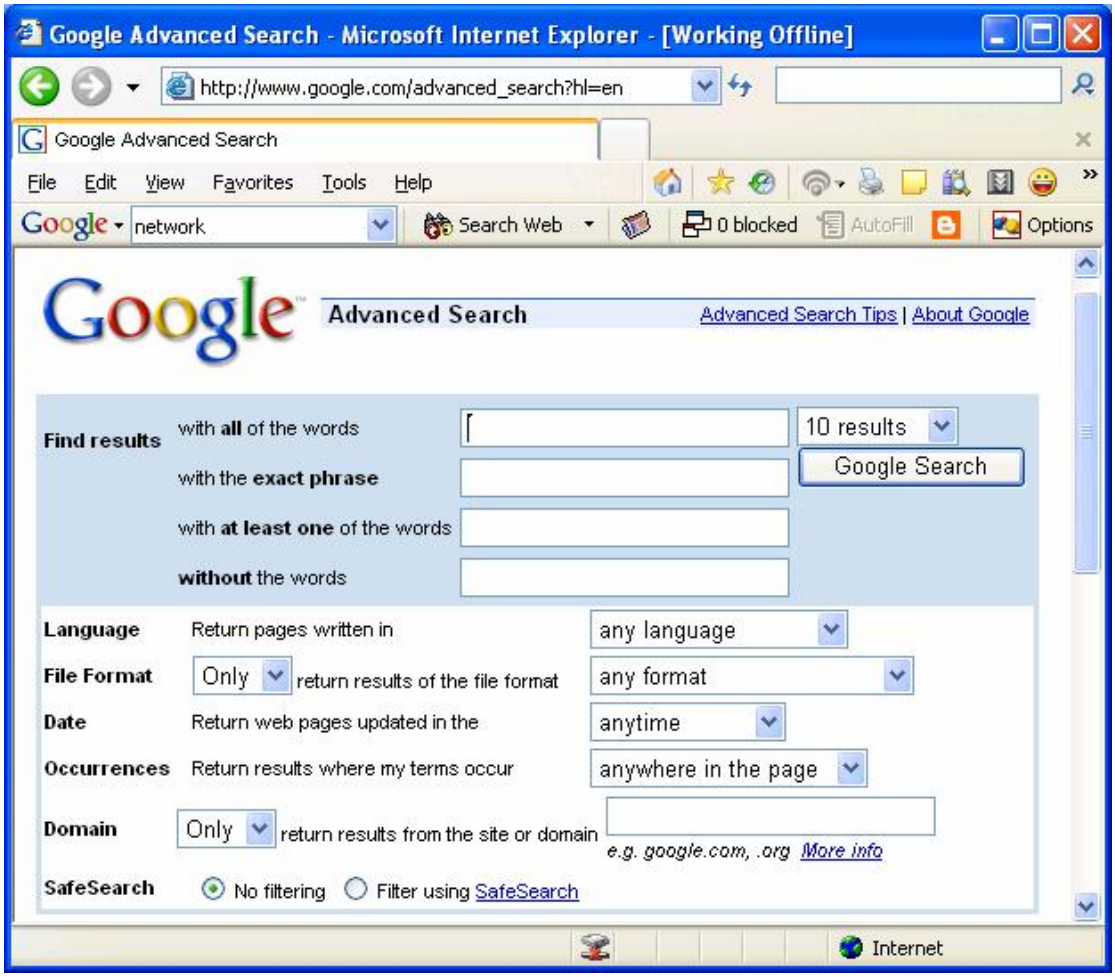
در تصویر شماره(۱) ما یک لغتی مانند"network" را در صفحه جستجوی گوگل نوشتیم. برای شروع به جستجوی این لغت بر روی دکمه "Google search" کلیک می کنیم تا گوگل شروع به جستجوی عبارت مورد نظر (که در این مثال خاص کلمه "network" می باشد) می کند.

در تصویر فوق گزینه های زیادی به چشم می خورد.

نوار ابزار گوگل The Google toolbar	**همانطور که در شکل شماره ۱ مشاهده می شود مرورگر اینترنت دارای نوار ابزار گوگل می باشد که در زیر نوار آدرس قرار دارد (این نوار ابزار رایگان می باشد و می توانید از آدرس toolbar.google.com دانلود نمایید) اگر چه این نوار ابزار دارای ظاهر های مختلفی است و به هیچ عنصری جهت جستجوی پیشرفته احتیاج ندارد. پس برای جستجوی پیشرفته می توان به آدرس سایت گوگل مراجعه نمود و جستجوی پیشرفته خود را از طریق این صفحه انجام داد.**

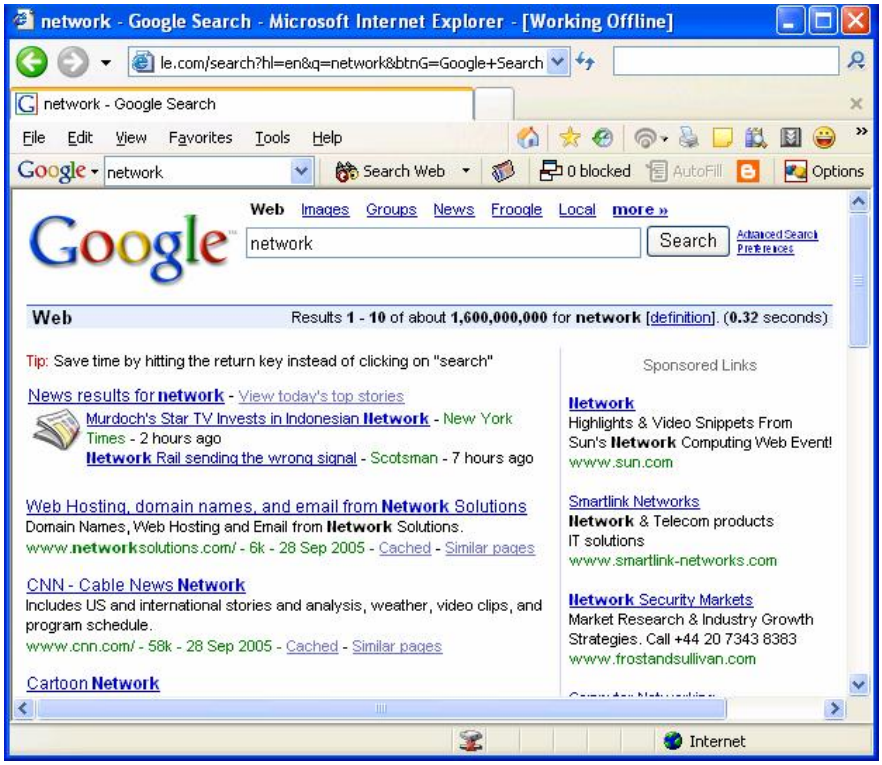
توضیحات قسمت های مختلف صفحه اصلی گوگل را در جدول زیر مشاهده می کنید:

نام لینک	توضیحات
Web, Images, Groups, Directory and News tabs	این لینک ها به ترتیب به شما اجازه جستجو در صفحات اینترنت، تصاویر، گروه های پستی، لیست دایرکتوری گوگل، اخبار را می دهد.
Search term input field	این بخش که درست زیر لینک های مذکور می باشد محل تایپ متن هایی که می خواهید جستجو کنید می باشد.
"Google Search"	این دکمه برای جستجوی کلمه وارد شده استفاده می شود در بسیاری از مرورگرها بعد از تایپ کلمه مورد نظر و فشردن کلید Enter می توان عبارت مورد نظر را جستجو نمود.
دکمه I'm Feeling Lucky	اگر بر روی این دکمه کلیک کنید گوگل لیست صفحاتی را به شما خواهد داد که بیشترین ارتباط را با عبارت جستجوی وارد شده دارند.
"Advanced Search"	با فشار دادن این لینک می توان جستجو در گوگل را به صورت پیشرفته انجام داد (به شکل شماره ۲ توجه نمایید).
"Preferences"	این گزینه به کاربران اجازه می دهد تا چندین گزینه را انتخاب نمایند. (ذخیره کوکی ها در کامپیوتر برای استفاده بعدی) و شامل زبان ها، فیلترها، مشخص کردن تعداد نتایج در صفحه و تنظیمات پنجره ها می باشد.
"Language tools"	این لینک به کاربران اجازه انتخاب زبان های مختلف را می دهد. به طور مثال اگر زبان را Persian انتخاب نمایید صفحه اصلی گوگل به زبان فارسی ترجمه شده و همینطور زبان های مختلف دیگری نیز وجود دارند.



شکل شماره۲- جستجوی پیشرفته در گوگل

طبق شکل زیر (شکل شماره ۳) هنگامی که کاربر دکمه Google search، یا دکمه Enter را فشار می دهد صفحه ای شامل نتایج پیدا شده برای کلمه وارد شده ظاهر می گردد.



شکل شماره۳- نتیجه جستجو در گوگل

صفحه نتایج به کاربر این امکان را می دهد که کاربر از بین نتایج ظاهر شده نتیجه مورد نظر خـود را انتخاب نماید .

در بالاترین خط در صفحه نتایج همانند شکل زیر عباراتی مشاهده می شود:

Web Results **1** - **10** of about **1,600,000,000** for **network** [definition]. (**0.32** seconds)

که توضیحات آن به شرح زیر می باشد:

۱- مکان جستجو : Web

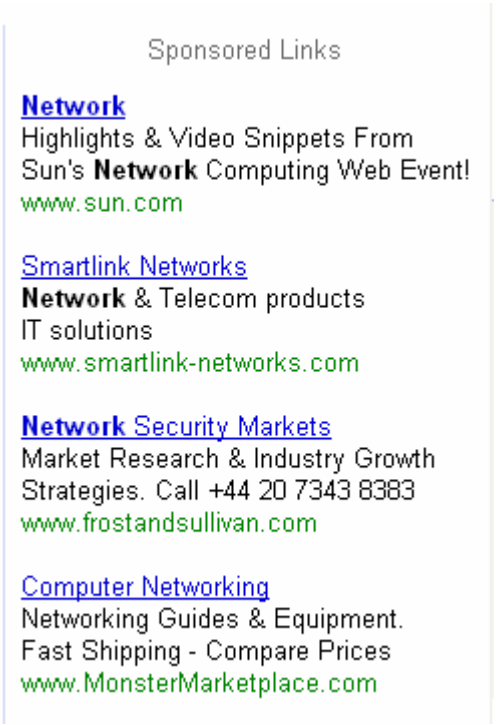
۲-نمایش یافته ها در هر صفحه: مثلا در این صفحه ۱۰ تا از یافته ها مشاهده می شود.

۳- تعداد یافته ها : که در اینجا مقدار 1,600,000,000 می باشد

۴- کلمه مورد جستجو: در اینجا Network

۵- زمان جستجو: که در اینجا 0.32 ثانیه می باشد.

- قسمت بعدی که در صفحه نتایج مشاهده می شود مطابق شکل زیر Sponsored Links می باشد.


Sponsored Links

Network
Highlights & Video Snippets From
Sun's **Network** Computing Web Event!
www.sun.com

Smartlink Networks
Network & Telecom products
IT solutions
www.smartlink-networks.com

Network Security Markets
Market Research & Industry Growth
Strategies. Call +44 20 7343 8383
www.frostandsullivan.com

Computer Networking
Networking Guides & Equipment.
Fast Shipping - Compare Prices
www.MonsterMarketplace.com

این قسمت مربوط به تبلیغات در گوگل می باشد که بر اساس کلمه ای که شما جستجو می کنید تبلیغات مربوط به آن کلمه ظاهر خواهد شد.

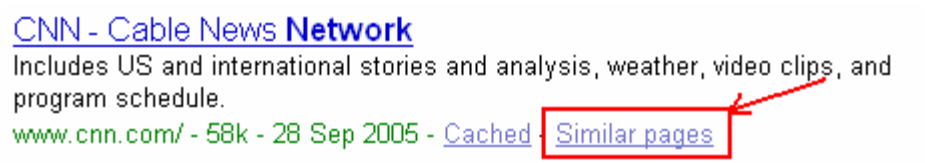
- قسمت بعدی که در صفحه نتایج گوگل مشاهده می شود عبارت Cached است.

اگر روی این عبارت کلیک کنید گوگل شما را به یک نمونه از صفحه ذخیره شده از

این سایت خواهد برد. این قسمت هنگامی کاربرد دارد که صفحه مورد نظر شما تغییر کرده باشد و شما بخواهید به مطالب قبلی آن سایت دسترسی داشته باشید.

.:: توضیحات کامل این بخش بعدا داده خواهد شد ::.

- قسمت بعد مطابق شکل زیر عبارت Similar pages می باشد که این قسمت ما را به صفحه‌هایی که شبیه به این صفحه و مرتبط با آن صفحه خواهد برد.



تکنیک های پایه جستجو

جستجوی عبارت در گوگل

برای جستجوی یک عبارت یا جمله در گوگل آن عبارت را بین علامت نقل قول[1] قرار می دهیم تا دقیقا عبارت نوشته شده بین این دو علامت مورد جستجو قرار گرفته شود نه تک‌تک کلمات به مثال های زیر توجه نمایید:

“The quick brown fox”

“Liberty and justice for all”

“Harry met sally”

[1] علامت نقل قول یا علامت "

جستجوی ترکیبی در گوگل

جستجوی ترکیبی در گوگل شامل یک کلمه تنها و علامت نقل قول می باشد:

Macintosh "Microsoft office"

نتیجه عبارت فوق در گوگل شامل عبارت "Microsoft Office" و لغت Macintosh می باشد.

عملگرهای بولی[1] در گوگل:

عملگر AND یا + :

عملگر پیش فرض گوگل AND می باشد به این مفهوم که اگر در گوگل چند کلمه بنویسید گوگل تمام آنها را جستجو می کند .

مثال: فرض کنید که در گوگل عبارت زیر را برای جستجو نوشته‌اید:

```
snowblower Honda "Green Bay"
```

گوگل تمام لغات را جستجو می کند .

هنگامی که ما در گوگل از چند کلمه برای جستجو استفاده می کنیم گوگل برای هر لغت یک لیست از صفحات مربوط به تک‌تک لغات به ما می دهد . در بعضی از موتورهای جستجوگر بجای استفاده از کلمه AND می توان از علامت جمع (+) استفاده نمود. اگر در گوگل بین دو کلمه از این علامت استفاده نماییم به مفهوم AND می باشد. عملگر + یکی از عملگرهای رایج برای جستجو در گوگل می باشد.

نکته: بین علامت جمع و کلمه مورد نظر برای جستجو نباید فاصله خالی وجود داشته باشد برای مثال به عبارات زیر توجه کنید :

---

[1] Bool

+where quick brown fox

Where +quick +brown fox

عملگر OR یا | :

اگر نخواهید که گوگل تمام لغات را جستجو کند و فقط یکی از لغات (یا snowblower یا Honda و یا عبارت "green bay") جستجو شود از این عملگر استفاده می کنیم.

نحوه استفاده از این عملگر به صورت زیر خواهد بود:

```
snowblower OR snowmobile OR "Green Bay"
```

عملگر پرانتز " ( ) "

اگر شما می خواهید یکی از عبارات را حتما داشته باشید و عبارت بعد را مانند OR داشته باشید از این عملگر استفاده می شود. به طور کلی تر با استفاده از این عملگر می توان ترکیب AND و OR را همزمان داشت. مثال:

```
snowblower (snowmobile OR "Green Bay")
```

نوع جستجوی فوق کلمه Snowmobile یا عبارت "Green Bay" را به همراه کلمه Snowblower مورد جستجو قرار می دهد.

همچنین می توان به جای استفاده از عملگر OR از علامت | استفاده نمود. (شایان به ذکر است که این علامت از فشردن دکمه شیفت به همراه علامت \ یا کلید ژ در فارسی تولید می شود)

مثال استفاده از علامت | :

```
snowblower (snowmobile | "Green Bay")
```

و مثال ترکیبی دیگر:

```
intext:password | passcode intext:username | userid |
user filetype:csv
```

و یا

```
intext:(password | passcode) intext:(username | userid | user) filetype:csv
```

اگر بعضی از قسمت های آن را متوجه نشدید نگران نباشید در ادامه به بررسی آنها هم پرداخته خواهد شد..

عملگر '-' [1] یا همان عملگر NOT :

این عملگر به معنی محروم کردن یک لغت برای جستجو است مثلا می خواهیم به دنبال سایت هایی بگردیم که کلمه Microsoft داشته باشد ولی کلمه Windows در آن صفحات نباشد پس در گوگل عبارت زیر را برای انجام این عمل تایپ می کنیم:

Microsoft –windows

Microsoft NOT windows

Quick –brown fox

و یا

snowblower snowmobile -"Green Bay"

جستجوی بالا هر دو کلمه snowblower و snowmobile را جستجو می کند به طوری که در صفحاتی که پیدا می شوند عبارت Green Bay وجود ندارد.

در این فصل آموختیم که چگونه از عملگرها برای یافتن موضوعات در گوگل استفاده کنیم و برای یافتن عبارت مورد نظر جستجوها را محدود کنیم تا به نتیجه دلخواه برسیم. امیدوارم که تا اینجا مطالب گفته شده را خوب یاد گرفته باشید. در فصل بعد به بررسی عملگرهای پیشرفته تر دیگری در گوگل خواهیم پرداخت.

[1] Dash

مؤلف: محمد بشیری

Site: http://bashiry.250free.com

فصل دوم

جستجوی پیشرفته در گوگل

عملگرهای پیشرفته در گوگل

گوگل به شما اجازه می دهد برای محدود کردن جستجو از عملگرهای از پیش تعیین شده ای استفاده کنید که استفاده از این عملگرهای پیشرفته بسیار ساده است و به صورت کلی زیر به کار می روند:

operator:search_term

عبارت مورد جستجو:عملگر

توجه کنید که هیچ فاصله خالی بین عملگر کالن (:) و عبارت مورد جستجو نیست. اگر اشتباها یک فاصله بعد از کالن " : " تایپ شود گوگل پیغام خطا به کاربر نمایش خواهد داد. اگر همین فاصله (Space) قبل ار کالن قرار گیرد گوگل از عملگر نامزد شما استفاده خواهد کرد و به جستجوی عبارت مورد نظر می پردازد.

بعضی از عملگرهای پیشرفته می تواند در قالب یک پرسش مستقل استفاده شود. برای مثال:

Cache:www.google.com

که در گوگل یک عبارت درست برای جستجو است.

و عملگر Site به همراه عبارت مورد جستجو آورده خواهد شد مانند زیر:

Site:www.google.com help

جدول شماره ۱- فهرست برخی از عملگرهای پیشرفته در گوگل

عملگر	توضیح	نیاز به آرگومان؟
Site:	عبارت مورد نظر را فقط در سایت مورد نظر جستجو می کند	دارد

Filetype:	**برای جستجوی فایلها با پسوند نوشته شده**	**دارد**
Link:	**پیدا کردن سایت هایی که به صفحه مورد نظر لینک داده اند.**	**ندارد**
Cache:	**نمایش نسخه ذخیره شده صفحه مورد نظر**	**ندارد**
Intitle:	**پیدا کردن عبارت نوشته شده به شرطی که عبارت در عنوان سایت باشد**	**ندارد**
Inurl:	**پیدا کردن عبارت به شرطی که عبارت در URL[1] سایت باشد.**	**ندارد**

موارد ذکر شده در جدول بالا بعدا به طور کامل توضیح داده خواهند شد.

جستجو در یک سایت خاص یا دامین (Domain) [2]

عملگر پیشرفته Site جستجوی گوگل را محدود به محدوده یا یک سایت می کند به طور مثال:

```
Site:www.sharif.ir  acm
site:loc.gov
site:thomas.loc.gov
site:edu
site:nc.us
```

در اولین مثال از مثالهای بالا در سایت دانشگاه صنعتی شریف به دنبال کلمه acm می گردد.

[1] *Uniform Resource Locator,*

[2] دامین در فارسی همان حوزه ترجمه می شود که ما دراین کتاب برای فهم بهتر همان دامین به کار می بریم

عملگر filetype: جستجو به دنبال یک فایل با پسوند خاص

عملگر Filetype هنگامی کاربرد دارد که ما به دنبال یک فایل با پسوند خاصی می گردیدم به طور مثال:

```
Filtype:pdf  internet
homeschooling filetype:pdf
"Leading economic indicators" filetype:ppt
```

که اولین مثال به دنبال فایل هایی با پسوند PDF[1] می گردد که در آنها کلمه Internet آمده باشد. توجه کنید که گوگل همه پسوند ها را نمی‌تواند جستجو کند برخی از پسوندهایی که توسط گوگل می تواند مورد جستجو قرار گیرند عبارتند از:

- **Adobe Portable Document Format (pdf)**
- **Adobe PostScript (ps)**
- **Lotus 1-2-3 (wk1, wk2, wk3, wk4, wk5, wki, wks, wku)**
- **Lotus WordPro (lwp)**
- **MacWrite (mw)**
- **Microsoft Excel (xls)**
- **Microsoft PowerPoint (ppt)**
- **Microsoft Word (doc)**
- **Microsoft Works (wks, wps, wdb)**
- **Microsoft Write (wri)**
- **Rich Text Format (rtf)**
- **Shockwave Flash (Swf)**
- **Text (ans, txt)**

[1] Adobe Portable Document Format

طبق سایت http://filext.org بیشتر از ۸۰۰۰ نوع پسوند فایل داریم و گوگل این پسوندها را در پایگاه داده های خود دارد و می تواند مانند عمل خزیدن[1] در این پسوند ها جستجو کند ولی ممکن است که با یک پسوند فایل ناشناخته ای سازگاری نداشته باشد.

در جدول زیر ۲۵ عدد از پسوندهای خیلی محبوب در جستجوی گوگل بر اساس تعداد برخوردها با آنها گردآوری شده است که توجه شما را به این پسوندهای محبوب جلب می کنم:

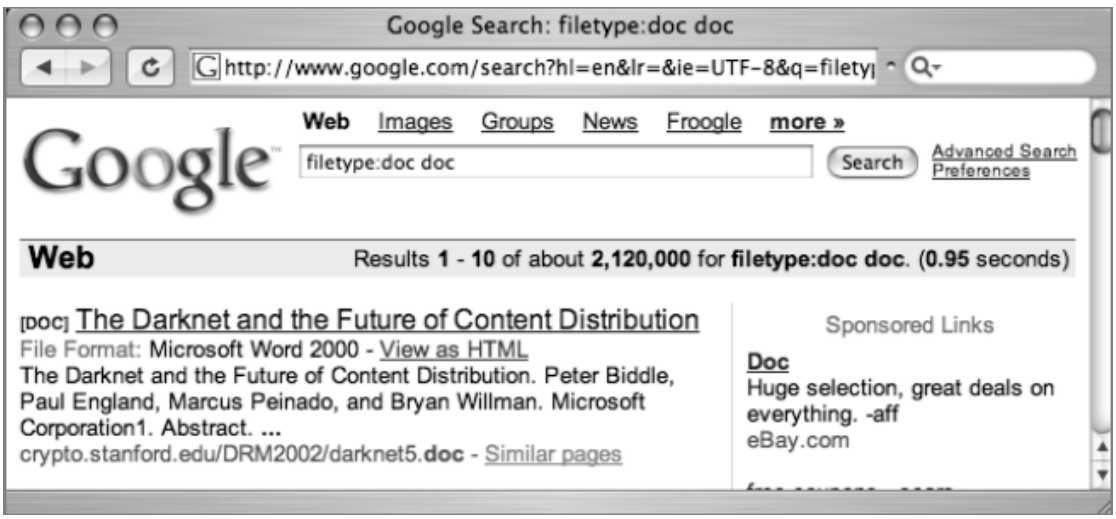
پسوند فایل	تعداد تقریبی برخوردها با پسوند
HTML	18,100,000
HTM	16,700,000
PHP	16,600,000
ASP	15,700,000
CGI	11,600,000
PDF	10,900,000
CFM	9,880,000
SHTML	8,690,000
JSP	7,350,000
ASPX	6,020,000
PL	5,890,000
PHP3	4,420,000
DLL	3,050,000
PHTML	2,770,000
FCGI	2,550,000
SWF	2,290,000
DOC	2,100,000
TXT	1,720,000

[1] crawl

PHP4	1,460,000
EXE	1,410,000
MV	1,110,000
XLS	969,000
JHTML	968,000
SHTM	883,000
BML	859,000

برای اطلاعات بیشتر در مورد انواع دیگر پسوند ها و پسوندهای نا آشنا برای شما می توانید بـه آدرس http://www.filext.com مراجعه کنید.

همچنین گوگل این امکان را دارد که هر سندی را برای دیدن آنلایـن بـه فرمـت HTML یـا text تبدیل می کند. به تصویر زیر دقت کنید:



به علامت [DOC] در ابتدای اولین نتیجه توجه کنید. DOC پسوند نرم افزار WORD از شـرکت مایکروسافت است همچنین می توانید این سند را در قالب HTML ببینید بدون اینکه از نـرم افـزار WORD بخواهیم استفاده کنیم. پس برای این کار بر روی لینک View as HTML کلیک کنید تا آن فایل را بلافاصله در فرمت HTML مشاهده کنید.

(در ضمن شما می توانید لیست این پسوند ها را از قسمت پرسش و پاسخ سایت گوگل با آدرس Http://www.google.com/help/faq_filetype.html به دست آورید.)

عملگر Link :

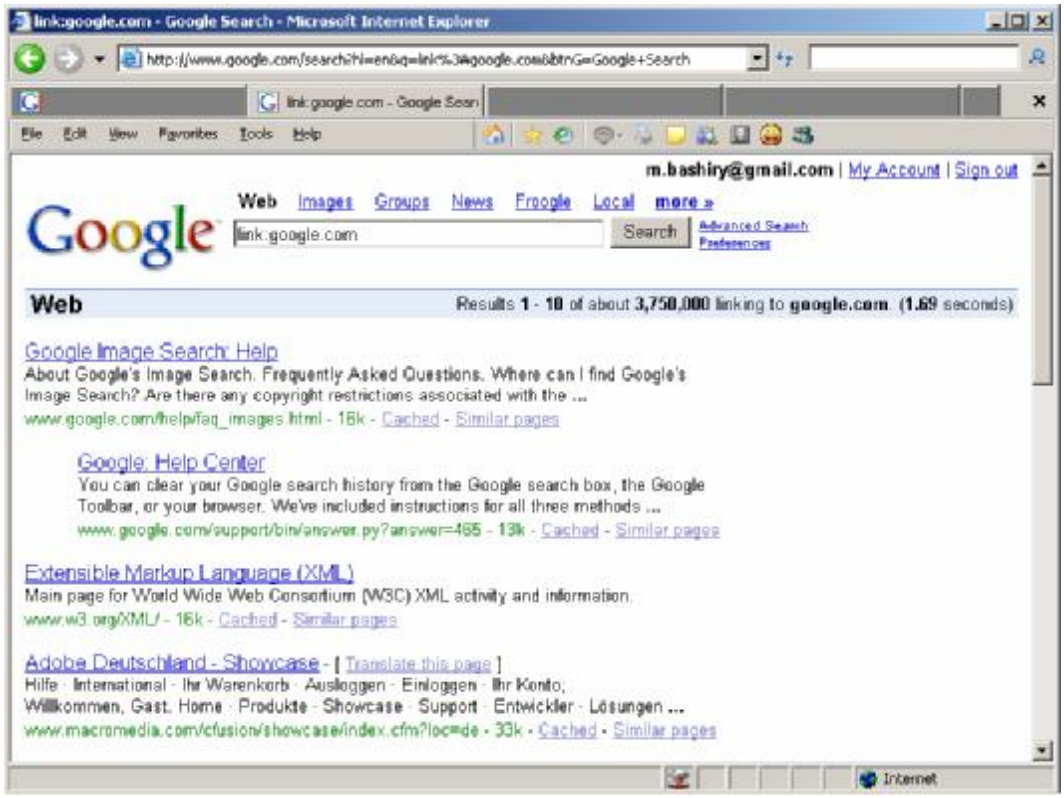
جستجو در سایت هایی که با صفحه مورد نظر متصل یا لینک هستند:

ابر لینک ها (Hyper link) در اینترنت نقش خیلی مهمی دارند. ابر لینک ها یک متن قابل انتخاب هستند که ما را به صفحه ای دیگر می برد که اغلب آنها دارای یک خط در زیرشان می باشد و می تواند در قالب متن، عکس، ویدئو و غیره باشد. عملگر Link در گوگل به همراه آدرس یک سایت بیانگر این است که گوگل به دنبال تمامی سایت هایی می گردد که به سایت مورد نظر لینک داده‌اند و یا به اصطلاحی دیگر با آن سایت در ارتباط باشد. به طور مثال:

Link:www.apple.com

نکته: عبارت فوق صفحاتی را به مرتبط با www.apple.com/ipod هستند را پیدا می کند.

برای توضیح بیشتر به تصویر زیر دقت نمایید:



Cache: عملگر

جستجو برای نسخه ذخیره شده یک سایت توسط گوگل

گوگل همیشه یک نسخه ذخیره شده از سایت ها را دارد و هنگامی استفاده می شود که صفحه مورد نظر موجود نباشد یا تغییر کرده باشد و ما بخواهیم به صفحه قبلی آن سایت مراجعه کنیم از این عملگر استفاده می کنیم. به طور مثال:

Cache:www.shabgard.org

Cache:irib.ir

پس همیشه این نکته را در ذهن داشته باشید که خیلی خیلی مهم است:

هر وقت سایتی را نتوانستید باز کنید و یا لینکی از آن سایت داشتید که با وارد کردن آن لینک صفحه مورد نظر نیامد و مسائلی از این دست از Cache در گوگل استفاده کنید تا سایت مورد نظر باز شود و بتوانید از امکانات آن سایت استفاده کنید.

intitle: عملگر

جستجو در عنوان یک سند

هنگامی که ما یک صفحه وب را باز می کنیم عنوان آن در مرورگر نشان داده خواهد شد که اگر ما بخواهیم فقط در آن عنوان جستجو کنیم از عملگر :Intitle استفاده می کنیم . این عملگر به هیچ آرگومان دیگری احتیاج ندارد .به طور مثال:

Intitle:learning

به چندین کاربرد از این عملگر توجه کنید:

☒ Intitle:google

باعث می شود که صفحاتی پیدا شوند که در عنوان آنها کلمه google باشد

☒ Intitle:"index of"

صفحاتی را خواهد داد که در عنوان آنها کلمه index of ظاهر شده باشد. همچنین می توانید به صورت روبرو بنویسید: intitle:index.of

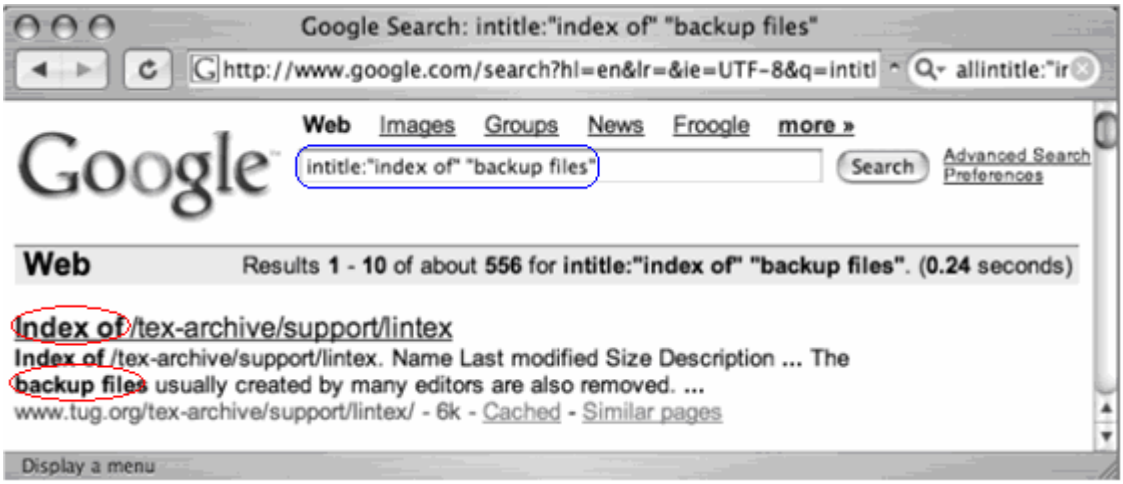
☒ Intitle:"index of" private

صفحاتی را به ما می دهد که در عنوان آنها کلمه index of ظاهر شده باشد و کلمه private[1] در هر کجای آن صفحات موجود باشد.

☒ Intitle:" index of" "backup files"

[1] خصوصی

صفحاتی را خواهد داد که در عنوان آنها کلمه index of ظاهر شده باشد و بعلاوه عبارت backup files[1] در هر کجای آن صفحات باشد.



allintitle: عملگر

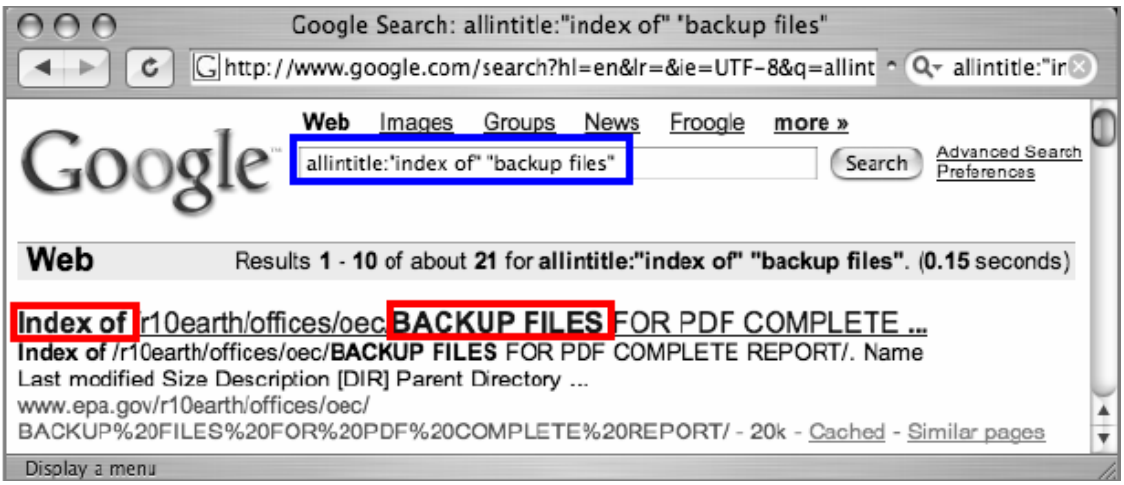
یک مشتق دیگری از این عملگر وجود دارد که مانند Intitle می باشد. به مثال زیر توجه کنید:

Allintitle:learning Computer

عبارت فوق در عنوان صفحه به دنبال دو عبارت Learning و Computer می گردد. در اصل به دنبال عبارت وارد شده در جلوی آن می گردد که عبارت ما در اینجا learning computer است.

و یا اگر بنویسیم "allintitle:"index of" "backup files نتایج به اینکه بنویسیم "intitle:"index of" "backup files تفاوت می کند. نتیجه جستجو به صورت زیر خواهد بود:

[1] فایلهای پشتیبان



عملگر inurl:

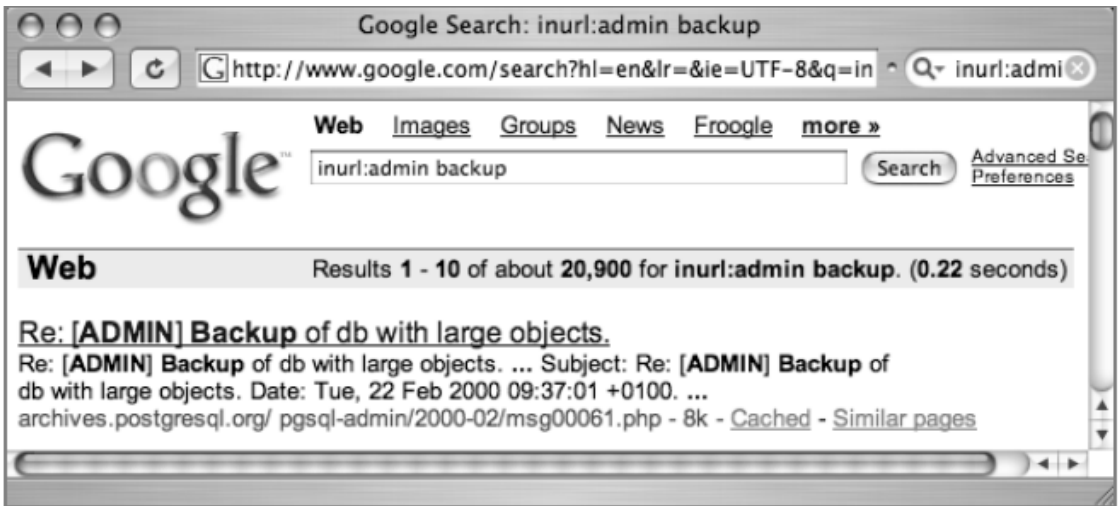
جستجو در آدرس اینترنتی [1] یک صفحه

این عملگر به هیچ آرگومان دیگری نیاز ندارد و در URL صفحه ها جستجو می کند به طور مثال:

Inurl:Ebook

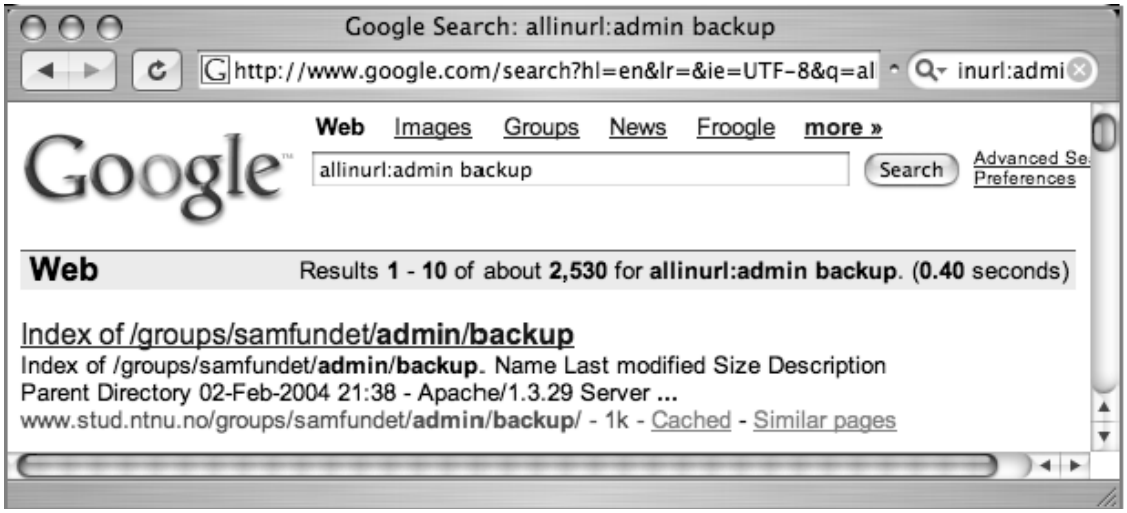
صفحاتی را نشان می دهد که در آدرس آن صفحه از عبارت Ebook استفاده شده مانند آدرس زیر:

http://bashiry.250free.com/Ebook/



[1] URL – (*Uniform Resource Locator*)

که این عملگر مشتق دیگری هم با نام Allinurl دارد که مانند allintitle عمل می کند ولی با این تفاوت که در آدرس سایت (URL) جستجو می کند.



