Advance Google Dorking

Searching for secrets
- By Vivek Pandit

Visit our website for advance hacking tutorials
www.thecyberblogs.com

Table OF Content:Theory

- Theory
  1. What is a Dorking ? Why do we use a dork ?
  2. Syntax of google dorking
  3. Decoding URL structure
  4. General Syntax Rules
  5. Extended Search Operators Syntax (e.g - + , -, &, "", | and etc.)
  6. Search Functions (e.g - intext: , inurl: and etc.)
  7. Advanced Dorking

Table OF Content: Practical (Exploitation)

- Practical
  1. Exploiting directory listing vulnerabilities.
  2. Dorking for plugins and themes of wordpress website.
  3. Exploiting SQL injection with google dorking.
  4. Exploiting apache and microsoft iis servers.
  5. Dorking application-generated system reports
  6. Prowling for Passwords
  7. Searching for personal data and confidential documents
  8. Finding phpmyadmin

Table OF Content: Bonus Section

- Bonus Section

1. Expl???????
2. Dorkse???????????
3. Googlepe?????

LET'S GET STARTED WITH THEORY OF GOOGLE DORKING

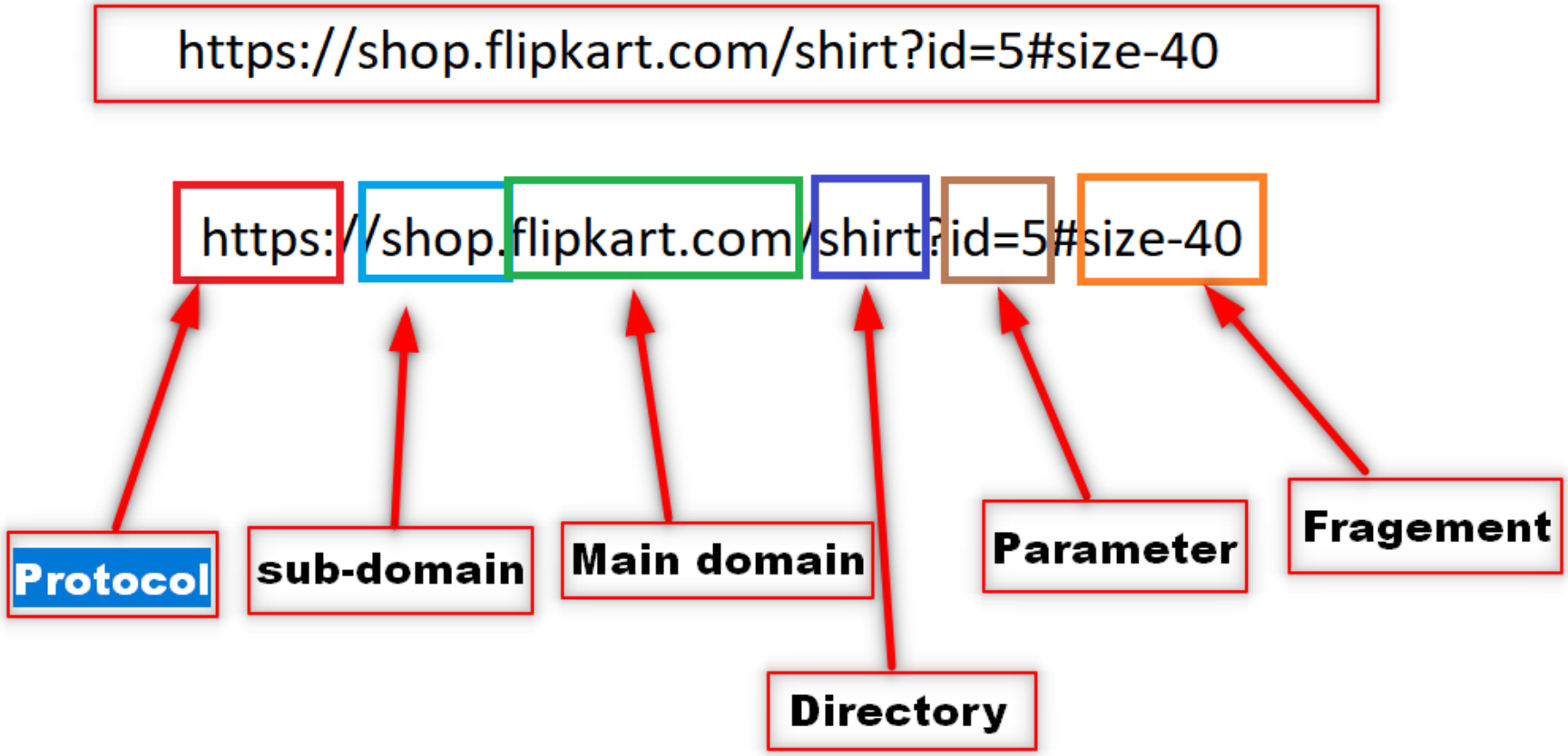
- What is a Dorking ? Why do we use a dork ?

