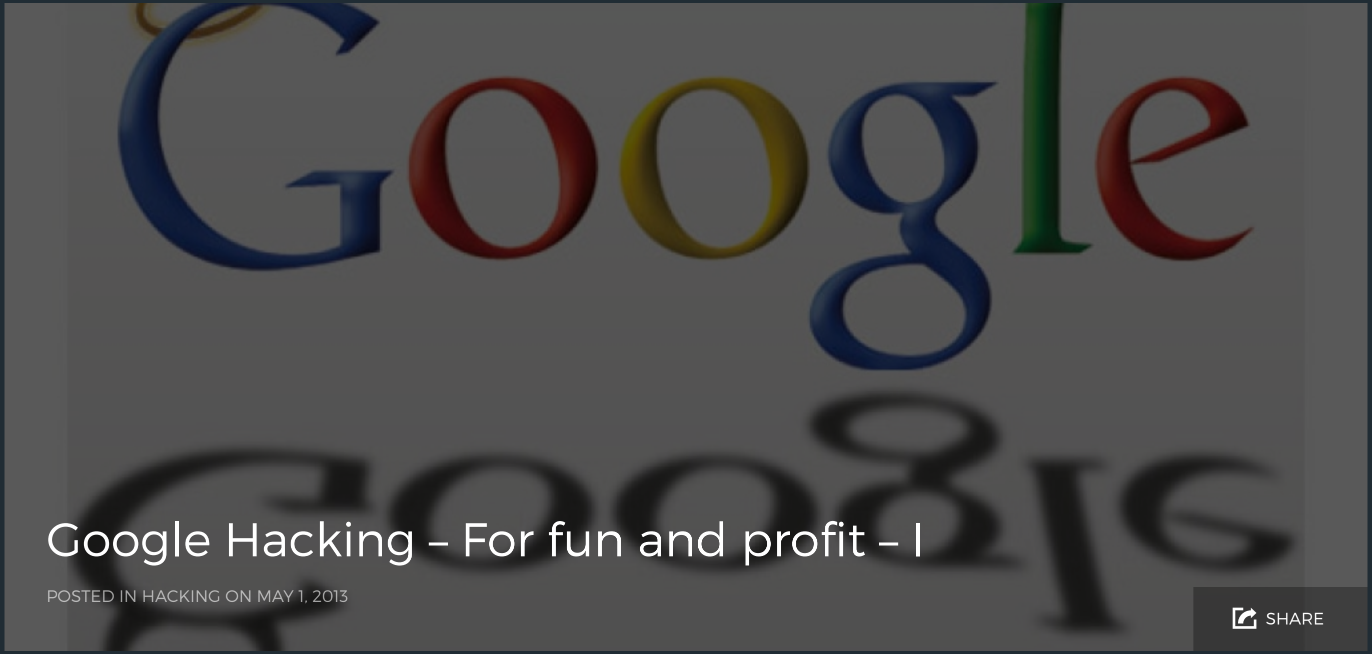


Google Hacking – For fun and profit – I

POSTED IN HACKING ON MAY 1, 2013

SHARE

lawyer to even the details of if you are pregnant. With so much intelligence built in to their systems, Google is surely a great information-gathering tool. As security analysts let's try to find out the proficiency of Google as a hacking tool in this article.

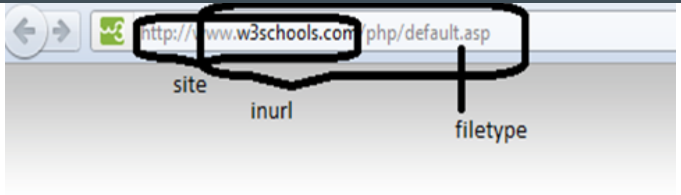
All of us have used Google for searching answers for our queries. What most of don't realize is the advantage of forming the search queries in Google to reveal sensitive information that we require to perform a successful attack. This can be accomplished by using the advanced operator features of Google. The basic syntax for using advanced operator in Google is as follows.