برای کسب اطلاعات کاملتر از عملگرهای پیشرفته در گوگل به آدرس زیر مراجعه نمایید:

Http://www.google.com/help/operators.html

intext: این عملگر فقط در بدنه و Body سایت ها جستجو می کند. بطور مثال از جستجو در URL، Title، Link صفحات چشم پوشی می کند.

مثال:

```
intext:"yahoo.com"
intext:html
```

Allintext: محل یک رشته از یک متنی در یک صفحه

این عملگر در همه جای صفحه به جزء عنوان[1] صفحه، URL صفحه و لینک ها آن به دنبال رشته مورد نظر می گردد.

توجه داشته باشید که این عملگر همراه با عملگرهای پیشرفته دیگر به کار نمی رود.

inanchor:

این عملگر می تواند با ترکیبی از عملگر link به کار رود و این در حالی ایست که هر دو به یافتن link ها کمک می کنند. به هر حال این عملگر بین لینک ها به دنبال متون می گردد اگرچه آن لینک ها آدرس URL واقعی نباشند.

به تصویر زیر دقت کنید:

در تصویر بالا لینک با نام current page در یک فرم معمولی نشان داده شده است. وقتی روی این ابر متن یا لینک کلیک می کنید آدرس URL آن چیزی شبیه زیر می شود:

```
www.kerneltraffic.org/kerneltraffic/latest.html
```

اگر به کد واقعی آن (HTML CODE) نگاه کنید به صورت زیر می باشد:

```
<A HREF=" http://www.kerneltraffic.org/kernel-traffic/latest.html">currentpage</A>
```

[1] Title

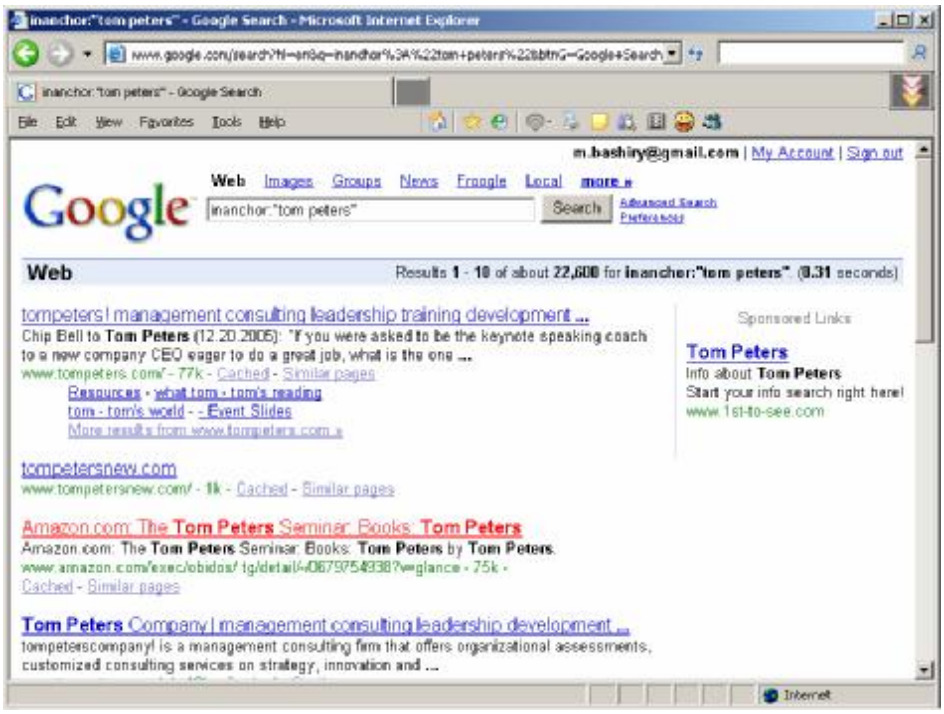
این عملگر به شما کمک می کند که در متن های لنگر گاه یا در اصطلاح انگلیسی آن anchor به دنبال متون بگردید که در این مثال عبارت "currentpage" در کد HTML بالا جستجو می شود.

مثالی دیگر:

در کد HTML زیر کلمه .O'Reilly and Associates لنگرگاه می باشد.

```
<a href="http://www.oreilly.com>O'Reilly and Associates</a>
```

نمونه دیگر : **inanchor:**"tom peters"



Daterange:

محدود کردن جستجو در یک بازه زمانی که توسط گوگل شاخص بندی شده است. (Indexed). نکته مهم این است جستجو به تاریخ ایجاد صفحات محدود نمی‌شود. پس تاریخ هایی که ما وارد می کنیم بر اساس زمان شاخص بندی توسط گوگل می باشد نه تاریخ ایجاد صفحات. توجه داشته باشید که تاریخ وارد شده بر اساس تقویم میلادی می باشد.

```
"George Bush" daterange:2452389-2452389
neurosurgery daterange:2452389-2452389
```

Numrange: جستجو برای یک عدد

این عملگر به دو پارامتر نیاز دارد. کمترین عدد و بیشترین عدد که با علامت خط تیره[1] از هم جدا می شوند. این عملگر برای استفاده از هکرها خیلی قدرتمند می باشد. این عملگر یکسری از اعداد را در یک رنج خاص را پیدا می کند. برای مثال عدد ۱۲۳۴۵ بین دو رنج ۱۲۳۴۴ و ۱۲۳۴۶ می باشد که به صورت روبرو می نویسیم: numrange:1234-12346

هنگام جستجوی اعداد ، گوگل از کاراکتر ها ی مثل کاما یا علامت پول ($) چشم پوشی می کند.

حالت دیگری از این عملگر وجود دارد بدین صورت که بین دو عدد از دو نقطه (..) استفاده می کنند. 12344..12346

همچنین به صورت 12344-12346 هم می توان استفاده نمود.

لازم به ذکر است که این عملگر می تواند با عملگرها و عبارت دیگر نیز استفاده شود.

[1] dash

Related:

این عملگر صفحه های مرتبط با یک صفحه خاص را پیدا می کند با این ویژگی که تمام صفحات مرتبط با هم را نشان نمی دهد. این نوع جستجو روش مناسبی برای پیدا کردن دسته[1] ای از صفحات است. مثلا جستجو برای `related:www.google.com` تمامی صفحاتی پیدا می شوند که مانند گوگل موتور جستجو گر هستند مانند `Yahoo!`، `AltaVista`، `HotBot` و غیره. توجه داشته باشید بین عملگر related و علامت دو نقطه و عبارت جلوی آن نباید فاصله خالی وجود داشته باشد.

کار این عملگر مانند این است که در صفحه نتایج بر روی لینک similar page کلیک کنید.

برای درک بهتر به تصویر زیر دقت کنید:

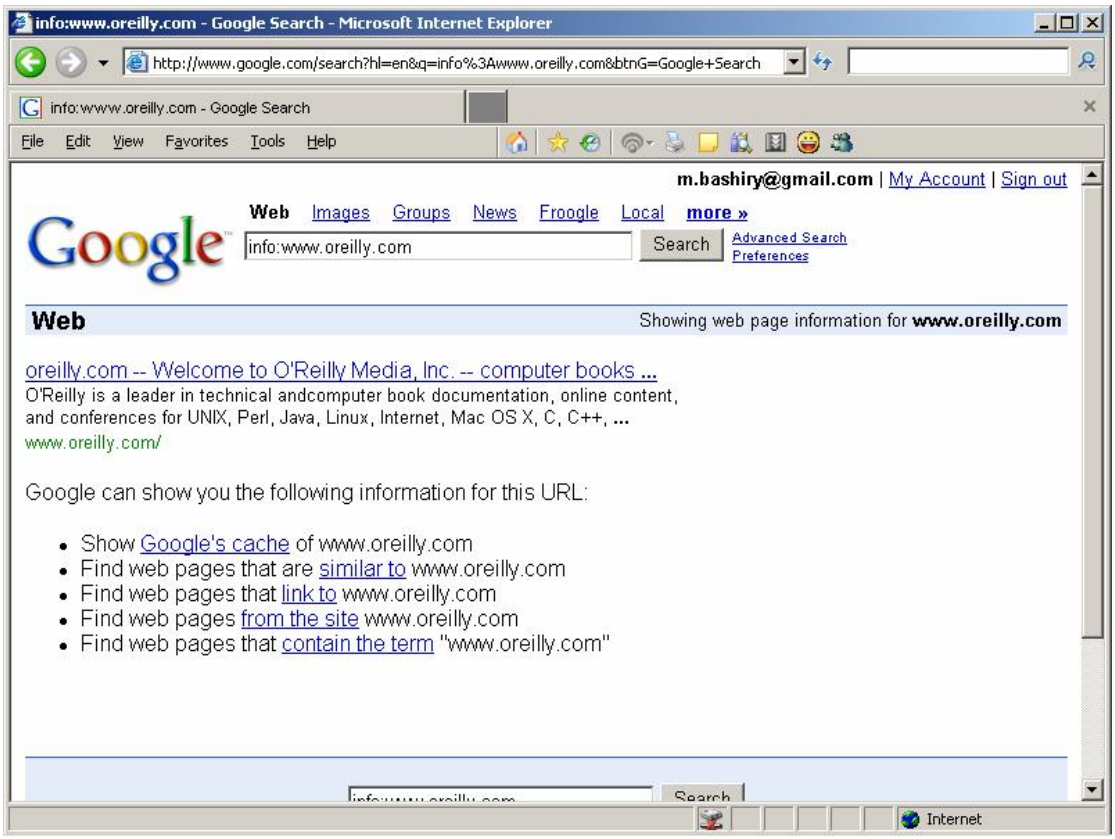
توجه کنید که این عملگر همراه با عملگرها یا عبارات دیگر استفاده نمی‌شود.

[1] Category

عملگر Info:

نتایجی را ارائه می دهد که اطلاعات بیشتری در مورد URL خاص و یا سایت را می دهد. اطلاعات شامل یک لینک از URL صفحات ذخیره شده یا Cache شده توسط گوگل باشد، یک لیست از صفحات Link شده به URL باشد، صفحاتی که با URL در ارتباط هستند (Relate) و محتوای خودِ آدرس URL. اگر آدرس مورد نظر در گوگل شاخص [1] نداشته باشد جستجو محدودتر خواهد شد. توجه کنید که اگر آدرس سایت را به طور مستقیم در جعبه متن در صفحه اصلی گوگل تایپ کنید با اینکه از این عملگر استفاده کنید هیچ تفاوتی نمی‌کند.

به تصویر زیر که در این ارتباط می باشد توجه کنید:



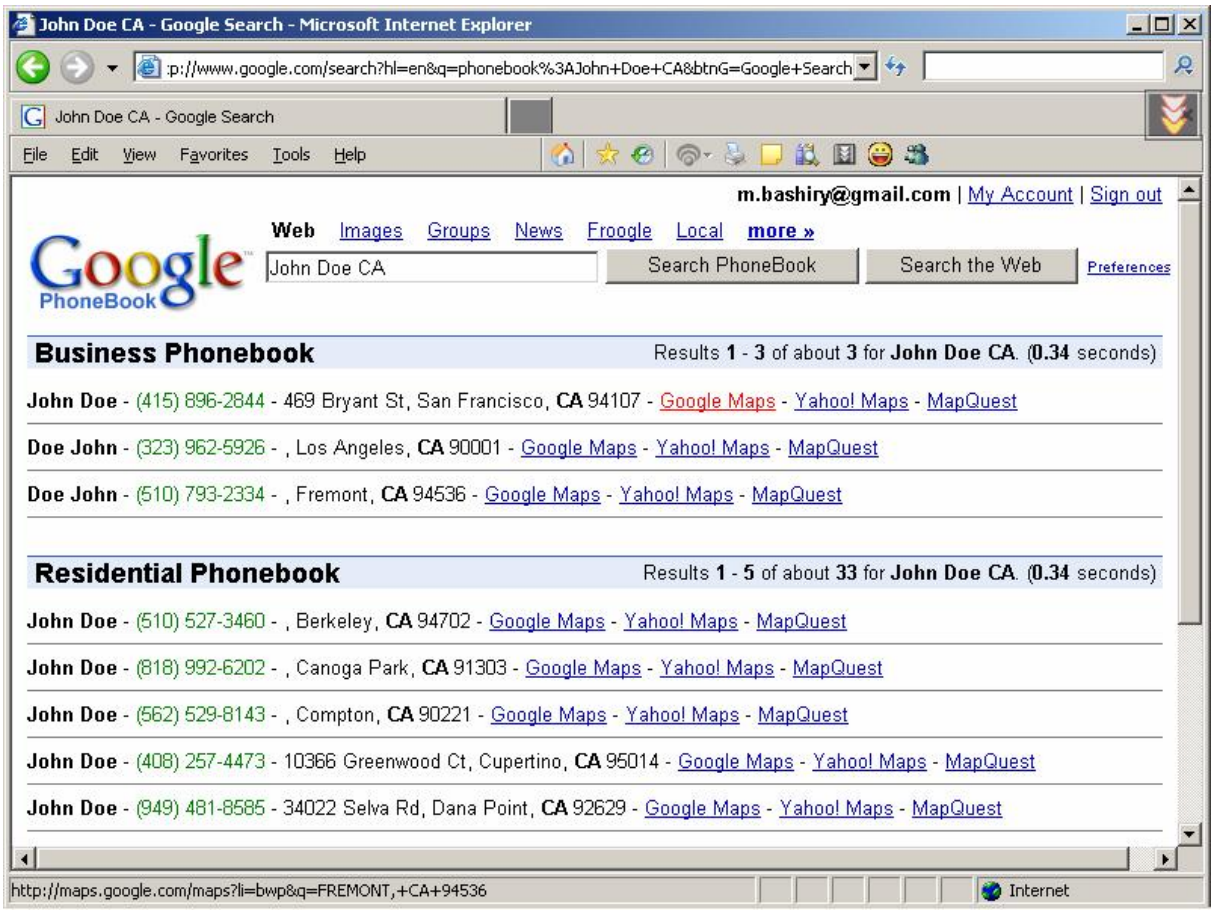
[1] Index

عملگر Phonebook:

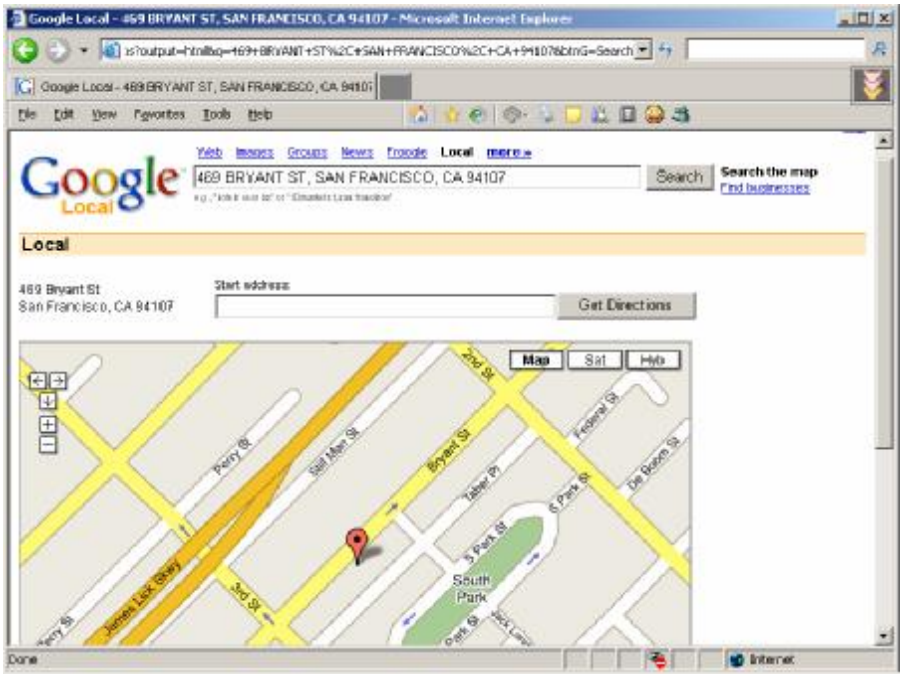
همانطور که از اسمش پیداست برای کار با شماره تلفن از قبیل یافتن شماره تلفن افراد و یا توضیح درباره یک شماره تلفن خاص و غیره استفاده دارد. حال فرقی نمی کند چه شماره تلفن مسکونی باشد و چه تجاری . این نوع جستجو تمامی اینگونه شماره تلفن ها را جستجو می کند.

```
phonebook:John Doe CA
phonebook:(510) 555-1212
```

برای مثال در گوگل phonebook: John Doe CA را تایپ کنید و بعد Enter بزنید تصویری مانند تصویر زیر خواهد آمد:



اگر در صفحه بالا بر روی Google Maps کلیک کنیم تصویری مانند تصویر زیر ظاهر می شود:



همانطور که ملاحظه کردید آدرس و محل دقیق شخص مورد نظر را به ما خواهد داد.

این امر می تواند برای هکر ها برای گرفتن اطلاعات بیشتر، بسیار مفید باشد.

همچنین چند عملگر دیگر مانند این داریم که به شرح زیر می باشد:

- `rphonebook`[1]: جستجوی تلفن های مسکونی
- `bphonebook`[2]: جستجوی تلفن های تجاری

پیدا کردن دفترچه تلفن ها با استفاده از گوگل:

اگر شما به دنبال دفترچه تلفن یا تلفن یک دانشگاه می گردید به ترتیب زیر جستجو کنید:

```
inurl:phone site:university.edu
```

و بجای `university.edu` نام دانشگاه و `domain` آن دانشگاه را وارد کنید.

[1] Residential PhoneBook
[2] Business PhoneBook

برای مثال برای پیدا کردن دفترچه تلفن های آنلاین دانشگاه شمال Carolina در Chapel Hill

به صورت زیر جستجو کنید:

```
inurl:phone site:unc.edu
```

اگر موفق نشدید به صورت زیر هم می توانید جستجو نمایید:

```
title:"phone book" site:unc.edu

(phonebook | "phone book") lookup faculty staff
site:unc.edu

inurl:help (phonebook | "phone book") site:unc.edu
```

معرفی دو سایت در این زمینه:

http://www.uiuc.edu/cgi-bin/ph/lookup

بیشتر از ۳۳۰ دفترچه تلفن

http://www.envmed.rochester.edu/www/ph.html

بیشتر از ۴۰۰ دفترچه تلفن

عملگر * [1]:

عملگر ستاره در گوگل در اصطلاح یک کاراکتر Wildcard هم گفته می شود و در گوگل این علامت به معنی هر چیز دیگر می باشد. به مثال زیر توجه کنید:

[1] asterisk

فرض کنید در گوگل عبارت *Moon را تایپ کنید و دکمه جستجو را فشار دهید. نتایجی که توسط گوگل به ما داده می شود می تواند کلمات زیر باشد:

Moonlight، Moonshot، Moonshadow و غیره

پس متوجه می شویم که همه کلمه moon را دارند و به جای علامت * هر کلمه دیگری می تواند بیاید.

مثال دیگر:

به دنبال "three * mice" می گردیم و نتایجی که به ما داده خواهد شد به صورت زیر خواهد بود:

"three blind mice,"

"three blue mice,"

"three red mice,"

مثال : فرض کنید یک عبارت جستجو به صورت زیر داریم:

```
we the people of the united states in order to form a
more perfect union establish justice
```

عبارت بالا شامل ۱۷ لغت می باشد. گوگل در جستجوی خود از بسیاری از لغات عبارت بالا صرفنظر می کند . لغات صرفنظر شده در زیر آورده شده است:

the، of، in، to و a

همچنین گوگل از جستجوی کلمه justice که آخرین کلمه هست نیز صرفنظر می کند چون محدوده ۱۰ لغت می باشد و justice کلمه ۱۱ می باشد (بدون کلمات a to و ...)

حال اگر ما بعضی از این لغات را با ستاره جایگزین کنیم (کاراکتر wildcard) به صورت زیر

```
"we * people * * united states * order * form * more
perfect * establish *"
```

گوگل دیگر از عبارات صرفنظر نخواهد کرد زیرا اینکه تعداد لغات ما کمتر از ۱۰ لغت می باشد.

یک سوال:

با استفاده از گوگل چگونه می توان تعداد Sub domain های یک سایت را مشخص نمود؟

برای پاسخ به این سوال می توان به راحتی عبارت زیر را در گوگل جستجو کرد:

```
inurl:"*.oreilly.com"
```

و اگر بخواهیم جستجوی بهتری داشته باشیم:

```
site:oreilly.com inurl:"*.oreilly" -inurl:"www.oreilly"
```

حالا با این نکته یک هکر می تواند اطلاعات ذی قیمتی را از تعداد sub domain های هدف جمع آوری کند.

جستجوی حوزه ها (Domain) با استفاده از عملگر :Site

این عملگر یکی از تکنیک های هک در گوگل می باشد اگرچه از لحاظ فنی یک بخشی از یک URL است اما برای یافتن Domain ها و سایت های یک server می تواند انتخاب مناسبی باشد.

این عملگر اجازه می دهد که در یک سایت خاص به دنبال عبارت مورد نظرتان بگردید.

مثال:

Site:gov secret

این عبارت در تمام سایت های با حوزه gov. به دنبال عبارت Secret می گردد.

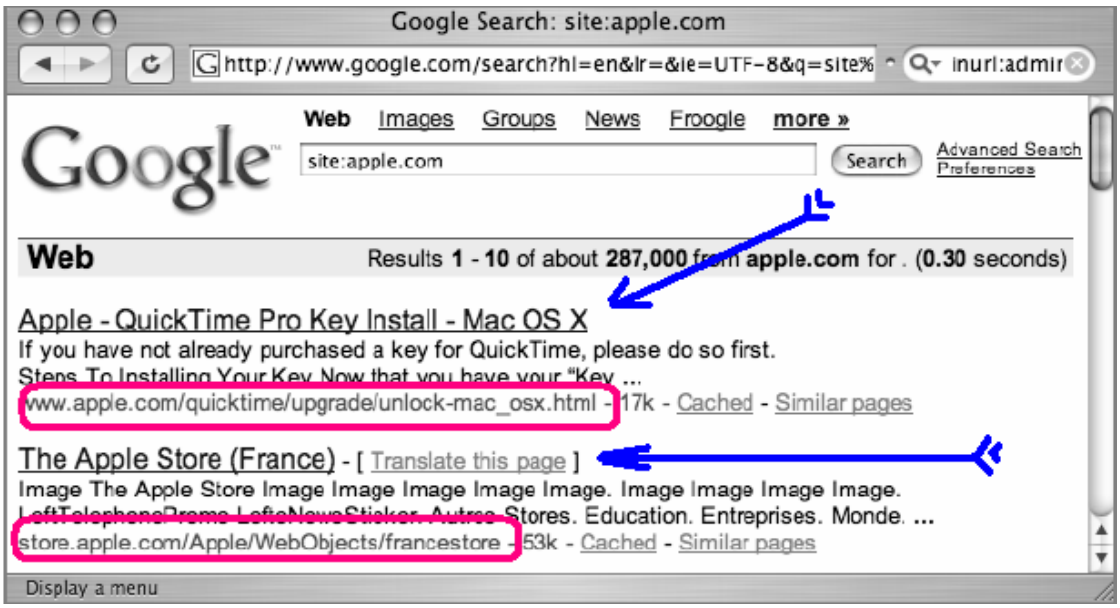
توجه کنید که عملگرهای Site می تواند مانند زیر هم باشد:

site:www.cia.gov

site:cia.gov

site:gov

site:apple.com



و عباراتی را که نمی توانیم به کار ببریم:

site:www.cia

site:www

site:cia

دلیل این کار هم این است که Cia و www نام حوزه یا دامین نیستند و معنی آن این است که نام های اینترنتی به cia و یا www ختم نمی شوند. اگرچه جستجوهای غیر معتبری شبیه به حالت بالا در گوگل به بخشی به نام 'googleturds' مربوط می شود . که در ادامه به معرفی آن می پردازیم.

این این تکنیک ها چگونه می توانیم استفاده کنیم ؟

۱- جاسوسان و انسان های فضول !! از این تکنیک می توانند برای بدست آوردن اطلاعات مالک یک سایت یا سازمان های دولتی استفاده کنند . (دامین سازمانهای دولتی در آمریکا **.gov** یا **.us** می باشد.)

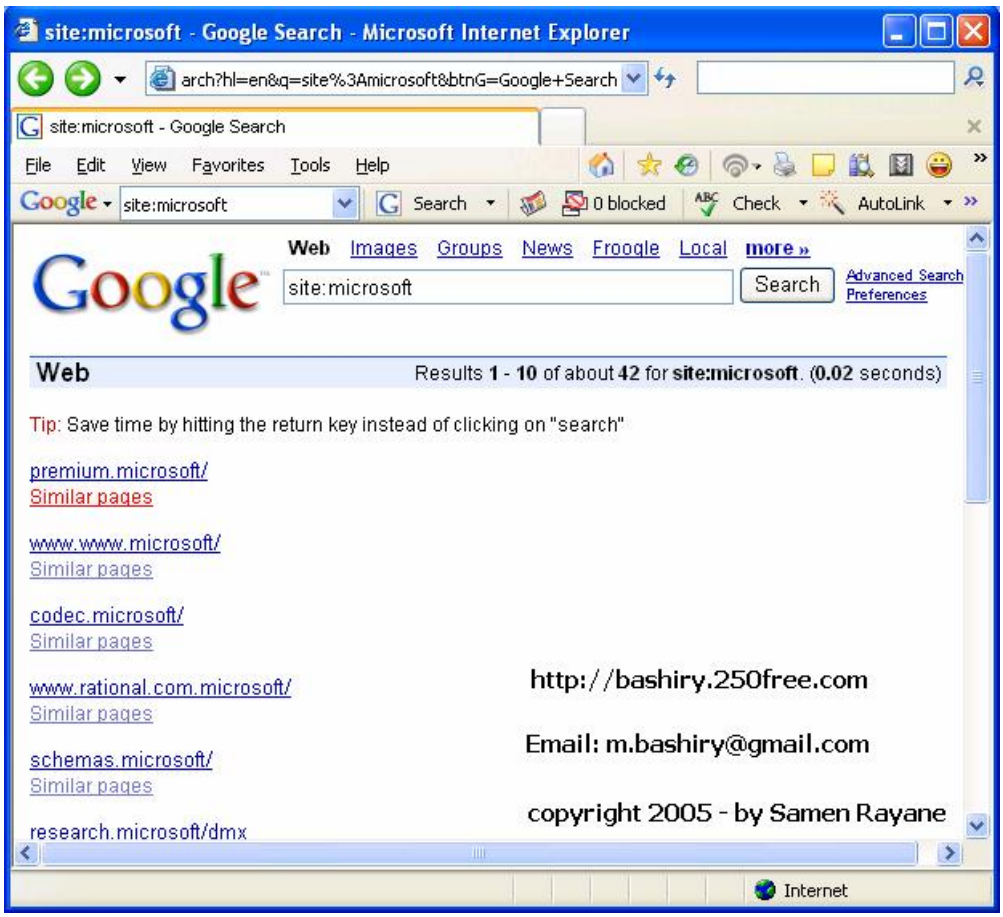
۲-جستجوی هکرها در جهت مقاصدشان بر خلاف سازمان های دولتی .

یافته های 'Googleturds' با استفاده از عملگر Site :

هنگامی که در گوگل یک عبارت غیر معتبر را وارد می کنیم گوگل برای آن لغت نتایجی را می دهد . گوگل این کار را مانند عمل خزیدن در یک صفحه انجام می دهد. برای فهم بیشتر به مثال های زیر توجه کنید:

Site:csc یا Site:microsoft

همانطور که از مثال فوق بر می آید عبارت یک عبارت نادرست برای این عملگر است زیرا فاقد نام حوزه یا Domain است با این وجود نتیجه این جستجو در گوگل جالب است (شکل شماره ۴)



شکل شماره۴- مثال برای googleturds

کاربرد این تکنیک در کجاست ؟

هکر ها از این تکنیک می توانند برای بدست آوردن اطلاعات جالبی از یک سایت یا شرکت استفاده کنند به طور مثال هکر اطلاعات حساسی را درباره شرکت ABCD می خواهد بدست آورد پس تایپ می کند Site:ABCD سپس توسط گوگل لینک های اشتباه زیادی لیست می شوند مانند: http://www.abcd بجای http://www.abcd.com که می تواند حاوی اطلاعات جالبی باشد.

Site mapping:

مطالب بیشتری در مورد عملگر Site

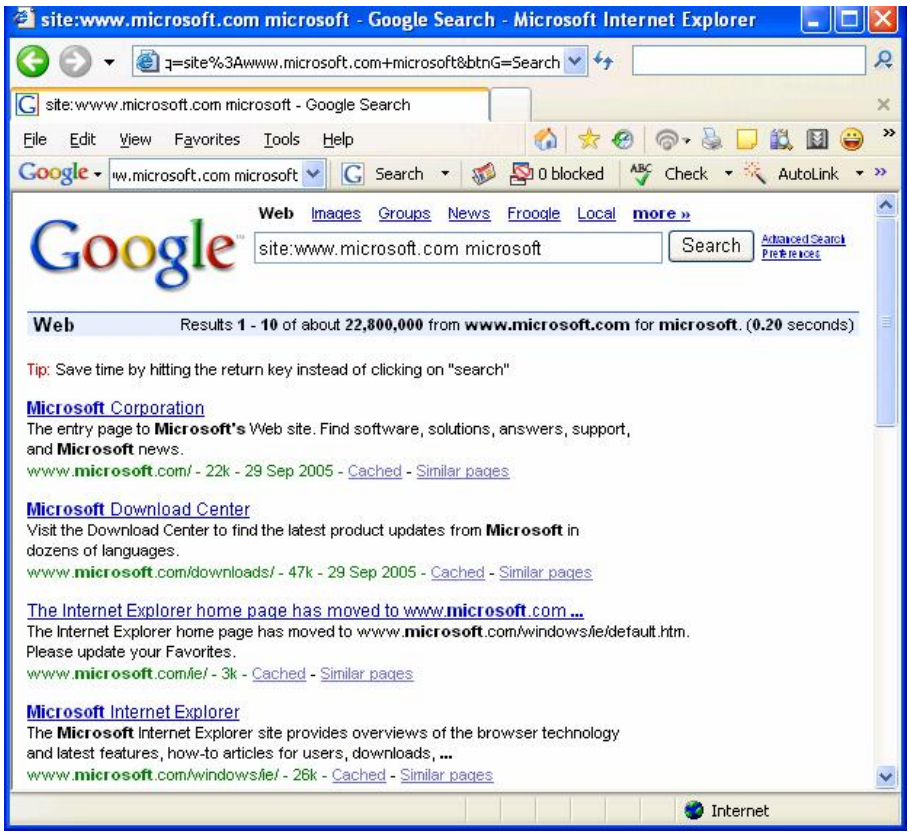
در گوگل نقشه برداری کردن از محتوای یک وب سرور (web server)[1] خیلی ساده است. به مثال زیر توجه کنید:

Site:www.microsoft.com Microsoft

این عبارت کلمه Microsoft را فقط در سایت www.microsoft.com جستجو می کند و تعداد زیادی صفحه از وب سرور مایکروسافت که حاوی این لغت هستند را لیست می کند اگرچه که همه آنها آدرس یک صفحه اینترنتی نیستند ولی عنوان (title) و آدرس (URL) خوبی هستند.

(شکل زیر)

[1] وب سرور چیست: همانطور که می دانید بعضی از زبانهای تحت وب مانند Html و java جهت اجرا نیاز به کامپایل ندارند اما برخی دیگر از جمله PHP و ASP احتیاج به سرویس دهنده ای برای اجرا دارند یعنی اینکه باید داده های صفحات خود راکه احتیاج به کامپایل دارند را به سمت سرویس دهنده ارسال نمایند تا پس از ثبت و اعمال تراکنش ها نتایج حاصل را برای سرویس گیرنده ارسال نماید.



که لغت Microsoft در URL هریک از صفحات (www.microsoft.com) ظاهر شده است. که حمله کننده (attacker) می تواند از نسخه قبلی این صفحه با کلیک بر روی لینک Cache که توسط گوگل ذخیره شده است استفاده کند .

چند استثنا در این حالت وجود دارد. اگر یک لینک از سایت مایکروسافت به IP روی وب سرور برگردد گوگل صفحات ذخیره شده را با داشتن آن IP به کاربر نشان می دهد و به طور خیلی ساده یک حمله کننده (attacker) می تواند به جای استفاده از کلمه Microsoft ، از آدرس IP آن روی وب سرور استفاده می کند.

اخیرا گوگل روشهای جدیدی را برای انجام این کار به امکانات خود اضافه کرده است. این تکنیک به کاربران گوگل اجازه می دهد که به سادگی آدرس آن سایت را جستجو کند مانند مثال زیر:

site:microsoft.com

کاربرد این تکنیک در کجاست ؟

این تکنیک خیلی ساده و جالب است به این صورت که می توانید بـه طـور مـستقیم بـدون مـشاهده صفحه یک نسخه کامل و قدیمی از یک صفحه وب را بدست آورید.

توضیح درباره Google URL

گاهی اوقات کاربران پیشرفته گوگل کارهای خود را از طریق نوار ابزار گوگل(Google toolbar) انجام می دهند یا به طور مـستقیم از URL اسـتفاده مـی کننـد بـرای مثـال مـا بـه دنبـال عبـارت Network در گوگل می گردیدم که بعد از جستجوURL یا آدرس سایت گوگـل بـه صـورت زیـر در خواهد آمد:

http://www.google.com/search?hl=en&ie=UTF-8&oe=UTF-8&q=Network

در ابتدا متوجه خواهیم شد که عبارت جستجو در گوگل به صورت زیر می باشد:

"http://www.google.com/search"

سپس توسط علامت سوال " ? " از URL تفکیک می شـود. و بعـد از آن آرگومـان هـای جـستجو آمده است . علامت & کاراکتر جدا کننده آرگومان ها است.

آرگومانها برای جستجو در گوگل در آدرس Http://www.google.com/apis آمده است.

که ما در زیر به برخی از آنها اشاره می کنیم:

hl : زبان محلی را نشان می دهد که در این مثال en نمایانگر English می باشد.

ie : کد گذاری داده های ورودی، که در این حالت UTF-8 است

oe: کد گذاری داده های خروجی، که در این حالت UTF-8 است

q: همان (Query) – جستجوی عبارت وارد شده که در اینجا کلمه Network آمده شده است (q=network)

ما می توانیم بسیاری از این آرگومانها را حذف کنیم به طور مثال URL فوق را می توانیم به صورت زیر خلاصه سازی کنیم:

http://www.google.com/search?q=Network

و عبارتهای دیگری را اگر بخواهیم مورد جستجو قرار دهیم از علامت + استفاده می کنیم . به مثال زیر توجه کنید:

http://www.google.com/search?q=Network+lan+router+computer

گوگل (و تعداد زیادی برنامه های مبتنی بر وب) از کاراکترهای ویژه ای نظیر علامت نقل قول استفاده می کنند. که در URL خود و برای نشان دادن این علامت در مبنای ۱۶ از علامت % استفاده می کنند. برای مثال برای جستجوی عبارت "the quick brown fox"

http://www.google.com/search?&q= %22the+quick+brown+fox%22

که ما به جای علامت نقل قول از عبارت %22 و برای نشان دادن فاصله خالی از علامت + استفاده کردیم.

یک مثال دیگر از Google URLs

فرض کنید می خواهیم به دنبال عبارت three blind mice بگردیم. نتیجه URL وابسته به نوع جستجوی شما می باشد اگر در این مثال به URL به دست آمده توسط گوگل نگاهی بیندازیم به نکات جالبی خواهیم رسید:

```
http://www.google.com/search?num=100&hl=en&q=
%22three+blind+mice%22
```

همانطور که در URL بالا مشاهده می کنید 22% همان علامت " می باشد که توسط گوگل کد گذاری[1] شده است و num=100 تعداد نتایج جستجو در هر صفحه می باشد. توجه داشته باشید که این عدد بین بازه ۱ تا ۱۰۰ می باشد و می توانید آن را به دلخواه خود تغییر دهید.

hl=en هم قبلا توضیح داده شد که نشان دهنده زبان انگلیسی می باشد. این زبان در صفحات و دکمه ها و قسمت های دیگر سایت مورد جستجو قرار می گیرد.

در جستجوی پیشرفته گوگل مقادیر زیادی از تنظیمات وجود دارد که ما تمامی آنها را از طریق تغییرات در URL بررسی می کنیم.

پارامترهای جستجو در گوگل در جدول زیر به طور کامل گرد آوری شده است:

متغیر	ارزش	توضیحات
q	عبارت جستجو	جستجوی معمولی عبارت مورد جستجو
start	صفر تا MAX	نمایش صفحات پیدا شده اولین صفحه با شماره صفر می باشد و همینطور الی آخر
num maxResults	۱ تا ۱۰۰	نمایش تعداد جستجو ها در هر صفحه
Filter	0 یا 1	اگر این پارامتر به صفر تنظیم شده باشد جستجوهای تکراری نیز نشان داده می شود
restrict	کد محدود	محدود کردن نتایج به یک کشور خاص
hl	کد زبان	این پارامتر زبانی را که گوگل برای

[1] Encode

		نمایش نتایج استفاده می کند را در خود نگه می دارد. (زبان اصلی مورد استفاده بدون ترجمه)
Ir	کد زبان	فقط صفحاتی را نمایش می دهد که به این زبان باشند.
Ie	UTF-8	رمز گذاری و یا encoding ورودی Input encoding
Oe	UTF-8	رمز گذاری و یا encoding خروجی output encoding
as_epq	عبارت جستجو	جستجو به دنبال یک عبارت توجه داشته باشید که در طرفین عبارت مورد نظر باید از علامت نقل قول یا " استفاده کرد.
as_ft	i= شامل شدن پسوند فایل e= شامل نشدن پسوند فایل	در این نوع از جستجو می توانید به گوگل بگویید که به دنبال چه پسوند هایی بگردد و چه پسوند هایی را جستجو نکند.
as_filetype	پسوند یک فایل	شامل شدن یا نشدن یک پسوند در as_ft می باشد.
as_qdr	M3= ماه های ۳ M6= ماه های ۶ Y = سال گذشته	محل صفحات به روز شده با یک timeframe خاص.
as_ nlo	عدد پایین	یافتن تعداد عددهای بین as_nlo و as_nhi
as_nhi	عدد بالا	یافتن تعداد عددهای بین as_nlo و as_nhi
as_oq	لیستی از لغات	پیدا کردن حداقل یکی از لغات
as_occt	Any = هرکجا Title = در موضوع	جستجو در محل های خاص

	صفحه متن صفحه = Body در آدرس = url صفحه در لینک ها = Links به صفحه مورد نظر	
as_dt	فقط شامل = i سایت یا حوزه خاص (domain) بر عکس i می = e باشد	-
as_sitesearch	حوزه یا سایت	-
Safe	فعال کردن = Active safesearch غیر فعال کردن = Off safesearch	
as_rq	URL	صفحاتی که شبیه به URL خاص هستند
as_lq	URL	صفحاتی که شبیه به URL خاص هستند

بعضی از پارامترهای جدول بالا مقدار می گیرند و دارای مقدار هستند.

