Google Dorking & Shodan

Abhishek Pandey
Exploring the world of Cyber Security

About Author

Diploma in Cyber law
Social engineering
OSINT
Digital Forensics
Red teaming
Numismatics

First Things First

Is it legal?

Are we doing anything wrong?

What to expect at the end?

"we will search for vulnerable server and user, and will not exploit it"

Index of /sb/delhi/ggsipu/docs

Name	Last modified	Size	Description
Parent Directory		-	
Execom 2011-12.rar	2011-05-15 08:44	1.5M	
Execom 2011-12.tar.gz	2011-05-15 07:39	1.6M	
TechVeda.pdf	2011-10-06 15:03	2.1M	
TechVeda_2010_12.pdf	2010-10-28 07:20	7.2M	

ame	Last modified	Size	Description
arent Directory		-	
01MSDCF/	2013-08-27 11:00	-	
01PNV01/	2014-09-20 10:20	-	
012-10-18/	2014-09-20 09:16	-	
014-03-21 10.26.32.jpg	2015-05-01 13:36	2.9M	
014-03-21 10.28.30.jpg	2015-05-01 13:36	2.9M	
014-03-21 10.29.39.jpg	2015-05-01 13:37	2.9M	
014-03-21 14.49.30.jpg	2015-05-01 13:38	2.9M	
014-03-21 19.12.44.jpg	2015-05-01 13:38	2.7M	
014-03-21 19.18.28.jpg	2015-05-01 13:39	2.5M	
014-03-21 19.25.23.jpg	2015-05-01 13:39	1.4M	
VF_INFO/	2013-08-26 20:19	-	
ORY'S iPhone/	2015-05-02 09:47	-	
DCIM/	2013-08-26 20:19	-	
FileZilla 3.6.0.2 wi..>	2014-11-09 17:23	-	
MOVIES/	2015-02-08 03:54	-	
MP_ROOT/	2013-08-26 20:23	-	
Marsha.pdf	2013-11-08 09:28	21M	
PICTURES/	2015-02-08 04:13	-	

Content

Part 1: Google Hacking
- Basic of google
- How does google work
- Advance operator
- Hacking Basics
- Document Grinding
- Hacking Google services
- How to protect yourself

Part 2: Shodan
- Basic of shodan
- How does shodan work
- ...many more

India

All   Maps   News   Images   Videos   More   Settings   Tools

Shopping

Books

Flights

About 7,33,00,00,000 results (1.15 seconds)   Finance

Personal

Top stories

Eminent Muslim citizens hail PM Modi's outreach to minorities

Times of India

14 hours ago

Missing IAF AN-32 aircraft underscores plague of accidents in India Air Force; list of...

Firstpost

4 hours ago

Only Electric Bikes, Scooters May be Sold in India from April 2025 as Govt Looks to Cur...

News18.com

16 mins ago

Italy   Turkey   China   Japan   South Korea

Iraq   Afghanistan

Iran   Pakistan

Libya   Egypt   Saudi Arabia   India   Thailand

Niger   Chad   Sudan

Nigeria   Ethiopia

DRC   Kenya   Indonesia   Map data ©2019

→ More for India

India

Country in South Asia

India, also known as the Republic of India, is a country in South Asia. It is the seventh-largest country by area, the second-most populous country, and the most populous democracy in the world. Wikipedia

Official languages: Hindi, Bengali, Tamil, Telugu, English, Punjabi,
MORE Trending

Why?

1. User
2. Hacker

Google

john wick

All   Images   News   Videos   Shopping   More   Settings   Tools

About 15,90,00,000 results (1.28 seconds)

Showtimes for John Wick: Chapter 3 – Parabellum
All times are in IST

Today

All times   Morning   Afternoon   Evening   Night

INOX - Map
2:30pm   10:30pm

PVR ICON - Oberoi - Map
5:30pm

Inox - Map
4:55pm

More film times

John Wick: Chapter 3 – Parabellum
2019 · Thriller/Mystery · 2h 10m

▶ Play trailer on YouTube

8/10	90%	73%
IMDb	Rotten Tomatoes	Metacritic

https://www.google.ca/preferences?hl=en

Google

Sign in

Search Settings

Search results

Languages

Help

SafeSearch Filters

SafeSearch can help you block inappropriate or explicit images from your Google Search results. The SafeSearch filter isn't 100% accurate, but it helps you avoid most violent and adult content.