Operator_name:keyword

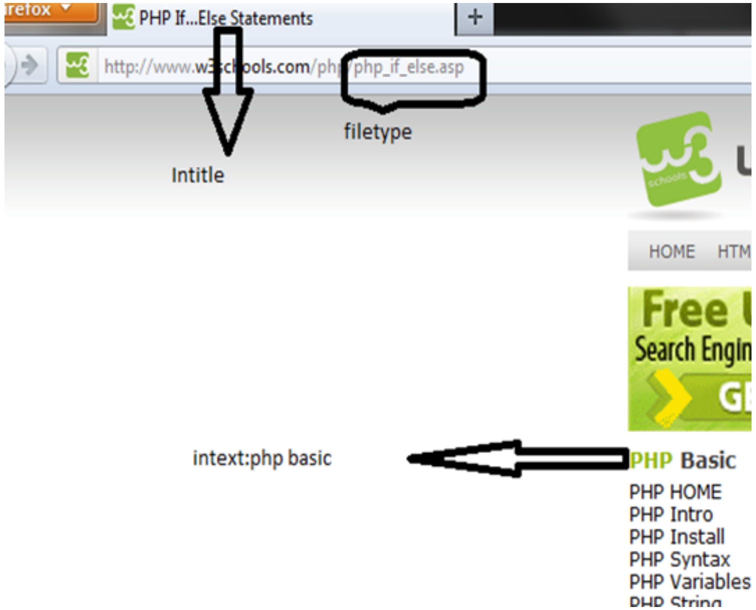
The syntax as shown above is a Google advanced operator followed by a colon, which is again followed by the keyword without any space in the string. This put together becomes an advanced query to Google. The usage of advanced operators in Google is termed as dorking. The strings are called Google Dorks a.k.a Google hacks. Dorks come in two forms vis-à-vis Simple dorks and complex dorks. Using a single advanced operator as your search string is called as simple dork whereas multiple advanced operators put together in a single search string is called as advanced dork. Each keyword/advance operator has a special meaning to the Google engine. It helps you filter out the unwanted results and narrows your searches by a great margin when these dorks are used. Let's take few examples of simple dorks.

Simple Google Dorks:

Allintext	Searches for occurrences of all the keywords given
Intext	Searches for the occurrences of keywords all at once or one at a time
Inurl	Searches for a URL matching one of the keywords
Allinurl	Searches for a URL matching all the keywords in the query
Intitle	Searches for occurrences of keywords in URL all or one
Allintitle	Searches for occurrences of keywords all at a time
Site	Specifically searches that particular site and lists all the results for that site
filetype	Searches for a particular filetype mentioned in the query
Link	Searches for external links to pages
Numrange	Used to locate specific numbers in your searches
Daterange	Used to search within a particular date range



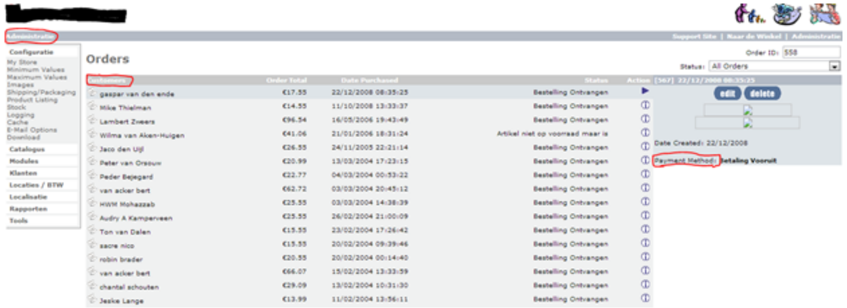
A single query can be used to get a particular result. But many single queries can be put in to one monster query and higher degree of filtration can be achieved resulting in the same particular page in your search results.



The above two diagrams illustrate few of the dorks in a pictorial manner. The same can be analogous to other advanced operators. So what can we find out using Google?

- Admin login pages
- Username and passwords
- Vulnerable entities
- Sensitive documents
- Govt/military data

admin catalog with detailed information of the customer names, payment methods, and order amounts. This information can be handy when performing social engineering on random targets.



[redacted]