  - Dorking is the art of understanding and utilizing a search engine to emit the desired results. If I wanted to find a file on anonfile; I can go on Google and use this search query, inurl:anonfile.com + Target File

❑Why do we use a dork ?

- ➢We use dorking to find implest form, finding basic, unprotected sites, compromising its security measures or lack of; exporting information of which is desired and then use them for other purposes.

❑ Decoding URL (Unfiform Resource Locator)



❑ Syntax of google dorking

- The most important thing to keep universal in the creation of ALL DORKS, is the concept of syntax. If I spoke English with a Chinese sentence structure, it wouldn't make any sense. It's the exact same to Google or Bing. If you don't speak their language, they won't understand you.

General syntax rules

Gaming shop.com

Gaming shop .com

Syntax Rules

1. Page Extension CANNOT go AFTER Parameter

   Wrong - id=25/.php

   Right - .php?id=25

2. Page Extension CANNOT go BEFORE Domain Extension

   Wrong - index .php bing.com

   Right – bing.com/index.php

3. Parameter CANNOT go BEFORE Page Extension

   Wrong - Id=25/index.php

   Right – index.php?id=25

Syntax Rules

4. Parameter CANNOT go BEFORE Directories

Wrong - Id=25 /apps/index.html

Right - /apps/index.html?id=25

5. Parameter CANNOT go BEFORE Domain Extension

Wrong - Id=25 bing.com

Right – bing.com?id=25

Extended Search Operators Syntax –1 :

Operator	Function	Examlples
.	wildcard for a single character	fire.fox will return documents containing the phrases fire fox, fireAfox, fire1fox, fire-fox etc.
+	Connect Queries	Usage: Gaming + Shop
&	AND	Gaming & Shop
|	OR	"fire fox" | firefox will return documents containing the phrase fire fox or the word firefox

Extended Search Operators Syntax – 2 :

Operator	Function	Examlples
~	Synonym	E.g: ~happy Results: Happy, joyful, ecstatic. Same theory with keywords
" "	String together input.	"fire fox" will return documents containing the phrase fire fox
( )	String data together	Usage: (Gaming Health)
-	specifies that a phrase must not oc-cur in results	-fire will return documents that don't contain the word fire

Extended Search Operators Syntax – 3 :

Operator	Function	Examlples
*	wildcard for a single word	fire * fox will return documents containing the phrases fire the fox, fire in fox, fire or fox etc.
[x-x] Or [xxx]	String together input.	Usage: [0-11] [A-Z] [12345] How Google See's It" [0,1,2,3,4,5,6,7,8,9,10,11] [a,b,c,d,e,f,g,h,etc] [1,2,3,4,5]

Extended Search Operators

Operator	Function	Examlples
Site:	restricts results to sites within the specified domain	site:google.com fox will find all sites containing the word fox, located within the *.google.com domain
Intitle:	restricts results to documents whose title contains the specified phrase	intitle:fox fire will find all sites with the word fox in the title and fire in the text
Allintitle:	restricts results to documents whose title contains all the specified phrases	allintitle:fox fire will find all sites with the words fox and fire in the title, so it's equivalent to intitle:fox and intitle:fire
Intext:	Find text on pages	Usage: intext:Good morning ladies and gentlemen Result: will get sites with most those words in a phrase
Allintext:	Finds all text on page	Usage: intext:Good morning ladies and gentlemen Result:exact copy of text