☐ Turn on SafeSearch   Lock SafeSearch

Results per page

| 10 | 20 | 30 | 40 | 50 | | 100 |

Faster   Slower

Where results open

☐ Open each selected result in a new browser window

Search history

When signed in, you can receive more relevant results and recommendations based on your search activity. You can turn off or edit your search history at any time.

Where results open

☐ Open each selected result in a new browser window

Search history

When signed in, you can receive more relevant results and recommendations based on your search activity. You can turn off or edit your search history at any time.

Region Settings

⦿ Current Region	○ Andorra	○ Armenia	○ Bahrain
○ Afghanistan	○ Angola	○ Australia	○ Bangladesh
○ Albania	○ Anguilla	○ Austria	○ Belarus
○ Algeria	○ Antigua & Barbuda	○ Azerbaijan	○ Belgium
○ American Samoa	○ Argentina	○ Bahamas	○ Belize

Show more ▾

Save   Cancel

Sign in to use any previous settings. Learn more

Google

साइन इन

खोज सेटिंग

खोज के नतीजे

भाषाएं

सहायता

सुरक्षित खोज फ़िल्टर

सुरक्षित खोज अनुपयुक्त या मुखर यौन चित्रों को आपके 'Google सर्च परिणामों से ब्लॉक करने में आपकी सहायता कर सकता है. सुरक्षित खोज फ़िल्टर 100% सटीक नहीं है, लेकिन यह ज़्यादातर हिंसक और वयस्क सामग्री से बचने में आपकी सहायता करता है.

☐ सुरक्षित खोज चालू करें   सुरक्षित खोज लॉक करें

प्रति पेज परिणाम

| 10 | 20 | 30 | 40 | 50 | | 100 |

ज़्यादा तेज़   धीमा
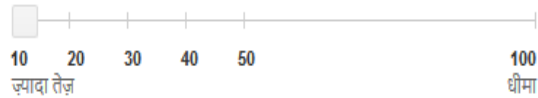
जहां परिणाम खुलें

☐ प्रत्येक चयनित परिणाम को एक नई ब्राउज़र विंडो में खोलें

تسجيل الدخول

Google

إعدادات البحث

نتائج البحث

اللغات

مساعدة

فلاتر البحث الآمن

يمكنك الاستفادة من البحث الآمن في حظر الصور غير الملائمة أو الإباحية من نتائج بحث Google، مع العلم بأن نسبة الدقة في فلتر البحث الآمن لا تصل إلى 100%، إلا أنه يساعدك في تجنب معظم محتوى العنف ومحتوى البالغين.

غلق البحث الآمن   ☐ تفعيل البحث الآمن

النتائج لكل صفحة

100			50	40	30	20	10
أبطأ							أسرع
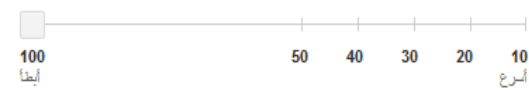
فتح النتائج في

☐ فتح كل نتيجة محددة في نافذة متصفح جديدة

سجل البحث

عند تسجيل الدخول، يمكنك استلام المزيد من النتائج والاقتراحات ذات الصلة استنادًا إلى نشاط البحث. ويمكنك إيقاف أو تعديل سجل البحث في أي وقت.