پارامتر (hl) گوگل صفحاتی را که به این زبانها می باشد بر می گرداند. بـه طـور مثـال lr=lang_ar فقط صفحاتی که به زبان عربی هستند را بر می گرداند.

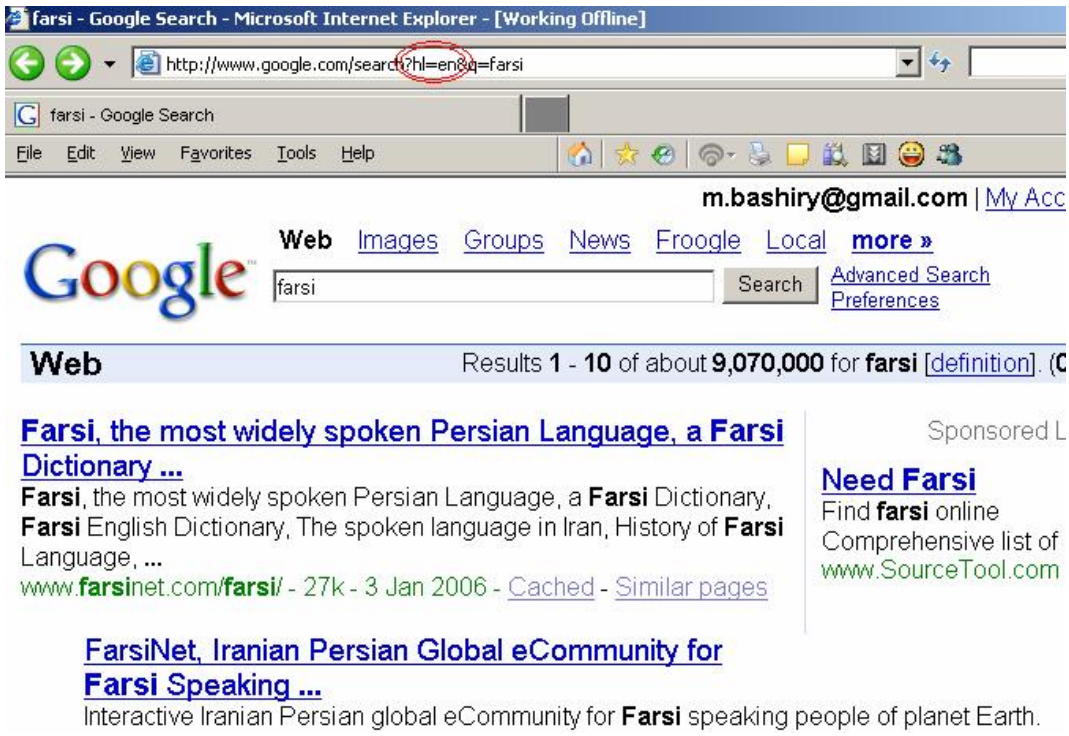
لیست زبانها که می توانند بجای lr به کار روند در جدول زیر آورده شده:

زبان	کد زبان lr
Arabic عربی	**lang_ar**
Bulgarian بلغاری	**lang_bg**
Catalan	**lang_ca**
Chinese (Simplified)	**lang_zh-CN**
Chinese (Traditional)	**lang_zh-TW**
Croatian	**lang_hr**
Czech چکوسلواکی	**lang_cs**
Danish دانمارکی	**lang_da**
Dutch هلندی	**lang_nl**
English انگلیسی	**lang_en**
Estonian استونی	**lang_et**
Finnish فنلاند	**lang_fi**
French فرانسوی	**lang_fr**
German آلمانی	**lang_de**
Greek یونانی	**lang_el**
Hebrew عبری-یهودی	**lang_iw**
Hungarian مجارستانی	**lang_hu**

Icelandic ایسلندی	**lang_is**
Indonesian اندونزی	**lang_id**
Italian ایتالیایی	**lang_it**
Japanese ژاپنی	**lang_ja**
Korean کره ای	**lang_ko**
Latvian	**lang_lv**
Lithuanian لیتوانی	**lang_lt**
Norwegian نروژی	**lang_no**
Polish لهستانی	**lang_pl**
Portuguese پرتقالی	**lang_pt**
Romanian رومانی	**lang_ro**
Russian روسی	**lang_ru**
Serbian صربستانی	**lang_sr**
Slovak چکوسلواکی	**lang_sk**
Slovenian	**lang_sl**
Spanish اسپانیایی	**lang_es**
Swedish سوئدی	**lang_sv**
Turkish ترکی	**lang_tr**

مثال برای hl : (به آدرس صفحه ها در تصاویر توجه کنید)

و نمونه ای دیگر به زبان انگلیسی:



تفاوت دو پارامتر hl و lr در این است که در hl تمامی نتایج به زبان وارد شده ظاهر می شود ولی

در lr لینک صفحات پیدا شده توسط گوگل به زبان انگلیسی می باشد.

پارامتر های hl در جدول زیر موجود می باشد:

زبان	کد زبان lr
Arabic عربی	**ar**
Bulgarian بلغاری	**bg**
Catalan	**ca**
Chinese (Simplified)	**zh-CN**
Chinese (Traditional)	**zh-TW**
Croatian	**hr**
Czech چکوسلواکی	**cs**
Danish دانمارکی	**da**
Dutch هلندی	**nl**
English انگلیسی	**en**
Estonian استونی	**et**
Finnish فنلاند	**fi**
French فرانسوی	**fr**
German آلمانی	**De**
Greek یونانی	**el**
Hebrew عبری-یهودی	**iw**
Hungarian مجارستانی	**hu**
Icelandic ایسلندی	**is**
Indonesian اندونزی	**id**
Italian ایتالیایی	**it**
Japanese ژاپنی	**ja**
Korean کره ای	**ko**
Latvian	**lv**
Lithuanian لیتوانی	**lt**

Norwegian نروژی	**no**
Polish لهستانی	**pl**
Portuguese پرتقالی	**pt**
Romanian رومانی	**ro**
Russian روسی	**ru**
Serbian صربستانی	**sr**
Slovak چکوسلواکی	**sk**
Slovenian	**sl**
Spanish اسپانیایی	**es**
Swedish سوئدی	**sv**
Turkish ترکی	**tr**

فصل سوم

مقدمات هک از طریق گوگل

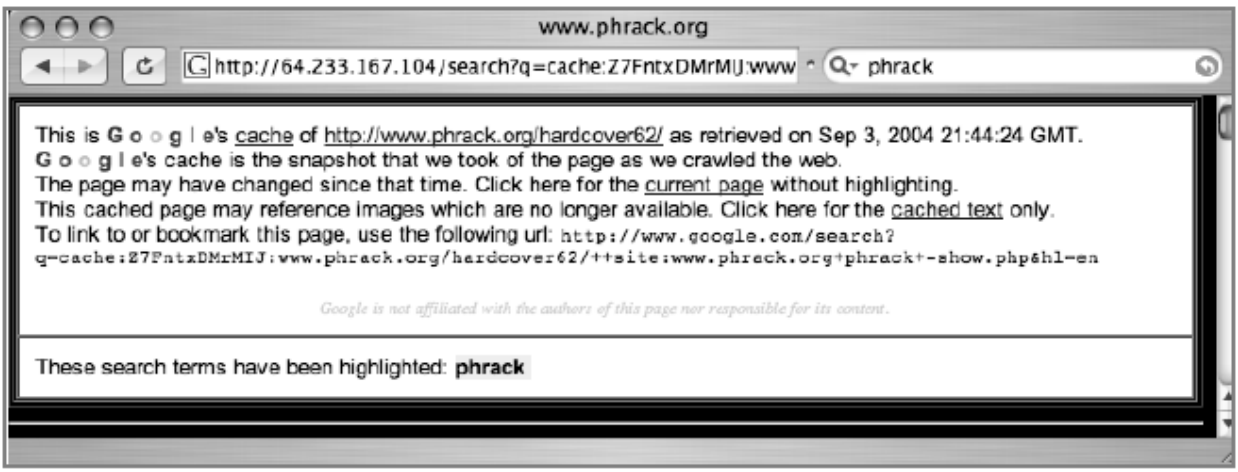
- کار با cache در گوگل
  - **استفاده از گوگل به عنوان سرور پروکسی**
- لیست دایرکتوریها (directory list)
  - **پیدا کردن لیست های دایرکتوری از طریق گوگل**
  - **بدست آوردن لیست دایرکتوری های خاص**
  - **پیدا کردن فایلهای خاص**
  - **دست آوردن نسخه نرم افزار وب سرور از طریق لیست دایرکتوری**
  - **تکنیک های پیمایش در لیست دایرکتوری ها (مسیرها)**
  - **و ...**
- استفاده از گوگل به عنوان پویشگر CGI
- استفاده از گوگل برای یافتن فایلها و مسیرهای جالب

آغازی بر گوگل هکینگ[1]

کار با Cache در گوگل:

یکی از امکانات خوبی گوگل امکان Cache باشد و این امکان برای هکر ها می تواند مفید واقع شود. هنگامی که شما قصد هک کردن سایتی را دارید پکت هایی[2] به سمت وب سرور ارسال می شود و این کارها در فایل Log ذخیره می شود. حال اگر از امکان Cache در گوگل استفاده کنید چون هیچ بسته یا پکتی به سمت وب سرور ارسال نمی شود پس در فایل Log هم اطلاعاتی قرار نمی گیرد و این برای یک هکر خیلی می تواند مفید باشد.

حال در گوگل دستور cache: www.phrack.org را می نویسیم و به بالای صفحه یا Banner نتیجه بدست آمده توجه می کنیم. در Banner آن اطلاعات جالبی موجود می باشد.



شکل شماره ۵

به این عبارت دقت کنید:

"This cached page may reference images which are no longer available."

---

[1] Google hacking
[2] Packet

این پیغام خیلی ساده است ولی یک راهنمای مهم را برای اینکه گوگل در پشت صحنه چه کارهایی را انجام می دهد فراهم می کند.

در پشت صحنه گوگل:

برای گرفتن یک دید بهتر که چه اتفاقاتی می افتد اطلاعات خروجی از این صفحه ذخیره شده را جمع می کنیم. برای این کار از دستور tcpdump –n

اطلاعاتی که از این دستور بدست می آید در جدول زیر نشان داده شده است.

Figure 3.2 *Tcpdump* Output Gathered While Viewing a Cached Page

```
21:39:24.648422 IP 192.168.2.32.51670 > 64.233.167.104.80
21:39:24.719067 IP 64.233.167.104.80  > 192.168.2.32.51670
21:39:24.720351 IP 64.233.167.104.80  > 192.168.2.32.51670
21:39:24.731503 IP 192.168.2.32.51670 > 64.233.167.104.80
21:39:24.897987 IP 192.168.2.32.51672 > 82.165.25.125.80
21:39:24.902401 IP 192.168.2.32.51671 > 82.165.25.125.80
21:39:24.922716 IP 192.168.2.32.51673 > 82.165.25.125.80
21:39:24.927402 IP 192.168.2.32.51674 > 82.165.25.125.80
21:39:25.017288 IP 82.165.25.125.80   > 192.168.2.32.51672
21:39:25.019111 IP 82.165.25.125.80   > 192.168.2.32.51672
21:39:25.019228 IP 192.168.2.32.51672 > 82.165.25.125.80
21:39:25.023371 IP 82.165.25.125.80   > 192.168.2.32.51671
21:39:25.025388 IP 82.165.25.125.80   > 192.168.2.32.51671
21:39:25.025736 IP 192.168.2.32.51671 > 82.165.25.125.80
21:39:25.043418 IP 82.165.25.125.80   > 192.168.2.32.51673
21:39:25.045573 IP 82.165.25.125.80   > 192.168.2.32.51673
21:39:25.045707 IP 192.168.2.32.51673 > 82.165.25.125.80
21:39:25.052853 IP 82.165.25.125.80   > 192.168.2.32.51674
```

اطلاعات بالا را بررسی می کنیم

در خط اول ما یک ارتباط وب (پورت۸۰) را که از 192.168.2.32 که آدرس ماشین مرورگر ما می باشد به 64.233.167.104 که آی پی[1] یکی از سرورهای گوگل است داریم.

[1] IP

خط ۲ و خط ۳ ، سه پکت آماده و حاضر را نشان می دهد که از سرور گوگل به ماشین ما می باشد.اینها در اثر ترافیک بر اثر نقل و انتقال با گول انتظار می رود و ما باید از خط ۵ شروع کنیم:

در این خط می بینیم که ماشین ما یک ارتباط با وب (پورت ۸۰) به 82.165.25.125 برقرار می کند که این بار بر خلاف دفعه قبل آدرس سرور گوگل نیست اگر ما از آن یک nslookup و یا دستور host روی آی پی بگیریم ما به a15151295.alturo-server.de خواهیم رسید. که برای گرفتن اطلاعات می توانیم به این سرور متصل شویم و اطلاعات کاملتری را بدست آوریم.(توسط tcpdump) جدول زیر یک درخواست جزئی HTTP که Header فیلد HOST را نشان می دهد می باشد.

0x0040	0d6c	4745	5420	2f67	7266	782f	3831	736d	.lGET./grfx/81sm
0x0050	626c	7565	2e6a	7067	2048	5454	502f	312e	blue.jpg.HTTP/1.
0x0060	310d	0a48	6f73	743a	2077	7777	2e70	6872	1..Host:.www.phr
0x0070	6163	6b2e	6f72	670d	0a43	6f6e	6e65	6374	ack.org..Connect
0x0080	696f	6e3a	206b	6565	702d	616c	6976	650d	ion:.keep-alive.
0x0090	0a52	6566	6572	6572	3a20	6874	7470	3a2f	.Referer:.http:/
0x00a0	2f36	342e	3233	332e	3136	312e	3130	342f	/64.233.161.104/
0x00b0	7365	6172	6368	3f71	3d63	6163	6865	3a4c	search?q=cache:L
0x00c0	4251	5a49	7253	6b4d	6755	4a3a	7777	772e	BQZIrSkMgUJ:www.
0x00d0	7068	7261	636b	2e6f	7267	2f2b	2b73	6974	phrack.org/++sit
0x00e0	653a	7777	772e	7068	7261	636b	2e6f	7267	e:www.phrack.org
0x00f0	2b70	6872	6163	6b26	686c	3d65	6e0d	0a55	+phrack&hl=en..U

در خط ۱ و ۲ جدول بالا یک فایل تصویری خاص مانند یک تصویر JPG که ما دانلود کرده ایم می باشد. (از طریق یک درخواست GET).

خط ۳ فیلد HOST را نشان می دهد که ما با وب سرور سایت www.phrack.com صحبت کردیم می باشد. در واقع یک پکت یا بسته به آدرس 82.165.25.125.80 ارسال شده که ما می

تـوانیم فـرض کنـیم کـه وب سـرور سـایت phrack واقعـی اسـت و محـل آدرس فیزیکـی آن در 82.165.25.125.80 قرار دارد. (در اصل یک میزبان[1] واقعی به نظر می رسد).

این به مفهوم دیدن یک نسخه ذخیره شده از وب سرور Phrack می باشد (همان cache)

خط ۶ تا ۱۲ فیلد REFERER را نشان می دهد که ما به سرور Phrack پاس کـردیم و در ادامـه آن آدرس سایت ذخیره شده توسط گوگل آمده است. توجه کنید مرورگر مـا وب سـرور را آگـاه مـی سازد پس همیشه یک هکر برای جستجو در اینگونـه سـایت هـا از آدرس پروکـسی[2] بـرای ناشـناس ماندن استفاده می کند و آدرس IP اصلی ما برای هدف ناشناس باقی می ماند.

برای پیدا کردن محل سرورهای پروکسی از طریق گوگل می توانیم به صورت زیر جستجو نماییم:

```
inurl:"nph-proxy.cgi" "Start browsing"
```

و یا

```
"this proxy is working fine!" "enter *" "URL***" *
visit
```

این جستجو ها محل Proxy server های عمومی آنلاین را برای تست اهداف به ما خواهد داد.

Cache Banner به ما امکانی را می دهد که بتوانیم بدون هیچگونه مرجع خارجی اطلاعات خود را ببینیم. همانطور که در شکل ۵ دیده شد لینکی داریک به اسم زیر:

```
"Click here for the cached text only."
```

با کلیک کردن روی این لینک و استفاده از tcpdump -n جدولی مانند جدول زیر بدست می آید:

---

[1] Host
[2] Proxy

Figure 3.4 Cached Text Only Captured with *Tcpdump*

```
IP 192.168.2.32.52912 > 64.233.167.104.80: S 2057734012:2057734012(0) win
65535 <mss 1460,nop,wscale 0,nop,nop,timestamp 3791662381 0>
IP 64.233.167.104.80 > 192.168.2.32.52912: S 4205028956:4205028956(0) ack
2057734013 win 8190 <mss 1460>
IP 192.168.2.32.52912 > 64.233.167.104.80: . ack 1 win 65535
IP 192.168.2.32.52912 > 64.233.167.104.80: P 1:699(698) ack 1 win 65535
IP 64.233.167.104.80 > 192.168.2.32.52912: . ack 699 win 15885

IP 64.233.167.104.80 > 192.168.2.32.52912: . 1:1431(1430) ack 699 win 15885
23:46:54.127202 IP 64.233.167.104.80 > 192.168.2.32.52912: .
1431:2861(1430) ack 699 win 15885
IP 64.233.167.104.80 > 192.168.2.32.52912: P 2861:3846(985) ack 699 win
15885
IP 192.168.2.32.52912 > 64.233.167.104.80: . ack 3846 win 65535
IP 192.168.2.32.52912 > 64.233.167.104.80: F 699:699(0) ack 3846 win 65535
IP 64.233.167.104.80 > 192.168.2.32.52912: F 3846:3846(0) ack 700 win 8190
IP 192.168.2.32.52912 > 64.233.167.104.80: . ack 3847 win 65535
```

خط ۱ تا ۳ استاندارد ارتباط TCP از پورت وب (port 80) بین مرورگر ماشین ما با آدرس (192.168.2.32) و سرور گوگل (64.233.167.104) می باشد.

خطوط ۴ تا ۹ اطلاعات ارسال شده از ماشین ما و دریافتی توسط سرور گوگل می باشد و خطوط ۱۰ تا ۱۲ Shutdown های موفق نرمال از ارتباط ما با سرور گوگل است.

اگر در این حالت یعنی حالتی که بر روی لینک cached text only کلیک کرده ایم به URL هم نگاهی بیندازیم پارامترهای مختلفی را مشاهده می کنیم:

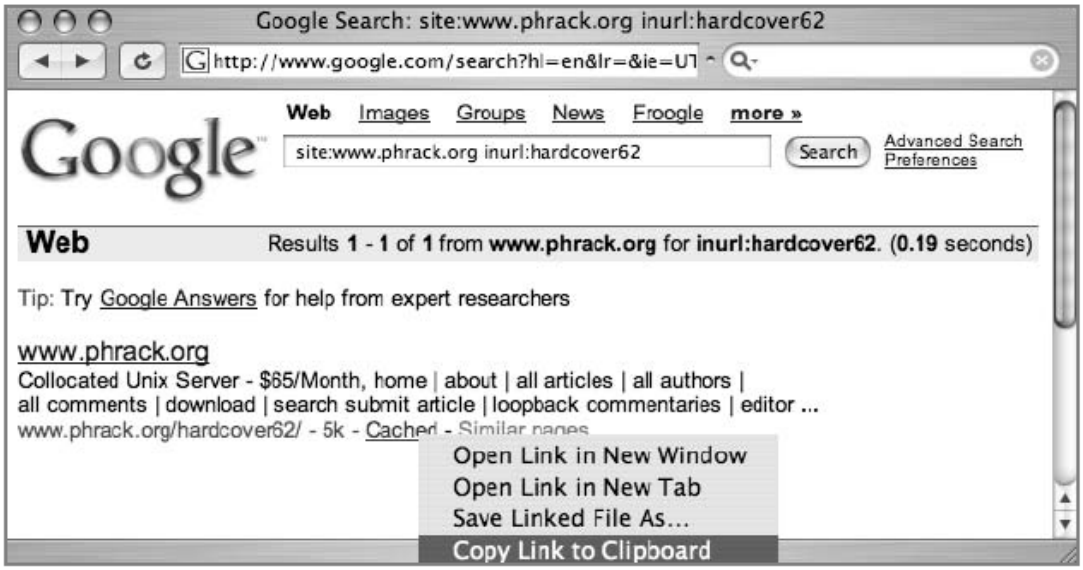
&strip=1 : این پارامتر معرف کلیک کردن بر روی این لینک است.

اجازه دهید که جستجوی زیر را در گوگل داشته باشیم:

site:phrack.org inurl:hardcover

این بار بجای کلیک کردن بر روی cached link بر روی آن راست کلیک می کنیم و از منوی ظاهر شده گزینه copy the URL to the Clipboard, را انتخاب می نماییم. سپس این آدرس را در بخش آدرس صفحه مورد نظر Paste می کنیم .تصویر زیر همین عملیات را نشان می دهد.

Figure 3.5 Anonymous Cache Viewing Via Cut and Paste



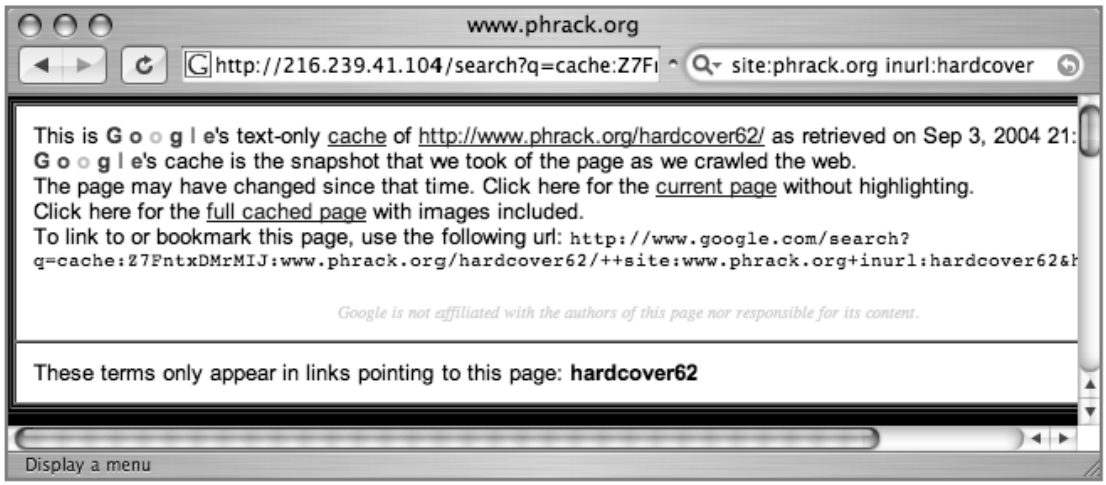
اگر به آدرس توجه کنیم در آخر آن پارامتر &strip=1 اضافه شده است.

URL کامل باید به صورت زیر باشد:

http://216.239.41.104/search?q=cache:Z7FntxDMrMIJ:www.phrack.org/hardcover62/++site:www.phrack.org+inurl:hardcover62&hl=en&strip=1.

بعد از ویرایش URL دکمه Enter را فشار دهید بعد از اینکه صفحه ظاهر شد اگر به Banner نگاهی بیندازیم کمی با قبل تفاوت دارد:

Figure 3.6 A Stripped Cached Page's Header



اگر دقت کرده باشید بجای عبارت

"This cached page may reference images which are no longer available"

عبارت جدیدی به صورت زیر جایگزین شده

"Click here for the full cached version with images included."

این صفحه ها یا به عبارتی Stripped page ها یا صفحات برهنه شامل گرافیک و عکس نیست لذا این صفحات می تواند تفاوت بسیاری با صفحه اصلی داشته باشد و در بعضی از مواقع ممکن است صفحه ناخوانا باشد. اگرچه در این حالت به load up کردن پروکسی سرور برای اصابت به صفحات خدشه ای وارد نمی کند ولی گوگل هکر های واقعی احتیاج به پروکسی سرورهای steenkin' ندارند.

در ادامه مطالب گوگل به عنوان پروکسی سرور به طور کامل مورد بررسی قرار می گیرد.

استفاده از گوگل به عنوان پروکسی سرور[1]

قبل از توضیح نقش گوگل به عنوان پروکسی سرور به توضیح اینکه اصلا پروکسی سرور یعنی چه و چه نقشی دارد خواهیم پرداخت:

Proxy Server چیست ؟

نرم افزاری است که در یک شبکه حد واسط بین اینترنت و کاربران واقع می شود. فلسفه ایجاد Proxy Server قراردادن یک خط اینترنت در اختیار تعداد بیش از یک نفر استفاده کننده در یک شبکه بوده است ولی بعدها امکانات و قابلیتهایی به Proxy Server افزوده شد که کاربرد آن را فراتر از به اشتراک نهادن خطوط اینترنت کرد . بطور کلی Proxy Server ها در چند مورد کلی استفاده می شوند .

یک کاربرد Proxy Server ها ، همان به اشتراک گذاشتن یک خط اینترنت برای چند کاربر است که باعث کاهش هزینه و کنترل کاربران و همچنین ایجاد امنیت بیشتر می شود .

کاربرد دوم Proxy Server ها ، در سایتهای اینترنتی به عنوان Firewall می باشد . کاربرد سوم که امروزه از آن بسیار استفاده می شود Caching ، اطلاعات است . با توجه به گران بودن هزینه استفاده از اینترنت و محدود بودن پهنای باند ارتباطی برای ارسال و دریافت اطلاعات ، معمولا" نمی توان به اطلاعات مورد نظر در زمان کم و با سرعت مطلوب دست یافت . امکان Caching اطلاعات ، برای کمک به رفع این مشکل در نظر گرفته شده است ، Proxy Server . سایتهایی را که بیشتر به آنها مراجعه می شود را دریک حافظه جداگانه نگاه می دارد. به این ترتیب برای مراجعه مجدد به آنها نیازی به ارتباط از طریق اینترنت نیست بلکه به همان حافظه مخصوص رجوع خواهد شد .

این امر باعث می گردد از یک طرف زمان دسترسی به اطلاعات کمتر شده و از سوی دیگر چون اطلاعات از اینترنت دریافت نمی شود ، پهنای باند محدود موجود با اطلاعات تکراری اشغال نشود . بخصوص آنکه معمولا" تغییرات در یک Website محدود به یک یا دو صفحه می باشد و گرفتن اطلاعات از اینترنت بدون

[1] Proxy Server

Cachingبه معنای گرفتن کل سایت می باشد حال آنکه با استفاده از **Proxy Server** و امکان **Caching** اطلاعات ، میتوان تنها صفحات تغییر کرده را دریافت کرد .

اگر چه این تکنیک ممکن است برای همیشه دوام نداشته باشد و زمانی که این کتاب نوشته می شود خود گوگل به عنوان Proxy server استفاده می شود.این تکنیک به Google-translated احتیاج دارد. Google-translated در آدرس www.google.com/translate_t می باشد.

اگر شما دو زبان را از بخش مخصوص خود انتخاب کنید و در فیلد Translated a web page یک آدرس URL را وارد کنید و سپس دکمه Translated که در مقابل آن می باشد را کلیک نمایید. (تصویر زیر) گوگل محتوای صفحه اینترنتی شما را به زبان مقصد که انتخاب کردید ترجمه می کند و یک آدرس URL از آن برای مراجعات بعدی تولید می کند.

آدرس اینترنتی تولید شده چیزی شبیه آدرس زیر می باشد:

```
http://www.google.com/translate?u=http%3A%2F%2Fwww.google.com&langpair=en%7Ces&hl=en&ie=Unknown&oe=ASCII
```

پارامترهای استفاده شده در آدرس بالا قبلا توضیح داده شده اما هنوز در باره پارامتر langpair صحبتی نکردیم. این پارامتر فقط موقعی مشاهده و استفاده می شود که از سرویس ترجمه گوگل استفاده می کنیم. این پارامتر به ترتیب زبان مقصد (ترجمه شده) و زبان مبدا (ترجمه نشده) را بیان می کند.

در این مثال خاص زبان مبدا انگلیسی و زبان مقصد اسپانیایی می باشد که این امر را می توان به راحتی از URL هم استنباط کرد. پارامتر hl هم قبلا توضیح داده شده و تنها قسمت باقیمانده در URL بخش Translated?u می باشد که به دنبال آن آدرس گوگل آمده است. و این را بیان می کند که ما تلاش کردیم صفحه گوگل را از اسپانیایی به انگلیسی ترجمه کنیم.

حال ببینیم اگر هر دو زبان را یکی انتخاب کنیم چه اتفاقی می افتد.

بعد از اینکه ما هر دو زبان را یکی انتخاب کردیم URL به صورت زیر در می آید:

```
http://www.google.com/translate?u=http%3A%2F%2Fwww.goog
le.com&langpair=en%7Cen&hl=en&ie=Unknown&oe=ASCII
```

اگر ما این آدرس را به مرورگرمان کپی کنیم (با این شرط که هر دو زبان انگلیسی انتخاب شده اند) بعد Enter کنیم صفحه ای همانند تصویر زیر ظاهر خواهد شد:

اگر به بخش بالای این صفحه توجه کنید شاهد یک Banner هستید که نشان دهنده فعال بودن سرویس ترجمه گوگل می باشد.

در پشت صحنه گوگل چه اتفاقی می افتد:

به مثالی دیگر توجه کنید. ما سایت www.phrack.org/hardcover62/ را مورد بررسی قرار می دهیم و اگر با استفاده از tcpdump –n –U –t ترافیک شبکه را زیر نظر بگیریم و یا به اصطلاحی monitor کنیم جدولی مانند تصویر زیر ظاهر خواهد شد:

Figure 3.9 Monitoring English to English Translation with *Tcpdump –n –U -t*

```
IP 192.168.2.32.53466 > 64.233.171.104.80: S 1120160740:1120160740(0) win
IP 64.233.171.104.80 > 192.168.2.32.53466: S 2337757854:2337757854(0) ack
IP 192.168.2.32.53466 > 64.233.171.104.80: . ack 1
IP 192.168.2.32.53466 > 64.233.171.104.80: P 1:678(677) ack
IP 64.233.171.104.80 > 192.168.2.32.53466: . ack 678
IP 64.233.171.104.80 > 192.168.2.32.53466: P 1:529(528) ack
IP 192.168.2.32.53466 > 64.233.171.104.80: . ack 529
IP 64.233.171.104.80 > 192.168.2.32.53466: P 529:549(20) ack
IP 192.168.2.32.53466 > 64.233.171.104.80: P 678:1477(799) ack
[snip]
IP 192.168.2.32.53470 > 216.239.37.104.80: S 3691660195:3691660195(0) win
IP 216.239.37.104.80 > 192.168.2.32.53470: S 2470826704:2470826704(0) ack
IP 192.168.2.32.53470 > 216.239.37.104.80: . ack 1
IP 192.168.2.32.53470 > 216.239.37.104.80: P 1:752(751) ack
IP 216.239.37.104.80 > 192.168.2.32.53470: P 1:1271(1270) ack
IP 216.239.37.104.80 > 192.168.2.32.53470: P 1271:1692(421) ack
IP 216.239.37.104.80 > 192.168.2.32.53470: P 1692:1712(20) ack
IP 192.168.2.32.53470 > 216.239.37.104.80: . ack 1712
```

در خط ۱ تا ۳ ما آدرس مرورگرمان (192.168.2.32:80) که با سرور گوگل در ارتباط است را می بینیم. در خطوط ۴ تا ۹ اطلاعات در حال رفت و برگشت می باشد(این امر را می توان به سادگی از IP ها دریافت کرد) و ارتباط مشابه دیگری در آدرس مشابهی برقرار شده است که با رسیدن به خط ۱۰ برای مدت کوتاهی از بین می رود.

در خطوط ۱۱ تا ۱۳ ماشین مرورگر ما (192.168.2.32) دوباره به وب سرور دیگری از گوگل و به پورت ۸۰ متصل می شود(216.239.37.104). در خطوط ۱۴ تا۱۸ دوباره اطلاعات به عقب و جلو (رفت و برگشت) می روند و سپس صفحه اینترنتی www.phrack.org/hardcover62/ در مرورگر ما نشان داده می شود. (تصویر زیر)

این همان صفحه است که از طریق proxy در گوگل آن را باز کردیم. (**فیلتر شکن خوب !!**)

توجه کنید که در این مثال هیچگونه اطلاعاتی به طور مستقیم از ماشین ما به وب سرور سایت phrack.org انتقال داده نشده و تمام عملیات به طور غیر مستقیم توسط proxy server انجام شده است.

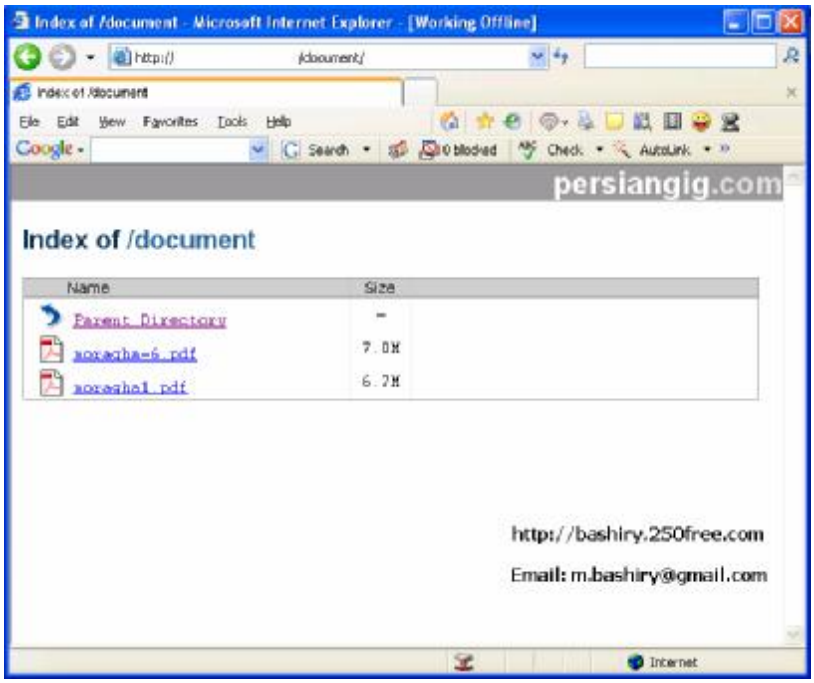
توجه داشته باشید که در این حال هم آدرس IP ما در فایل log مقصد ثبت می شود ولی با این حال گوگل صفحه مورد نظر را برای ما بدست می آورد.

اگر مایلید که آدرس IP شما ثبت نشود می توانید از یک چک کننده پروکسی در آدرس زیر کمک بگیرید:

www.all-nettools.com/pr.htm

پیدا کردن لیست دایرکتوری ها (directory) در اینترنت

لیست دایرکتوری ها مطابق شکل زیر یک لیست از فایل ها و پوشه ها و مسیرها می باشد و نـوعی از محیط گرافیکی و متنی است.



مکان لیست دایرکتوری ها اغلب روی وب سرورها است که به صورت درختی هستند و به کاربر ایـن امکان را می دهد که بتواند فایل های مورد نیاز خود را دانلود نمایـد.و بـرای هکـر هـا ممکـن اسـت چیزهای جالبی در لیست دایرکتوری ها پیدا شود.

همانطور که در عنوان شکل بالا مـشاهده مـی کنیـد عنـوان اکثـر لیـست دایرکتـوری هـا بـا کلمـه "Index of" شروع می شوند. پس ما برای پیدا کردن این نوع از صفحات در گوگـل مـی تـوانیم بـه صورت زیر جستجو کنیم:

Intitle:index.of

به خاطر داشته باشید که علامت نقطه به عنوان یک کاراکتر در گوگل به کار می رود.

متاسفانه تعداد جستجوهایی که از این راه بدست می آید خیلی زیاد می باشد و می تواند شامل عبارات زیر هم شود:

Index of Native American Resources on the Internet

LibDex - Worldwide index of library catalogues

Iowa State Entomology Index of Internet Resources

برای جلوگیری از این کار در گوگل به صورت زیر جستجو می کنیم:

intitle:index.of "parent directory"

intitle:index.of name size

پس از این طریق می توان جستجو را محدود به صفحات دلخواه خود کنیم تا تعداد صفحات پیدا شده توسط گوگل کاهش یابد.

موارد دیگر از این نمونه جستجو در زیر آورده شده است:

"index of /admin"
"index of /root"
"index of password"
"index of /" +passwd

تمرین:

عبارت جستجوی زیر چه کاری انجام می دهد؟ !!!

intitle:"index of" +("/ebooks"|"/book") +(chm|pdf|zip)

از این تکنیک چگونه می توان استفاده کرد ؟

این تکنیک به هکرها اجازه میدهد که به سادگی و با سرعت خیلی زیاد در یک سایت هدایت شوند و می تواند اجزای مختلف یک سایت را مشاهده کند سپس می تواند اطلاعات جالب و حساسی

را از طریق لیست دایرکتوری آن سایت به دست آورد . لیست دایرکتوری یک واسطی پدید مـی آورد که با استفاده از آن یک هکر می تواند نسخه یا نرم افزار وب سرور، فایل و ... را بدست آورد.