Extended Search Operators

Operator	Function	Examlples
inurl :	restricts results to sites whose URL contains the specified phrase	inurl:fox fire will find all sites containing the word fire in the text and fox in the URL
Allinurl:	restricts results to sites whose URL contains all the specified phrases	allinurl:fox fire will find all sites with the words fox and fire in the URL, so it's equivalent to inurl:fox inurl:fire
cache:	Cached version of site on google	cache:site.com
Filetype:, ext:	restricts results to documents of the specified type	filetype:pdf fire will return PDFs containing the word fire, while filetype:xls fox will return Excel spreadsheets with the word fox
Numrange:	restricts results to documents con-taining a number from the specified range	numrange:1-100 fire will return sites containing a number from 1 to 100 and the word fire. The same result can be achieved with 1..100 fire Result:exact copy of text

Extended Search Operators

Operator	Function	Examlples
Link:	Restricts results to sites containing links to the specified location	**link:www.google.com** will return documents containing one or more links to www.google.com
Inanchor:	Find pages that are being linked to with specific anchor text. For this example, any results with inbound links containing either "apple" or "iphone" in the anchor text will be returned.	**inanchor:apple iphone**
Allinanchor:	Similar to "inanchor," but only results containing *all* of the specified words in the inbound anchor text will be returned.	**allinanchor:apple iphone**

Extended Search Operators

Operator	Function	Examlples
Info:	Show Google's Summary Information about a particular thing	info: linux
Related:	The related operator displays sites that Google has determined are related to a site,	related:linux
Group:	This operator allows you to search the title of Google Groups posts for search terms	group:*.forsale

Advance Dorking

Advanced Dorking is including Search Operators into your Dorks. This is pretty straightforward. The way we do this is simply by using our big brains to link phrases we wantto connect. If we want certain keywords to combine, we will use Search Operators todo that.If we want to prioritize a certain keyword, we can do that. This is about makingyour Dorksas optimized as they can get.

EXPLOITATION USING GOOGLE DORKING

Google queries for locating various Web servers

Query	Server
"Apache/1.3.28 Server at" intitle:index.of	Apache 1.3.28
"Apache/2.0 Server at" intitle:index.of	Apache 2.0
"Apache/* Server at" intitle:index.of	any version of Apache
"Microsoft-IIS/4.0 Server at" intitle:index.of	Microsoft Internet Information Services 4.0
"Microsoft-IIS/5.0 Server at" intitle:index.of	Microsoft Internet Information Services 5.0
"Microsoft-IIS/6.0 Server at" intitle:index.of	Microsoft Internet Information Services 6.0
"Microsoft-IIS/* Server at" intitle:index.of	any version of Microsoft Internet Information Services
"Oracle HTTP Server/* Server at" intitle:index.of	any version of Oracle HTTP Server
"IBM_HTTP_Server/* * Server at" intitle:index.of	any version of IBM HTTP Server
"Netscape/* Server at" intitle:index.of	any version of Netscape Server
"Red Hat Secure/*" intitle:index.of	any version of the Red Hat Secure server
"HP Apache-based Web Server/*" intitle:index.of	any version of the HP server

Queries for discovering standard post-installation Web server pages

Query	Server
`intitle:"Test Page for Apache Installation" "You are free"`	Apache 1.2.6
`intitle:"Test Page for Apache Installation" "It worked!" "this Web site!"`	Apache 1.3.0 – 1.3.9
`intitle:"Test Page for Apache Installation" "Seeing this instead"`	Apache 1.3.11 – 1.3.33, 2.0
`intitle:"Test Page for the SSL/TLS-aware Apache Installation" "Hey, it worked!"`	Apache SSL/TLS
`intitle:"Test Page for the Apache Web Server on Red Hat Linux"`	Apache on Red Hat
`intitle:"Test Page for the Apache Http Server on Fedora Core"`	Apache on Fedora
`intitle:"Welcome to Your New Home Page!" Debian`	Apache on Debian
`intitle:"Welcome to IIS 4.0!"`	IIS 4.0
`intitle:"Welcome to Windows 2000 Internet Services"`	IIS 5.0
`intitle:"Welcome to Windows XP Server Internet Services"`	IIS 6.0