إعدادات المنطقة

Basic Operators

A+B   A-B

      A|B

1..10   A * C   "A
B C"

ABC = Variables

+"mahatma" +"gandhi"
+"mahatma" -"gandhi"
+"mahatma" |"gandhi"
+"mahatma gandhi"

Tips

1. Word limit:- 32

1. Stop words:- Where, How

1. Query processing is done from left to right

1. www.google.com/search?variable1=value1&VA2=VU2

1. %20=space

1. %22="

1. Intext:password | passcode intext:username | userid | user filetype:csv

1. Intext:(password | passcode) intext:(username | userid | user) filetype:csv

Advance Search Operator

oprator:SearchTerm or operator:"Search Term" or operator:Search Term	
Intitle:	allintitle:
filetype:	allintext:
site:	link:
inanchor:	daterange:
cache:	Info:
related:	phonebook:
rphonebook:	bphonebook:
author:	insubject:
msgid:	group:

Intitle:google intitle:"index of"

intitle:google

All · News · Maps · Images · Videos · More · Settings · Tools

About 57,50,00,000 results (0.74 seconds)

Google
https://www.google.com/ ▾
Settings Your data in Search H
YouTube · Play · News · Gmail
Google Account · Google News

Index of /download/Q/Q

Name	Last modified	
Parent Directory	-	
01-qrion-beach.mp3	28-Apr-2017 12:39	6.5M
02-qrion-mizu.mp3	28-Apr-2017 12:45	5.2M
03-qrion-sink.mp3	28-Apr-2017 12:51	6.0M
04-qrion-nothing.mp3	28-Apr-2017 12:57	4.0M
05-qrion-iphone_bubbling.mp3	28-Apr-2017 13:03	3.8M

https://www.

Index of /assets/data

- Parent Directory
- BedrRollAvailAndFare.json
- Loungesummery.json
- PKGdescription.json
- RRconfirmation.json
- WCTermsAndCon.html
- aa.json
- bedrollPaymentResponse.json
- getPckgOverViewDetails.json
- home.json
- laungedetail.json
- searchList.json

18

Intitle:"index of" "backup file"

intitle:"index of" "backup files"

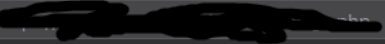**All** Images Videos News

About 3,710 results (0.20 seconds)

Index of /backup-files

Name	Last modified	Size	Description
Parent Directory		-	
2017/	2013-09-25 16:18	-	
bromilow2018.zip	2018-07-26 12:23	518M	
calculator.zip	2018-07-26 12:46	3.9M	
calculator_bk/	2017-10-20 18:44	-	
dev/	2018-07-26 12:26	-	
old_backup.zip	2018-07-26 12:25	899M	
sites/	2018-07-26 12:26	-	

```
'@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
'@@@@@@@@@  User Backup Script                        @@@@@@@@@
'@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

'&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&
'&&   Script: userbackup.vbs
'&&   Written By: Arian Padron
'&&   Purpose:  Backup My Documents, Desktop and Favorites to User network share
'&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&

'Create necessary objects
set shellObj = WScript.CreateObject("WScript.Shell")
set netObj = CreateObject("WScript.Network")
set fsObj = CreateObject("Scripting.FileSystemObject")

'*******************************************************************
'Global Settings
'       contains variables, constants, or other settings that are used throughout
'   the script
'*******************************************************************
set objWMIService = GetObject("winmgmts:\\.\root\cimv2")

'Query data via WMI
'*******************************************************************
'set SYSTEMINFO = objWMIService.ExecQuery("Select Name, UserName from Win32_ComputerSystem")
'set IPINFO = objWMIService.ExecQuery("Select IPAddress from Win32_NetworkAdapterConfiguration where IPEnabled=TRUE")
Dim objNetwork, objUser, CurrentUser
Set objNetwork = CreateObject("WScript.Network")
Set objUser = CreateObject("ADSystemInfo")
Set CurrentUser = GetObject("LDAP://" & objUser.UserName)
```

Index of /GTA.SA.BACKUP

Name	Last modified	Size	Description
Parent Directory		-	
cutscene.img/	2011-06-05 18:09	-	
files.sa-mp.com/	2011-06-05 18:28	-	
gta3.img/	2011-06-05 20:46	-	

