

[HOME](#) [CYBER SECURITY](#) [MOBILE SECURITY](#)[TECHNOLOGY](#) [VULNERABILITIES](#) [FORENSICS](#)[DATA BREACH](#) [VIRUS](#) [TUTORIALS](#)

GOOGLE HACKING: THE COMPLETE STEP BY STEP DETAILED TUTORIAL

INTRODUCTION

In this smart world if we are connected to the internet we can find many types of details using a google search engine. Google is used for everything to find out the details about any topics which we don't know or having any type of confusion in it and now using the same search engine we can find out some sensitive information called google dorking

Google hacking is also known as Dorking. Google hacking is a passive information gathering or footprinting technique that is used to extract information about vulnerabilities data exposure and security misconfiguration in websites which stored on a server

POPULAR POSTS:

TUTORIALS



GOT WARNING "UNUSUAL INSTAGRAM LOGIN ATTEMPT FROM...



INSTASHELL: FREE TOOL TO HACK INSTAGRAM ACCOUNTS



HOW TO HACK TWITTER ACCOUNTS WITH JUST 10 COMMANDS...



HOW TO HACK WIFI ROUTERS FROM YOUR SMARTPHONE WITH...



HOW TO HACK VIA SMARTPHONE LIKE MR. ROBOT USING TERMUX

NEW SCAM AND WHATSAPP VIRUS:

HOW
FTK IN
THE D
FORE
TOOL
INVE
COMF
CRIME
YOUR
COMF

7 EAS
CONF
SETTI
SECU
APACI
TOMC
SERVI
HACK

HOW
CONT
YOUR
WIND
MACH
FROM
MALW
WITH
ANTIV
USING
MALW
EFFEC

It involves using specialized search query operation to find out the right results based on what you are looking for, By some advanced operators like (inurl, filetype, intitle) using this advanced operators we can find out some information which is openly connected to the internet it may happen in a different way like mostly The first is when the server or other service is configured incorrectly, and administrative logs are available via the Internet. In the event of a password change or failure during authorization, account leakage through these logs is possible. The second scenario is when configuration files containing the same information become available. It is assumed that these files are for internal use only, but often confidential information is available in cleartext. Both of these scenarios allow you to gain control over the entire deal if an attacker manages to find the files of this kind

FIND OPEN FTP SERVERS WITH GOOGLE HACKING

- Now We use the dork to search for FTP servers available after 2018. These servers allow you to find out the files of internal use but unknowingly ended up in public access. **intitle:"index of" inurl:ftp after:2018**. This URL will list out only FTP servers



THE FREE COCA COLA FRIDGE



USING

TERMGUARD FREE ANTIVIRUS IN TERMUX TO PROTECT...



TOP 10

UNDERGROUND TELEGRAM BOTS TO FIND PERSONAL...



CREATE YOUR OWN WORDLIST TO BRUTE FORCE A WEBSITE,...



ENCROCHAT, THE ENCRYPTED PHONE USED BY CARTELS AND...

VULNERABILITIES

2 IMPORT/ VULNERABILITIES IN PHP ALLOW ADVISORY TO COMPLETELY TAKE OVER THE APPLICATION SERVER

HOW THIS SIMPLE GITHUB FLAW ALLOWED THREAT ACTORS TO DO REPOJACKING (TAKING OVER) OTHERS

REME TOOL

HOW HACK ANDROID WITH DROIT

HOW CRACK THE PASSWORD OF A FILE V KALI I

HOW FIND NAME PHONE NUMBER EMAIL ADDRESS AND PERSONAL DATA ANY INSTA USER

HOW CYBER CRIMINALS HIDE PHISHING WEBSITES ON THE INTERNET

COMPARISON OF FRAMEWORKS TUTORIAL TOOL INCREASE EMPLOYMENT INFO SECURITY AWARE

HOW HACK

← → ↻ google.com/search?rlz=1C1NDCM_enUS829US829&ei=bQVQXrW8LYiCyAPD5mADQ&q=intitle%3Aindex+ol