Orders

Order ID: 558
Status: All Orders

Customers	Order Total	Date Purchased	Status	Action
gaspar van den ende	€17.55	22/12/2008 08:35:25	Bestelling Ontvangen	▶
Mike Thielman	€14.55	11/10/2008 13:33:37	Bestelling Ontvangen	ⓘ
Lambert Zweers	€96.54	16/05/2006 19:43:49	Bestelling Ontvangen	ⓘ
Wilma van Aken-Huigen	€41.06	21/01/2006 18:31:24	Artikel niet op voorraad maar is	ⓘ
Jaco den Uijl	€26.55	24/11/2005 22:21:14	Bestelling Ontvangen	ⓘ
Peter van Orsouw	€20.99	13/03/2004 17:23:15	Bestelling Ontvangen	ⓘ
Peder Bejegard	€22.77	04/03/2004 00:53:22	Bestelling Ontvangen	ⓘ
van acker bert	€62.72	03/03/2004 20:45:12	Bestelling Ontvangen	ⓘ
HWM Mohazzab	€25.55	03/03/2004 14:38:39	Bestelling Ontvangen	ⓘ
Audry A Kamperveen	€25.55	26/02/2004 21:00:09	Bestelling Ontvangen	ⓘ
Ton van Dalen	€15.55	23/02/2004 17:26:42	Bestelling Ontvangen	ⓘ
sacre nico	€15.55	20/02/2004 09:39:46	Bestelling Ontvangen	ⓘ
robin brader	€20.55	20/02/2004 00:14:40	Bestelling Ontvangen	ⓘ
van acker bert	€66.07	15/02/2004 13:33:59	Bestelling Ontvangen	ⓘ
chantal schouten	€29.09	13/02/2004 10:31:30	Bestelling Ontvangen	ⓘ
Jeske Lange	€13.99	11/02/2004 13:56:11	Bestelling Ontvangen	ⓘ

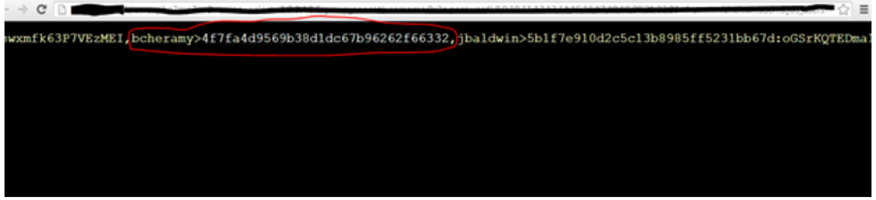
[567] 22/12/2008 08:35:25

Date Created: 22/12/2008

Payment Method: Betaling Vooruit

Dork: filetype:php inurl:catalog/admin/

This is an example of a simple query. Next, let’s see some juicy stuff, which comes in handy due to the efficiency of Google crawlers.

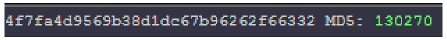


[redacted]

```
swxmfk63P7VEzMEI,bcheramy>4f7fa4d9569b38d1dc67b96262f66332,jbaldwin>5b1f7e910d2c5c13b8985ff5231bb67d:oGSrKQTEDmal
```

Dork: inurl:group_concat(username, filetype:php intext:admin

In the above screenshot, we were able to tap in to some of the SQL injection results done by somebody else on the sites. Unfortunately, the residue is still left in the search results. We happened to get our hands on username and password combinations, one of the accounts listed with the md5 hashes had the hash cracked, and the following combination was uncovered. The combination is bcheramy : 130270

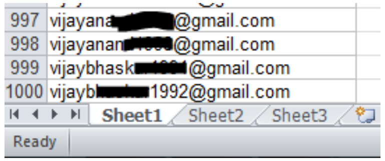


```
4f7fa4d9569b38d1dc67b96262f66332 MD5: 130270
```

The search results took, 0.25 Google seconds to appear. Does this mean we hacked an account in 0.25 seconds Google time? ;)

By now, I am sure; you would have got an idea as to how dangerous a tool Google can be. The usernames and passwords got from here can be used to strengthen our dictionary attacks by adding these used passwords to the list we already have. This can also be used in user profiling which seems to be in demand in the underground market. The above queries where just simple dorks which gave out sensitive information.

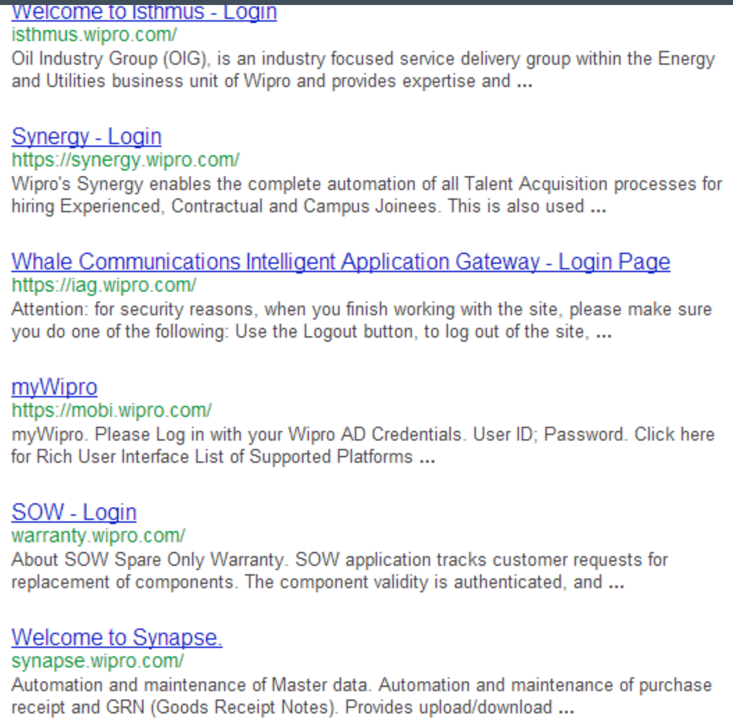
in no time!