Index of /backup/files/u578609749/.logs

- Parent Directory
- php_error.log
- php_error.log-20161120.gz
- php_error.log-20161121.gz
- php_error.log-20161122.gz
- php_error.log-20161123.gz
- php_mail.log
- php_mail.log-20161120.gz
- php_mail.log-20161121.gz
- php_mail.log-20161122.gz
- php_mail.log-20161123.gz

https://wikileaks.org/sony/docs/bonus/1/Password/group password list.txt

```
"Password List",
"Service","Web Address","User Name","Password","Additional Notes"
"diigo","http://www.diigo.com/user/sonypicturesresearch","sonypicturesresearch","spii"
"eBizMailer","https://66.161.124.152/ebiz40/listhome.do","spicture","sony12##"
"eMarketer","http://www.emarketer.com/Extranet.aspx?sony","mclemente@sonypictures.com","sony123"
"eMarketer","http://www.emarketer.com/Extranet.aspx?sony","nelshafie@sonypictures.com","sony1234"
"Falk","http://admin.as-us.falkag.net/login.php ","reports ","sonylogin1 "
"Forrester","http://www.forrester.com","ekhan@sonypictures.com","forrester","Individual accounts, Contact: hthompson@forrester.com"
"Forrester","http://www.forrester.com","kkuo@imageworks.com","spii"
"Forrester","http://www.forrester.com","mclemente@sonypictures.com","12345678"
"Forrester","http://www.forrester.com","nelshafie@sonypictures.com","sony1234"
"Google Search","https://10.200.31.161:8443/","kkuo","kuok","Contact: Brian Franke"
"Hitwise","https://login.hitwise.com/","mclemente","mikecard","Contact: nicole.swetley@hitwise.com  (Client Engagement Mgr) or david.constantino@hitwise.com (Client Development Mgr)"
"Hitwise","https://login.hitwise.com/","kkuo","sony12345"
"Hitwise","https://login.hitwise.com/","nadjae","sony1234"
"IPSH","http://ipsh03.ipsh.net/clientreports.nsf/sonybanners ","sonybanners","sony$3banners "
"Kishkee","http://www.kishkee.com","int-webdevelopment@sonypictures.com","s0ny!2011"
"Limelight","https://control.llnw.com/portal/login.do","sony-pictures","nrtds83 "
"Limelight","https://control.llnw.com/portal/login.do","nel-shafie","nadja123","for flash reports"
"Microsoft Tag Manager","http://tag.microsoft.com/consumer/index.aspx","int-webdevelopment@sonypictures.com","0ment@5","Contact: Amrish Parekh"
"Mobile Sales Application","https://wc.giantm.com/mgire","bspahr","th3c4ge "
"mQube","https://partners.m-qube.ca/index2.asp","bspahr","fruqa8eh "
"Nielsen//Netratings","http://www.nielsen-online.com/login.jsp","mclemente@sonypictures.com","Michael","Individual accounts, Contact: Gnotek, Tony [Tony.Gnotek@nielsen.com]"
"Sony.com Info","http://www.sony.com/SCA/info/documents/index.shtml ","sonydotcomresources ","info4you "
"Telephia","http://telephia.com","SONYRSCOTTO","SPDMOBILE12"
"Trymedia for AOL Games","https://rep.trymedia.com","trymedia-aolreports@sonypictures.com","4aolrep "
"Trymedia for Sony Games","https://rep.trymedia.com","trymedia-reports@sonypictures.com","4sonyrep "
"Variety.com","http://www.variety.com","rscotto","SPDRESEARC"
"Wallstreet Journal","http://online.wsj.com/home/media","rscotto","wallstreet","Security Question: ""What is your pet's name?"", Answer: dog"
"Web Analytics Association","http://www.webanalyticsassociation.org/index.asp","rscotto","imageworks"
"Yankee Group","http://www.yankeegroup.com","rscotto","413615"
"EXPIRED"
"The Platform","http://www.theplatform.com/","afredman@sonypictures.com ","5446Thatsmynumber"
"Clearspring Domestic","http://www.clearspring.com","sonypictures","sonypictures1"
"Clearspring (Hancock Intl Widget)","http://www.clearspring.com","SonyIntl","sonypictures"
"Clearspring (Pineapple Express Intl Widget)","http://www.clearspring.com","pesonyintl","s0nyr3vi3w"
"Harvest/Site Clarity (INTL)","https://reports.siteclarity.com/spdeintl/cgi-bin/index.pyc","rscotto ","spdharvest "
"Harvest/Site Clarity (US)","https://reports.siteclarity.com/spde/cgi-bin/index.py","rscotto ","spdharvest "
"Jupiter Research","http://www.jupiterresearch.com/","rscotto1 ","sony"
"Atomz","https://center.atomz.com","rscotto@sonypictures.com","sonysearch"
"Insight Express","http://www.insightexpress.com/","rscotto@sonypictures.com","spdsite2"
```