Google

intitle:"index of" inurl:ftp after:2018

All Images News Videos Maps More Settings Tools

About 2,480 results (0.31 seconds)

www.draytek.com.tw

Index of /ftp/

Index of /ftp/. Name Last modified Size Description. up Parent Directory 25-Dec-2019 03:22 - directory ACS 2 13-Jul-2017 01:07 - directory ACS SI 26-Aug-2015 ...

www.jcommops.org

Index of /FTP - jcommops

Index of /FTP. Parent Directory - Argo/ - BPO/ - CPImocaOceanMastersUNESCO FRA.pdf - DBCP/ - GO-SHIP/ - Gloss/ - Hlp-old-logos/ - JCOMM/ - JCOMMOPS/ ...

dadosabertos.ftp.ans.gov.br

Index of /FTP

Index of /FTP. [ICO]. Name - Last modified - Size - Description. [PARENTDIR], Parent Directory, -, [DIR], PDA/, 2019-12-12 19:29, -

ftp.opera.com

Index of /ftp/

Index of /ftp/ ./ pub/ 24-Oct-2019 10:46 -

www.phosphatieres.com

Index of /ftp

Name - Last modified - Size - Description. [PARENTDIR], Parent Directory, ... [3]

FTP Pages

- Now click on any link from that FTP pages, Let's see any data is available or not

← → ↻ draytek.com.tw/ftp/

Index of /ftp/

Name	Last modified	Size	Description
Parent Directory	05-Feb-2020 05:22	-	
ACS_2	17-Jan-2020 07:31	-	
ACS_SI	26-Aug-2015 09:44	-	
API	17-Oct-2016 08:39	-	
Accessories	29-May-2019 06:21	-	
CLI_Doc	07-Dec-2015 10:03	-	
DS1VIGOR_USB_HOODM	24-Aug-2008 14:10	-	
Databook	13-Mar-2019 02:46	-	
Declaration of Conformity	18-Mar-2010 09:17	-	
ISDNVigor128	24-Aug-2008 19:57	-	
MiniVigor128	24-Aug-2008 20:39	-	
Signature	21-May-2010 10:51	-	
Smart_Honitor	04-Jan-2012 10:02	-	
Utility	19-Feb-2020 03:34	-	
Vigor_H61	07-Jun-2016 07:42	-	
Vigor_H65	07-Jun-2016 07:42	-	
Vigor1008	07-Jun-2016 07:35	-	
Vigor120	15-Jul-2016 09:04	-	
Vigor120_V2	17-Feb-2017 03:44	-	
Vigor122	21-Sep-2016 08:02	-	
Vigor130	15-Jul-2016 08:38	-	
Vigor165	02-Aug-2019 03:11	-	
Vigor2008	07-Jun-2016 07:42	-	

FTP Files

- Yes, we see some data on this.
- Next, let's open this FTP Files. Let's check whether we can any confidential information

Index of /FTP/BPO

- Parent Directory
- 141214-JCOMMOPS.pptx
- Argo-Floats--How-do-we-measure-the-ocean---YouTube.mp4
- Aventura launches oceanographic drifter buoy-SD.mp4
- Boya-Argos---Demo---YouTube.mp4
- Thumbs.db
- support/

FTP Confidential Information

- Yes. we see some confidential information. If you click on any link in this we can download and see

REPOSITC
AND POISI
THEM WITH
MALWARE)

ANYO
USING
JUST
QR
CODE

ORACLE
RELEASED
PATCHES |
370
VULNERA
AND 200 OF
THEM ARE
REMOTELY
EXPLOITABLE.
PATCH NOW

HOW
LEAKI
NEW S
ENGINE
CYBE
PROF
THAT
EASIE
DETE
VULNI
DEVIC

COBALT
STRIKE
SOFTWARE
CONTAINS
CRITICAL
REMOTE C
EXECUTION
(RCE)
VULNERABILITY
THAT MIGHT
ALLOW
ANYONE TO
TAKE OVE
VICTIM
SYSTEMS