Querying for application-generated system reports

Query	Type of information
"Generated by phpSystem"	operating system type and version, hardware configuration, logged users, open connections, free memory and disk space, mount points
"This summary was generated by wwwstat"	web server statistics, system file structure
"These statistics were produced by getstats"	web server statistics, system file structure
"This report was generated by WebLog"	web server statistics, system file structure
intext:"Tobias Oetiker" "traffic analysis"	system performance statistics as MRTG charts, network configuration
intitle:"Apache::Status" (inurl:server-status | inurl:status.html | inurl:apache.html)	server version, operating system type, child process list, current connections
intitle:"ASP Stats Generator *.*" "ASP Stats Generator" "2003-2004 weppos"	web server activity, lots of visitor information
intitle:"Multimon UPS status page"	UPS device performance statistics
intitle:"statistics of" "advanced web statistics"	web server statistics, visitor information
intitle:"System Statistics" +"System and Network Information Center"	system performance statistics as MRTG charts, hardware configuration, running services
intitle:"Usage Statistics for" "Generated by Webalizer"	web server statistics, visitor information, system file structure
intitle:"Web Server Statistics for ****"	web server statistics, visitor information
inurl:"/axs/ax-admin.pl" -script	web server statistics, visitor information
inurl:"/cricket/grapher.cgi"	MRTG charts of network interface performance
inurl:server-info "Apache Server Information"	web server version and configuration, operating system type, system file structure
"Output produced by SysWatch *"	operating system type and version, logged users, free memory and disk space, mount points, running processes, system logs

Google queries for locating passwords - 1

Query	Result
`"http://*:*@www" site`	passwords for site, stored as the string `"http://username:password@www..."`
`filetype:bak inurl:"htaccess|passwd|shadow|htusers"`	file backups, potentially containing user names and passwords
`filetype:mdb inurl:"account|users|admin|administrators|passwd|password"`	*mdb* files, potentially containing password information
`intitle:"Index of" pwd.db`	*pwd.db* files, potentially containing user names and encrypted passwords
`inurl:admin inurl:backup intitle:index.of`	directories whose names contain the words admin and backup
`"Index of/" "Parent Directory" "WS_FTP.ini" filetype:ini WS_FTP PWD`	*WS_FTP* configuration files, potentially containing FTP server access passwords
`ext:pwd inurl:(service|authors|administrators|users) "# -FrontPage-"`	files containing *Microsoft FrontPage* passwords
`filetype:sql ("passwd values *****" | "password values *****" | "pass values *****")`	files containing SQL code and passwords inserted into a database
`intitle:index.of trillian.ini`	configuration files for the *Trillian IM*
`eggdrop filetype:user user`	configuration files for the *Eggdrop* ircbot

Google queries for locating passwords - 2

`filetype:conf slapd.conf`	configuration files for *OpenLDAP*
`inurl:"wvdial.conf" intext:"password"`	configuration files for *WV Dial*
`ext:ini eudora.ini`	configuration files for the Eudora mail client
`filetype:mdb inurl:users.mdb`	*Microsoft Access* files, potentially containing user account information
`intext:"powered by Web Wiz Journal"`	websites using *Web Wiz Journal*, which in its standard configuration allows access to the passwords file – just enter `http://<host>/journal/journal.mdb` instead of the default `http://<host>/journal/`

`"Powered by DUclassified" -site:duware.com`
`"Powered by DUcalendar" -site:duware.com`
`"Powered by DUdirectory" -site:duware.com`
`"Powered by DUclassmate" -site:duware.com`
`"Powered by DUdownload" -site:duware.com`
`"Powered by DUpaypal" -site:duware.com`
`"Powered by DUforum" -site:duware.com`
`intitle:dupics inurl:(add.asp | default.asp | view.asp | voting.asp) -site:duware.com`
	websites using the *DUclassified*, *DUcalendar*, *DUdirectory*, *DUclassmate*, *DUdownload*, *DUpaypal*, *DUforum* or *DUpics* applications, which by default make it possible to obtain the passwords file – for DUclassified, just enter `http://<host>/duClassified/_private/duclassified.mdb` instead of `http://<host>/duClassified/`