Inurl:admin index

Admin Login

USERNAME

User Name

This connection is not secure. Logins entered here could be compromised. Learn More

View Saved Logins

☐ Stay Signed in   Forgot Password ?

SIGN IN ➔

PTI LAHORE

Welcome, Please login

Username

Password

-- Select UC --

Create a New User   Log In

© 2017 Rapidzz
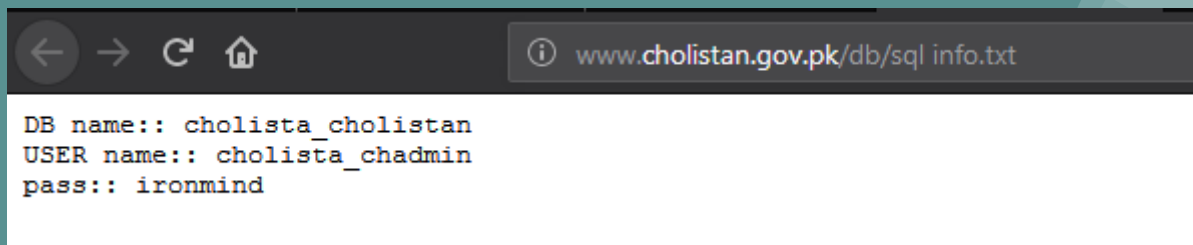
Firefox (1.x->3.x) Passwords:

serv - http://fr-fr.facebook.com
email   : roi_de_la_casse@hotmail.com
pass   : zzqqh9qy
----

serv - http://fr.youtube.com
username   : Sargerans
password   : zzqqh9qy
----

serv - http://snowtigers.net
username   : Maxter
password   : WOW071789788
----

serv - https://login.facebook.com
email   : roi_de_la_casse@hotmail.com
pass   : zzqqh9qy
----

serv - http://hostarea.org
login   : Sargeran
pass   : zzqqh9qy
----

serv - http://www.facebook.com

www.cholistan.gov.pk/db/sql info.txt

```
DB name:: cholista_cholistan
USER name:: cholista_chadmin
pass:: ironmind
```