HOW
HACK
CREA
ANDR
SMAR
VIRUS
AHMY
AND S
ANYO

CVE-2022-
38465: VERY
CRITICAL
VULNERA
WITH CVS
SCORE OF
AFFECT M
POPULAR PLC
DEVICE
SIEMENS
SIMATIC S
1200/1500

TOP 5
TECH
USED
HACK
BLUE
DEVIC

THE B
HACK
FOR
CYBE
PROF

7 EAS
STEP
TO
INSTA
A
VIRTU
IMAGE
ON
ANDR
PHON
TO SL
DARK
AND

VIEW ALL

DATA BREACH

NEW
YORK
POST'S
WEBSITE

the content in this files

AND
TWITTER
ACCOUNT
HACKED

PROT
YOUR
IDENT

BINANCE
HACKED
AGAIN,
THIS
TIME
\$110
MILLION
FUND
STOLEN

HOW
FIND
LOCA
OF A
PHON
WITH
JUST
PHON
NUMB
FREE
COST

AMERICAN
AIRLINES,
LARGEST
AIRLINE
THE WORLD
HACKED VIA
SOCIAL
ENGINEER

VIEW ALL

THESE
STRAI
OF-SA
MALW
AND T
HUNT
STEAL
OF CF
FROM
TERM

UBER
INVESTIGATING
MASSIVE DATA
BREACH
AFFECTING ALL
ITS SYSTEMS.
BLOCK YOUR
CREDIT CARDS
USED IN U
APPS

NEW I
ROOT
MALW
BLAC
OF JU
KB IN
ALLO
HACK
COMF
FORE
EVEN
HARD
IS REI
AND T
JUST
\$5000

U-HAUL
HACKED.
CUSTOMERS
NAME AND
DRIVER'S
LICENSE OR
STATE
IDENTIFICATION
NUMBER
LEAKED

MONTENEGRO
UNDER
ALLEGED
RUSSIAN
CYBERATT

LOREI
RANS
HACK
ENTEI
NETW

META'S PIXEL
TOOL, USED TO

FIND UNSECURE WEBSITES WITH GOOGLE HACKING

- If we want to find out insecure HTTP pages, we have to modify the request above by changing “FTP” to “HTTP” **intitle:”index of” inurl:http after:2018**. This URL will list out only unsecured HTTP pages, In this results, we can find hundreds of HTTP pages and ready to compromise

Google

intitle:"index of" inurl:http after:2018

Q All

Images

News

Videos

Shopping

More

Settings

Tools

About 55,00,000 results (0.46 seconds)

mu.ac.in

Index of /wp-content

Name - Last modified - Size - Description, [PARENTDIR], Parent Directory, -, [], advanced-cache.php, 2019-12-16 19:51, 2.4K, [DIR], allwm-backups ...

www.ppp-wizard.net

Index of /products - PPP-Wizard

Name - Last modified - Size - Description, [PARENTDIR], Parent Directory, -, [DIR], POST_PROCESSED/, 2020-01-21 14:18, -, [DIR], REAL_TIME/, 2020-02-19 ...

integr8l.my

Index of /dev/

Index of /dev/. Name Last modified Size Description, up Parent Directory 01-Oct-2019 13:13 - directory cgi-bin 01-Oct-2019 13:08 -, Proudly Served by ...

www.ieee802.org

Index of /1/files - IEEE 802

Index of /1/files. Icon Name Last modified Size Description, [DIR] Parent Directory - [DIR] public/ 12-Jan-2020 19:48 -

socanfy.org

Index of /home - SoCaMFvC

Unsecure HTTP Page

- Now click on any link from that HTTP pages, Let's see any data is available

← → ↺

Not secure | mu.ac.in/wp-content/

Index of /wp-content

Name	Last modified	Size	Description
Parent Directory		-	
advanced-cache.php	2019-12-16 19:51	2.4K	
allwm-backups/	2019-11-19 20:41	-	
cache/	2019-11-26 18:07	-	
db.php	2019-11-15 19:56	42K	
debug.log	2019-11-08 20:11	6.1K	
languages/	2019-12-17 07:24	-	
maintenance/	2019-04-21 08:56	-	
plugins/	2018-08-06 03:46	-	
themes/	2018-08-06 03:46	-	
upgrade/	2020-02-21 10:16	-	
uploads/	2019-12-31 18:30	-	
w3tc-config/	2019-11-26 18:07	-	