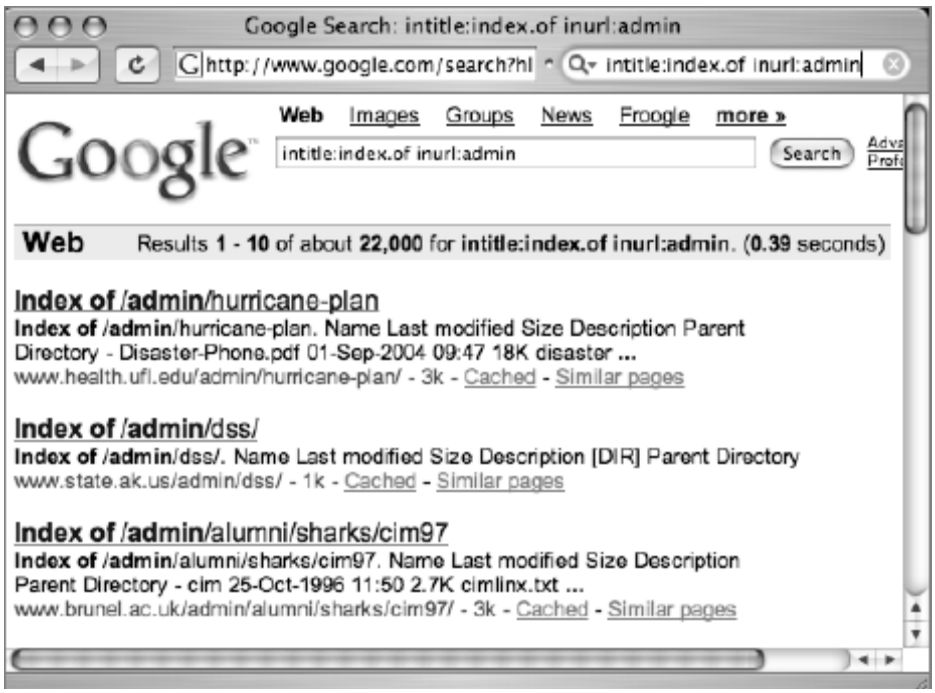
بدست آوردن لیست دایرکتوری های خاص

برای این کار می توانید از عبارات زیر استفاده کنید:

intitle:index.of.admin

intitle:index.of inurl:admin

به تصویر زیر در همین مورد توجه نمایید:



پیدا کردن فایل های خاص

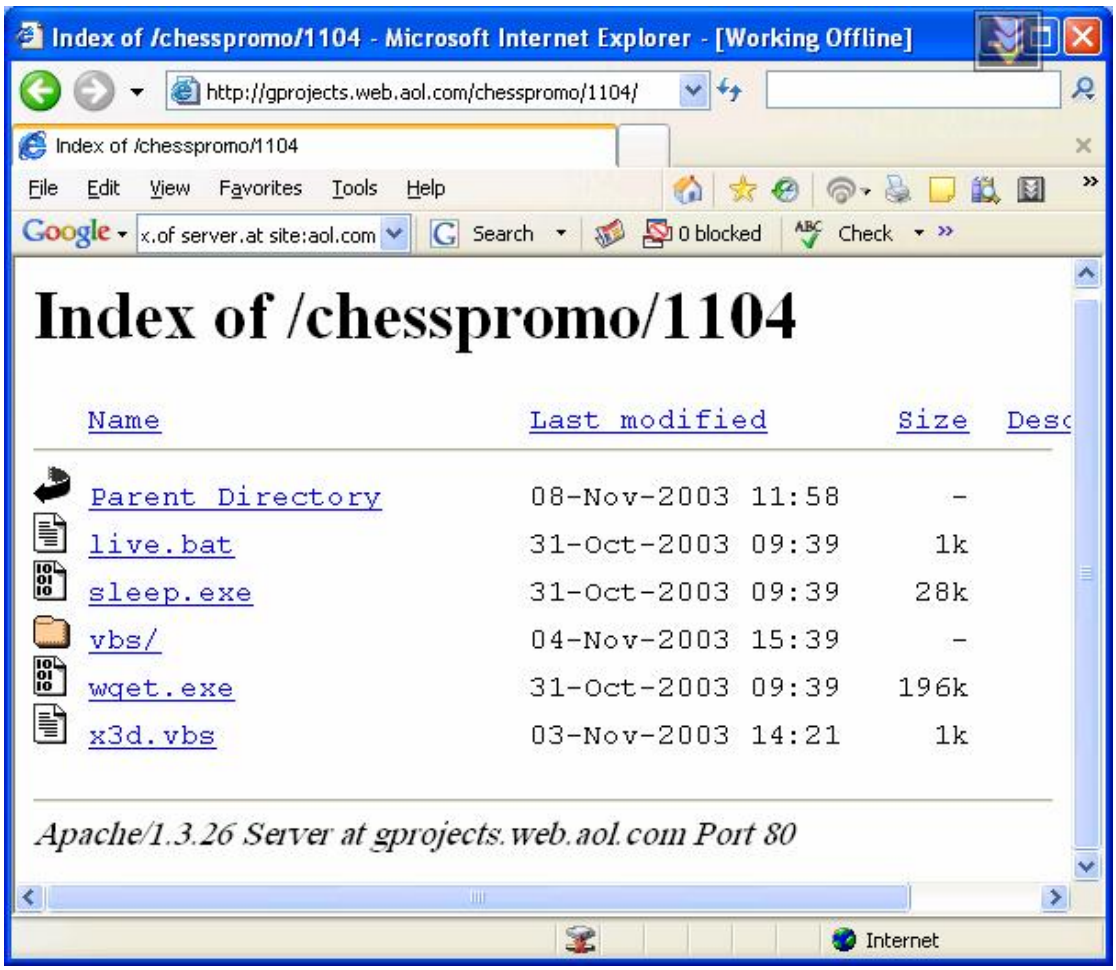
به دلیل اینکه حالت لیست دایرکتوری ها به صورت درخت می باشد می توانید فایل هـای حـساس و جالبی را از آنها بدست آورید:

برای مثال log file ، WS_FTP مانند زیر جستجو کنید:

intitle:index.of ws_ftp.log,

به دست آوردن نسخه نرم افزار وب سرور از طریق لیست دایرکتوری (directory listing)

هکر قبل از حمله به یک سرور به نسخه نرم افزاری که روی وب سرور در حال اجراست احتیاج دارد و می تواند به هکر کمک زیادی را در پیشبرد اهداف آن کند. اگر هکر به طور مستقیم به پورت وب یا همان پورت ۸۰ یک وب سرور متصل شود، سربرگ Http (Header) در صفحه وب می تواند این اطلاعات را به هکر بدهد که این اطلاعات را می توان از طریق گوگل و بدون اتصال به وب سرور به دست آورد. راه دیگر برای انجام این عمل مطابق شکل زیر از طریق لیست دایرکتوری می باشد:



همانطور که در شکل فوق دیده می شود در پایین صفحه لیست دایرکتوری نام نرم افزار سرور (server) و نسخه آن قرار دارد و یک هکر می تواند از این اطلاعات استفاده نماید.

یک مدیر سایت باهوش می تواند با تغییر تگ[1]های سرور مربوطه این اطلاعات را جعل کند ولی غالبا این اطلاعات درست می باشند و مدیران آن را دستکاری نمی کنند.

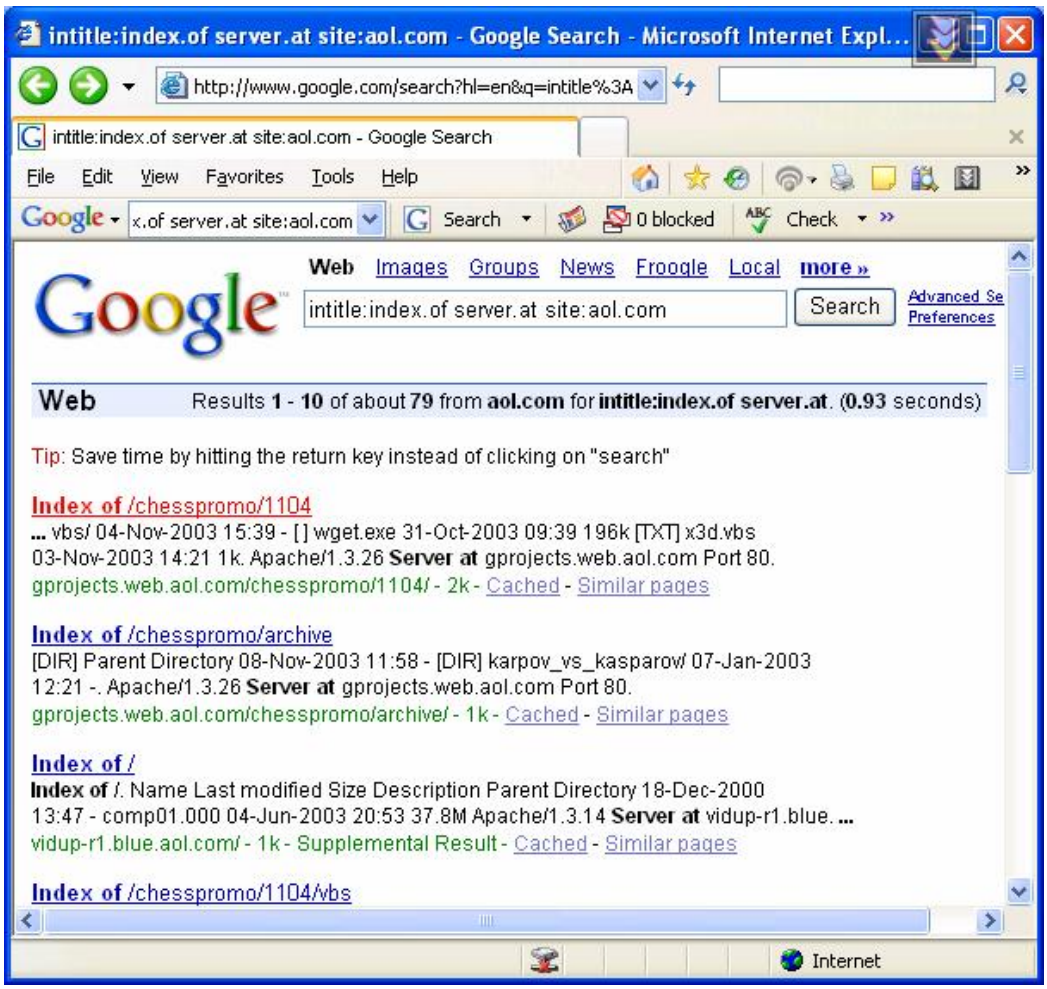
گرفتن اطلاعات فوق از طریق جستجو در گوگل:

کلمه اصلی برای جستجو "index of" در عنوان سایت و "server at" می باشد که این نوع از جستجو در زیر آورده شده است البته همراه با علامت نقطه :

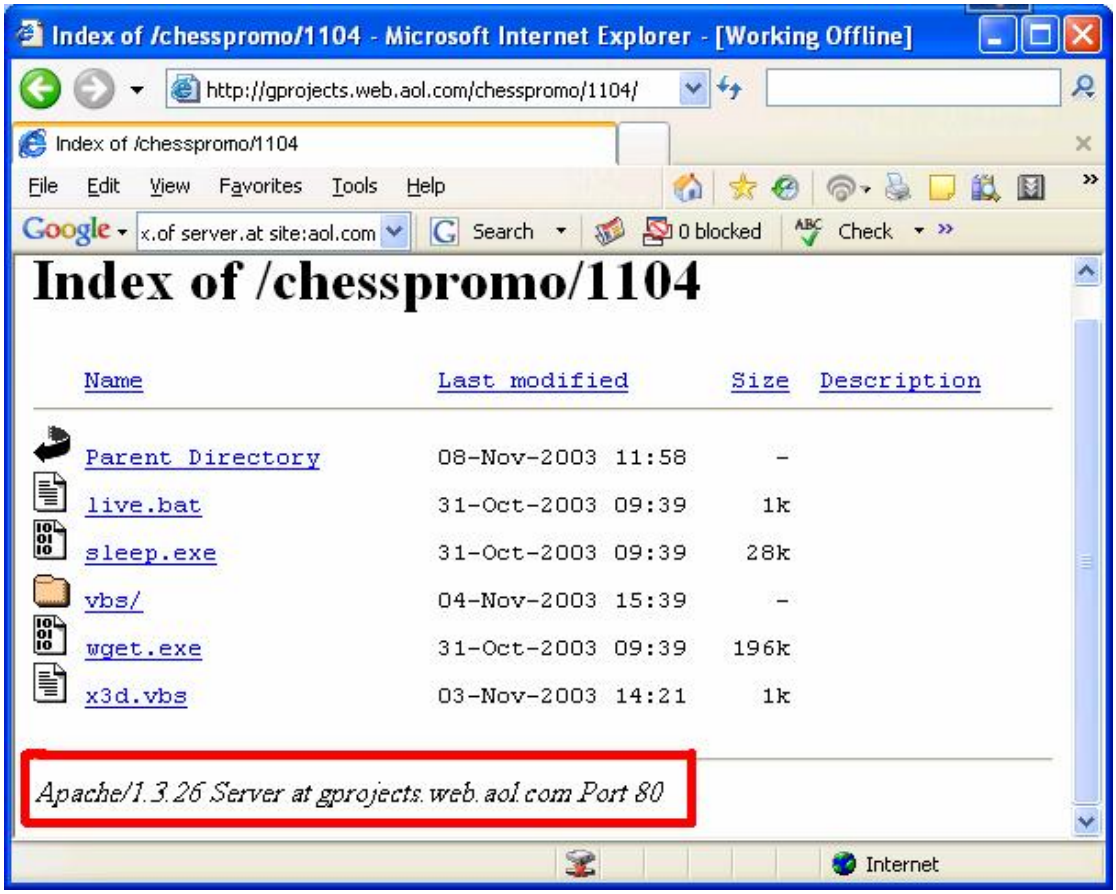
[1] tag

intitle:index.of server.at site:aol.com

در شکل زیر یافته های گوگل را بعد از جستجوی عبارت بالا را می بینید:



که نتیجه این جستجو برای یکی از آن یافته ها در قسمت پایین شکل زیر دیده می شود:



همچنین از این تکنیک نیز می توان برای پیدا کردن سرورهایی که که یک نسخه خاصی از نرم افـزار مذکور روی آنها در حال اجراست . که برای این کار عبارت زیر را در گوگل جستجو می کنیم:

intitle:index.of "Apache/1.3.0 Server at"

از این تکنیک چگونه می توان استفاده نمود ؟

این تکنیک هنگامی که در لیست دایرکتوری نسخه نرم افزار وب سـرور نباشـد کـاربرد نخواهـد داشت که تکنیک پیشرفته تر دیگری برای پی بردن به نسخه نرم افزار مورد نظر وجود دارد.

که این تکنیک شامل جمع آوری اطلاعات از Header سایت ، عنوان سایت و فرمت های دیگـری از این لیست دایرکتوری می باشد که به تکنیـک "profiling" معـروف اسـت کـه بـا اسـتفاده از ایـن تکنیک یک هکر لایق می تواند خیلی راحت نسخه نرم افزار در حال اجـرا روی وب سـرور را بدسـت آورد. در حالت کلی وقتی که یک هکر یک اکسپلویت (Exploit) برای نـسخه خاصـی از سـرورهای

Apache دارد خیلی به سرعت می تواند در گوگل سایت هایی را که دارای این نسخه از نرم افزار روی وب سرور هستند را شناسایی کرده و اقدام به نفوذ نماید.

در جدول زیر بعضی از محل سرورهای خاص از طریق لیست دایرکتوری (شاخه ها) آورده شده :

اگر در گوگل موارد زیر را بنویسید لیست دایرکتوری مربوط به آن سرور را به شما می دهد
“AnWeb/1.42h” intitle:index.of
“Apache Tomcat/” intitle:index.of
“Apache-AdvancedExtranetServer/” intitle:index.of
“Apache/df-exts” intitle:index.of
“Apache/” “server at” intitle:index.of
“Apache/AmEuro” intitle:index.of
“Apache/Blast” intitle:index.of
“Apache/WWW” intitle:index.of
“Apache/df-exts” intitle:index.of
“CERN httpd 3.0B (VAX VMS)” intitle:index.of
*fitweb-wwws * server at intitle:index.of*
“HP Apache-based Web “Server/1.3.26” intitle:index.of
“HP Apache-based Web “Server/1.3.27 (Unix) mod_ssl/2.8.11 OpenSSL/0.9.6g” intitle:index.of
*“httpd+ssl/kttd” * server at intitle:index.of*
“JRun Web Server” intitle:index.of
“MaXX/3.1” intitle:index.of
“Microsoft-IIS/ server at” intitle:index.of*
“Microsoft-IIS/4.0” intitle:index.of
“Microsoft-IIS/5.0 server at” intitle:index.of
“Microsoft-IIS/6.0” intitle:index.of
“OmniHTTPd/2.10” intitle:index.of
“OpenSA/1.0.4” intitle:index.of
“Oracle HTTP Server Powered by Apache” intitle:index.of

“Red Hat Secure/2.0” intitle:index.of
“Red Hat Secure/3.0 server at” intitle:index.of
*SEDWebserver * server +at intitle:index.of*

همچنین جدول زیر لیست دایرکتوری ها که سرور آنها آپاچی[1] می باشد را نشان می دهد:

لیست دایرکتوری مربوط به سرور آپاچی
“Apache/1.0” intitle:index.of
“Apache/1.1” intitle:index.of
“Apache/1.2” intitle:index.of
“Apache/1.2.0 server at” intitle:index.of
“Apache/1.2.4 server at” intitle:index.of
“Apache/1.2.6 server at” intitle:index.of
“Apache/1.3.0 server at” intitle:index.of
“Apache/1.3.2 server at” intitle:index.of
“Apache/1.3.1 server at” intitle:index.of
“Apache/1.3.1.1 server at” intitle:index.of
“Apache/1.3.3 server at” intitle:index.of
“Apache/1.3.4 server at” intitle:index.of
“Apache/1.3.6 server at” intitle:index.of
“Apache/1.3.9 server at” intitle:index.of
“Apache/1.3.11 server at” intitle:index.of
“Apache/1.3.12 server at” intitle:index.of
“Apache/1.3.14 server at” intitle:index.of
“Apache/1.3.17 server at” intitle:index.of
“Apache/1.3.19 server at” intitle:index.of
“Apache/1.3.20 server at” intitle:index.of
“Apache/1.3.22 server at” intitle:index.of
“Apache/1.3.23 server at” intitle:index.of

[1] وب سرورها به طور کلی به دو دسته تقسیم می شوند:

الف)وب سرورهای تحت ویندوز مانند IIS

ب) وب سرورهای تحت لینوکس مانند Apache

"Apache/1.3.24 server at" intitle:index.of
"Apache/1.3.26 server at" intitle:index.of
"Apache/1.3.27 server at" intitle:index.of
"Apache/1.3.27-fil" intitle:index.of
"Apache/1.3.28 server at" intitle:index.of
"Apache/1.3.29 server at" intitle:index.of
"Apache/1.3.31 server at" intitle:index.of
"Apache/1.3.35 server at" intitle:index.of
"Apache/2.0.32 server at" intitle:index.of
"Apache/2.0.35 server at" intitle:index.of
"Apache/2.0.36 server at" intitle:index.of
"Apache/2.0.39 server at" intitle:index.of
"Apache/2.0.40 server at" intitle:index.of
"Apache/2.0.42 server at" intitle:index.of
"Apache/2.0.43 server at" intitle:index.of
"Apache/2.0.44 server at" intitle:index.of
"Apache/2.0.45 server at" intitle:index.of
"Apache/2.0.46 server at" intitle:index.of
"Apache/2.0.47 server at" intitle:index.of
"Apache/2.0.48 server at" intitle:index.of
"Apache/2.0.49 server at" intitle:index.of
"Apache/2.0.49a server at" intitle:index.of
"Apache/2.0.50 server at" intitle:index.of
"Apache/2.0.51 server at" intitle:index.of
"Apache/2.0.52 server at" intitle:index.of

محل های خاص و نسخه سرورهای محرمانه از طریق لیست دایرکتوری ها
"Apache/1.3.12 (Unix) mod_fastcgi/2.2.12 mod_dyntag/1.0 mod_advert/1.12 mod_czech/3.1.1b2" intitle:index.of

“Apache/1.3.12 (Unix) mod_fastcgi/2.2.4 secured_by_Raven/1.5.0” intitle:index.of

“Apache/1.3.12 (Unix) mod_ssl/2.6.6 OpenSSL/0.9.5a” intitle:index.of

“Apache/1.3.12 Cobalt (Unix) Resin/2.0.5 StoreSense-Bridge/1.3 ApacheJServ/1.1.1 mod_ssl/2.6.4 OpenSSL/0.9.5a mod_auth_pam/1.0a FrontPage/4.0.4.3 mod_perl/1.24” intitle:index.of

“Apache/1.3.14 - PHP4.02 - Iprotect 1.6 CWIE (Unix) mod_fastcgi/2.2.12 PHP/4.0.3pl1” intitle:index.of

“Apache/1.3.14 Ben-SSL/1.41 (Unix) mod_throttle/2.11 mod_perl/1.24_01 PHP/4.0.3pl1 FrontPage/4.0.4.3 rus/PL30.0” intitle:index.of

“Apache/1.3.20 (Win32)” intitle:index.of

“Apache/1.3.20 Sun Cobalt (Unix) PHP/4.0.3pl1 mod_auth_pam_external/0.1 FrontPage/4.0.4.3 mod_perl/1.25” intitle:index.of

“Apache/1.3.20 Sun Cobalt (Unix) PHP/4.0.4 mod_auth_pam_external/0.1 FrontPage/4.0.4.3 mod_ssl/2.8.4 OpenSSL/0.9.6b mod_perl/1.25” intitle:index.of

“Apache/1.3.20 Sun Cobalt (Unix) PHP/4.0.6 mod_ssl/2.8.4 OpenSSL/0.9.6 FrontPage/5.0.2.2510 mod_perl/1.26” intitle:index.of

“Apache/1.3.20 Sun Cobalt (Unix) mod_ssl/2.8.4 OpenSSL/0.9.6b PHP/4.0.3pl1 mod_auth_pam_external/0.1 FrontPage/4.0.4.3 mod_perl/1.25” intitle:index.of

“Apache/1.3.20 Sun Cobalt (Unix) mod_ssl/2.8.4 OpenSSL/0.9.6b PHP/4.0.3pl1 mod_fastcgi/2.2.8 mod_auth_pam_external/0.1 mod_perl/1.25” intitle:index.of

"Apache/1.3.20 Sun Cobalt (Unix) mod_ssl/2.8.4 OpenSSL/0.9.6b PHP/4.0.4 mod_auth_pam_external/0.1 mod_perl/1.25" intitle:index.of

"Apache/1.3.20 Sun Cobalt (Unix) mod_ssl/2.8.4 OpenSSL/0.9.6b PHP/4.0.6 mod_auth_pam_external/0.1 FrontPage/4.0.4.3 mod_perl/1.25" intitle:index.of

"Apache/1.3.20 Sun Cobalt (Unix) mod_ssl/2.8.4 OpenSSL/0.9.6b mod_auth_pam_external/0.1 mod_perl/1.25" intitle:index.of

"Apache/1.3.26 (Unix) Debian GNU/Linux PHP/4.1.2 mod_dtcl" intitle:index.of

"Apache/1.3.26 (Unix) PHP/4.2.2" intitle:index.of

"Apache/1.3.26 (Unix) mod_ssl/2.8.9 OpenSSL/0.9.6b" intitle:index.of

"Apache/1.3.26 (Unix) mod_ssl/2.8.9 OpenSSL/0.9.7" intitle:index.of

"Apache/1.3.26+PH" intitle:index.of

"Apache/1.3.27 (Darwin)" intitle:index.of

"Apache/1.3.27 (Unix) mod_log_bytes/1.2 mod_bwlimited/1.0 PHP/4.3.1 FrontPage/5.0.2.2510 mod_ssl/2.8.12 OpenSSL/0.9.6b" intitle:index.of

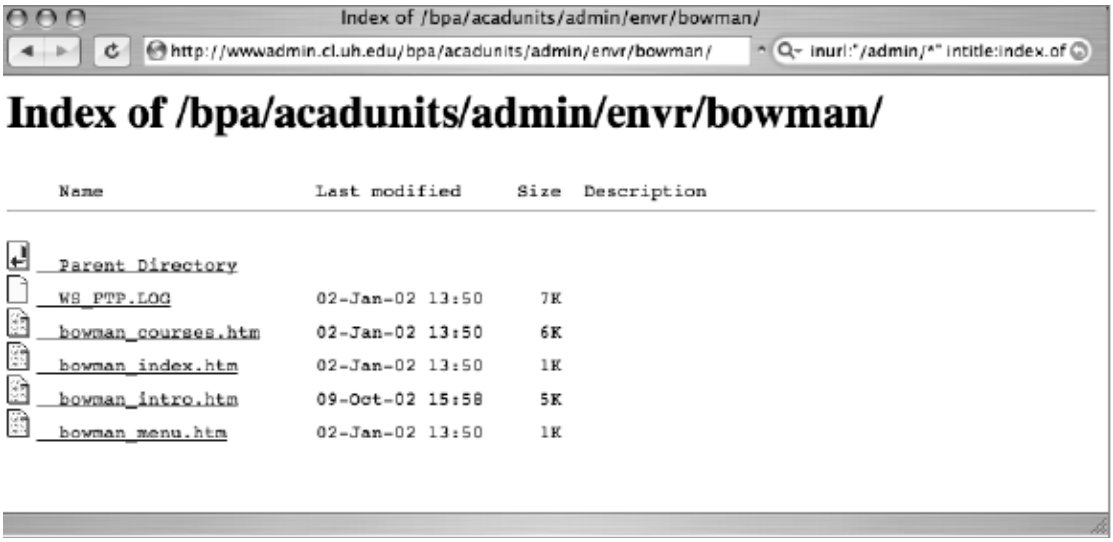
"Apache/1.3.27 (Unix) mod_ssl/2.8.11 OpenSSL/0.9.6g FrontPage/5.0.2.2510 mod_gzip/1.3.26 PHP/4.1.2 mod_throttle/3.1.2" intitle:index.of

تکنیک پیمایش در لیست دایرکتوریها

برای اینکه بدانیم که لیست دایرکتوریها چگونه می تواند مفید باشد جستجوی زیر را در گوگل انجام می دهیم

intitle:index.of inurl:“/admin/*”

در ادامه یکی از نتایج آن در تصویر زیر نشان داده شده است:



اگر با توجه به آدرس آن در تصویر دقت کنید می بینید که ما در مسیر bowman قرار داریم و مسیر admin که مورد نظر ماست در دو سطح قبل قرار دارد لذا برای رسیدن به آن سطح بر روی لینک parent directory کلیک می کنیم. اولین کلیک ما را به شاخه envr انتقال می دهد. پس به همین صورت و به راحتی هر چه تمام تر می توانیم بین سطوح مختلف آن انتقال پیدا کنیم. حتی می توانیم با یک جستجوی بهتر برای یافتن فایلهای خاص مانند جستجوی زیر به نتایج جالبتری برسیم:

```
site:cl.uh.edu inurl:bpa/acadunits/admin ws_ftp.log
```

همچنین با ویرایش کردن نوار آدرس هم می توانیم بین سطوح مختلف جابجا شویم.

مثال ساده دیگر اینکه ما بجای کلمه admin کلمه student یـا public را جـایگزین مـی کنـیم و غیره. همچنین می توانیم به بخش هایی در یک وب سرور دسترسی پیدا کنیم که در خود سایت یـا سرور اجازه دسترسی به آن بخش را نداریم .

اگر یک وب سرور در آدرس /var/www نـصب شـده باشـد و اسـناد عمـومی شـبکه وب در مـسیر /var/www/htdocs قرار داشته باشد و در حالت پیش فرض هر کاربری کـه بـه یـک دایرکتـوری سطح بالا در وب سرور اتصال پیدا کند فایل هایی که در محـل /var/www/htdocs مـی باشـد را می تواند ببیند. .

یک URL نرمال که برای این محصول می تواند به صورت زیر باشد:

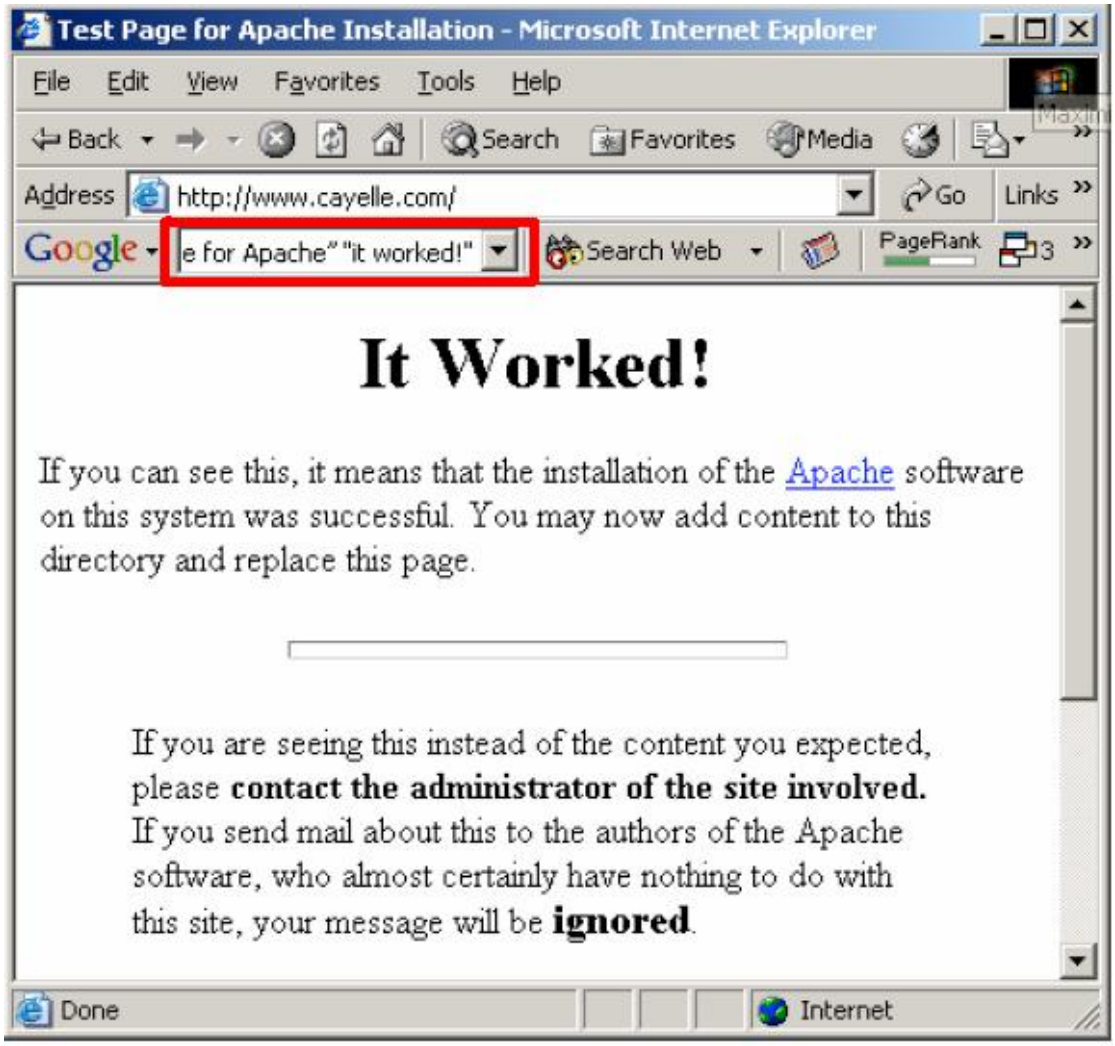
```
www.somesadsite.org/badcode.pl?page=/index.html
```

این URL می تواند برنامه درون badcode.pl را به محل /var/www/htdocs/index.html واکشی[1] کرده و آن را به کاربر نشان دهد.

راه دیگر از طریق صفحه پیش فرض (Default pages)

هنگامی که یک وب سرور نصب می شود همانند شکل زیر در صفحه پیش فرض آن نسخه وب سـرور مورد نظر وجود دارد . (شکل زیر صفحه تست Apache می باشد) همچنین محـصولی از نـرم افـزار نصب شده بر روی سرور نام دایرکتوریها را به عنوان آرگومان می پذیرد

[1] Fetch



از این تکنیک چگونه می توان استفاده نمود؟

کافی است یک جستجوی ساده مانند عبارت زیر انجام دهیم:

intitle:Test.Page.for.Apache it.worked!

عبارت فوق سایت هایی که Apache 1.2.6 روی آنها در حال اجراست با یک صفحه پیش فرض را بر می گرداند.

جستجو های دیگر نتایج Apache های دیگری را به دست می دهد.

نسخه سرور Apache	عبارت وارده برای جستجو
Apache 1.3.0 – 1.3.9	Intitle:Test.Page.for.Apache It.worked! this.web.site!
Apache 1.3.11 – 1.3.26	Intitle:Test.Page.for.Apache seeing.this.instead
Apache 2.0	Intitle:Simple.page.for.Apache Apache.Hook.Functions
Apache SSL/TLS	Intitle:test.page "Hey, it worked !" "SSL/TLS-aware"

و جدول زیر هم نسخه IIS (Internet information Services) و در قالب صفحه وب را بـه مـا می دهد:

نسخه سرور Apache	عبارت وارده برای جستجو
Many	intitle:welcome.to intitle:internet IIS
UnKnown	intitle:"Under construction" "does not currently have"
IIS 4.0	intitle:welcome.to.IIS.4.0
IIS 4.0	allintitle:Welcome to Windows NT 4.0 Option Pack
IIS 4.0	allintitle:Welcome to Internet Information Server
IIS 5.0	allintitle:Welcome to Windows 2000 Internet Services
IIS 6.0	allintitle:Welcome to Windows XP Server Internet Services

در شکل زیر هم نمونه ای از یافته IIS 5.0 در گوگل را مشاهده می کنید:

که این وب سرور مبتنی بر مایکروسافت است که به درستی نسخه نرم افزار وب سرور را مشخص نمی کند ولی سیستم عامل (در اینجا ویندوز ۲۰۰۰) وserver pack آن را به خوبی نشان می دهد. که این اطلاعات برای هکر فوق العاده مهم است و می تواند به سیستم عامل نفوذ کرده و از درون سیستم عامل کنترل وب سرور را به دست بگیرد و به دستکاری آن بپردازد.

در شکل زیر صفحه پیش فرض سرور Netscape را ملاحظه می کنید:

مؤلف: محمد بشیری

Site: http://bashiry.250free.com

جدول زیر جستجو ها برای یافتن صفحه پیش فرض سرور Netscape می باشد:

نسخه سرور Netscape	عبارت وارده برای جستجو
Many	allintitle:Netscape Enterprise Server Home Page
Unknown	allintitle:Netscape FastTrack Server Home Page

جدول زیر شامل بیشتر وب سرورها یا برنامه های ویژه و محرمانه می باشد:

Server/version	عبارت وارده برای جستجو
Jigsaw / 2.2.3	intitle:"jigsaw overview" "this is your"
Jigsaw / Many	intitle:”jigsaw overview”
iPlanet / Many	intitle:"web server, enterprise edition"
Resin / Many	allintitle:Resin Default Home Page
Resin / Enterprise	allintitle:Resin-Enterprise Default Home Page

allintitle:default home page java web server	JWS / 1.0.3 – 2.0
intitle:"default j2ee home page"	J2EE / Many
"KF Web Server Home Page"	KFSensor honeypot
"Congratulations! You've created a new Kwiki website."	Kwiki
"Welcome to your domain web page" matrix	Matrix Appliance
intitle:"default domain page" "congratulations" "hp web"	HP appliance sa1*
"congratulations on choosing" intel netstructure	Intel Netstructure
"default web page" congratulations "hosting appliance"	Generic Appliance
intitle:"Welcome to Your New Home Page!" debian	Debian Apache
"micro webserver home page"	Cisco Micro Webserver 200

راه دیگر به طریق دستی، صفحات Help و برنامه های نمونه (Sample programs)

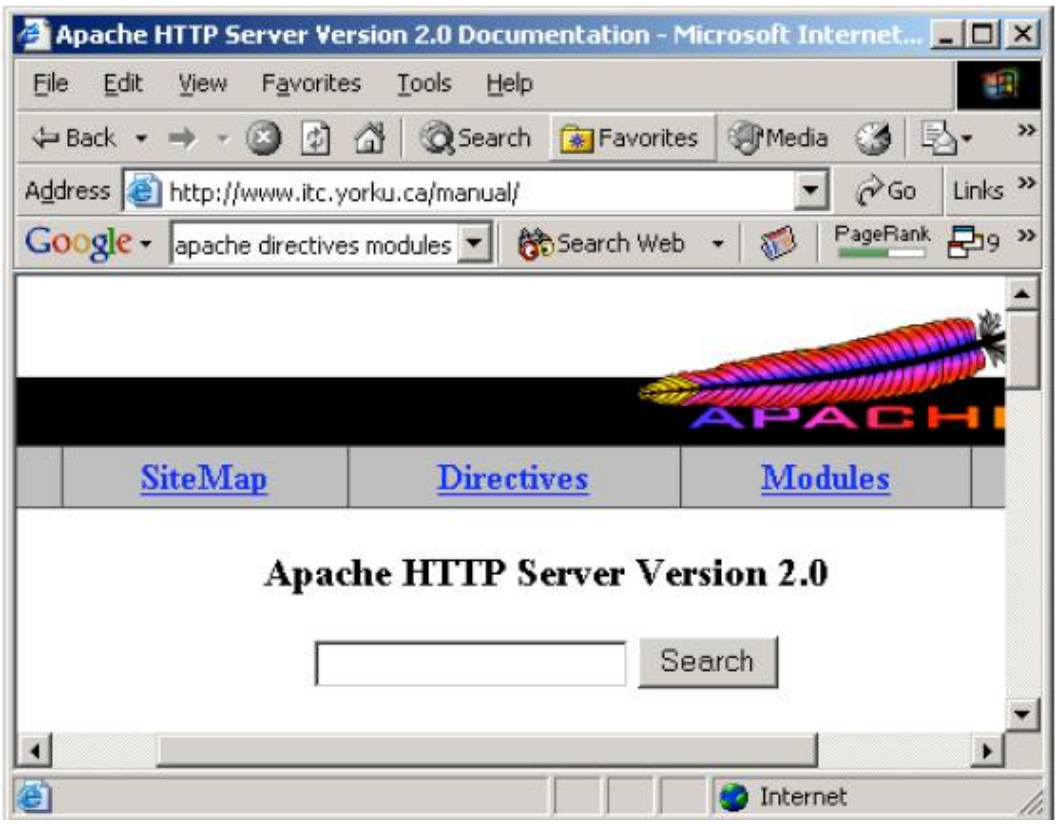
راه دیگر برای شناسایی نسخه سرور، جستجو به صورت دستی در صفحات Help و برنامه های نمونه که احتمالا روی سایت نصب شده اند می باشد. تعداد زیادی از وب سرورها نصب دستی صفحات و برنامه های نمونه را در محل پیش فرض توضیح می دهد. در سال های اخیر هکر ها برای دسترسی به وب سرور اکسپلویت های بسیاری در اختیار داشتند و می توانستند از طریق همین کدهای نمونه (sample code) به سرور مورد نظر نفوذ کنند. بیشتر فروشندگان وب سرورها به مدیران سایت ها اسرار داشتند که قبل از قرار دادن سرور خود روی اینترنت این کدهای نمونه را حذف کنند تا از دسترسی هکرها به سرورهای آنها جلوگیری شود.

چگونگی استفاده از این تکنیک:

برای شناسایی نسخه وب سرور یک هدف خاص هکر می تواند با استفاده از این تکنیک حفره هایی را که در وب سرور وجود دارد را کشف نماید. به مثال زیر توجه کنید:

inurl:manual apache directives modules

این جستجو صفحاتی را به ما می دهد که آن صفحات شامل وب سرور آپاچی هستند. که این صفحات شامل بسته های نصب پیش فرض در نسخه های مختلفی از سرور Apache هستند. که این نسخه های مختلف دارای صفحات مختلف و در جاهای مختلف قرار دارند. برای فهم بیشتر این مطلب به شکل شماره ۶ توجه کنید . همانطور که در شکل دیده می شود نسخه این سرور در بالای صفحه نوشته شده است.