	Territory Code	Territory Name	Salesperson Code	Country	Province-State	Status	Classification
1	Territory Code	Territory Name	Salesperson Code	Country	Province-State	Status	Classification
2	1000	Iowa, Dealers	5473	US	IA	ACT	DEALERS
3	1001	Ohio, Dealers	5434	US	OH	ACT	DEALERS
4	1002	Utah, Dealers	5445	US	UT	ACT	DEALERS
5	1004	Florida South E. Dealers	5381	US	FL	ACT	DEALERS
6	1005	Idaho, Dealers	5445	US	ID	ACT	DEALERS
7	1006	Maine, Dealers	5491	US	ME	ACT	DEALERS
8	1008	Alaska, Dealers	5302	US	AK	ACT	DEALERS
9	1009	Hawaii, Dealers	5302	US	HI	ACT	DEALERS
10	1010	Kansas, Dealers	5471	US	KS	ACT	DEALERS
11	1011	National Mexico, Dealers	5302	MX		ACT	DEALERS
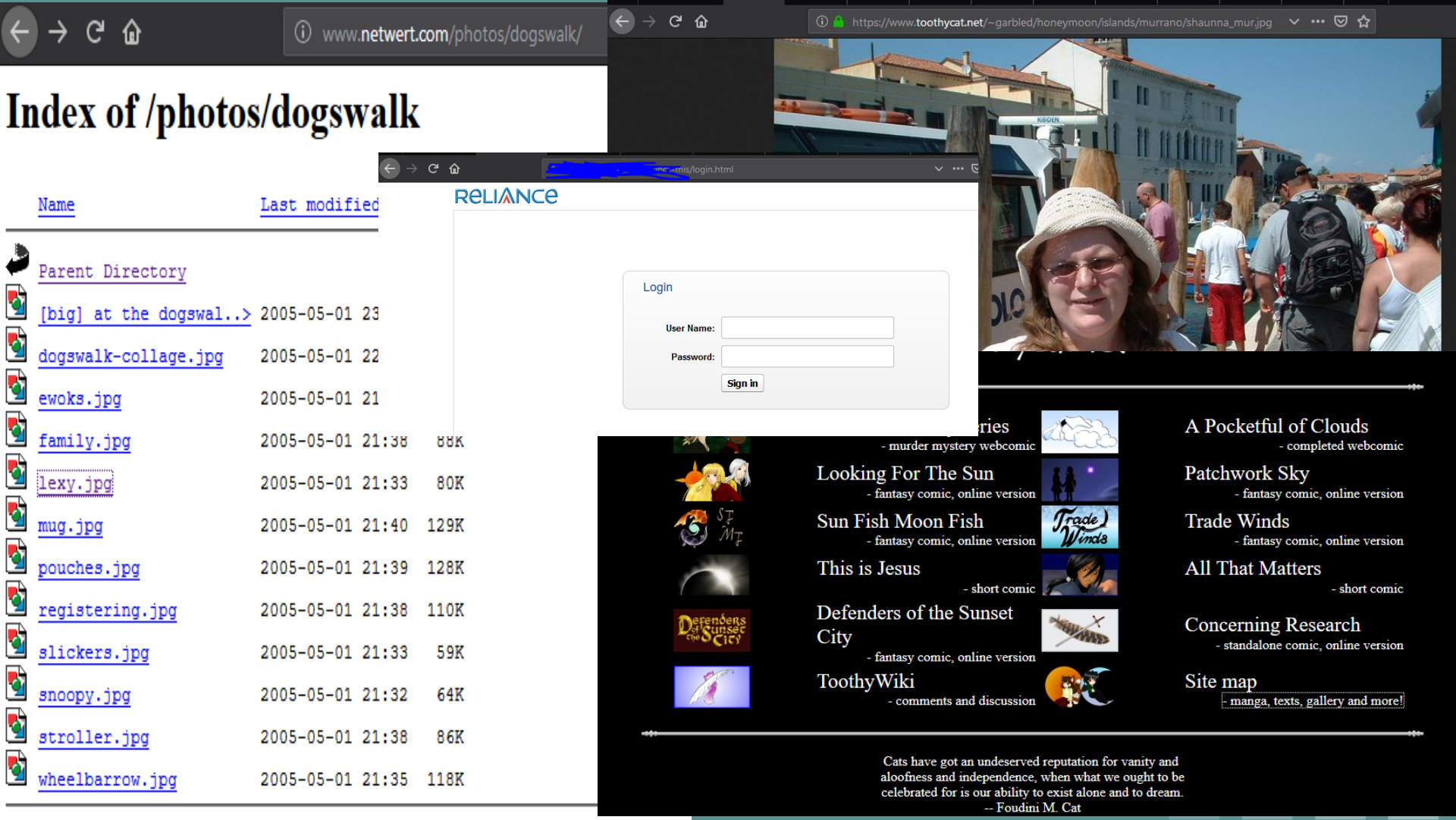
Index of /photos/dogswalk