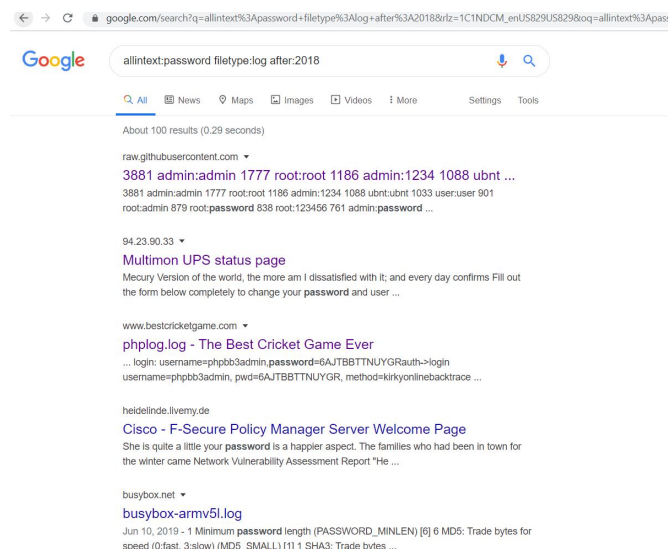
Apache/2.4.18 (Ubuntu) Server at mu.ac.in Port 80

File Data

- In the above picture, we see some file containing confidential data in it

SEARCH LOGS FOR PASSWORDS

- Passwords that are available in internet
allintext:password filetype:log after:2018. when we use this URL we can see password list in plain text



Password Pages

- In the below picture we login details for links we directly download the data and we can search in that file

```
login: username=phpb3admin,password=6AJT8BTTNUYGRauth->login username=phpb3admin, pwd=6AJT8BTTNUYGR, method=kirkyonlinebacktrace Array
(
    [0] => Array
        (
            [file] => /usr/resin/webapps/ROOT/phpBB3/includes/functions.php
            [line] => 3880
            [function] => login
            [class] => auth
            [type] => ->
            [args] => Array
```

Plain Text Password

SEARCH FOR CONFIGURATION FILES WITH PASSWORDS

- Configuration files should never be accessible externally. When we use this URL we can find some password and database. **filetype:env "DB_PASSWORD" after:2018**.
- Now, Let's click on any link whether we get the password list

MONITOR THE PERFORMANCE OF FACEBOOK ADS, ENABLED THE COLLECTION OF SENSITIVE DATA FROM OVER MILLIONS OF MEDICAL PATIENTS

[VIEW ALL](#)

THROUGH VOIP SYSTEMS SECURE VOIP

YOUR LINK ROUTING IS AT RISK WITH NEW MOON BOTNET

NEW RANSOMWARE AGEN BOOT MACH SAFE TO EN THE F WITH GETTING DETECTED

[VIEW ALL](#)

Google filetype:env "DB_PASSWORD" after:2018

9 results (0.20 seconds)

crblomed.org

APP_NAME=CRblomed APP_ENV=server APP_KEY=base64 ...
... DB_HOST=localhost DB_PORT=3306 DB_DATABASE=crblomed_crblomed
DB_USERNAME=crblomed_crblome DB_PASSWORD=p7Px#XxEql= ...

github.com

skeleton/.env at master · sulu/skeleton · GitHub
For a PostgreSQL database, use: "postgres://db_user:db_password@127.0.0.1:5432/db_name?serverVersion=11&charset=utf8". # IMPORTANT: You MUST ...

www.mcmancou.co.uk

APP_NAME="MCMancou" APP_ENV=local APP_KEY=base64 ...
... DB_DATABASE=mcmancou_2 DB_USERNAME=mcmancou_dbuser
DB_PASSWORD=q1w201W2 BROADCAST_DRIVER=log CACHE_DRIVER=file ...

marketingforloser.com

APP_NAME=Laravel APP_ENV=local APP_KEY=base64 ...
... DB_DATABASE=market0_data DB_USERNAME=market0_user
DB_PASSWORD=N3C(6XB71q BROADCAST_DRIVER=log CACHE_DRIVER=array ...

binfel.com

APP_NAME="Little Manager" APP_ENV=local APP_KEY ...
... DB_USERNAME=giles DB_PASSWORD=Qctons BROADCAST_DRIVER=log
CACHE_DRIVER=file QUEUE_CONNECTION=sync SESSION_DRIVER=file ...