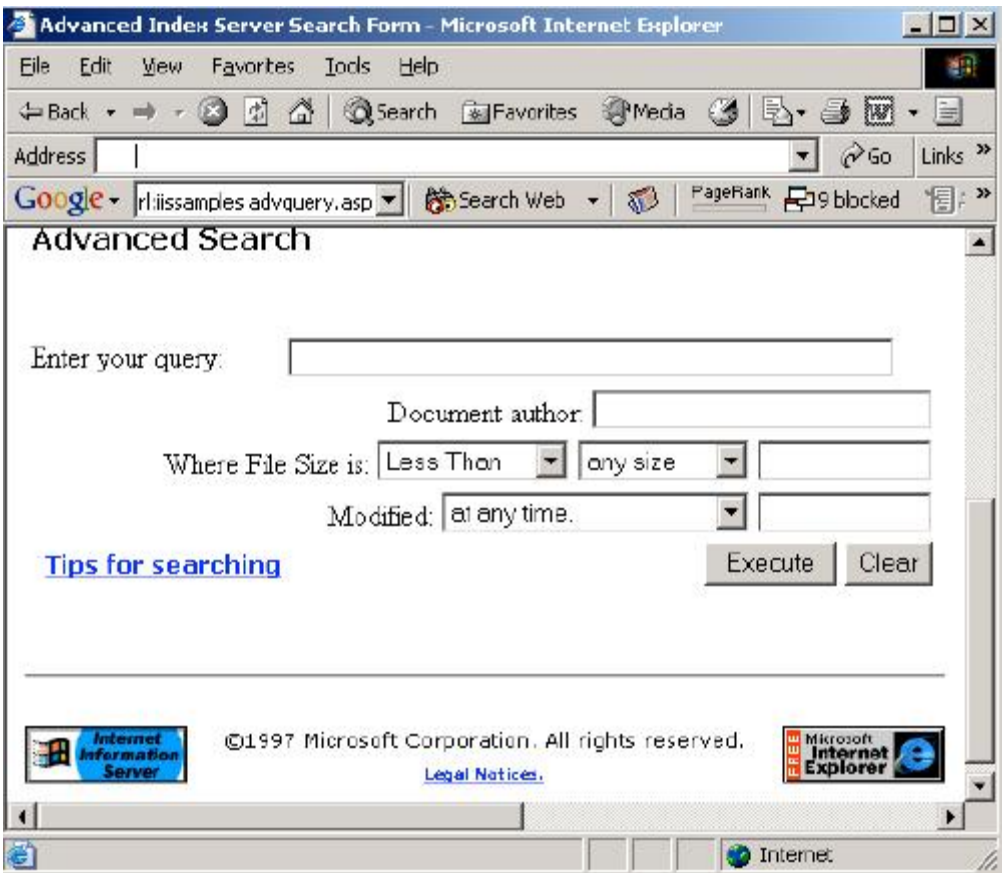
شکل شماره۶- شناسایی نسخه سرور آپاچی از طریق Server manuals

همین مطلب را عینا برای جستجوی IIS های شرکت مایکروسافت داریم که برای یافتن نسخه این سرورها عبارت مقابل را جستجو می کنیم: Allinurl:iishelp core

تعداد زیادی از IIS ها هنگام نصب برنامه های اختیاری دیگری نصب می کنند که خیلی وقتها این برنامه ها در یک دایرکتوری ذخیره می شوند که اصطلاحا به آنها iissamples گویند که برای جستجوی این ها از عبارت روبرو استفاده می کنیم: Inurl:iissamples

به علاوه نام این برنامه ها می تواند مانند عبارت زیر جستجو شوند که نتیجه جستجو را در تصویر شماره ۷ ملاحظه می کنید.

Inurl:iissamples advquery.asp



تصویر شماره ۷- یک سرور IIS با کدهای نمونه نصب روی آن

گاهی اوقات این زیر شاخه ها (subdirectory) می توانند درون شاخه های یا دایرکتوری های نمونه باشند که یک صفحه شامل دایرکتوری IIS و دایرکتوری Sdk را می توان مانند عبارت زیر جستجو نمود.

استفاده از گوگل به عنوان پویشگر CGI (CGI scanner)

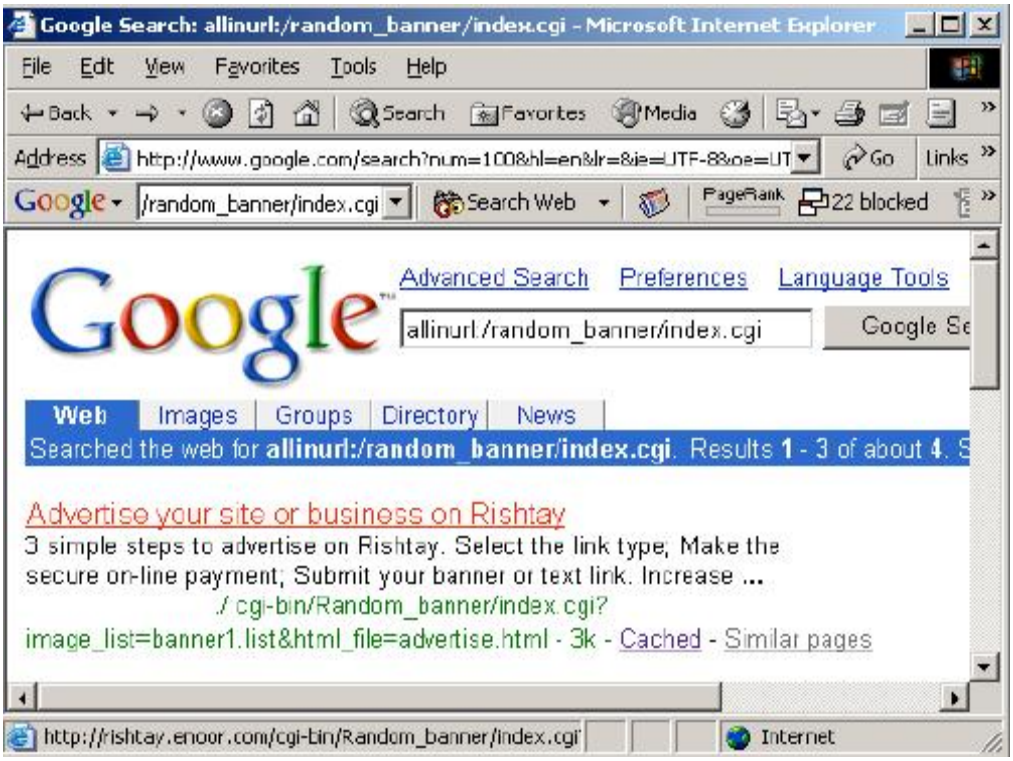
پویشگر CGI یا پویشگر WEB یک کار واجب و حیاتی در هک کردن وب سرورهاست که این عمل باعث جستجو در یک وب سرور، شاخه ها، کدهای نمونه برای یافتن آسیب پذیری وب سرور می باشد که این عمل آسیب پذیری ها را در یک فایل ذخیره می کند مانند عبارت زیر:

/cgi-bin/cgiemail/uargg.txt
/random_banner/index.cgi
/random_banner/index.cgi
/cgi-bin/mailview.cgi
/cgi-bin/maillist.cgi
/cgi-bin/userreg.cgi
/iissamples/ISSamples/SQLQHit.asp
/iissamples/ISSamples/SQLQHit.asp
/SiteServer/admin/findvserver.asp
/scripts/cphost.dll
/cgi-bin/finger.cgi

از این تکنیک چگونه می توان استفاده نمود:

عبارات آسیب پذیری که توسط گوگل پیدا می شوند برای هکر ها مانند نقشه راهنمای جاده می ماند. به طور خلاصه برای جستجوی اینگونه از آسیب پذیری ها در گوگل از عبارت زیر استفاده می کنیم که نتیجه آن را در شکل شماره ۸ می بینید.

allinurl:/random_banner/index.cgi



تصویر شماره ۸- مثالی برای جستجو در گوگل برای پویش کردن CGI

که یک هکر با استفاده از این نتایج می تواند فایلی را که شامل کلمه های عبور می باشد را دریافت نماید (تصویر زیر)

```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin: daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm: lp:x:4:7:lp:/var/spool/lpd: sync:x:5:0:sync:/sbin:/bin/sync
halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:
news:x:9:13:news:/var/spool/news: uucp:x:10:14:uucp:/var/spool/uucp:
operator:x:11:0:operator:/root: games:x:12:100:games:/usr/games:
gopher:x:13:30:gopher:/usr/lib/gopher-data: ftp:x:14:50:FTP
User:/home/ftp:/usr/local/bin/noshell nobody:x:99:99:Nobody:/:
postgres:x:100:233:PostgreSQL Server:/var/lib/pgsql:/bin/tcsh aijaz:x:500:500:Aijaz A.
Ansari:/home/aijaz:/bin/bash ron:x:501:501::/home/ron:/bin/bash
ics:x:502:502::/home/ics:/bin/tcsh qss:x:503:503::/home/qss:/bin/tcsh
ayesha:x:504:504::/home/ayesha:/usr/local/bin/noshell
arshad:x:505:505::/home/arshad:/bin/bash
school:x:506:506::/home/school:/usr/local/bin/noshellyesftp
comtel:x:507:507::/home/comtel:/usr/local/bin/noshell
ajmar:x:508:508::/home/ajmar:/usr/local/bin/noshellyesftp
fatiha:x:509:509::/home/fatiha:/usr/local/bin/noshell
newedge:x:510:510::/home/web/WWW/WWWrmc:/usr/local/bin/noshellyesftp
enoor:x:511:511::/home/enoor:/usr/local/bin/noshellyesftp brian:x:512:512:Brian
Burdick:/home/brian:/usr/local/bin/noshell if:x:513:513::/home/if:/usr/local/bin/noshell
```

در ضمن نرم افزار GooScan که توسط J0hnny نوشته شده است کار بالا را به صورت خودکار انجام می دهد.

جستجو برای آسیب پذیری روی سرورها

Entries for category : **Advisories and Vulnerabilities** **These searches locate vulnerable servers. These searches are often generated from various security advisory posts, and in many cases are product or version-specific.**
Entry name
"1999-2004 FuseTalk Inc" -site:fusetalk.com
"2003 DUware All Rights Reserved"
"Active Webcam Page" inurl:8080
"BlackBoard 1.5.1-f | © 2003-4 by Yves Goergen"
"BosDates Calendar System " "powered by BosDates v3.2 by BosDev"
"Calendar programming by AppIdeas.com" filetype:php
"Copyright 2004 © Digital Scribe v.1.4"
"Copyright © 2002 Agustin Dondo Scripts"
"delete entries" inurl:admin/delete.asp
"driven by: ASP Message Board"
"Enter ip" inurl:"php-ping.php"
"IceWarp Web Mail 5.3.0" "Powered by IceWarp"
"Ideal BB Version: 0.1" -idealbb.com
"inurl:/site/articles.asp?idcategory="
"Maintained with Subscribe Me 2.044.09p"+"Professional" inurl:"s.pl"
"Mimicboard2 086"+"2000 Nobutaka Makino"+"password"+"message" inurl:page=1
"Obtenez votre forum Aztek" -site:forum-aztek.com
"Online Store - Powered by ProductCart"
"portailphp v1.3" inurl:"index.php?affiche" inurl:"PortailPHP" -site:safari-msi.com
"Powered *: newtelligence" ("dasBlog 1.6"| "dasBlog 1.5"| "dasBlog

1.4"|"dasBlog 1.3")
"Powered by A-CART"
"Powered by AJ-Fork v.167"
"Powered by and copyright class-1" 0.24.4
"powered by antiboard"
"Powered by AzDg" (2.1.3 | 2.1.2 | 2.1.1)
"Powered by Coppermine Photo Gallery"
"Powered by Coppermine Photo Gallery" ("v1.2.2 b" | "v1.2.1" | "v1.2" | "v1.1" | "v1.0")
"powered by CubeCart 2.0"
"Powered by CubeCart"
"Powered by CuteNews"
"Powered by DCP-Portal v5.5"
"Powered by DMXReady Site Chassis Manager" -site:dmxready.com
"Powered by FUDForum 2.6" -site:fudforum.org -johnny.ihackstuff
"Powered by FUDForum 2.7" -site:fudforum.org -johnny.ihackstuff
"Powered by FUDforum"
"powered by Gallery v" "[slideshow]"|"images" inurl:gallery
"Powered by Gallery v1.4.4"
"Powered by GTChat 0.95"+"User Login"+"Remember my login information"
"Powered by IceWarp Software" inurl:mail
"Powered by Ikonboard 3.1.1"
"powered by ITWorking"
"Powered by MD-Pro" | "made with MD-Pro"
"Powered by Megabook *" inurl:guestbook.cgi
"Powered by MercuryBoard [v1"
"powered by minibb" -site:www.minibb.net -intext:1.7f
"Powered by My Blog" intext:"FuzzyMonkey.org"
"Powered by ocPortal" -demo -ocportal.com
"Powered by PHP Advanced Transfer Manager"
"powered by PhpBB 2.0.15" -site:phpbb.com
"Powered by PowerPortal v1.3"
"Powered by WordPress" -html filetype:php -demo -wordpress.org -bugtraq
"Powered by WowBB" -site:wowbb.com

"Powered by YaPig V0.92b"
"Powered by yappa-ng"
"Powered by Zorum 3.5"
"Powered by: Land Down Under 800" | "Powered by: Land Down Under 801" - www.neocrome.net
"running: Nucleus v3.1" -.nucleuscms.org -demo
"Software PBLang" 4.65 filetype:php
"SquirrelMail version 1.4.4" inurl:src ext:php
"This page has been automatically generated by Plesk Server Administrator"
+"Powered by Invision Power Board v2.0.0..2"
+"Powered by phpBB 2.0.6..10" -phpbb.com -phpbb.pl
+intext:"powered by MyBulletinBoard"
Achievo webbased project management
allintitle:aspjar.com guestbook
E-market remote code execution
EarlyImpact Productcart
ext:php intext:"Powered by phpNewMan Version"
ext:pl inurl:cgi intitle:"FormMail *" -"*Referrer" -"* Denied" -sourceforge -error -cvs -input
filetype:cgi inurl:nbmember.cgi
filetype:cgi inurl:pdesk.cgi
filetype:cgi inurl:tseekdir.cgi
filetype:php intitle:"paNews v2.0b4"
filetype:php inurl:index.php inurl:"module=subjects" inurl:"func=*" (listpages| viewpage | listcat)
http://www.google.com/search?q=intitle:%22WEB//NEWS+Personal +Newsmanagement%22 +intext:%22%C2%A9+2002-2004+by+Christian+Scheb+- +Stylemotion.de%22%2B%22
intext:"Calendar Program © Copyright 1999 Matt Kruse" "Add an event"
intext:"Powered by flatnuke-2.5.3" +"Get RSS News" -demo
intext:"Powered by phpBB 2.0.13" inurl:"cal_view_month.php"|inurl:"downloads.php"
intext:"Powered By: Snitz Forums 2000 Version 3.4.00..03"

intext:("UBB.threads™ 6.2"|"UBB.threads™ 6.3") intext:"You * not logged *" -site:ubbcentral.com
intitle:"blog torrent upload"
intitle:"EMUMAIL - Login" "Powered by EMU Webmail"
intitle:"Looking Glass v20040427" "When verifying an URL check one of those"
intitle:"MRTG/RRD" 1.1* (inurl:mrtg.cgi | inurl:14all.cgi |traffic.cgi)
intitle:"myBloggie 2.1.1..2 - by myWebland"
intitle:"osTicket :: Support Ticket System"
intitle:"PowerDownload" ("PowerDownload v3.0.2 ©" | "PowerDownload v3.0.3 ©") -site:powerscripts.org
intitle:"View Img" inurl:viewimg.php
intitle:"WebJeff - FileManager" intext:"login" intext:Pass|PAsse
intitle:"WordPress > * > Login form" inurl:"wp-login.php"
intitle:guestbook "advanced guestbook 2.2 powered"
intitle:guestbook inurl:guestbook "powered by Advanced guestbook 2.*" "Sign the Guestbook"
intitle:guestbook inurl:guestbook "powered by Advanced guestbook 2.*" "Sign the Guestbook"
intitle:welcome.to.horde
inurl:"/cgi-bin/loadpage.cgi?user_id="
inurl:"/login.asp?folder=" "Powered by: i-Gallery 3.3"
inurl:"/site/articles.asp?idcategory="
inurl:"comment.php?serendipity"
inurl:"forumdisplay.php" +"Powered by: vBulletin Version 3.0.0..4"
inurl:"messageboard/Forum.asp?"
inurl:"slxweb.dll"
inurl:/SiteChassisManager/
inurl:cal_make.pl
inurl:chitchat.php "choose graphic"
inurl:citrix/metaframexp/default/login.asp? ClientDetection=On
inurl:comersus_message.asp
inurl:directorypro.cgi
inurl:gotoURL.asp?url=
inurl:index.php fees shop link.codes merchantAccount

inurl:sphpblog intext:"Powered by Simple PHP Blog 0.4.0"
inurl:technote inurl:main.cgi*filename=*
inurl:ttt-webmaster.php
inurl:wiki/MediaWiki
Invision Power Board SSI.PHP SQL Injection
mnGoSearch vulnerability
phpLDAPadmin intitle:phpLDAPadmin filetype:php inurl:tree.php | inurl:login.php | inurl:donate.php (0.9.6 | 0.9.7)
powered.by.instaBoard.version.1.3
Powered.by:.vBulletin.Version ...3.0.6
Quicksite demopages for Typo3
ReMOSitory module for Mambo
uploadpics.php?did= -forumintext:Generated.by.phpix.1.0? inurl:$mode=album
vBulletin version 3.0.1 newreply.php XSS
VP-ASP Shopping Cart XSS

استفاده از گوگل برای یافتن فایلها و دایرکتوری های جالب

گاهی اوقات پیش می آید که این نوع جستجو به ما پاسخی نمی‌دهد ولی در عوض اطلاعات حساسی را که در دسترس عموم نیست را برای ما پیدا می کند. که بیشتر افراد این اطلاعات را روی وب سرور خود جای می گذارند که گوگل بدون هیچ سر و صدایی این اطلاعات را مانند عمل خزیدن در صفحات را مورد جستجو قرار می دهد.

رایجترین کار برای این دستور یافتن جستجو برای اطلاعات حساس مالی، اطلاعات پزشکی، امنیت و چیزهایی شبیه به این موارد است.

از این تکنیک چگونه می توان استفاده نمود؟

این تکنیک برخلاف تکنیک های گفته شده سخت می باشد و بستگی به شانس هم دارد و گاهی اوقات بهترین راه برای یافتن اطلاعات مهم و حساس انتخاب می شود و گاهی اوقات هم نه .

مثال:

بیشتر اوقات اطلاعات افراد یک مجموعه در یک شاخه ای با نام Backup ذخیره می شوند که ما بـه راحتی می توانیم با عبارت جستجوی زیر پیدا نماییم:

Inurl:backup

و یا همینطور برای کاهش نتایج از عبارت زیر می توان استفاده کرد:

inurl:backup intitle:index.of inurl:admin

عبارت inurl:admin دایرکتوری مدیران سیستم ها را آشکار می کند و همینطور چندین ترکیـب از این عبارات جستجو می توان مفید باشد، بطور نمونه:

inurl:admin intitle:login

که این عبارت صفحه ورود مدیران سیستم را آشکار می کند.

یا

inurl:admin filetype:xls

که این عبارت به دنبال فایل های صفحه گسترده (فایل های نرم افزار اکسل) که مربـوط بـه ادمـین (Admin) می باشد می گردد.

یا

inurl:admin inurl:userlist

این جستجو اطلاعات کاربران را از قبیل: کلمه عبور، شماره تلفن، آدرس و ... را به ما می دهد.

و یا

inurl:admin filetype:asp inurl:userlist

این دستور در صفحات asp به دنبال عبارات مورد نظر که در عنوان آن کلمـه Admin، و در آدرس آن سایت کلمه Userlist به کار رفته است می گردد.

مؤلف: محمد بشیری

Site: http://bashiry.250free.com

فصل چهارم

یافتن نام های کاربری،

کلمات عبور و غیره

Usernames, passwords, secret stuff

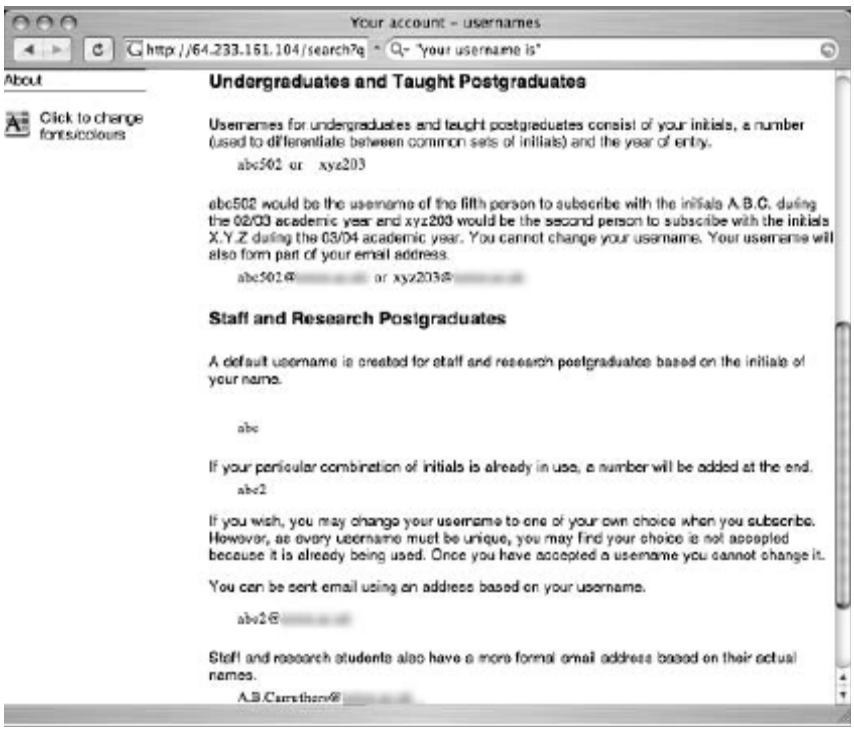
فهرست مطالب این بخش:

یافتن نام های کاربری، کلمات عبور و اطلاعات حساس دیگر

- **یافتن نام های کاربری یا Usernames**
- **جستجو برای یافتن کلمات عبور Passwords**
- **جستجو برای اطلاعات مالی و حسابداری**
- **جستجو برای اطلاعات حساس دیگر**
- **هک پایگاه داده ها از طریق گوگل**

جستجو برای نام های کاربری

امروزه مکانیسم اکثر مجوزهای ورود برای محافظت از اطلاعات بر اساس نام کاربری و کلمه عبور می باشد. روشهای زیادی برای کشف نام های کاربری وجود دارد که در فصول بعد طریقه شناسایی و کشف نام های کاربری از طریق پیغام های خطایی که از سوی پایگاه داده ها به ما داده می شود خواهیم پرداخت اما در این فصل به یافتن نام های کاربری یا username بر روی وب سرورها و همچنین برنامه های کاربردی با استفاده از پیغام های خطای تولید شده از سوی آنها خواهیم پرداخت. این پیغام های خطا گاهی اوقات شامل همین Username ها می باشد. این روش غیر مستقیم برای نام های کاربردی مفید است اما یک حمله کننده[1] با جستجوی ساده عبارت "your username is" به طور مستقیم نام های کاربری را بدست آورد. این صفحات صفحاتی می باشند که username شخص در آنها پردازش و توضیح داده می شود. به تصویر زیر در همین ارتباط توجه نمایید.



[1] Attacker

یک هکر از این username ها می تواند برای یافتن اطلاعات بیشتر از آن شخص استفاده کند . مانند جستجو در group ها یا لیست تلفن ها و غیره. همچنین username ها می توانند از طرق مختلف دیگر بدست آیند از قبیل کرم های[1] بر مبنای spam یا مهندسی اجتماعی[2] و موارد دیگر.

همچنین می تواند از منابع مختلف اقدام به جمع username ها کند.

جدول زیر موارد جستجوهای مختلف را برای یافتن username ها می باشد:

جستجو ها	توضیحات
`inurl:admin inurl:userlist`	**دریافت فایلهای userlist**
`inurl:admin filetype:asp inurl:userlist`	**دریافت فایلهای userlist**
`inurl:php inurl:hlstats intext:Server Username`	**فایلهای آماری** Half-life **لیست** username **ها و اطلاعات دیگر**
`filetype:ctl inurl:haccess.ctl Basic`	**نمایش اطلاعات اعتبارسنجی در** Microsoft FrontPage equivalent of htaccess
`filetype:reg reg intext:"internet account manager"`	Microsoft Internet Account Manager
`filetype:wab wab`	Microsoft Outlook Express Mail address books **دفترچه تلفن مربوط به برنامه آوتلوک**
`filetype:mdb inurl:profiles`	**تنظیمات شخصی مربوط به نرم افزار** Microsoft Access databases
`index.of perform.ini`	mIRC IRC ini file **شامل اطلاعات IRC و اطلاعات دیگر**

[1] worm
[2] Social engineering

inurl:root.asp?acs=anon	Outlook Mail Web Access directory
filetype:conf inurl:proftpd.conf -sample	فایهای پیکربندی PROFTP FTP server
filetype:log username putty	PUTTY SSH client logs
filetype:rdp rdp	Remote Desktop Connection فایلهای اعتبار سنجی در برنامه بالا
intitle:index.of .bash_history	UNIX bash shell history نام های کاربری اغلب در قالب آرگومانهای رشته ای ذخیره می شوند.
intitle:index.of .sh_history	دستورات موجود در **shell** سیستم عامل یونیکس (UNIX shell history) نام های کاربری اغلب در قالب آرگومانهای رشته ای ذخیره می شوند.
"index of " lck	لیست **Lock** فایل های متنوع
+intext:webalizer +intext:Total Usernames +intext:"Usage Statistics for"	صفحات آماری **webalizer** حاوی اطلاعات آماری و لیست **username** ها
filetype:reg reg HKEY_CURRENT_USER username	دریافت **username** ها از طریق رجیستری ویندوز

یکی از راه ها برای دریافت username ها در لیست های دایرکتوری نوشتن عبارات جستجوی زیر است:

intitle:index.of install.log

filetype:log inurl:install.log

گاهی اوقات username ها می توانند از برنامه های آماری تحت وب بدست آیند. این برنامه ها فعالیت های WEB را چک می کنند.

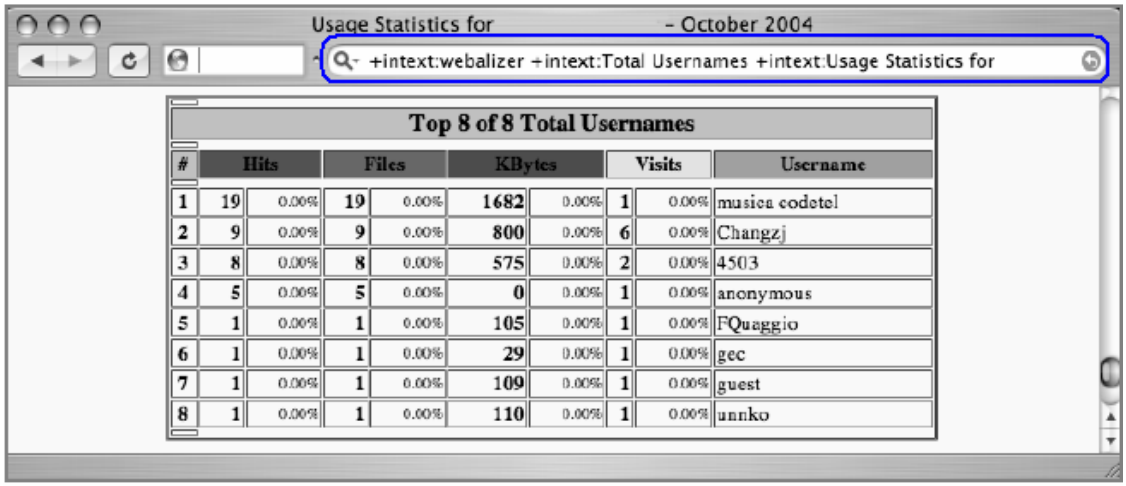
برنامه Webalizer اطلاعات مرتب شده را که توسط وب سرور استفاده می شود را نشان می دهد.

برای یافتن فایلهای خروجی برنامه Webalizer می توانید به صورت زیر جستجو کنید:

```
intext:webalizer intext:"Total Usernames" intext:"Usage Statistics for"
```

اکثر اطلاعات بدست آمده نام های کاربری هستند که کاربران برای ورود به وب سرور از آنها استفاده می کنند. (تصویر زیر)

The Webalizer Output Page Lists Web Usernames



Email:m.bashiry@gmail.com site:http://bashiry.250free.com

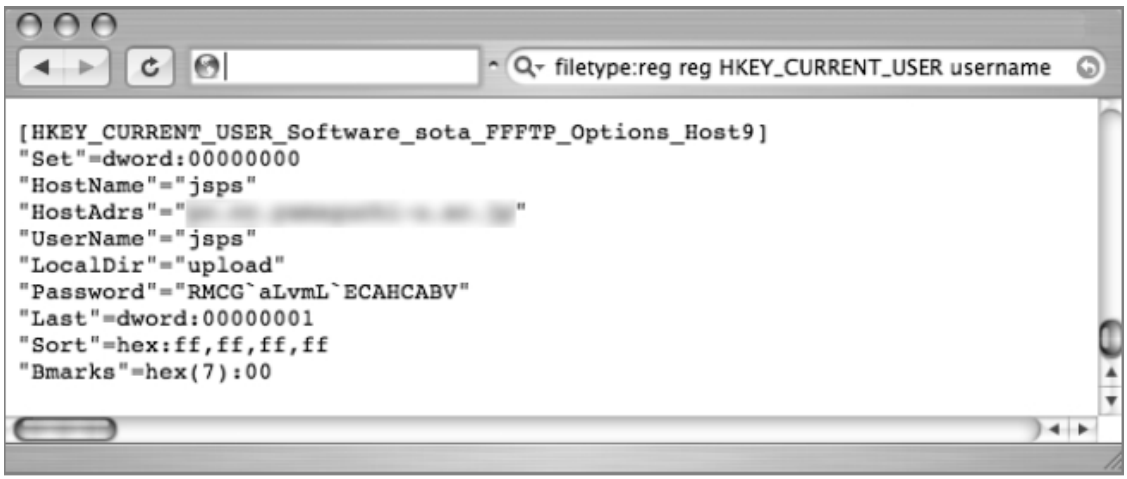
با این وجود در بعضی مواقع اطلاعات username ها درست نیستند و یا نامعتبرند. اما ستون visit در شکل بالا تعداد دفعاتی است که یک نام کاربری از حساب خود در آن دوره استفاده کرده است و همین امر می تواند به هکر برای تشخیص حسابهای کاربری درست از نادرست کمک بسیاری کند.

رجیستری ویندوز تمامی اطلاعات از قبیل username و password ها را در خود به طور مرتب شده‌ای نگهداری می کند.

هنگامی که این فایل ها یا همان فایلهای مربوط به رجیستری ویندوز برروی وب قرار می گیرند می توانید از طریق عبارت جستجوی زیر آنها را یافته (در حدود ۱۰۰ یافته) و از آنها استفاده کنید:

filetype:reg HKEY_CURRENT_USER username,

به تصویر جالب زیر دقت کنید:



مثالی دیگر:

در گوگل عبارت جستجوی inurl:root.asp?acs=anon برای یافتن پورتال[1] Microsoft Outlook Web Access استفاده کنید . با استفاده از این عبارت جستجو حدود ۵۰ سایت نشان داده خواهد شد (البته این نتیجه در زمانی است که این کتاب تالیف می شود) مطمئنا نتیجه ها از ۵۰ تا بیشتر می باشد . به تصویر زیر توجه کنید...

[1] Portal

Microsoft Outlook Web Access Hosts a Public Directory

یک public directory یا دایرکتوری عمومی به شما اجازه این را می دهد که به صفحات جستجو برای یافتن نامهای کاربران دسترسی داشته باشید. در این حالت جستجو از طریق کلمات wildcard امکان پذیر نیست.(قبلا گفتیم که عملگر * یکی از عملگرهای wildcard است) در نتیجه جستجو برای * لیست تمام کاربران را بر خلاف انتظار به ما نخواهد داد.

جستجو برای کلمات عبور (passwords)

password ها یکی از اهداف اصلی هکر برای نفوذ به یک سرور یا ماشین می باشد. متاسفانه عبارتهای جستجوی زیادی در گوگل وجود دارد که می توانند محل کلمات عبور را پیدا کنند.

جدول زیر حاوی عبارات جستجو برای یافتن کلمات عبور در گوگل می باشد:

عبارات جستجو	توضیحات
`inurl:/db/main.mdb`	ASP-Nuke passwords
`filetype:cfm "cfapplication name" password`	ColdFusion source with potential passwords

filetype:pass pass intext:userid	dbman credentials[1]
allinurl:auth_user_file.txt	DCForum user passwords
eggdrop filetype:user user	Eggdrop IRC user credentials
filetype:ini inurl:flashFXP.ini	FlashFXP FTP credentials
filetype:url +inurl:"ftp://"+inurl:"@"	FTP bookmarks cleartext passwords
inurl:zebra.conf intext: password -sample -test -tutorial -download	GNU Zebra passwords
filetype:htpasswd htpasswd	HTTP htpasswd Web user credentials
intitle:"Index of" ".htpasswd" "htgroup" -intitle:"dist" -apache -htpasswd.c	HTTP htpasswd Web user credentials
intitle:"Index of" ".htpasswd" htpasswd.bak	HTTP htpasswd Web user credentials
"http://:*@www" bob:bob*	**کلمات عبور** HTTP **یک نمونه ساده از نام کاربری است** Bob
"sets mode: +k"	IRC channel keys (passwords)
*"Your password is * Remember this for later use"*	IRC NickServ registration passwords
signin filetype:url	**مجوزهای اعتبارسنجی** javascript
LeapFTP intitle:"index.of./" sites.ini modified	LeapFTP client login credentials
inurl:lilo.conf filetype:conf password -tatercounter2000 -bootpwd -man	LILO passwords

[1] اعتبار ستجی - اعتبارنامه

filetype:config config intext: appSettings "User ID"	Microsoft .NET application credentials
filetype:pwd service	Microsoft FrontPage Service Web passwords
intitle:index.of dministrators.pwd	Microsoft FrontPage Web credentials
"# -FrontPage-" inurl:service.pwd	Microsoft FrontPage Web passwords
ext:pwd inurl:_vti_pvt inurl: (Service | authors | administrators)	Microsoft FrontPage Web passwords
inurl:perform filetype:ini	mIRC nickserv credentials
intitle:"index of" intext: connect.inc	mySQL database credentials
intitle:"index of" intext: globals.inc	mySQL database credentials
filetype:conf oekakibbs	Oekakibss user passwords
filetype:dat wand.dat	Opera, ÄúMagic Wand,Äù Web credentials
inurl:ospfd.conf intext:password -sample -test -tutorial -download	OSPF Daemon Passwords
index.of passlist	Passlist user credentials
inurl:passlist.txt	passlist.txt file user credentials
filetype:dat "password.dat"	password.dat files
inurl:password.log filetype:log	password.log file reveals usernames, passwords, and hostnames

filetype:log inurl:"password.log"	password.log files cleartext passwords
inurl:people.lst filetype:lst	People.lst generic password file
intitle:index.of config.php	PHP Configuration File database credentials
inurl:config.php dbuname dbpass	PHP Configuration File database credentials
inurl:nuke filetype:sql	PHP-Nuke credentials
filetype:conf inurl:psybnc.conf "USER.PASS="	psyBNC IRC user credentials
filetype:ini ServUDaemon	servU FTP Daemon credentials
filetype:conf slapd.conf	slapd configuration files root password
inurl:"slapd.conf" intext: "credentials" -manpage -"Manual Page" -man: -sample	slapd LDAP credentials
inurl:"slapd.conf" intext: "rootpw" -manpage -"Manual Page" -man: -sample	slapd LDAP root password
filetype:sql "IDENTIFIED BY" -cvs	SQL passwords
filetype:sql password	SQL passwords
filetype:ini wcx_ftp	Total Commander FTP passwords
filetype:netrc password	UNIX .netrc user credentials
index.of.etc	UNIX /etc directories contain various credential files

intitle:"Index of..etc" passwd	UNIX /etc/passwd user credentials
intitle:index.of passwd passwd.bak	UNIX /etc/passwd user credentials
intitle:"Index of" pwd.db	UNIX /etc/pwd.db credentials
intitle:Index.of etc shadow	UNIX /etc/shadow user credentials
intitle:index.of master.passwd	UNIX master.passwd user credentials
intitle:"Index of" spwd.db passwd -pam.conf	UNIX spwd.db credentials
filetype:bak inurl:"htaccess|passwd|shadow|htusers	UNIX various password file backups
filetype:inc dbconn	Various database credentials
filetype:inc intext:mysql_connect	Various database credentials, server names
filetype:properties inurl:db intext:password	Various database credentials, server names
inurl:vtund.conf intext:pass -cvs	Virtual Tunnel Daemon passwords
inurl:"wvdial.conf" intext: "password"	wdial dialup user credentials
filetype:mdb wwforum	Web Wiz Forums Web credentials
"AutoCreate=TRUE password="*	Website Access Analyzer user passwords
filetype:pwl pwl	Windows Password List user credentials

`filetype:reg reg +intext: "defaultusername" intext: "defaultpassword"`	Windows Registry Keys containing usercredentials
`filetype:reg reg +intext: "internet account manager"`	Windows Registry Keys containing user credentials
`"index of/" "ws_ftp.ini" "parent directory"`	WS_FTP FTP credentials
`filetype:ini ws_ftp pwd`	WS_FTP FTP user credentials
`inurl:/wwwboard`	wwwboard user credentials

کلمات عبور پیدا شده در بیشتر اوقات پنهانی[1] (انکریپت شده) و یا درهم شده یا رمز گذاری[2] شده می باشند. حال با توجه به اینکه این کلمات عبور رمز گذاری شده اند آنها را می توان با یک جستجو کننده کلمات عبور که معروفترین آنها نرم افزار John the Ripper می باشد. این نرم افزار در سایت www.openwall.com/john قابل بارگذاری[3] است. در شکل زیر نتیجه یکی از جستجو ها برای عبارت زیر آورده شده است.

ext:pwd inurl:_vti_pvt inurl:(Service | authors | administrators),

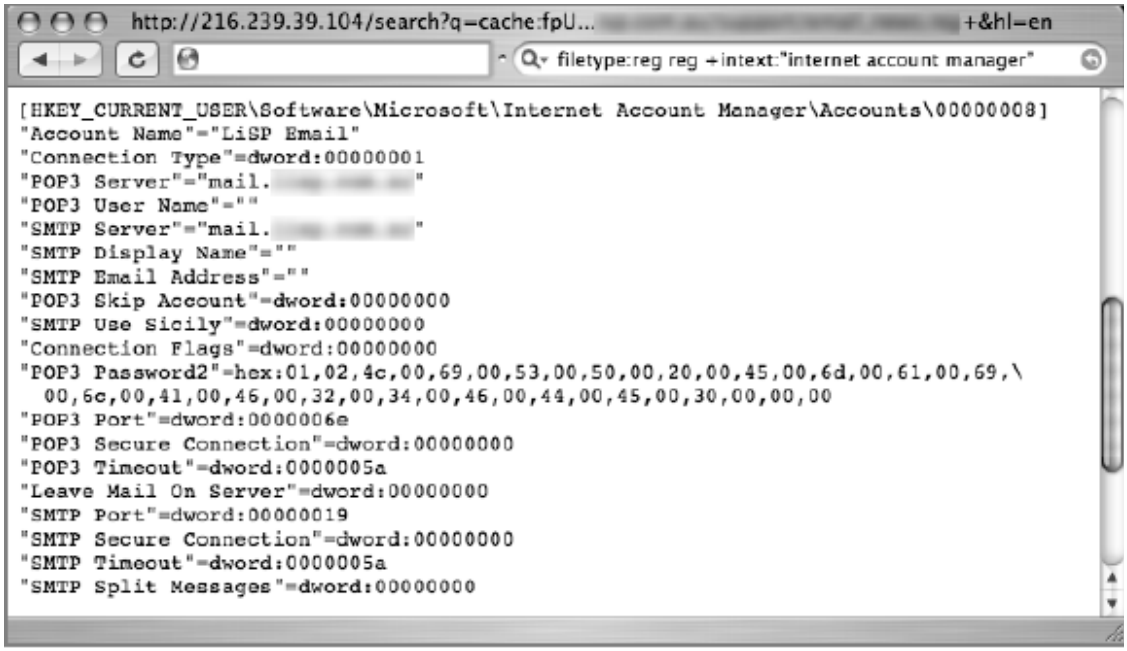
این جستجوی ترکیبی برخی فایل های نرم افزار Microsoft front page را بر خواهد گرداند.