997	vijayana[redacted]@gmail.com
998	vijayanan[redacted]@gmail.com
999	vijaybhask[redacted]@gmail.com
1000	vijayb[redacted]1992@gmail.com

Dork: intext:@gmail.com filetype:xls

Other capabilities of Google include site crawling/Network mapping. We use few other keywords to achieve this feat. What is so special about site crawling/Network mapping i.e. enumerating domain and hostnames? Well, all this is done without any probing at the target. The target that you are trying to enumerate cannot get a hint that you have already started plotting your attack against it. Google APIs used with a script combined with search results can give a big boost in this part of your attack. Let's see some example for the same.



Welcome to Isthmus - Login
isthmus.wipro.com/
Oil Industry Group (OIG), is an industry focused service delivery group within the Energy and Utilities business unit of Wipro and provides expertise and ...

Synergy - Login
https://synergy.wipro.com/
Wipro's Synergy enables the complete automation of all Talent Acquisition processes for hiring Experienced, Contractual and Campus Joinees. This is also used ...

Whale Communications Intelligent Application Gateway - Login Page
https://iag.wipro.com/
Attention: for security reasons, when you finish working with the site, please make sure you do one of the following: Use the Logout button, to log out of the site, ...

myWipro
https://mobi.wipro.com/
myWipro. Please Log in with your Wipro AD Credentials. User ID; Password. Click here for Rich User Interface List of Supported Platforms ...

SOW - Login
warranty.wipro.com/
About SOW Spare Only Warranty. SOW application tracks customer requests for replacement of components. The component validity is authenticated, and ...

Welcome to Synapse.
synapse.wipro.com/
Automation and maintenance of Master data. Automation and maintenance of purchase receipt and GRN (Goods Receipt Notes). Provides upload/download ...

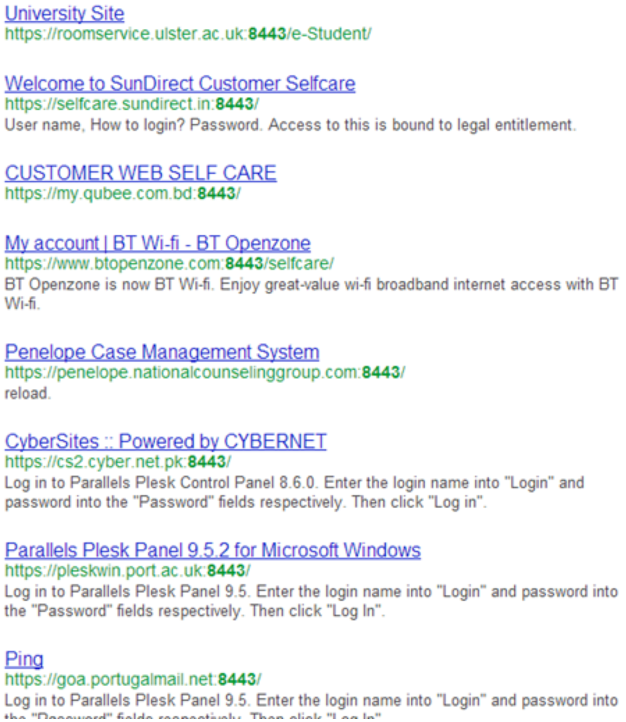
Dork:

site:wipro.com -site:www.wipro.com -site:careers.wipro.com

In the above example, you can see the usage of multiple simple dorks. Well, this is the negation operator provided by Google. The negation operator helps you subtract unwanted results from the search. The explanation for the above dork is as follows: Search the site wipro.com excluding the main site (www.wipro.com) and also exclude the subdomain (careers.wipro.com). In the search results, we are able to see few login pages. As every one of us is aware that, an organization's security is as strong as its weakest link (quoted from a blackhat-euro presentation), finding these third party logins and links allows an attacker to gain trusted entry into the target if these have some loopholes in them!