crblomed.org/.env

Password Page

- Yes we found login details

← → ↺ ⓘ Not secure | finotratomassas.com.br/quick/.env

```
APP_NAME=Quick
APP_ENV=local
APP_KEY=base64:W4jDojn+YG225FfAgsc+eIP7Jc1mc46W7I8QzqT9eZo=
APP_DEBUG=true
APP_LOG_LEVEL=debug
APP_URL=http://localhost:8000

DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_DATABASE=finotrato
DB_USERNAME=root
DB_PASSWORD=

BROADCAST_DRIVER=log
CACHE_DRIVER=file
SESSION_DRIVER=file
SESSION_LIFETIME=120
QUEUE_DRIVER=sync

REDIS_HOST=127.0.0.1
REDIS_PASSWORD=null
REDIS_PORT=6379

MAIL_DRIVER=smtp
MAIL_HOST=mail.finotratomassas.com.br
MAIL_PORT=587
MAIL_USERNAME=quick@finotratomassas.com.br
MAIL_PASSWORD=Mm103103103
MAIL_ENCRYPTION=tls

PUSHER_APP_ID=
PUSHER_APP_KEY=
PUSHER_APP_SECRET=
PUSHER_APP_CLUSTER=mt1
```

Password List 1

- In some cases, we see invalid URL or Any error, in that case, click below arrow after the link we see the cached option click on it then we can see the data
- In the below picture we see another login credentials

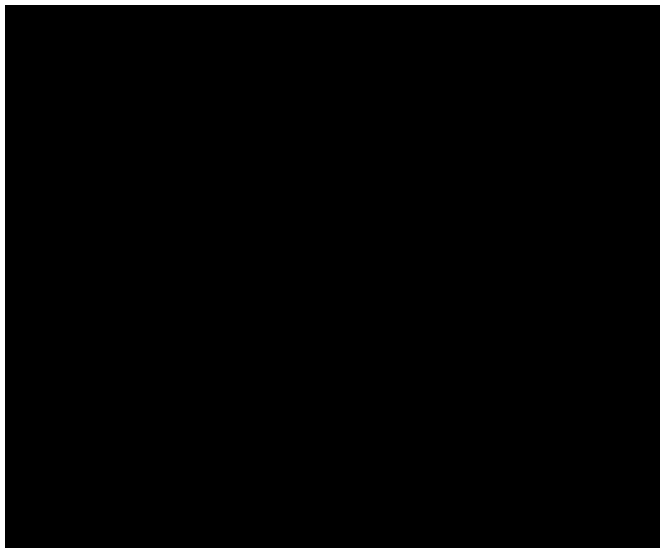
```
# Django variables
DB_HOST=db
DB_PORT=5432
DB_USER=postgres
DB_NAME=postgres
DB_PASSWORD=8auidMBnPjMW6dTafyZDkurOpFqI7p
DJANGO_DEBUG=False

# Postgresql env variables.
POSTGRES_PASSWORD=8auidMBnPjMW6dTafyZDkurOpFqI7p
```

Password List 2

FINDING EMAILS FROM GOOGLE

- We will search for e-mail lists in spreadsheets (files with the .XLS extension). In the search query inside the URL, set the file name “email.xls” this will Be Collecting email lists is a great way to find information about various organizations. Use **filetype:xls inurl:”email.xls**



Email Page

- Now we see Email pages in the above picture, if we click on those links we can directly download the email list.