[1] Encrypted

[2] encoded

[3] download

فایلهای صادر شده یا پشتیبان رجیستری ویندوز در بیشتر موارد شامل کلمات عبـور رمزگـذاری شده است. این فایل ها را با جستجوی عبارت *filetype:reg intext:"internet account manager"* در گوگل می توان یافت و می توانند شامل اطلاعات جالبی باشند. به تـصویر زیـر در همـین ارتبـاط توجه نمایید.



تصویر زیر توسط یک عبارت جستجو در گوگل به دست آمده که حاوی کلمات عبور، cleartext ها، نام های کاربری و hostname ها می باشد. که یک host از آنها برای مجوز ورود استفاده می کند.

این عبارات جستجو عبارات عجیب غریب و جادویی نیستند !! و یک هکر باهوش به راحتی می تواند آن عبارات را نوشته و به دنبال کلمات عبور بگردد. مثلا عبارت

"Your password" forgot

این صفحات شامل صفحاتی است که سعی بر بازگردانی کلمات عبور برای آن کاربر را دارند. توجه داشته باشید که برای این گونه کلمات عبور مهندسی اجتماعی بسیار می تواند مفید واقع شود.

یک نمونه دیگر جستجو برای دریافت کلمات عبور می تواند به صورت زیر باشد:

intext:(password | passcode | pass) intext:(username | userid | user)

این عبارت حاوی لغات رایج برای کلمات عبور وuserid می باشد. اکثر نتایج ظاهر شده در عبارت فوق حاوی صفحات " کلمات عبور فراموش شده" می باشند و شامل لیستی از کلمات عبور در خود هستند حتی اگر کلمات عبوری هم نباشد حاوی لینک ها و یا اطلاعات تماس جالبی می باشند.

همچنین برای یافتن کلمات عبور هم می توان از سرویس ترجمه گوگل استفاده کرد. همانطور که در فصول قبل ذکر شده این سرویس در آدرس زیر قابل دسترسی است:

http://translate.google.com/translate_t

جدول زیر ترجمه های انگلیسی برای کلمه password است:

Language	Word	Translation
German	password	Kennwort
Spanish	password	contraseña
French	password	mot de passe
Italian	password	parola d'accesso
Portuguese	password	senha
Dutch	password	Paswoord

به طور مثال اگر به جدول بالا نگاهی بیندازید کلمه password در انگلیسی معادل paswoord در زبان هلندی است.

Note: کلمه username و userid در بیشتر زبانها به شکل خودشان ترجمه می شود.

جستجو برای اطلاعات مالی یا حسابداری

امروزه با گسترش کامپیوترهای شخصی هزاران برنامه مالی شخصی تولید شده. بسیاری از این برنامه های مالی فایلهایی با پسوند های مخصوص به خود ایجاد می کنند که این پسوندها میتوانند توسط گوگل مورد جستجو قرار گیرد.

در جدول زیر لیست اینگونه پسوندها به همراه توضیح مختصری آورده شده است.

پسوند فایل	توضیحات
Afm	برنامه مدیریت مالی Abassis
zb4	فایلهای حسابداری و تجاری
mmw	فایلهای AceMoney
lqd	گزارشات وجوه مالیاتی AmeriCalc Mutual
et2	فایلهای امنیتی مالیات های الکترونیکی(استرالیا)
tax	Intuit TurboTax Tax Return
t98-t04	Kiplinger Tax Cut File (extension based on two-digit return year)
mny	فایلهای پولی داده ای از Microsoft Money 2004
mbf	فایلهای پشتیبان Microsoft Money
inv	فایلهای سرمایه گذاری MSN Money
ptdb	پایگاه داده ای حسابداریPeachtree
qbb	فایلهای مالی QuickBooks که اطلاعات مالی را فاش می کند
qdf	اطلاعات مالی شخصی Quicken
soa	نرم افزار حسابداری Sage MAS 90

sdb	حسابداری ساده
stx	فرمهای حسابداری ساده
tmd	زمان و ردیابی هزینه یا Time and Expense Tracking
tls	زمان نامناسب و هزینه ها
fec	U.S. Federal Campaign Expense Submission
wow	فایلهای حسابداری Wings

جستجو برای اطلاعات حساس دیگر

گوگل می تواند به عنوان محل همه اطلاعات مرتب شده حساس استفاده شود. در این بخش بـه بررسی چگونگی یافتن اینگونه اطلاعات می پردازیم. این اطلاعات می توانند شامل دفترچه تلفن هـا، فایل های log در چت و گزارش آسیب پذیری سرورها و غیره باشند.

در جدول زیر عبارات جستجو برای یافتن اطلاعات حساس گردآوری شده است.

عبارات جستجو	توضیحات
*intext:"Session Start * * * *:*:* *" filetype:log*	فایلهای log، AIM و IRC
filetype:blt blt +intext: screenname	AIM buddy lists
buddylist.blt	AIM buddy lists
intitle:index.of cgiirc.config	CGIIRC (Web-based IRC client) config file,shows IRC servers and user credentials
inurl:cgiirc.config	CGIIRC (Web-based IRC client) config file,shows IRC servers and user credentials

“Index of” / “chat/logs”	فایلهای log در چت
intitle:”Index Of” cookies.txt “size”	cookies.txt file reveals user information
*“phone * * *” “address *” “e-mail” intitle:”curriculum vitae”*	Curriculum vitae (resumes) reveal names and address information
ext:ini intext:env.ini	Generic environment data
intitle:index.of inbox	Generic mailbox files
“Running in Child mode”	Gnutella client data and statistics
“:8080” “:3128” “:80” filetype:txt	لیستهای پروکسی HTTP
intitle:”Index of” dbconvert.exe chats	ICQ chat logs
“sets mode: +p”	کانالهای اطلاعات خصوصی IRC
“sets mode: +s”	کانالهای اطلاعات محرمانه IRC
“Host Vulnerability Summary Report”	گزارشات نرم افزار ISS vulnerability scanner
“Network Vulnerability Assessment Report”	آسیب پذیری های نهانی روی میزبانها و شبکه ها
filetype:pot inurl:john.pot	نتایج نرم افزار کشف رمز و کرک کننده رمز John the Ripper
intitle:”Index Of” -inurl:maillog maillog size	Maillog files reveals e-mail traffic information
ext:mdb inurl:.mdb inurl:fpdb shop.mdb*	پوشه های پایگاه داده نرم افزار طراحی صفحات وب Front Page
filetype:xls inurl:contact	اطلاعات تماس از کاربرگ های نرم افزار Excel محصول شرکت مایکروسافت
intitle:index.of haccess.ctl	Microsoft FrontPage equivalent(?)of htaccess shows Web authentication info
ext:log “Software: Microsoft Internet	Microsoft Internet Information

*Information Services *.*"*	Services (IIS) log files
filetype:pst inurl:"outlook.pst"	فایلهای پشتیبان Microsoft Outlook e-mail and calendar
intitle:index.of mt-db-pass.cgi	فایلهای پیش فرض Movable Type
filetype:ctt ctt messenger	لیست اطلاعات MSN Messenger
"This file was generated by Nessus"	گزارشات پویشگر آسیب پذیر نرم افزار NESSUS در هاست ها و شبکه ها
inurl:"newsletter/admin/"	اطلاعات مدیران روزنامه ها
inurl:"newsletter/admin/" *intitle:"newsletter admin"*	اطلاعات مدیران روزنامه ها
filetype:eml eml intext: *"Subject" +From*	فایلهای ایمیل Outlook Express
intitle:index.of inbox dbx	Outlook Express Mailbox files
intitle:index.of inbox dbx	Outlook Express Mailbox files
filetype:mbx mbx intext:Subject	Outlook v1–v4 or Eudora mailbox files
inurl:/public/?Cmd=contents	پوشه های عمومی یا ملاقات های نرم افزار Outlook Web Access
filetype:pdb pdb backup (Pilot *| Pluckerdb)*	فایلهای پایگاه داده های Palm Pilot Hotsync
"This is a Shareaza Node"	اطلاعات و آمار کلاینت Shareaza
inurl:/_layouts/settings	اطلاعات پیکربندی Sharepoint
inurl:ssl.conf filetype:conf	فایلهای پیکربندی SSL
site:edu admin grades	نمرات دانشجویان
intitle:index.of mystuff.xml	Trillian user Web links
inurl:forward filetype:forward –cvs	UNIX mail forward files reveal e-mail addresses

intitle:index.of dead.letter	ایمیل های ناتمام UNIX
filetype:conf inurl:unrealircd. conf -cvs –gentoo	UnrealIRCd config file reveals configuration information
filetype:bkf bkf	فایلهای پشتیبان ویندوزهای xp یا 2000

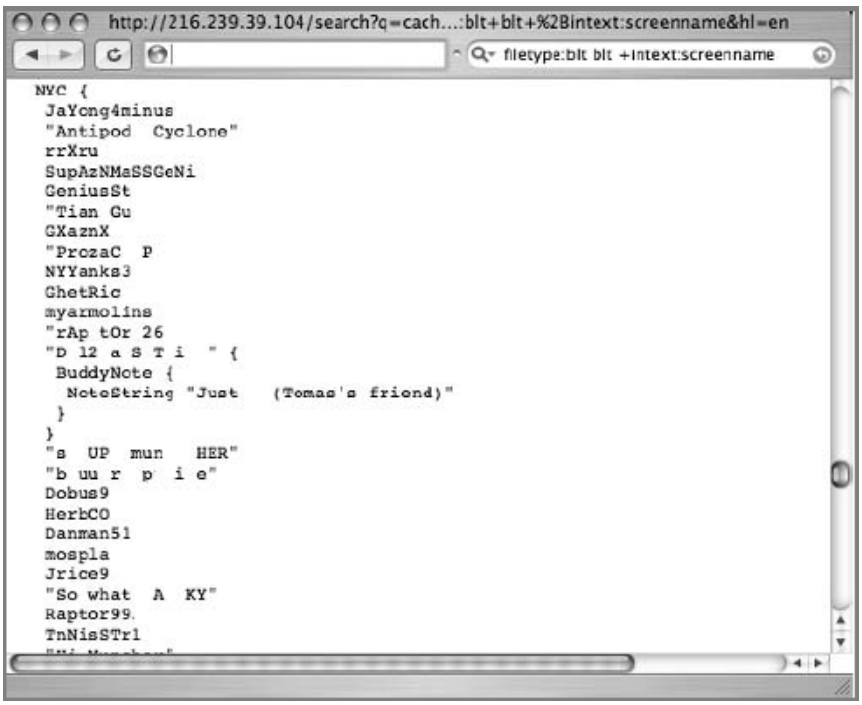
کار با بعضی از این عبارات جستجو واقعا ساده است بطور مثال لیست تماسهای مسنجر MSN می تواند با جستجو کردن عبارت زیر در گوگل بدست آید:

filetype:ctt messenger

و یا لیستBuddy های مسنجر AOL [1] که می تواند توسط عبارت جستجوی زیر در گوگل یافت شود:

filetype:blt blt +intext:screenname

به تصویر زیر توجه نمایید:



[1] AOL instant Messenger(AIM)

یک هکر با استفاده از اطلاعات بالا می توان اقدام به تکنیک مهندسی اجتماعی برای دوست نشان دادن خود به هدف استفاده کند.

به مثال دیگر توجه کنید: فایلهای خروجی نرم افزار پویشگر شبکه NESSUS[1] را به دقت بررسی کنید. این نرم افزار یکی از نرم افزار های پویشگر شبکه open-source است که حاوی یکسری ابزار جهت بررسی تست امنیت یک شبکه می باشد و بعد از تست آسیب پذیری ها گزارشاتی را ارائه می دهد. یک هکر از این اطلاعات و یا گزارشات میتواند برای مقاصد خود استفاده کند. حال با این همه تفاسیر نحوه یافتن گزارشات این نرم افزار پر قدرت در زیر آورده شده است:

نحوه جستجو به صورت روبرو می باشد :

"This file was generated by Nessus"

تصویر زیر یک نمونه از این گزارشات می باشد که حاوی آدرس های IP به ازای تست هر ماشین و همچنین گزارش کاملی از آسیب پذیری های آن ماشین ها می باشد.

[1] www.nessus.org

آسیب پذیری های ارائه شده اکثرا قابل اکسپلویت شدن هستند و هکر می تواند با به دست آوردن exploit ها و یا نوشتن این کد های مخرب اقدام به نفوذ به ماشین مقابل نماید.

هک کردن پایگاه داده ها در گوگل(GHDB)- googledorks

در جدول زیر که از سایت J0hny آمده یکسری از جستجوهای عمومی و همچنین تازه ترین جستجو ها در گوگل لیست شده‌اند که واقعاً جستجو های جالبی هستند. این جستجو ها بیشتر برای هک کردن پایگاه داده ها (Database) سایت ها بکار می رود و در اصطلاح به این نوع جستجوgoogledorks گفته می شود.

به چگونگی جستجو در جدول زیر توجه کنید نکات مفید و آموزنده ای یاد خواهید گرفت.

Welcome to the Google Hacking Database (GHDB)!

We call them 'googledorks' (gOO gÃ´l'DÃ´rk, noun, slang) : An inept or foolish person as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe! Stop by our forums to see where the magic happens!

10 most popular entries	10 most recent entries
1) "http://*:*@www" domainname	1) "admin account info" filetype:log
2) index.of.password	2) "Warning: Supplied argument is not a valid File-Handle resource in"
3) "access denied for user" "using password"	3) "Maintained with Subscribe Me 2.044.09p"+"Professional" inurl:"s.pl"
4) "AutoCreate=TRUE password=*"	4) "Warning:" "SAFE MODE Restriction in effect." "The script whose uid is" "is not allowed to access owned by uid 0 in" "on line"
5) The Master List	5) intitle:"Admin Login" "admin login" "blogware"
6) "# -FrontPage-" ext:pwd inurl:(service | authors | administrators | users) "# -FrontPage-" inurl:service.pwd	6) intitle:"net2ftp" "powered by net2ftp" inurl:ftp OR intext:login OR inurl:login
7) passlist.txt (a better way)	7) "your password is" filetype:log
8) "A syntax error has occurred" filetype:ihtml	8) "Powered by GTChat 0.95"+"User Login"+"Remember my login information"
9) auth_user_file.txt	9) http://www.google.com/search?q=intitle:%22WEB//NEWS+Personal+Newsmanagement%22+intext:%22%C2%A9+2002-2004+by+Christian+Scheb+-+Stylemotion.de%22%2B%22

10) allinurl: admin mdb	**10) inurl:/modcp/ intext:Moderator+vBulletin**

فصل پنجم
۹ نوع جستجوی امنیتی ساده

مطالب این فصل:

- site
- intitle:index.of
- error | warning
- login | logon
- username | userid | employee.ID | “your username is”
- password | passcode | “your password is”
- admin | administrator
- –ext:html –ext:htm –ext:shtml –ext:asp –ext:php
- inurl:temp | inurl:tmp | inurl:backup | inurl:bak

مقدمه:

با وجود این همه عبارات مختلف برای جستجو در گوگل دانستن اینکه در یک مدت زمان کم بهترین عبارت جستجو را بنویسیم و با استفاده از آن به بهترین نتیجه دست یافت امری مهم و ضروریست.

در این فصل به بررسی ۱۰ نوع از این عبارات که برای تشخیص امنیت خیلی خوب هستند خواهم پرداخت.

Site

عملگر Site در طی تشخیص و جمع آوری اطلاعات فوق العاده است. اگر با یک host یا domain ترکیب شود نتایجی بسیار جالب را به همراه خواهد داشت. در فصول قبلی به توضیحات کامل این عملگر پرداخته شده است. در حالت کلی این عملگر به طور میانگین در جستجوهای ساده و پایه استفاده می شود.

به مثال ساده زیر و تصویر آن توجه کنید:

site:washingtonpost.com –site:www.washingtonpost.com

همانطور که از عبارت جستجو بر می آید و همچنین استفاده از عملگر – برای جستجو می توان فهمید که آدرس های پیدا شده شامل www نباید باشند . پس آدرس های پیدا شده در این مثال خاص مانند زیر خواهند بود:

yp.washingtonpost.com/E/V/WASDC/0015/60/65/3.html - Similar pages

eg.washingtonpost.com/user_review?mode=request_

washingtonpost.com/wp-srv/national/colawars032399.htm - Similar pages

topics.washingtonpost.com/wp-srv/ topics/crime-law-and-justice/justice-a

همانگونه که از خطوط فوق پیداست سه حوزه (Domain) به ترتیب زیر پیدا شدند:

yp.washingtonpost.com

eg.washingtonpost.com

topics.washingtonpost.com

همچنین یکی از نتایج نام سرور بدون عبارت www است (washingtonpost.com).

یک جستجوی DNS به راحتی نقاطی را که دارای IP یکسانی د ر washingtonpost.com هستند را آشکار خواهد کرد. (حتما متوجه کاربرد این عملگر شدید).

Intitle:index.of

این عملگر یکی از عملگرهای عمومی برای یافتن directory listings است. بیشتر یافته ها یافته های مبتنی بر سرورهای آپاچی هستند . (قبلا به تفصیل توضیح داده شده است.)

Error | warning

از پیامهای خطا ظاهر شده در نتایج می توانیم اطلاعات مفیدی را از مقصد به دست آوریم. اغلب این خطاها حاوی موارد زیر می توانند باشند:

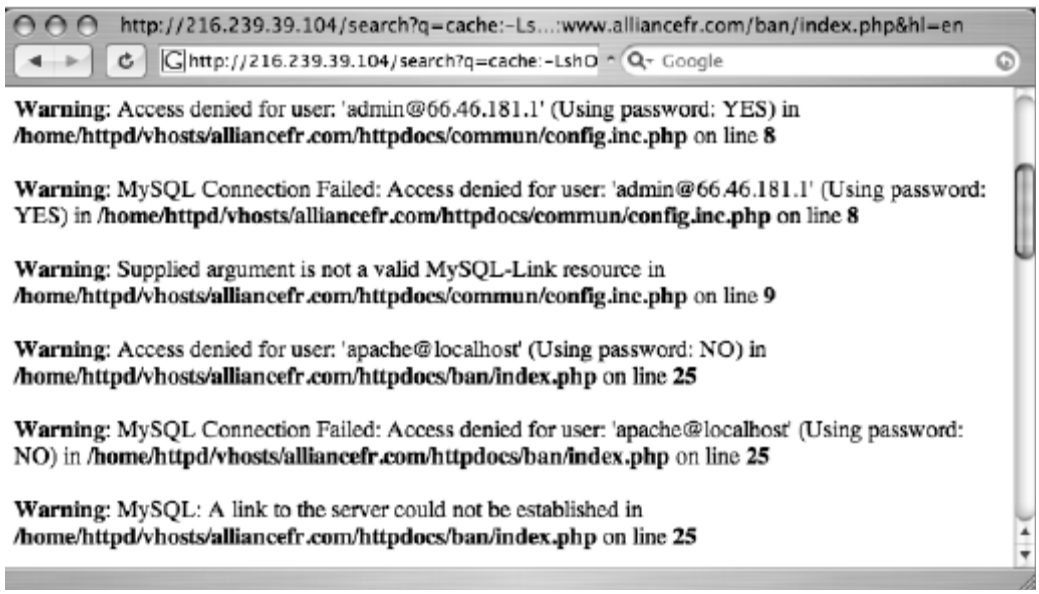
- معماری شبکه
- نام کاربران متصل به شبکه و یا آنلاین
- نوع سیستم عامل و برنامه های کاربردی روی آن
- و ...

هیچکدام از پیامهای خطا مفید نیستند و تعداد آن نیز زیاد می باشد. یک جستجوی ساده در گوگل برای عبارت جستجوی intitle:error همانطور که در تصویر زیر دیده می شود بیش از ۵۵ میلیون نتیجه در بر خواهد داشت:

همانطور که در زیر نشان داده شده است می توان با عبارت جستجوی

“access denied for user” “using password”

صفحات خطای SQL را نمایش داد.



همانطور که در تصویر بالا ملاحظه می کنید حاوی اطلاعات زیر است:

- Username ها (نام های کاربری)
- Filename ها (اسامی فایلها)
- Path information مسیرهای اطلاعات

- IP Address آدرسهای آی پی
- و غیره

Login | Logon

همانطور که در دروس گذشته توضیح داده شد یک فرم login همانند درب جلویی یک سایت می باشد. صفحات ورود نرم افزار و سیستم عامل هدف را برمی گرداند. در تعداد زیادی از این صفحات لینکی برای کاربرانی که در ورود به سیستم خود دچار مشکل شده اند به چشم می خورد و این لینک ها حاوی اسنادی برای کمک به کاربر می باشد. اگر کاربری کلمه عبور خود را فراموش کند این صفحه می تواند به او برای یافتن کلمه عبورش کمک نماید و همین امر موجب می شود که هکرها برای بدست آوردن اطلاعات و ورود به سایت از این صفحات استفاده نمایند.

بیشتر اوقات کلمات عبور فراموش شده در صفحات ورود به سایت به یک آدرس ایمیل یا شماره تلفن شخص و یا به آدرس URL سایت خاصی برای به خاطر آوردن پسفورد ارسال می شوند. (مهندسی اجتماعی اینجا خیلی به درد می خوره).

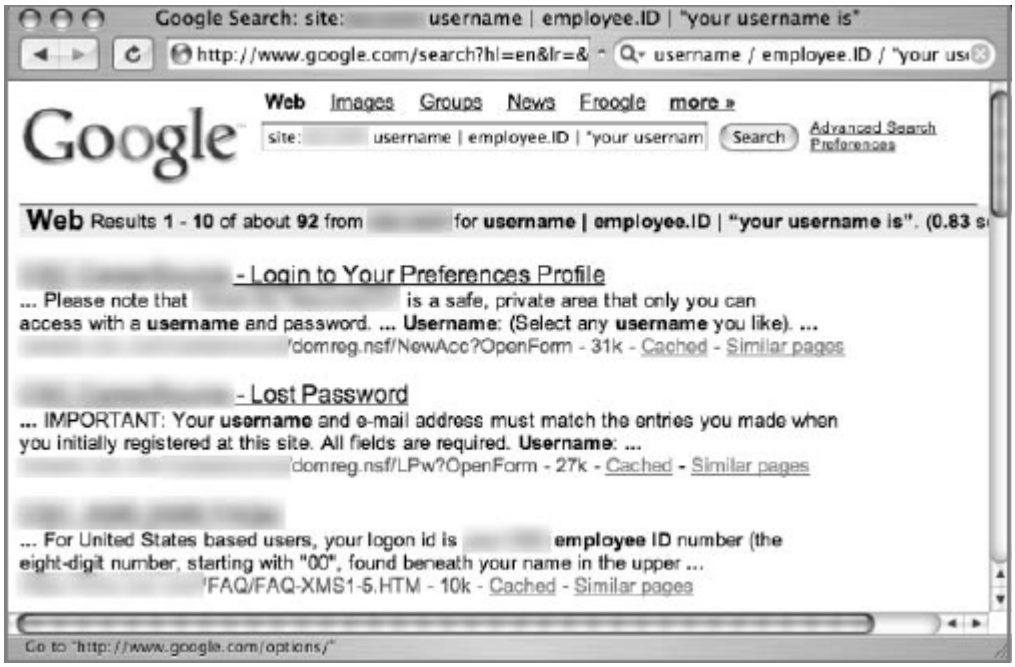
تصویر زیر تصویر مربوط به عبارت جستجوی login | logon در گول است که بیش از ۱۲ میلیون صفحه برگردانده شده است.

توجه داشته باشید که بسیاری از نتایج اولیه در متن صفحات کلمه login trouble وجود دارد.

username | userid | employee.ID | "your username is"

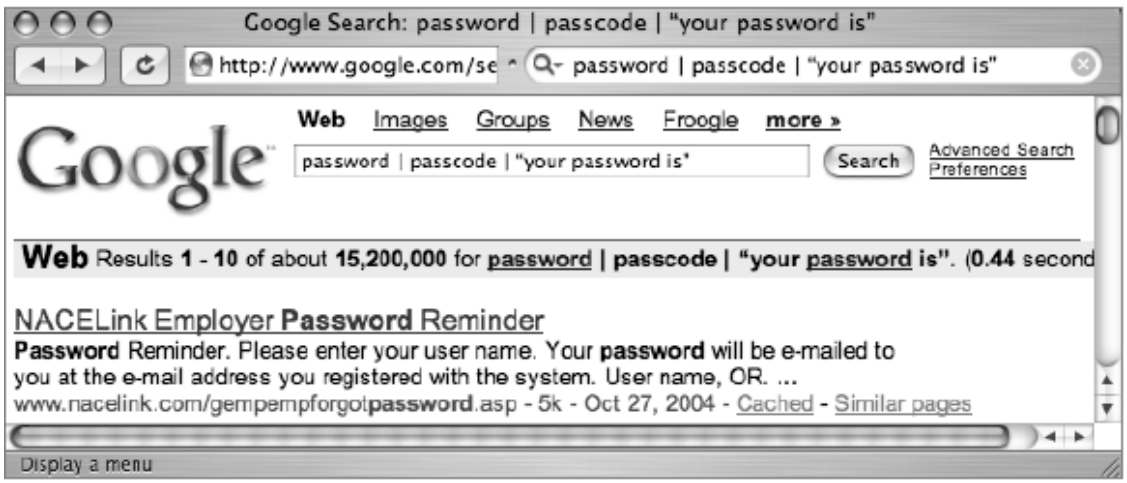
همانطور که در دروس قبل گفتیم راه های بسیاری برای بدست آوردن username ها وجود داشت.

Username ها نصفی از دسترسی کامل به یک سایت هستند. (نصفی دیگر کلمه عبور است).



Password | passcode | "your password is"

کلمه password در اینترنت جزو یکی از کلمات رایج است به طوری در یک جستجوی ساده بیش از ۷۳ میلیون نتیجه پیدا خواهد شد.

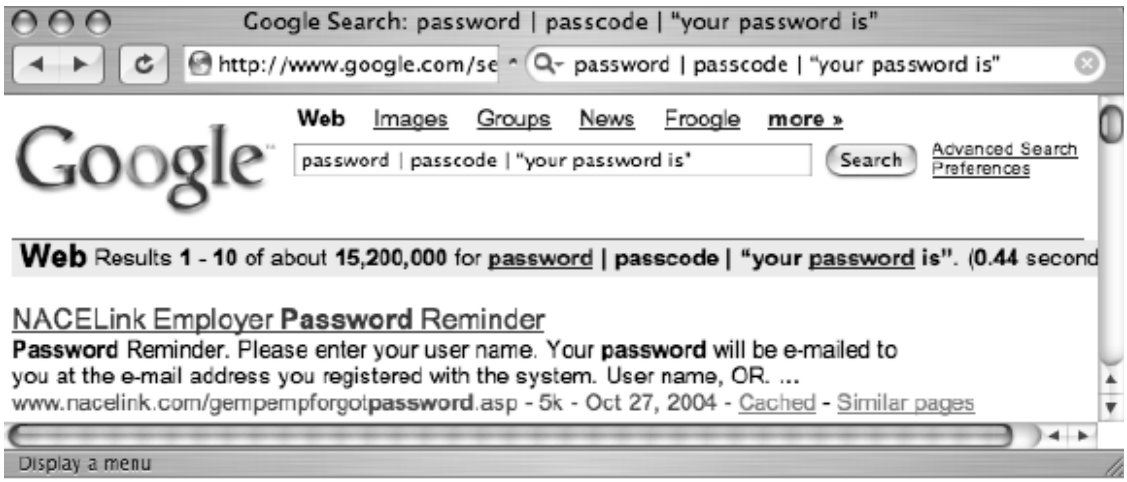


پیدا کردن سایت مورد نظر از بین این همه نتیجه کار دشواری است پس برای رفع این مشکل از عملگر Site استفاده می کنیم و نتایجی که با استفاده از این عملگر ظاهر می شوند شامل صفحاتی می باشند که به کاربر کمک می کنند که کلمه عبور گم شده خود را پیدا کنند. (طریقه پیدا کردن این صفحات در همین کتاب در فصل جداگانه ای توضیح داده شده است).

Admin | administrator

کلمه administrator غالبا به شخصی اطلاق می شود که مدیریت شبکه ای را بر عهده دارد. در اینترنت منابع زیادی وجود دارند که حاوی این دو کلمه هستند مثلا در یک جستجو برای این کلمه بیشتر از ۱۵ میلیون نتیجه یافت می شود.

مانند حالت قبل باید برای کاهش تعداد یافته ها از عملگر Site استفاده کنیم و برای یک سایت خاص به دنبال این کلمه بگردیم . به خطا در شکل زیر توجه کنید ←



عبارت Contact your administrator یک عبارت رایج خوب در وب است که دارای چندین اشتقاق است. یکی از آنها را می توان با عبارت جستجوی

"Please contact your * administrator"

بدست آورد. عبارت جستجوی بالا Company یا شرکت ها یا سازمان و اداره یا سایت یا سیستم سرور شبکه، پایگاه داده ها، آدرس پست الکترونیک و حتی مدیران تنیس را هم می تواند پیدا کند و در اختیار جستجوگر قرار دهد.

یک عبارت جستجو برای "administrative login" و یا "admin login" می تواند صفحات ورود به سایت را به ما بدهد.

-ext:html –ext:htm –ext:shtml –ext:asp –ext:php

کلمه ext مترادف با عملگر filetype است. در اصل در عبارت جستجوی بالا تمامی صفحاتی که پسوند html، htm، shtml، asp و php را دارد کنار می گذارد و در آنها جستجو نمی کند. پس چه صفحاتی را به ما می دهد؟ به تصویر توجه کنید←

البته از عملگر site برای محدود کردن نتیجه برای یک سایت استفاده شده است.

همانطور که در تصویر بالا مشاهده می کنید در اولین نتیجه یک صفحه با پسوند aspx نمـایش داده شده است. پس در ابتدا این پسوند را هم کم می کنیم تا دیگر این صـفحات اینترنـت در آن سـایت مورد جستجو قرار نگیرند.

در تصویر مسیرهای جالبی پیدا شدند که می توانید از این مسیرها استفاده کنید.

مثلا:

/research/files/summaries

/event/archives/strategiesNAM2003 آرشیو مثلا سال ۲۰۰۳ و ...

فایلهای پیدا شده با پسوند PDF، ppt و .. می باشند. ☺

کاربردهای این عبارت جستجو بسیار جالب است و فقط با کمی تجربه می توانید کار بـا ایـن عبـارت جستجو را و استفاده از نتایج ظاهر شده را فرا بگیرید.

inurl:temp | inurl:tmp | inurl:backup | inurl:bak

استفاده از عبارت جستجوی بالا به همراه عملگر site صفحاتی را پیدا می کند که شامل موارد زیر باشند:

۱) فایلهای موقت یا پشتیبان temporary or backup files

۲) مسیرهای روی یک سرور

اگر چه این عبارت جستجو فقط متوجه فایلها و مسیرهای پشتیبان یا موقت هستند می توان کلمات رایج را در آن به کار برد و از آن استفاده کرد. همچنین استفاده از عملگر inurl برای یافتن پسوند ها مانند index.html.bak می تواند مفید باشد.

فصل ششم

یافتن محل اکسپلویت ها و پیدا کردن نقاط آسیب پذیری روی اهداف

مقدمه

یافتن محل اکسپلویت ها

یافتن محل سایت های دارای اکسپلویت های عمومی

یافتن محل اکسپلویتها از طریق کدهای رشته ای رایج

یافتن محل آسیب پذیری روی اهداف

مقدمه

کد های اکسپلویت[1] یا بطور کلی اکسپلویت‌ها ابزار حیاتی برای یک هکر هستند. این کد ها برای نفوذ به یک مقصد استفاده می شوند. گاهی اوقات به این کدها کدهای مخرب هم می گویند که ما در این کتاب از همان واژه اکسپلویت استفاده می کنیم. اکثر هکرها مجموعه ای از این کدها را دارند و در مواقع لزوم و با استفاده از آن اقدام به هک می کنند. بعضی از اکسپلویت ها – (Zero day 0dat) برای مدت زمانی به صورت مخفی یا در اصطلاح هکرها زیر زمینی باقی می مانند تا از سوی یک یا چند سایت و یا گروه های خبری در شبکه جهانی اینترنت share ویا public شود.

بعضی از سایت ها اقدام به توزیع اینگونه کدها در سایت های خود می‌کنند و همین نکته باعث می شود که ما بتوانیم از طریق گوگل به یافتن ایم ابزارها یا کدها بپردازیم.

در این فصل ما محل اکسپلویت ها را جستجو می کنیم تا بتوانیم از طریق آسیب پذیریهایی که روی ماشین های مقصد وجود دارد به آنها نفوذ کنیم.

یافتن محل اکسپلویتها

سایت های بسیار زیادی تصمیم به انتشار اکسپلویتها در شبکه جهانی اینترنت کردند. هکرهای کلاه سیاه این کدها را برای کمک به خود و راحتی کارشان در هک تولید می کنند و هکرهای کلاه سفید از این کدها در جنبه مثبت استفاده می کنند و بیشتر برای هشدار به مدیران شبکه ها استفاده می کنند. یک نمونه جستجو در گوگل می تواند به صورت جستجوی کلمات یا عبارات Remote exploit و یا vulnerable exploit باشد. نمونه دیگری می تواند به صورت

[1] Exploit Code

inurl:0day باشد که استفاده این عبارت جستجو به خوبی استفاده از inurl:sploits نیست.

(sploit اصطلاح قدیمی تر 0day می باشد)

یافتن محل سایت های دارای اکسپلویت های عمومی [1]

یکی از راه های پیدا کردن این کدهای منبع یا Source code جستجو در پسوند این کدها است و همانطور که میدانید این کدها با زبان برنامه نویسی های گوناگون نوشته می شوند که پرکاربردترین و بیشترین زبانی که مورد استفاده می‌گردد زبان برنامه نویسی C می باشد. فایل های این زبان دارای پسوند .c می باشند.

جستجوی مقابل در حدود ۵۰۰۰۰۰ نتیجه به ما می دهد: filetype:c c

پس متوجه می شویم که جستجو را باید محدودتر کنیم. لذا عبارت filetype:c exploit را مورد جستجو قرار می دهیم که تعداد نتایج حدود ۵۰۰۰ را به ما می دهد. با استفاده از تکنیک page-scraping می توانیم این سایت ها را با اجرا کردن دستور زیر در یونیکس ایزوله کنیم:

```
grep Cached exp | awk -F" -" '{print $1}' | sort -u
```

جدول زیر بیشترین نتایج رایج برای جستجوی عبارت *filetype:c exploit* در گوگل است:

سایت	مسیر یا دایرکتوری
packetstorm.linuxsecurity.com	packetstorm.linuxsecurity.com/0101-exploits/
synnergy.net	synnergy.net/downloads/exploits/
unsecure.altervista.org	unsecure.altervista.org/security/
www.blacksheepnetworks.com	www.blacksheepnetworks.com/security/hack/
www.circlemud.org	www.circlemud.org/pub/jelson/gethostbyname/
www.dsinet.org	www.dsinet.org/tools/Technotronic/
www.metasploit.com	www.metasploit.com/tools/
www.nostarch.com	www.nostarch.com/extras/hacking/chap2/

[1] Locating Public Exploit Sites

www.packetstormsecurity.org	www.packetstormsecurity.org/0409-exploits/
www.rosiello.org	www.rosiello.org/archivio/
www.safemode.org	www.safemode.org/files/zillion/exploits/
www.security-corporation.com	www.securitycorporation.com/download/exploit/
www.thc.org	www.thc.org/exploits/

یافتن محل اکسپلویت ها طریق کدهای رشته ای رایج [1]

وب سایت ها به طرق مختلف Source code های اکسپلویت ها را در صفحات خود نشان می دهند مخصوصا صفحات PHP ممکن است که این کدها را که به زبان C یا زبان دیگری نوشته به صورت متنی نشان دهد. همانطور که می دانید اکثر برنامه هایی که به زبان C نوشته می شوند در ابتدای کد آنها کلمات #include وجود دارد. مثلا #include <stdio.h>

پس این نکته را متوجه می شویم که به راحتی می توان سورس کد ها را با جستجوی این قبیل دستورات به راحتی پیدا کنیم. یک نمونه جستجو می تواند به صورت عبارت زیر باشد:

#include <stdio.h> exploit

در تصویر زیر نتایج ارائه شده از طرف گوگل را برای جستجوی عبارت #include <stdio.h> usage exploit ملاحظه می فرمایید:

[1] Common Code strings

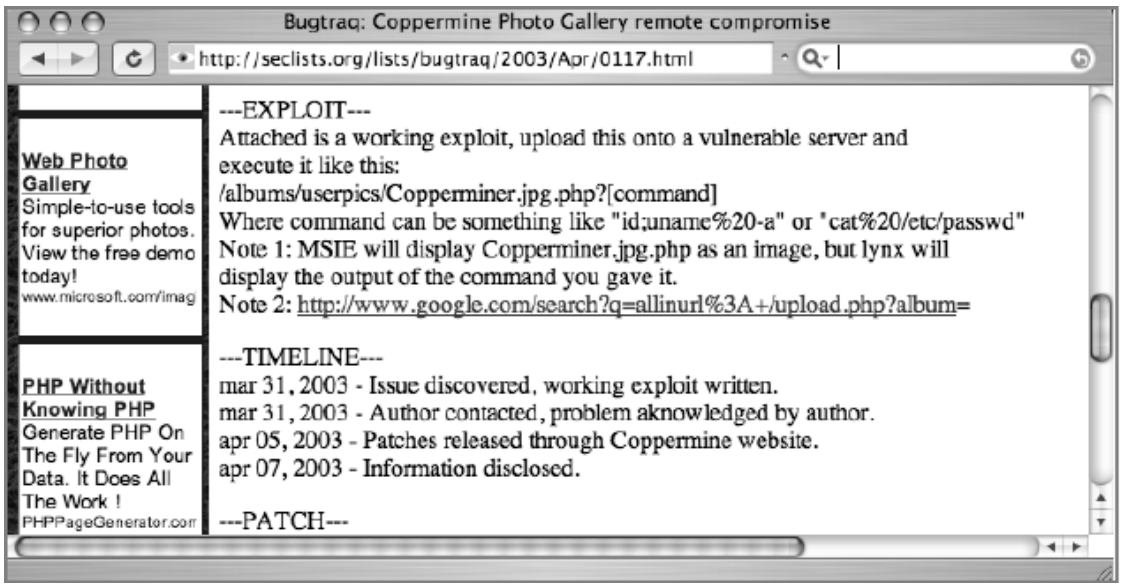
جدول زیر بسته به زبان برنامه نویسی برای آن اکسپلویت، جستجوهای مختلفی را ارائه میدهد:

زبان برنامه نویسی	پسوند	رشته نمونه
asp.net (C#)	Aspx	*“<%@ Page Language=”C#”” inherits*
asp.net (VB)	Aspx	*“<%@ Page Language=”vb”” inherits*
asp.net (VB)	Aspx	*<%@ Page LANGUAGE=”JScript”*
C	C	*“#include <stdio.h>”*
C#	Cs	*“using System;” class*
c++	Cpp	*“#include “stdafx.h””*
Java	J, JAV	*class public static*
JavaScript	JS	*“<script language=”JavaScript”>“*
Perl	PERL, PL, PM	*“#!/usr/bin/perl”*
Python	Py	*“#!/usr/bin/env”*
VBScript	.vbs	*“<%@ language=”vbscript” %>”*
Visual Basic	Vb	*“Private Sub”*

در استفاده از جدول بالا به این نکته توجه داشته باشید که پسوند فایلها کاملا اختیاری است ولـی در صورت استفاده جستجوی کاملتری خواهیم داشت.