`intext:"BiTBOARD v2.0" "BiTSHiFTERS Bulletin Board"`	websites using the *Bitboard2* bulletin board application, which on default settings allows the passwords file to be obtained – enter `http://<host>/forum/admin/data_passwd.dat` instead of the default `http://<host>/forum/forum.php`

Error message queries

Query	Result
`"A syntax error has occurred" filetype:ihtml`	*Informix* database errors, potentially containing function names, filenames, file structure information, pieces of SQL code and passwords
`"Access denied for user" "Using password"`	authorisation errors, potentially containing user names, function names, file structure information and pieces of SQL code
`"The script whose uid is " "is not allowed to access"`	access-related PHP errors, potentially containing filenames, function names and file structure information
`"ORA-00921: unexpected end of SQL command"`	*Oracle* database errors, potentially containing filenames, function names and file structure information
`"error found handling the request" cocoon filetype:xml`	*Cocoon* errors, potentially containing *Cocoon* version information, filenames, function names and file structure information
`"Invision Power Board Database Error"`	*Invision Power Board* bulletin board errors, potentially containing function names, filenames, file structure information and piece of SQL code
`"Warning: mysql_query()" "invalid query"`	*MySQL* database errors, potentially containing user names, function names, filenames and file structure information
`"Error Message : Error loading required libraries."`	CGI script errors, potentially containing information about operating system and program versions, user names, filenames and file structure information
`"#mysql dump" filetype:sql`	*MySQL database errors, potentially containing information about database structure and contents*

Searching for personal data and confidential documents

Query	Result
`filetype:xls inurl:"email.xls"`	*email.xls files*, potentially containing contact information
`"phone * * *" "address *" "e-mail" intitle: "curriculum vitae"`	CVs
`"not for distribution" confidential`	documents containing the confidential clause
`buddylist.blt`	*AIM* contacts list
`intitle:index.of mystuff.xml`	*Trillian IM* contacts list
`filetype:ctt "msn"`	MSN contacts list
`filetype:QDF QDF`	database files for the *Quicken* financial application
`intitle:index.of finances.xls`	*finances.xls* files, potentially containing information on bank accounts, financial summaries and credit card numbers
`intitle:"Index Of" -inurl:maillog maillog size`	*maillog* files, potentially containing e-mail
`"Network Vulnerability Assessment Report" "Host Vulnerability Summary Report" filetype:pdf "Assessment Report" "This file was generated by Nessus"`	reports for network security scans, penetration tests etc.

Queries for locating network devices

Query	Device
`"Copyright (c) Tektronix, Inc." "printer status"`	PhaserLink printers
`inurl:"printer/main.html" intext:"settings"`	Brother HL printers
`intitle:"Dell Laser Printer" ews`	Dell printers with EWS technology
`intext:centreware inurl:status`	Xerox Phaser 4500/6250/8200/8400 printers
`inurl:hp/device/this.LCDispatcher`	HP printers
`intitle:liveapplet inurl:LvAppl`	Canon Webview webcams
`intitle:"EvoCam" inurl:"webcam.html"`	Evocam webcams
`inurl:"ViewerFrame?Mode="`	Panasonic Network Camera webcams
`(intext:"MOBOTIX M1" | intext:"MOBOTIX M10") intext:"Open Menu" Shift-Reload`	Mobotix webcams
`inurl:indexFrame.shtml Axis`	Axis webcams
`SNC-RZ30 HOME`	Sony SNC-RZ30 webcams
`intitle:"my webcamXP server!" inurl:":8080"`	webcams accessible via *WebcamXP Server*
`allintitle:Brains, Corp. camera`	webcams accessible via *mmEye*
`intitle:"active webcam page"`	USB webcams

Folow me on instagram click here

Getting bored of theory let's go to the practical section.Get set started for real hacking.

For advance hacking tutorial visit

www.thecyberblogs.com