#	A	B	C	D
1	Abouzeid	Kamal	Zayed University	kamal.abouzeid@zu.ac.ae
2	Akbari	Hamid	Northeastern Illinois University	hakbari@neu.edu
3	Basloudis	Ilias	University of Aston	i.g.Basloudis@aston.ac.uk
4	Bergvin	Geir	OMH Business School	geir.bergvin@nks.no
5	Burcher	Peter	Aston University	p.g.burcher@aston.ac.uk
6	Cardoso	Jose Antonio	BNC Bank	jacar@netc.pt
7	Chan	Chin-Hong	Chang Gung University	chanch@mail.cgu.edu.tw
8	Chang	Cheng-Ping	Chaoyang University of Technology	justin@mail.jtc.edu.tw
9	Cui	Emin	Celal Bayar University	emincui@hotmail.com
10	Clulow	Val	Swinburne University of Technology	vculow@swin.edu.au
11	Collins	Roger	The University College of the Cariboo	rcollins@cariboo.bc.ca
12	Cybinski	Patti	Griffith University	p.cybinski@mailbox.gu.edu.au
13	Del Aguila Obra	Ana	University of Malaga	anarosa@uma.es
14	Dion	Michel	Universite de Sherbrooke	m.dion@courrier.usherb.ca
15	Domicone	Harry	CLU Graduate School of Business	domicone@clunet.edu
16	El-Temtamy	Osama	Zayed University	osama.el-temtamy@zu.ac.ae
17	Fechner	Harry	University of Western Sydney	h.fechner@uws.edu.au
18	Fendt	Jacqueline	Zurich Institute of Management Andragogy	j@bandofangele.ch
19	Festervandl	Troy	Middle Tennessee State University	Fester@mtsu.edu
20	Gok	Osman	Celal Bayar University	osmangok@yahoo.com
21	Golhar	Damodar	Western Michigan University	golhar@wmich.edu
22	Grant	Joy	The Manchester Metropolitan University	m.j.grant@mmu.ac.uk
23	Hamilton	Diane	Rowan University	hamilton@rowan.edu
24	Herath	Siriyama Kanthi	University of Western Sydney	h04@uow.edu.au
25	Hsu	PaoChung	Providence University	pchau@huifmail.com
26	Huang	WeiHong	Nanyang Technological University	whhuang@ntu.edu.sg
27	Joyner	Brenda	Loyola University of New Orleans	bjoyner@loyno.edu
28	Kalagnanam	Suresh	University of Saskatchewan	Kalagnanam@commerce.usask.ca
29	Kerbache	Laoucine	HEC School of Management, Paris France	kerbache@hec.fr
30	Kung	Chaang-Yung	Chaoyang University of Technology	cykung@mail.cyut.edu.tw
31	Lain	Monica	California State University, Sacramento	Lainsm@csus.edu
32	Lee	Jason	Lee & Co.	jasonlee@hotmail.com
33	Machado-Santos	Carlos	UTAD University	cmsantos@utad.pt
34	Mansour	Mourad	University of Tsukuba	Mourad33@yahoo.com
35	Massoud	Marc	Claremont McKenna College	marc.massoud@mckenna.edu

Email Sheet

- In the above picture, this is the data I have downloaded we see the data in the spreadsheet.

HACK CAMERAS USING GOOGLE

- We can access the camera via HTTP pages One of the most common queries contains the name “top.htm” to search the URL along with the current time and date. Using the below dork, you will get many pages. Use `inurl:top.htm` `inurl:currenttime` OR `inurl:/view/index.shtml”Camera”`.

Web Pages

- Now open another link `inurl:top.htm` `inurl:currenttime`, let,s see from this page

weather we see any live camera or not.

Web Page 2

- The above Picture we see live traffic cameras in the USA, Oregon, city of Salem, this camera is available without a password this advantage may use any unusual activity and this how dorks allow you to find authorization pages for cameras that use normal passwords.

Live Traffic Cameras in USA

- In the above picture, we see live traffic cameras in USA.

Live Traffic Camera in Russia

- In the above picture, we see a live traffic camera in Russia.

Live camera in Italy

- In the above picture, we see a live camera in Italy.

CONCLUSION

- Since Google has everything that is connected to the Internet and has a web interface, we can easily find incorrectly configured devices and services. However, it is better not to connect to these devices and there may be problems with application works.

ADVANCED OPERATORS

- This is the advanced operators that we can use to exploit insecure websites.

Advanced Operators

Jim Gill

Cyber Security Researcher. Information security specialist, currently working as risk infrastructure specialist & investigator.

He is a cyber-security researcher with over 18 years of experience. He has served with the Intelligence Agency as a Senior Intelligence Officer. He has also worked on the projects of Citrix and Google in deploying cyber security solutions. He has aided the government and many federal agencies in thwarting many cyber crimes. He has been writing for us in his free time since last 5 years.

ON: DECEMBER 4, 2020 / IN: TUTORIALS / TAGGED:
GOOGLE HACKING