یافتن محل آسیب پذیری روی اهداف

اکثر هکرها از گوگل برای یافتن آسیب پذیری اهـداف مبتنـی بـر وب[1] بـرای آن اکـسپلویت خـاص استفاده می کنند. به تصویر زیر دقت کنید:



[1] Web-base

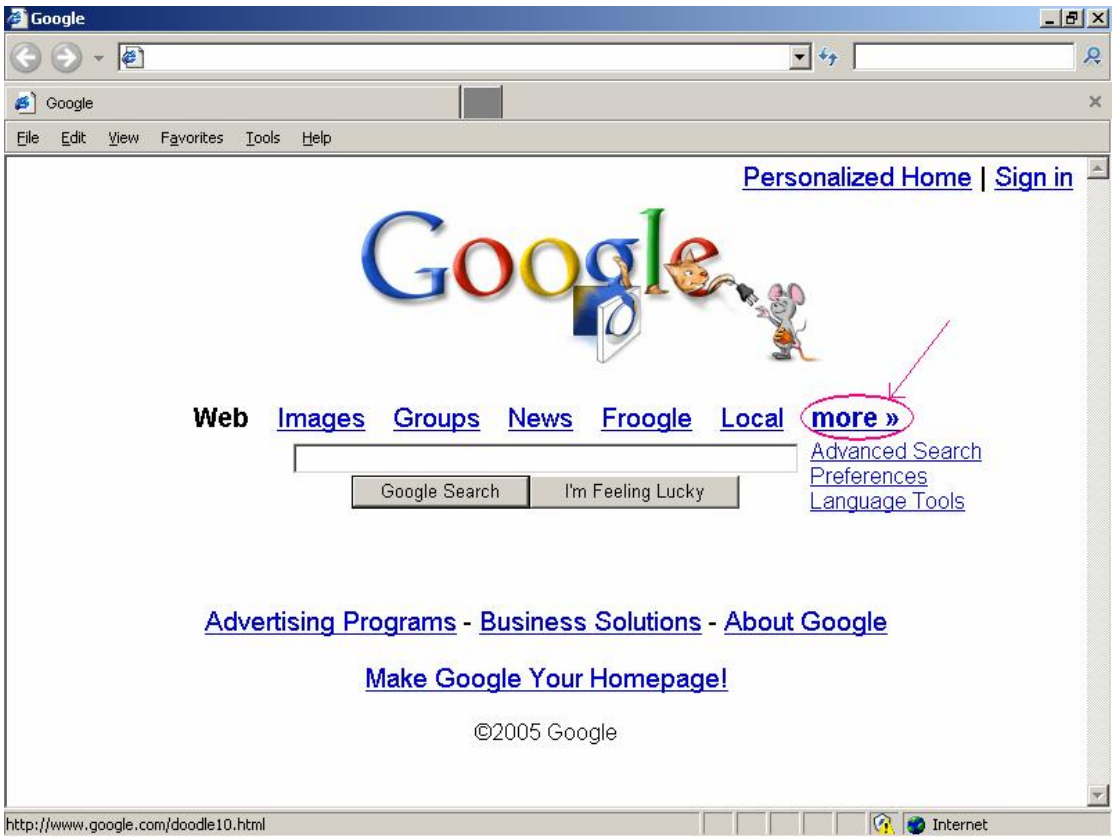
مؤلف: محمد بشیری
Site: http://bashiry.250free.com

فصل هفتم

امکانات و سرویسهای دیگر در گوگل

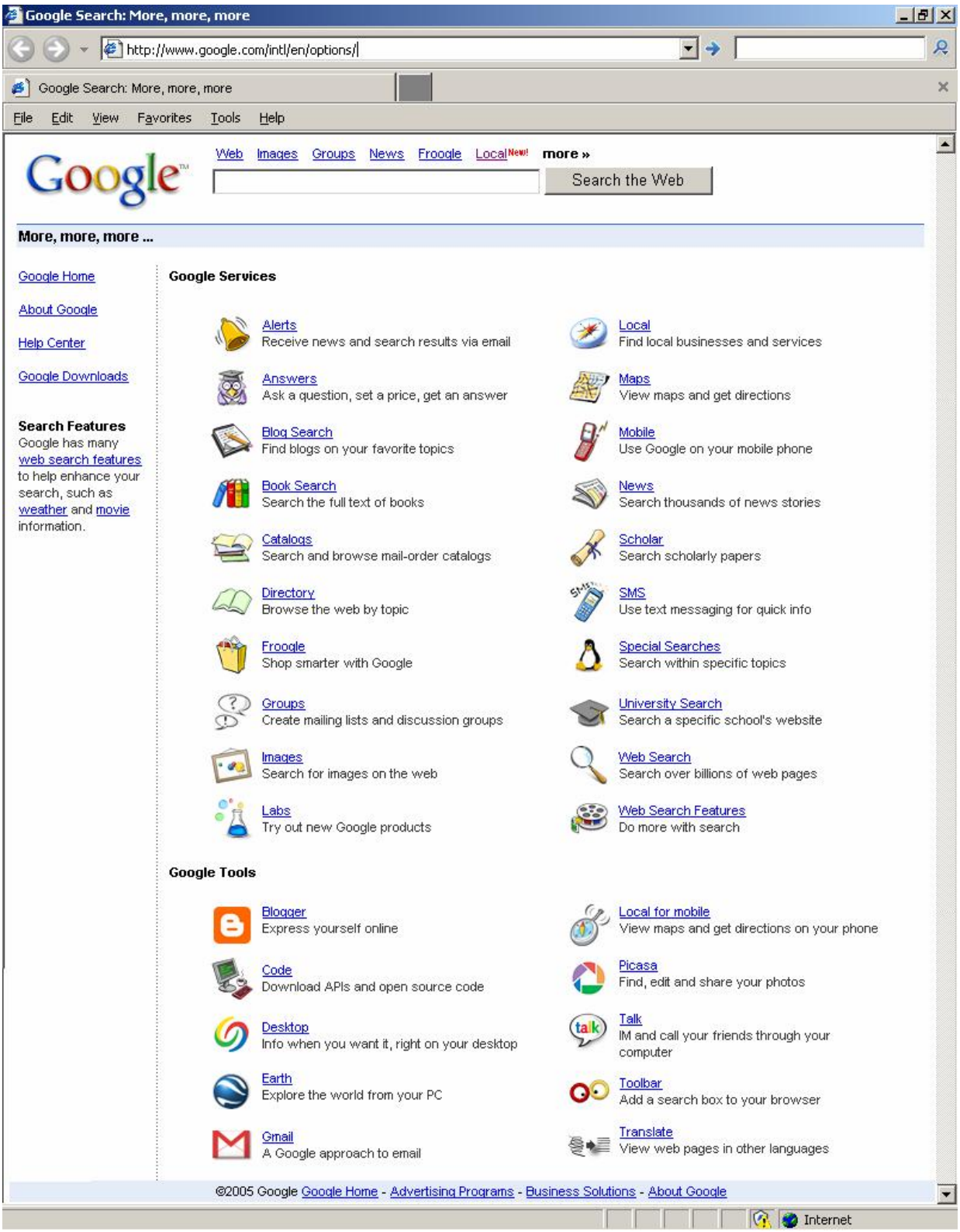
امکانات و سرویس های دیگر گوگل

گوگل دارای امکانات بیشتری نیز می باشد برای دیدن برخی از این امکانات می توانید مانند تصویر زیر بر روی گزینه More در صفحه اصلی گوگل کلیک نمایید.



بعد از این کار صفحه ای مطابق تصویر زیر ظاهر می شود که حاوی امکانات و ابزار موتور جستجو گر گوگل می باشد که در قسمت بعد این کتاب به توضیح تک تک این امکانات خواهیم پرداخت.

امیدوارم که تا حالا خسته نشده باشید !!! پس ادامه می دهیم...


Google Search: More, more, more
http://www.google.com/intl/en/options/
Google Search: More, more, more
File Edit View Favorites Tools Help
Google
Web Images Groups News Froogle Local New! more »
Search the Web
More, more, more ...
Google Home
About Google
Help Center
Google Downloads
Search Features
Google has many web search features to help enhance your search, such as weather and movie information.
Google Services
Alerts
Receive news and search results via email
Answers
Ask a question, set a price, get an answer
Blog Search
Find blogs on your favorite topics
Book Search
Search the full text of books
Catalogs
Search and browse mail-order catalogs
Directory
Browse the web by topic
Froogle
Shop smarter with Google
Groups
Create mailing lists and discussion groups
Images
Search for images on the web
Labs
Try out new Google products
Local
Find local businesses and services
Maps
View maps and get directions
Mobile
Use Google on your mobile phone
News
Search thousands of news stories
Scholar
Search scholarly papers
SMS
Use text messaging for quick info
Special Searches
Search within specific topics
University Search
Search a specific school's website
Web Search
Search over billions of web pages
Web Search Features
Do more with search
Google Tools
Blogger
Express yourself online
Code
Download APIs and open source code
Desktop
Info when you want it, right on your desktop
Earth
Explore the world from your PC
Gmail
A Google approach to email
Local for mobile
View maps and get directions on your phone
Picasa
Find, edit and share your photos
Talk
IM and call your friends through your computer
Toolbar
Add a search box to your browser
Translate
View web pages in other languages
©2005 Google Google Home - Advertising Programs - Business Solutions - About Google
Internet

همانطور که از شکل بالا پیداست صفحه More به دو قسمت اصلی تقسیم شده است.

بخش اول: خدمات و امکانات گوگل

بخش دوم: ابزار گوگل (در این کتاب گفته نمی شه. ان شاء الله اگه عمری باشه

بعدا در کتابی دیگه یا در همین کتاب توضیح می دم)

فهرست خدمات گوگل به ترتیب زیر می باشند :

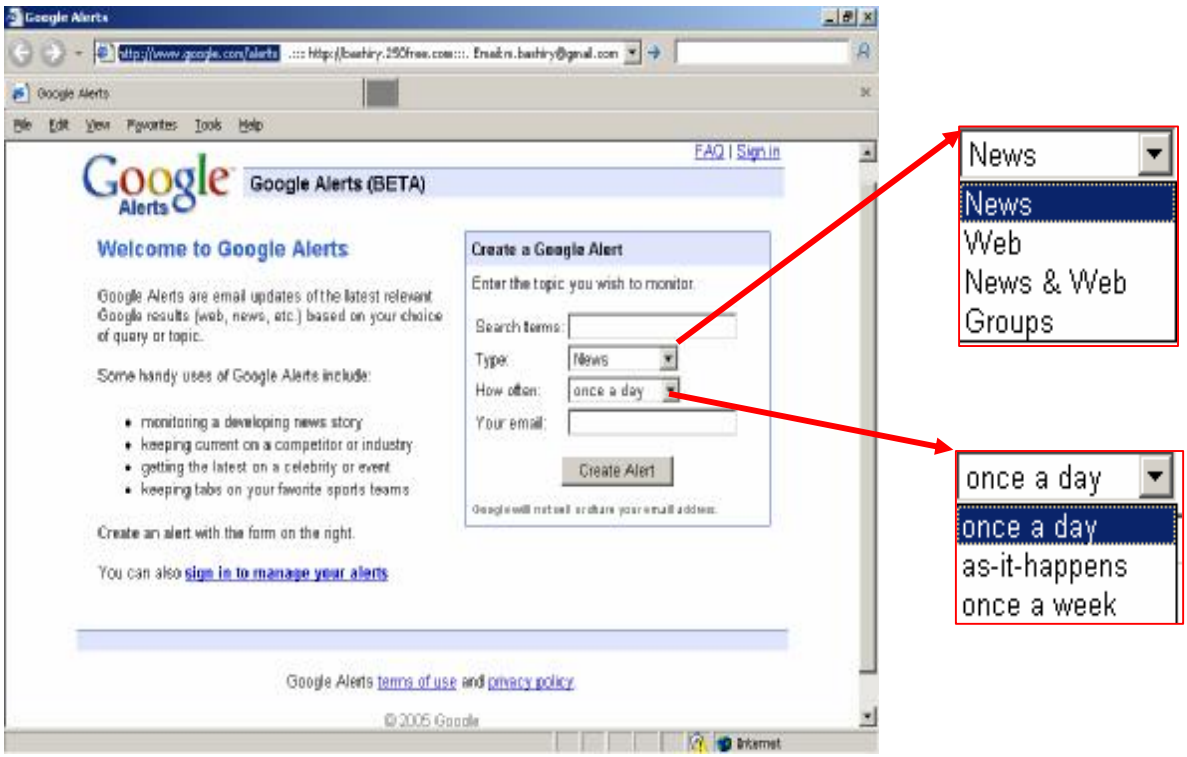
- Alerts : دریافت اخبار و نتایج جستجو از طریق ایمیل
- Local : پیدا کردن خدمات و محلهای تجاری
- Answers: بخش مطرح کردن سوالات و دریافت پاسخ سوالات
- Maps : نمایش نقشه ها و مسیرها
- Blog Search : یافتن بلاگ ها در موضوع مورد علاقه شما
- Mobile : کاربرد گوگل در تلفن همراه
- Book Search: جستجو در کتابها
- News: جستجو در اخبار
- Catalogs: کاتالوگ ها
- Scholar: گوگل مخصوص دانشجویان – مقالات
- Directory: جستجو در گوگل بر حسب موضوع یا رشته خاص
- SMS: ارسال پیام کوتاه متنی
- Froogle: فروشگاه
- Special Search: جستجو بر حسب موضوع خاص

- Groups: ایجاد کردن گروه های مباحثه
- University Search: جستجو در یک دانشگاه یا مدرسه خاص
- Images : جستجوگر تصویر گوگل
- Web Search: جستجوی معمولی در گوگل
- Labs: بخش آزمایشات در گوگل
- Videoجدیدا هم یک امکان جالب برای یافتن فیلم و یا فایلهای ویدیویی با آدرس http://video.google.com هم اضافه شده که شما دوستان می توانید به این آدرس بروید و به دنبال فیلم های مورد علاقه خود بگردید.

در ادامه به توضیح تک تک این خدمات و سرویس ها خواهم پرداخت :

آدرس اینترنتی این قسمت http://www.google.com/alerts می باشد.

بعد از کلیک بر روی علامت فوق صفحه مربوط به آن مطابق شکل زیر ظاهر خواهد شد:



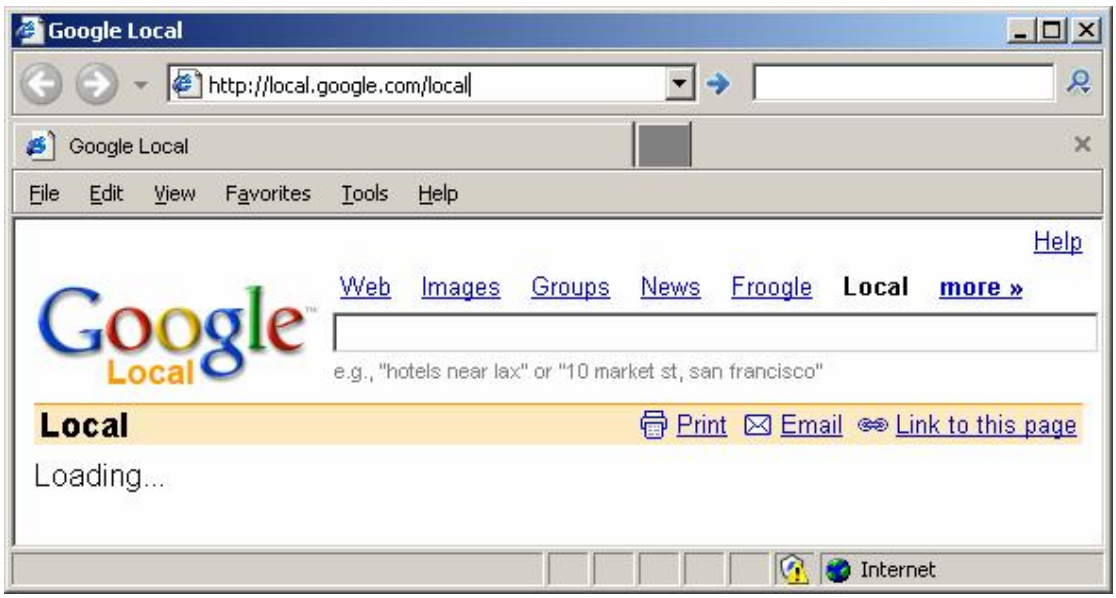
در هشدار دهنده گوگل نتایج آخرین جستجوها در وب، اخبار و ... برای فرد ارسال می شود.

بعضی از استفاده های Google Alert در زیر آورده شده است:

- ❖ زیر نظر گرفتن آخرین و تازه ترین اخبار
- ❖ دریافت آخرین اطلاعات از رقابتها و یا صنعت ها.
- ❖ گرفتن وقایع مهم
- ❖ آخرین نتایج تیمهای ورزشی مورد علاقه شما

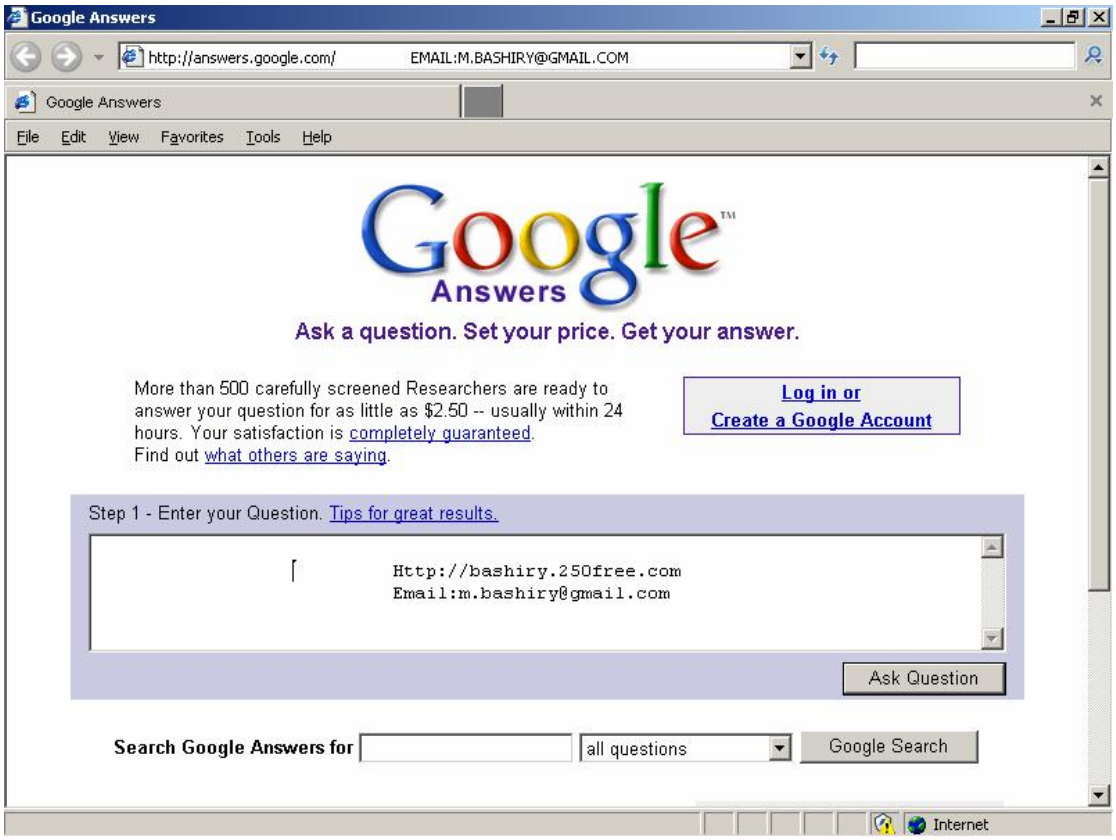
آدرس اینترنتی این سرویس گوگل **http://local.google.com** می باشد.

بعد از کلیک بر روی علامت فوق صفحه مربوط به آن مطابق شکل زیر ظاهر خواهد شد:



این سرویس در گوگل به ما امکان پیدا کردن خدمات و محل های تجاری را می دهد.

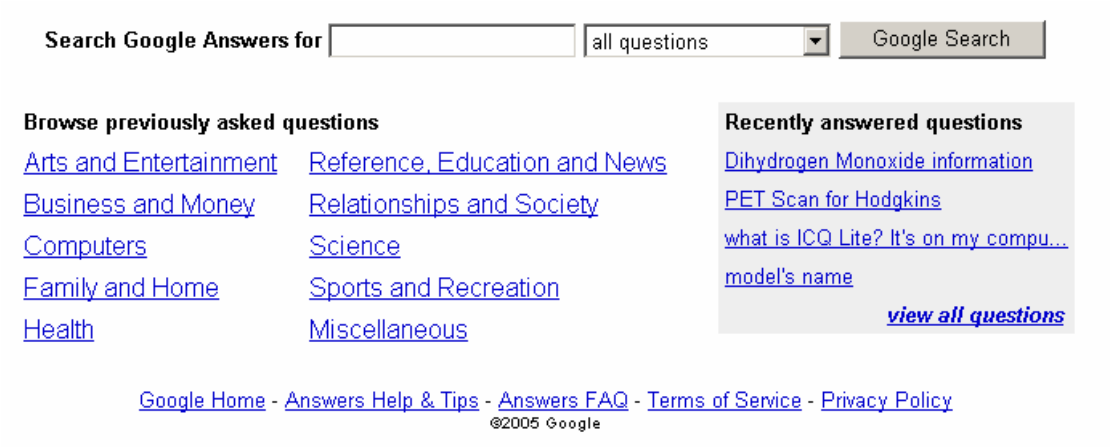
آدرس اینترنتی این سرویس گوگل http://answers.google.com می باشد.



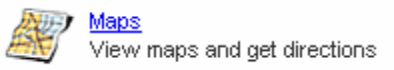
در این بخش از گوگل می توانید بعد از طرح سوال خود و پرداخت مبلغی کمتر از $ 2.50 جواب آن سوال را ظرف ۲۴ ساعت بگیرید. در ضمن بیشتر از ۵۰۰ پژوهشگر با دقت هر چه تمام تر آماده پاسخ به سوالات می باشند.

طریقه کار به این صورت است که بعد از رفتن بـه آدرس http://answers.google.com در بخـش Step1 سوال خود را تایپ نموده و سپس بر روی Ask questions کلیک نمایید و بعد از این کـار مراحل را دنبال نمایید.

در این صفحه همچنین مانند تصویر زیر می توانید در پرسش و پاسخهای قبلی نیز جستجویی داشته باشید:



برای جستجوی پرسـش و پاسـخ هـای قبلـی در کـادر Search Google Answers for عبـارت جستجوی خود را وارد نمایید و بر روی دکمه Google Search کلیک کنید تـا عملیـات جـستجو آغاز گردد.



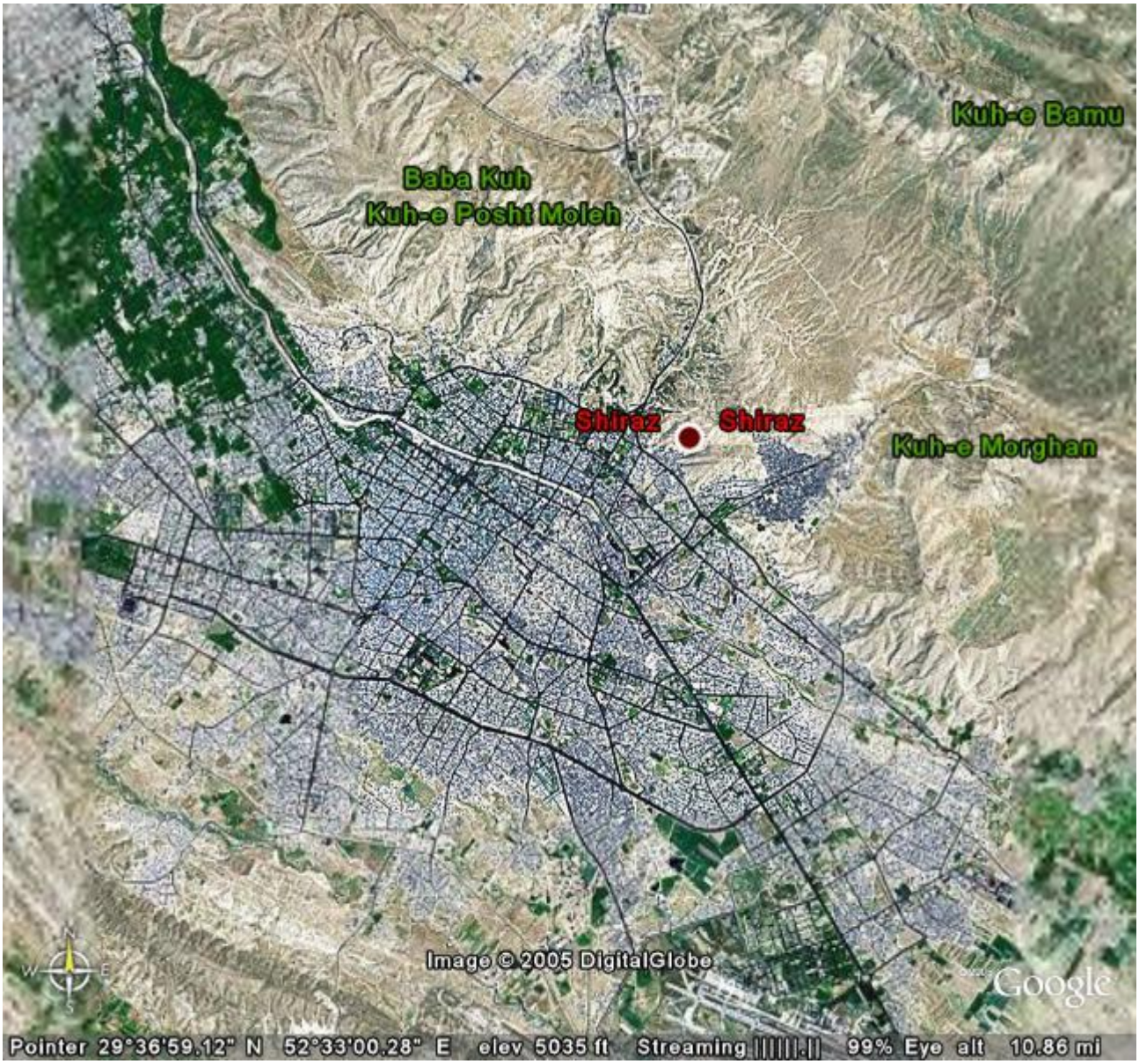
آدرس URL نقشه گوگل: http://maps.google.com

در Google map می توانید مسیرها و همچنین نقشه های کشورهای مختلف جهان را به سادگی هر چه تمام تر پیدا کنید. برای مثال در بخش جستجو Iran را تایپ کنید تا نقشه کشور ایران را ملاحظه کنید.

توجه شما را به چند تصویر زیبا که توسط نرم افزار نقشه گوگل گرفته شده است جلب می کنم:

برای کسب اطلاعات بیشتر و دانلود نرم افزار در مورد این نرم افزار می توانید به آدرس http://earth.google.com مراجعه کنید .


Tehran
Tehran
Kuh-e Bibi Shahr
Image © 2005 DigitalGlobe
Google
Pointer 35°39'36.40" N 51°24'26.44" E elev 3672 ft Streaming 100% Eye alt 11.84 mi


Kuh-e Bamu
Baba Kuh
Kuh-e Posht Moleh
Shiraz
Shiraz
Kuh-e Morghan
Image © 2005 DigitalGlobe
Google
Pointer 29°36'59.12" N 52°33'00.28" E elev 5035 ft Streaming 99% Eye alt 10.86 mi


Shiraz
Shiraz
Kuh-e Morghan
Kuh-e Kaftarak
Image © 2005 EarthSat
Image © 2005 DigitalGlobe
Google
Pointer 29°32'45.27" N 52°37'44.58" E elev 4864 ft Streaming 99% Eye alt 14.43 mi

آدرس های مختلف برای دسترسی به این سرویس گوگل:

http://blogsearch.google.com

http://www.google.com/blogsearch

/http://search.blogger.com

http://www.blogger.com/home

این سرویس در گوگل این امکان را به کاربران می دهد که به دنبال موضوعهای مورد علاقه شان در blog ها بگردند. همچنین این سرویس می تواند در پست های شخصی کـه در بـلاگ هـا مطـرح شده اند جستجو نماید و در صورت یافتن آن پست لینک آن را نمایش دهد.

سوال: جستجوی بلاگ چه عملگرهای جستجویی را پشتیبانی می کند؟

- link:
- site:
- intitle:

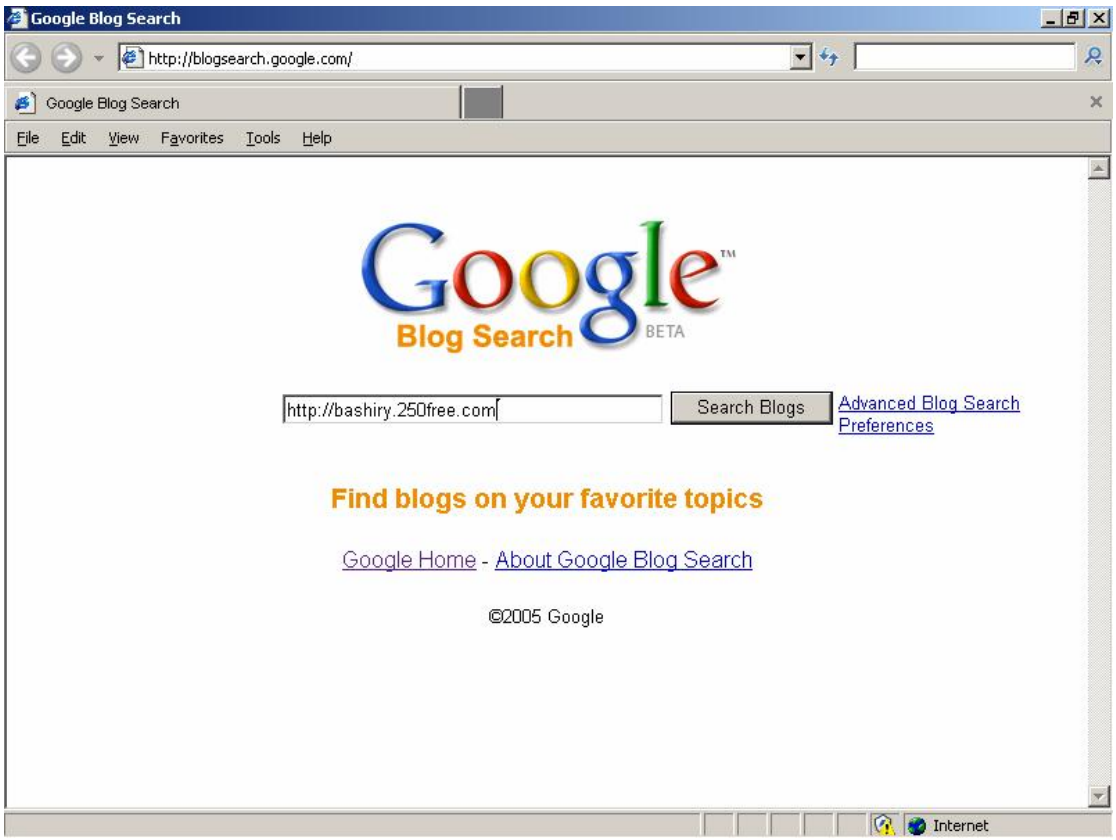
و همچنین چند عملگر مخصوص خود نیز دارد که به ترتیب زیر می باشند:

- inblogtitle:
- inposttitle:
- inpostauthor:
- blogurl:

مثال : جستجو بر حسب مؤلف پست ارسالی

```
Mandolin inpostauthor:Graham
```

تصویر زیر صفحه اصلی جستجوگر blog گوگل را نشان می دهد:



Mobile
Use Google on your mobile phone

استفاده از گوگل برای تلفن همراه یا تلفن

آدرس اینترنتی : http://mobile.google.com

این سرویس برای کسانی است که می خواهند از طریق موبایل یا تلفن خود در گوگل جستجو کنند.

جستجو در وب از طریق تلفن همراه

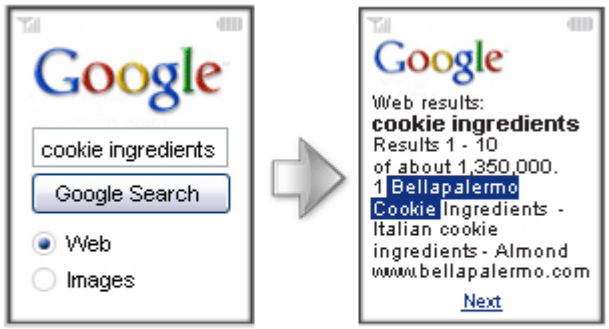
مراحل زیر را به ترتیب انجام دهید:

۱- در مرور گر موبایل و در بخش URL آدرس www.google.com را تایپ کنید. توجه کنید که اگر با پیغام خطایی مواجه شدید آدرس http://www.google.com/xhtml را وارد کنید

۲- عنوان جستجوی خود را وارد کنید.

۳- دکمه رادیویی WEB را فعال کنید و سپس دکمه جستجوی گوگل را انتخاب کرده و دکمه Enter را فشار دهید.

۴- نتیجه جستجو نمایش داده خواهد شد.



Enter your search query

Select the desired result by scrolling through the results page

جستجوی تصاویر از طریق تلفن همراه:

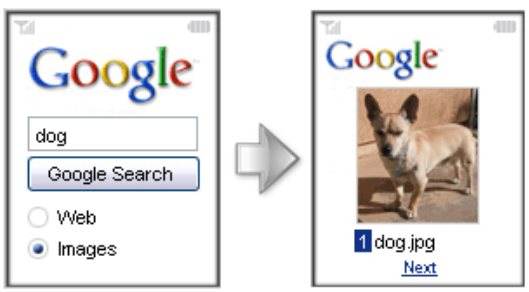
مراحل زیر را به ترتیب انجام دهید:

۵- در مرورگر موبایل و در بخش URL آدرس www.google.com را تایپ کنید. توجه کنید که اگر با پیغام خطایی مواجه شدید آدرس http://www.google.com/xhtml را وارد کنید

۶- عنوان جستجوی تصویر خود را وارد کنید. (مثلا کلمه dog)

۷- دکمه رادیویی Images را فعال کنید و سپس دکمه جستجوی گوگل را انتخاب کرده و دکمه Enter را فشار دهید.

۸- نتیجه جستجو نمایش داده خواهد شد.



Enter your image search query and select "Images"

Select the desired image by scrolling through the results page

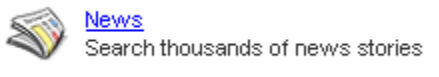
آدرس دسترسی به جستجوگر کتاب گوگل: http://books.google.com

این بخش نیاز به توضیح اضافی ندارد.