Another key word that I want you to try would be the Link operator whose usage is similar to that of site. A link to a site doesn't really carry much importance to an attacker, but a link from a site would mean that there is some form of trust connection between the two sites. Link command in Google can be used for finding external links to a site from another site.

as to how it can be achieved.



University Site
https://roomservice.ulster.ac.uk:**8443**/e-Student/

Welcome to SunDirect Customer Selfcare
https://selfcare.sundirect.in:**8443**/
User name, How to login? Password. Access to this is bound to legal entitlement.

CUSTOMER WEB SELF CARE
https://my.qubee.com.bd:**8443**/

My account | BT Wi-fi - BT Openzone
https://www.btopenzone.com:**8443**/selfcare/
BT Openzone is now BT Wi-fi. Enjoy great-value wi-fi broadband internet access with BT Wi-fi.

Penelope Case Management System
https://penelope.nationalcounselinggroup.com:**8443**/
reload.

CyberSites :: Powered by CYBERNET
https://cs2.cyber.net.pk:**8443**/
Log in to Parallels Plesk Control Panel 8.6.0. Enter the login name into "Login" and password into the "Password" fields respectively. Then click "Log in".

Parallels Plesk Panel 9.5.2 for Microsoft Windows
https://pleskwin.port.ac.uk:**8443**/
Log in to Parallels Plesk Panel 9.5. Enter the login name into "Login" and password into the "Password" fields respectively. Then click "Log In".

Ping
https://goa.portugalmail.net:**8443**/
Log in to Parallels Plesk Panel 9.5. Enter the login name into "Login" and password into the "Password" fields respectively. Then click "Log In".

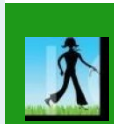
Dork: inurl:8443 -intext:8443

This dork lists all the sites running on port 8443. The query calls for sites with 8443 in the URL but excludes the redundant occurrence of 8443 in the text body thereby giving us URLs with respective ports. An automated scan on important ports can give interesting results.

In this article, we have seen a few common uses and some uncommon uses of Google dorks in getting some sensitive information. As said earlier the possibilities with Google are limitless. The limit is given by your creativity. There are lots more interesting details that Google can provide you. But I am storing them for the next installment of the article on Google hacks! Until then happy Googling :D

INFOSEC INFOSEC IQ TECHEXAMS

INFOSEC TOPICS ▾ CERTIFICATIONS ▾ EVENTS ▾ CAREERS CONTRIBUTORS ABOUT INFOSEC



AUTHOR

Karthik

Karthik is a cyber security researcher at Infosec Institute and works for Cyber Security and Privacy Foundation (a non-profit organization) as a researcher, in India. He finds deep interest in Information security as a whole, and is particularly interested in VA/PT and serving to the cause for Nation's Security.

FREE TRAINING TOOLS

Phishing Simulator

Security Awareness

- Keeping your cybersecurity skills relevant in 2019
- Top 50 Network Administrator Interview Questions [Updated for 2019]
- Reverse Engineering C++
- Malware: What are Trojans?
- Degree vs. certification: Entry-level IT auditor
- CySA+ domain #15: Implementing security best practices in the software development life cycle
- Access Control Models for ICS/SCADA environments
- Hack the Box (HTB) machines walkthrough series — Waldo
- Biggest data breaches of 2019 so far (Toyota, Capital One, AMCA and more)
- 7 most common application backdoors
- From hacker to lawyer: An expert in cybersecurity law
- A look at the first big GDPR fines
- FinCEN BEC attacks report: Analysis
- Bootcamp training vs. self-paced online training: A comparison for potential students

Security Awareness

DoD 8140

Ethical Hacking

Hacker Training Online

Security+

Computer Forensics

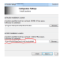
CISA

CCNA

PMP

Incident Response

MORE POSTS BY AUTHOR


Android Exploitation with Kali

Key Management

Analyzing Quantum Insert Attacks

2 responses to "Google Hacking – For fun and profit – I"

Haywood Jablome says:
December 10, 2013 at 3:14 pm
derp.
Reply

moreproject says:
September 17, 2018 at 2:06 am
thk. good article
Reply

Leave a Reply
Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Save my name, email, and website in this browser for the next time I comment.

– 2 = 7

Post Comment

Connect with us

Stay up to date with Infosec

Like 226 Follow @infosecedu

Join our newsletter

Get the latest news, updates & offers straight to your inbox.

ENTER YOUR EMAIL SUBSCRIBE