نمای کوچک کتاب

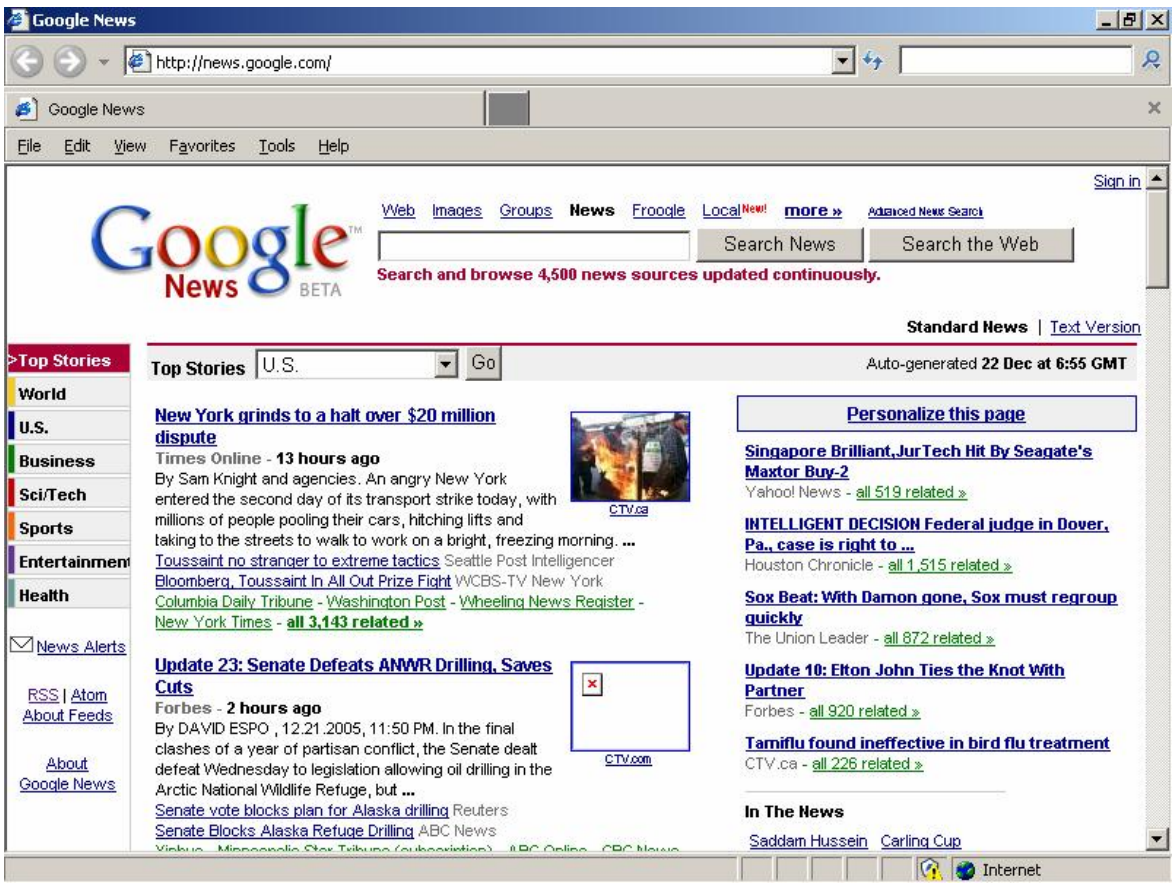
نمایش یک صفحه نمونه

نمایش تمام متنی



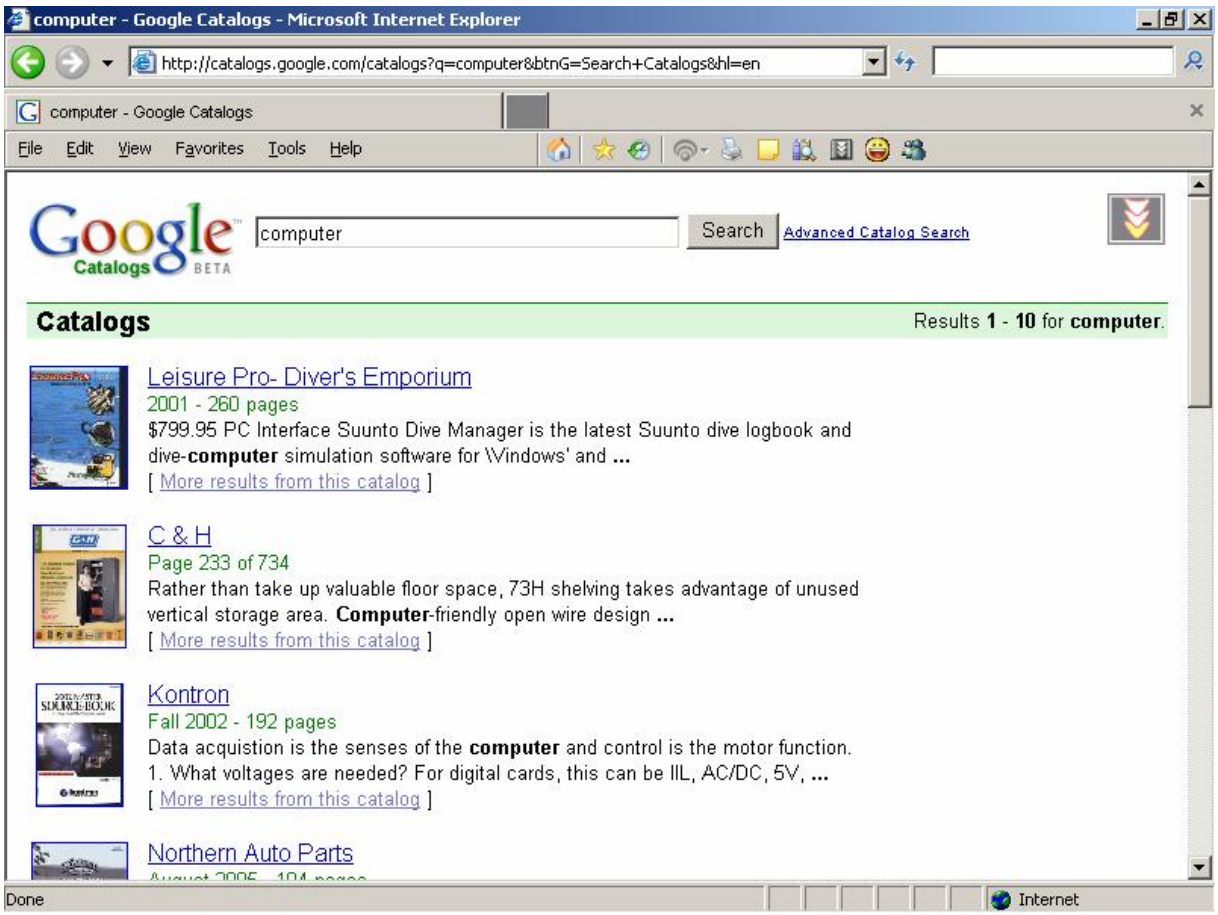
آدرس اینترنتی : http://news.google.com

این سرویس گوگل به کاربران امکان می دهد که در هزاران منابع خبری مختلف به جستجو بپردازند.



آدرس: http://catalogs.google.com

همانطور که از اسمش بر می آید کاتالوگ ابزارها و تولیدات مختلف را جستجو می کند . تـصاویر زیـر خود گویای این مطلب می باشد.



جستجو در صفحات و مطالب دانشگاهی (بیشتر برای دانشجویان استفاده می شود)

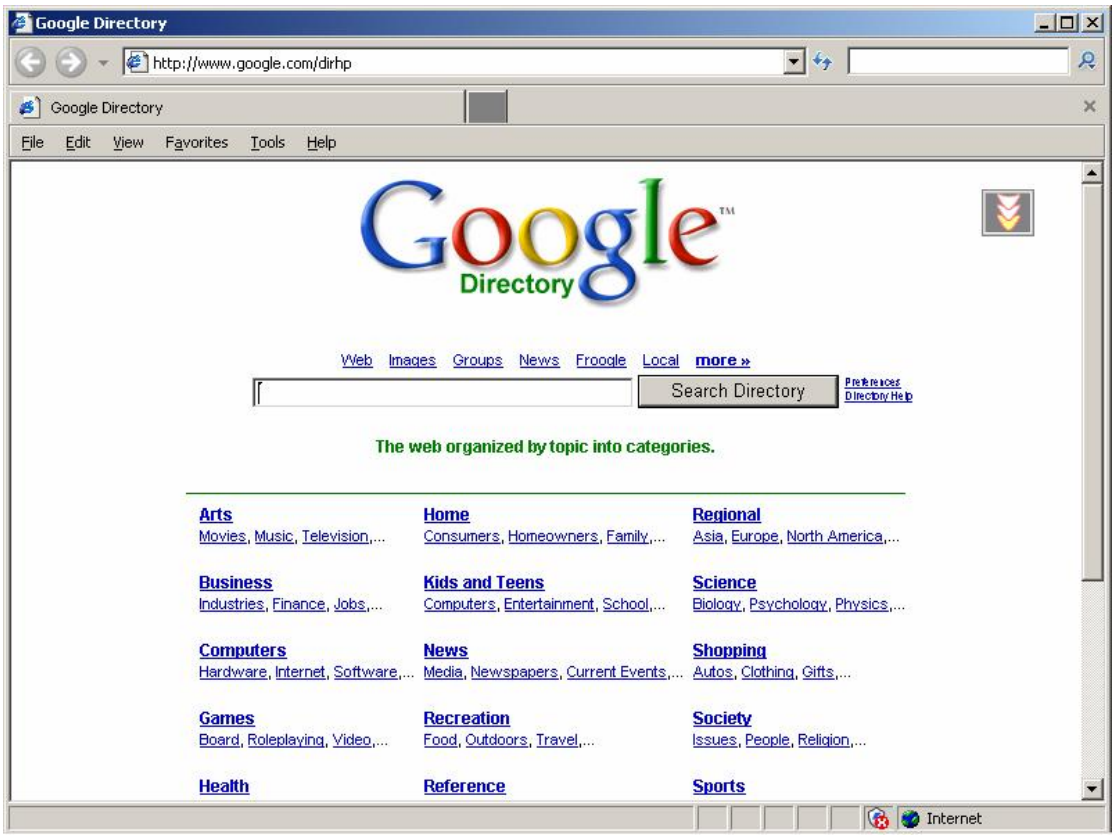
آدرس URL برای دسترسی به این سرویس گوگل: http://scholar.google.com

تصویر زیر صفحه اصلی scholar Google را نشان می دهد.

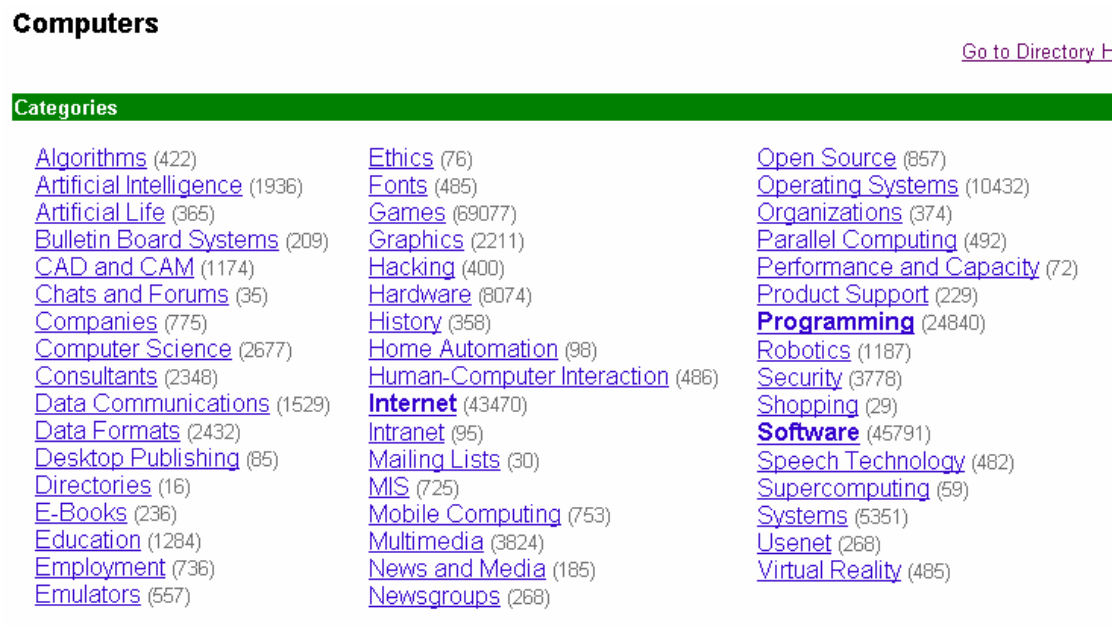
کار با آن بسیار ساده است و نیازی به توضیح اضافی هم نیست.

جستجو در وب بر اساس موضوع

آدرس URL: http://www.google.com/dirhp



و در تصویر بعد موضوع کامپیوتر انتخاب شده است (Computers) و بعد از انتخاب آن دایرکتوری تمامی موارد مربوط به آن ظاهر می شود مانند الگوریتم ها، بازیها، قلم ها، برنامه نویسی، اینترنت، کتابهای الکترونیکی و غیره



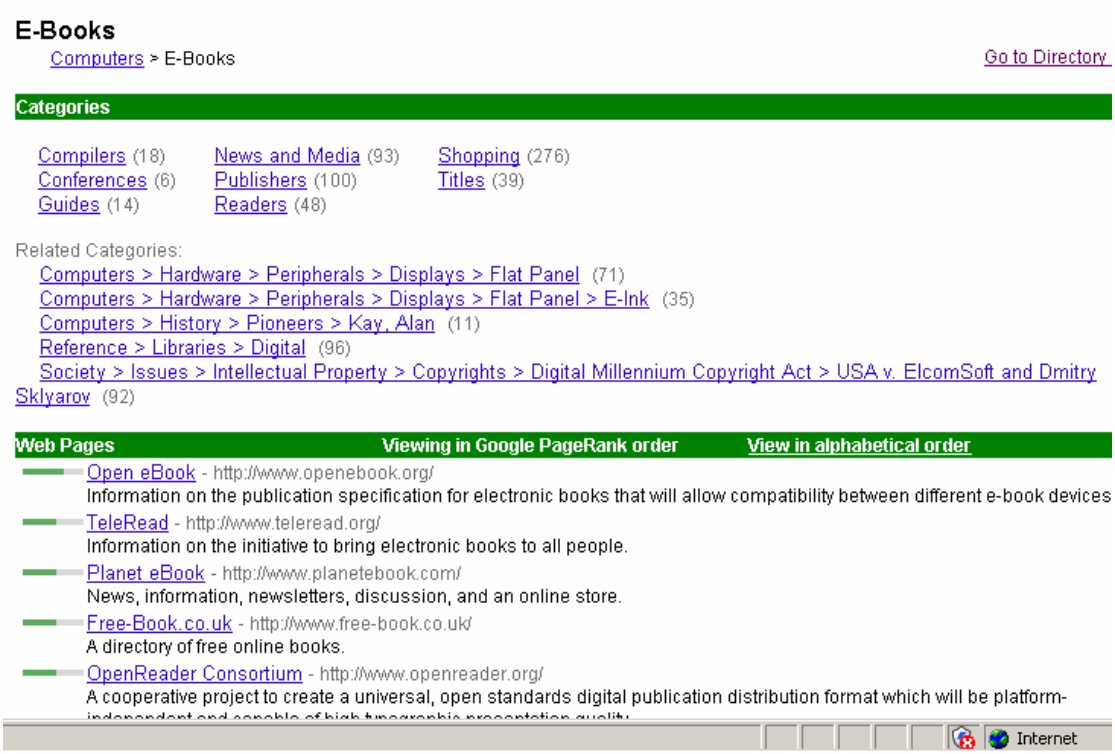
Computers

Go to Directory

Categories

Algorithms (422)
Artificial Intelligence (1936)
Artificial Life (365)
Bulletin Board Systems (209)
CAD and CAM (1174)
Chats and Forums (35)
Companies (775)
Computer Science (2677)
Consultants (2348)
Data Communications (1529)
Data Formats (2432)
Desktop Publishing (85)
Directories (16)
E-Books (236)
Education (1284)
Employment (736)
Emulators (557)
Ethics (76)
Fonts (485)
Games (69077)
Graphics (2211)
Hacking (400)
Hardware (8074)
History (358)
Home Automation (98)
Human-Computer Interaction (486)
Internet (43470)
Intranet (95)
Mailing Lists (30)
MIS (725)
Mobile Computing (753)
Multimedia (3824)
News and Media (185)
Newsgroups (268)
Open Source (857)
Operating Systems (10432)
Organizations (374)
Parallel Computing (492)
Performance and Capacity (72)
Product Support (229)
Programming (24840)
Robotics (1187)
Security (3778)
Shopping (29)
Software (45791)
Speech Technology (482)
Supercomputing (59)
Systems (5351)
Usenet (268)
Virtual Reality (485)

اگر از موارد فوق گزینه Ebook را انتخاب کنیم صفحه ای به صورت زیر خواهد آمد:



E-Books

Computers > E-Books

Go to Directory

Categories

Compilers (18)
Conferences (6)
Guides (14)
News and Media (93)
Publishers (100)
Readers (48)
Shopping (276)
Titles (39)

Related Categories:

Computers > Hardware > Peripherals > Displays > Flat Panel (71)
Computers > Hardware > Peripherals > Displays > Flat Panel > E-Ink (35)
Computers > History > Pioneers > Kay, Alan (11)
Reference > Libraries > Digital (96)
Society > Issues > Intellectual Property > Copyrights > Digital Millennium Copyright Act > USA v. ElcomSoft and Dmitry Sklyarov (92)

Web Pages | Viewing in Google PageRank order | View in alphabetical order

Open eBook - http://www.openebook.org/
Information on the publication specification for electronic books that will allow compatibility between different e-book devices

TeleRead - http://www.teleread.org/
Information on the initiative to bring electronic books to all people.

Planet eBook - http://www.planetebook.com/
News, information, newsletters, discussion, and an online store.

Free-Book.co.uk - http://www.free-book.co.uk/
A directory of free online books.

OpenReader Consortium - http://www.openreader.org/
A cooperative project to create a universal, open standards digital publication distribution format which will be platform-

Internet

برای ارسال پیام کوتاه استفاده می شود.

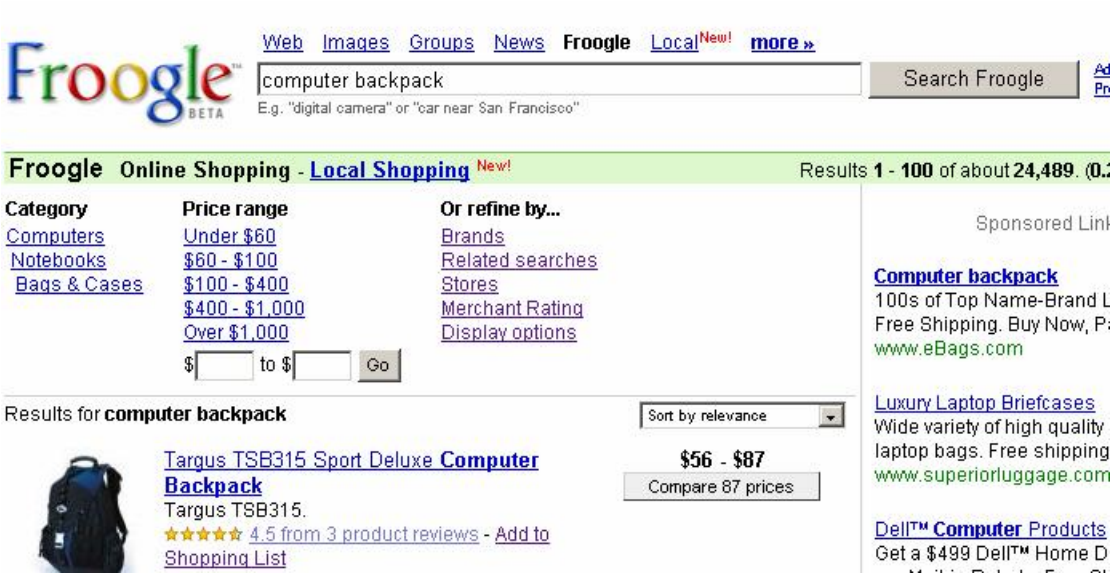
آدرس دسترسی به این سرویس http://sms.google.com می باشد

برای دریافت اطلاعات بیشتر در مورد این سرویس می توانید به سایت گوگل مراجعه نمایید.

این سرویس برای خرید و فروش اینترنتی استفاده می شود و صفحه اصلی آن به صورت زیر می باشد.

آدرس اینترنتی : http://froogle.google.com

یک نمونه جستجو در Froogle در زیر آورده شده



امکان بعدی گوگل  Special Searches
Search within specific topics می باشد. که در محل های خاص چه علمی و چه وب سایت های مدارس خاص جستجو میکند.

آدرس آن http://www.google.com/options/specialsearches.html می باشد و صفحه اصلی آن به صورت زیر می باشد:

در پایین تصویر زیر هم به وضوح دیده می شود و شامل موارد زیر می باشد:

☒ U.S. Government دولت ایالت متحده آمریکا

☒ Linux لینوکس

☒ BSD بی اس دی

☒ Apple Macintosh سیستم عامل مکینتاش از شرکت apple

☒ Microsoft مایکروسافت

که برای دسترسی به هر کدام می توانید به آدرسهای زیر مراجعه کنید:

☒ http://www.google.com/unclesam

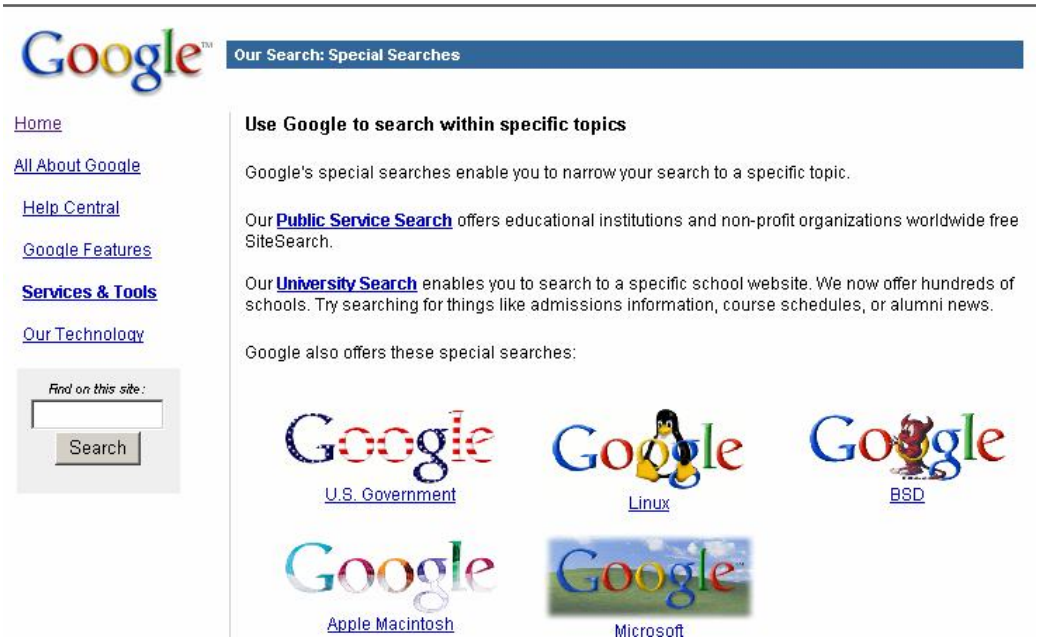
☒ http://www.google.com/linux

☒ http://www.google.com/bsd

☒ http://www.google.com/mac.html

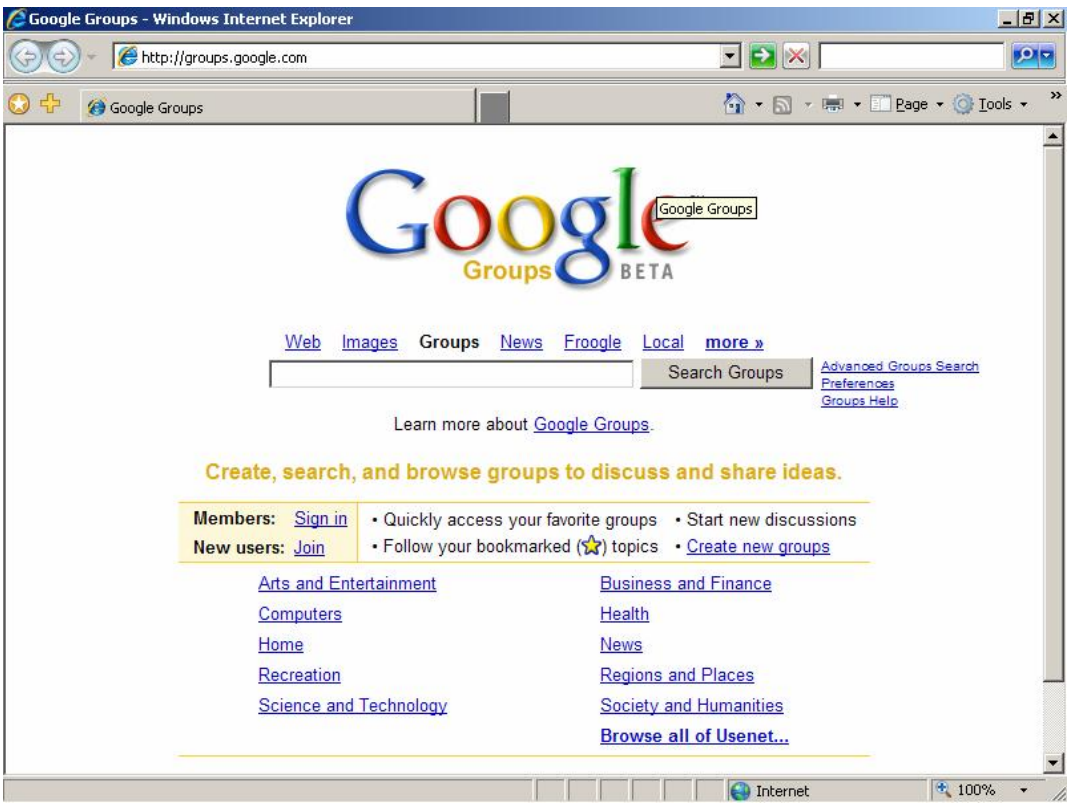
☒ http://www.google.com/microsoft

و همچنین از آدرس http://www.google.com/options/universities.html می توان برای جستجو در دانشگاههای خاص استفاده کرد.



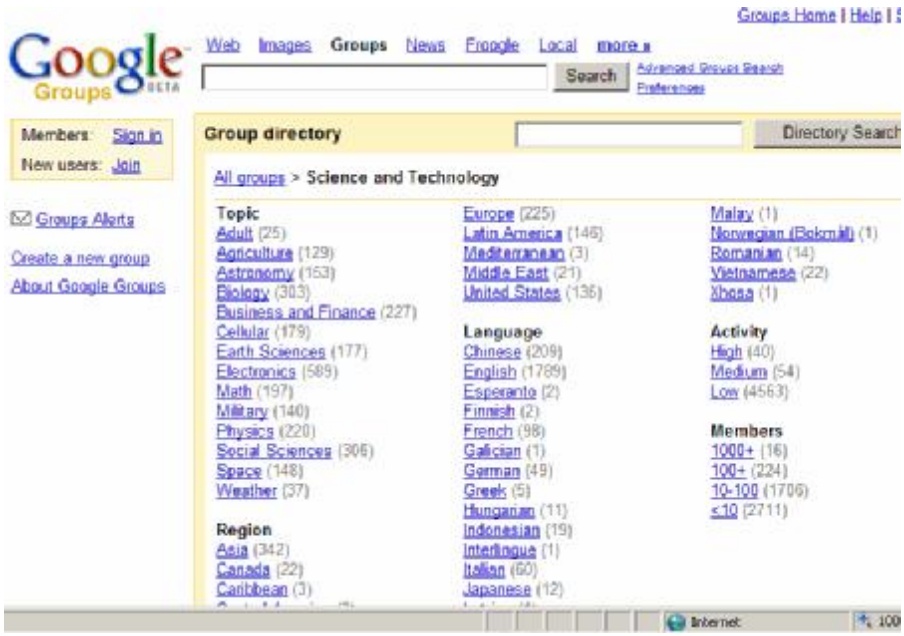
اگر در صفحه بالا روی لینک Microsoft کلیک نماییم صفحه ای همانند تصویر زیر ظاهر می شود که در سایت مایکروسافت و سایت های در ارتباط با آن سایت جستجو می کند.

Groups



آدرس دسترسی به این سرویس http://groups.google.com

همانطور که از شکل پیداست می توان در گوگل عملیات جستجو را محدود به گروه کرد. مثلا در بخش computer فقط به مباحث مرتبط به کامپیوتر پرداخته می شود. در تصویر زیر گروه Science and Technology را انتخاب کرده ایم:

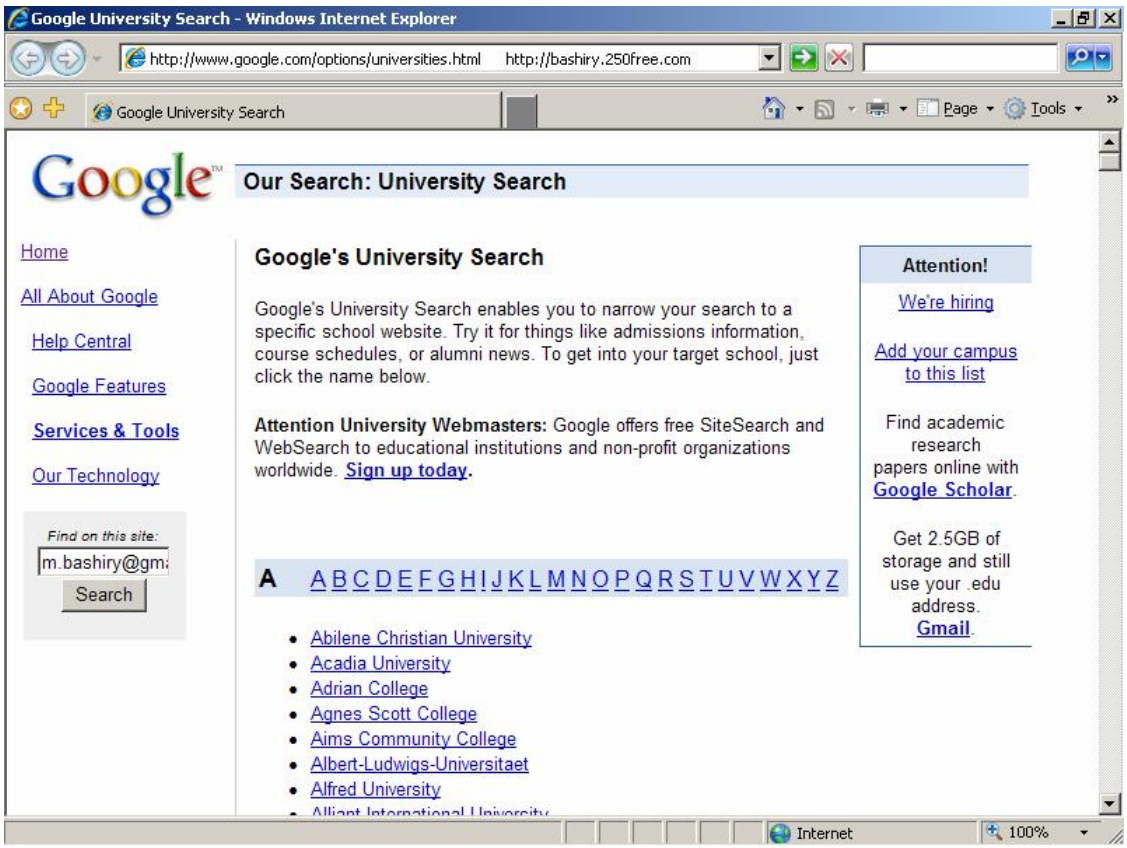


Google's University Search

کاربرد: جستجوی گوگل اما در دانشگاه انتخاب شده.

آدرس اینترنتی: http://www.google.com/options/universities.html

تصویر مربوطه:



IMAGE

جستجوی تصاویر گوگل در آدرس http://images.google.com

این سرویس نیاز به توضیح ندارد. دیگه فکر کنم همه شما استاد جستجوی تصویر هستید ☺

همچنین جستجو در وب هم که به طور کامل در این کتاب مورد بررسی قرار گرفت.

آدرس اینترنتی: http://labs.google.com

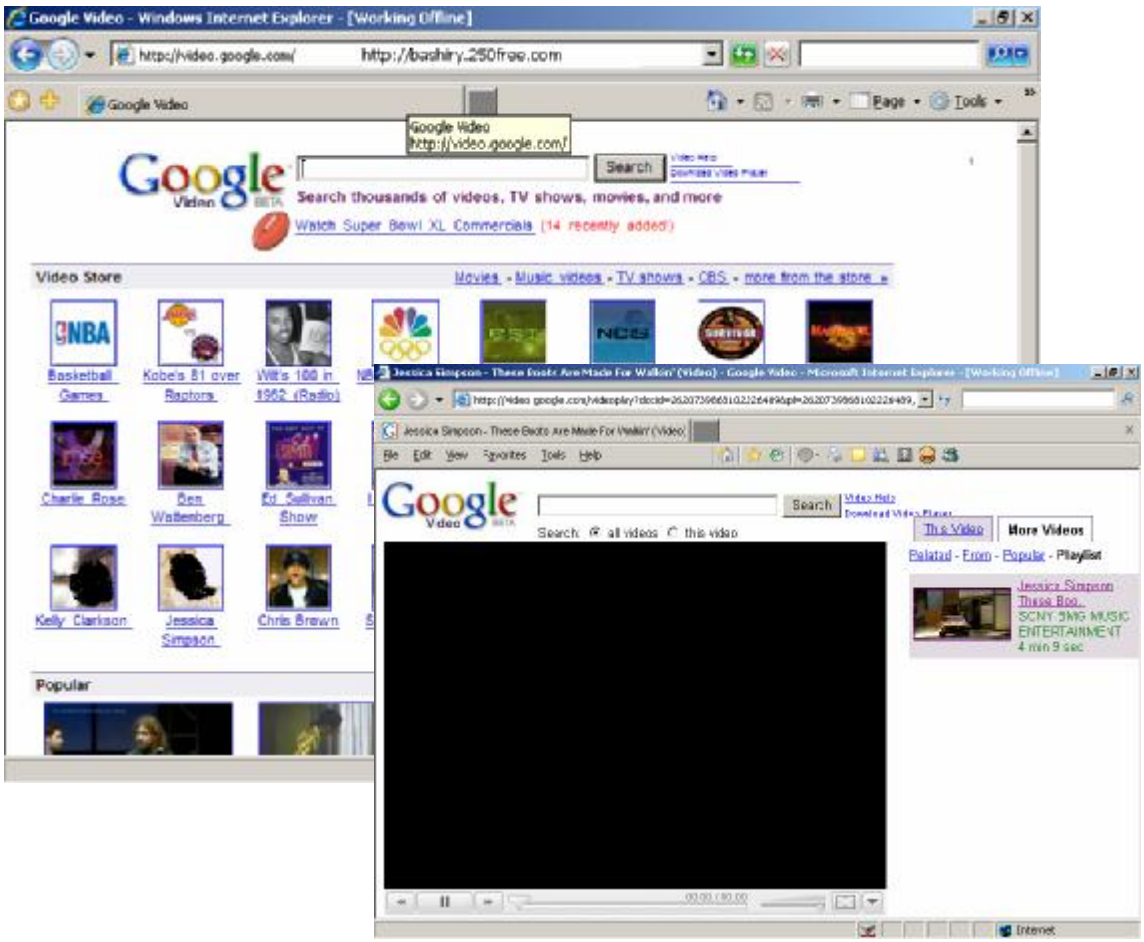
تعریف بخش آزمایشگاه های گوگل:

آزمایشگاه گوگل همانند یک زمین بازی برای مهندسان گوگل و همچنین کاربران حادثه جو می ماند. این یک فکر جالب از طرف گوگل است که بتواند از طریق شما کاربران به نتایج تحقیقات در حال انجام دست یابند. به این صورت که هنگامی که در اینترنت هستید و کاری انجام نمی دهید کامپیوتر شما بخشی از آن محاسبات عظیم را بدست آورده و نتیجه حاصله را به گوگل می فرستد . سپس نتایجی که از کاربران مختلف بدست آمده اند ترکیب می شوند و ادامه مراحل برای به جواب رسیدن آن تحقیق.

برای کسب اطلاعات بیشتر در مورد این سرویس می توانید به بخش پرسش و پاسخ در گوگل با آدرس http://labs.google.com/faq.html مراجعه نمایید.

Video.google.com

این سرویس سرویسی است که گوگل اخیرا آن را در بخش خدمات خود قرار داده. با استفاده از این سرویس می توانید در وب به دنبال برنامه های تلویزیونی و ویدئو کلیپ های با پسوندهای گوناگون بپردازید و همچنین می توانید فیلم های مورد علاقه خود را که توسط گوگل پیدا شده تماشا نمایید. البته بعضی از فیلم ها فقط پیش نمایشی از آن را می توانید مشاهده کنید و برای دیدن کل فیلم از شما درخواست پول می کند (پول وده پول وده !!) ولی بعضی ها رایگان هستند و می توانید فیلم را دانلود کنید و یا به طور کامل ببینید. کار کردن با این سرویس همانند جستجوی تصاویر در گوگل است و نیاز به توضیح اضافی چندانی ندارد. در زیر توجه شما را به چند تصویر در همین رابطه جلب می کنم.



در خبرها داشتیم ساختمان جدید اداری گــوگل در منطقه ویکتوریای لندن افتتاح شد.گوگل در یک کار جالب برای برای دادن لوگو و نشانه به این ساختمان از دانش آموزان دبستان نزدیک به این ساختمان دعوت شده که برای این ساختمان با موضوعات دلخواهی لوگو طراحی کنند که از صدها لوگو رسیده و طبقه بندی آن ها در نهایت ۵ لوگو انتخاب شدند که از بین آن ها نیز لوگو زیر از Lisa Waiwaina دانش آموز ۱۱ ساله برگزیده شد. (توجه داشته باشید تصاویر زیر عینا از فروم سایت http://sohail2d.com آورده شده است).

Lisa Waiwaina, age 11

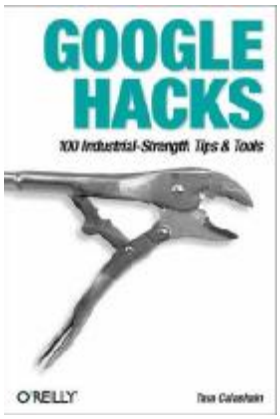
Tori Savage, age 10

Tiggy Philipps, age 11

Katherine Vetter, age 5

منابع و مو اخذ

منبع شماره ۱)



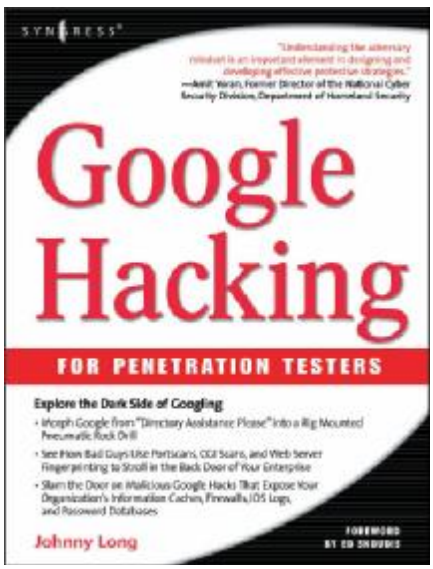
The Google hackers guide by Johnny Long

منبع شماره ۲)

Google Hacks by O'Reilly

منبع شماره۳) موتور جستجوگر Google

منبع شماره ۴) Google hacking for penetration testers



مؤلف: محمد بشیری

Site: http://bashiry.250free.com

تشکر و قدردانی

در ابتدا این کتاب را به استاد خوبم استاد **پویا لعل بخش** و بچه های خوب **شبگرد** تقـدیم می کنم که با نظرات و استقبال شان از نسخه اول باعث شدند من نسخه دوم این کتاب را تهیه کنم.

از تمامی دوستانم و طرفداران سایت http://bashiry.250free.com به خاطر نظـرات و انتقـادات سازنده شان تشکر و قدردانی می کنم.

در انتها جا دارد از مدیریت سایت امنیتی سیمرغ http://www.simorgh-ev.org و مخصوصا مدیریت سایت امنیتی شبگرد www.shabgard.org به خاطر حمایتشان از نسخه اول این کتاب تشکر و قدردانی نمایم .

آدرس پست الکترونیک:

m.bashiry@gmail.com

mohamad_bashiry@yahoo.com

منتظر انتقادات و نظرات شما هستم.

موفق و پیروز باشید.

Fri3nds of Shabgard