Name	Last modified	
Parent Directory		
[big] at the dogswal..>	2005-05-01 23	
dogswalk-collage.jpg	2005-05-01 22	
ewoks.jpg	2005-05-01 21	
family.jpg	2005-05-01 21:38	88K
lexy.jpg	2005-05-01 21:33	80K
mug.jpg	2005-05-01 21:40	129K
pouches.jpg	2005-05-01 21:39	128K
registering.jpg	2005-05-01 21:38	110K
slickers.jpg	2005-05-01 21:33	59K
snoopy.jpg	2005-05-01 21:32	64K
stroller.jpg	2005-05-01 21:38	86K
wheelbarrow.jpg	2005-05-01 21:35	118K

RELIANCE

Login

User Name:

Password:

Sign in

A Pocketful of Clouds
- completed webcomic

...ries
- murder mystery webcomic

Patchwork Sky
- fantasy comic, online version

Looking For The Sun
- fantasy comic, online version

Trade Winds
- fantasy comic, online version

Sun Fish Moon Fish
- fantasy comic, online version

All That Matters
- short comic

This is Jesus
- short comic

Concerning Research
- standalone comic, online version

Defenders of the Sunset City
- fantasy comic, online version

Site map
- manga, texts, gallery and more!

ToothyWiki
- comments and discussion

Cats have got an undeserved reputation for vanity and
aloofness and independence, when what we ought to be
celebrated for is our ability to exist alone and to dream.
-- Foudini M. Cat

intitle:index.of ws_ftp.log

Index of /servicios

Name	Last modified	Size	Description
Parent Directory		-	
1.act	2012-10-30 12:42	1.9K	
WS_FTP.LOG	2012-10-30 12:42	2.3K	
ahorroperu.act	2012-10-30 12:42	12K	
cheques.act	2012-10-30 12:42	128	
compraventa.act	2012-10-30 12:42	2.2K	
index.act	2012-10-30 12:42	5.4K	
interclick.act	2012-10-30 12:42	7.3K	
monedas.act	2012-10-30 12:42	757	
pagoimportaciones.act	2012-10-30 12:42	114	
procedimientos.act	2012-10-30 12:42	4.6K	
receppagos.act	2012-10-30 12:42	124	
seguroargentina.act	2012-10-30 12:42	227	

intitle:index.of "server at"

Index of /server/publ

Name	Last modified	Size	Description
Parent Directory		-	
AsDRF1/	07-Apr-2009 16:55	-	
CGR.2004/	23-Jul-2004 00:07	-	
JME.1996/	23-Jul-2004 00:07	-	
PLOS.2005/	25-May-2005 00:56	-	
PNAS.1997/	23-Jul-2004 00:07	-	
PNAS.2004/	23-Jul-2004 00:07	-	
TEMP/	23-Jul-2004 00:07	-	
ZEB/	23-Jul-2004 00:07	-	

Apache/2.2.34 (Amazon) Server at www.girinst.org Port 443

Index of /downloads/Server/2.3.8

Name	Last modified	Size	Description
Parent Directory		-	
UrBackup Server 2.3.8(x64).msi	2019-03-20 09:40	7.0M	
UrBackup Server 2.3.8.exe	2019-03-20 09:40	31M	
debian/	2019-03-20 09:42	-	
urbackup-server-2.3.8.tar.gz	2019-03-20 09:40	7.6M	
urbackup-server-dbg_2.3.8_amd64.deb	2019-03-20 09:40	1.8M	
urbackup-server_2.3.8_amd64.deb	2019-03-20 09:40	3.7M	
urbackup-server_2.3.8_armhf.deb	2019-03-20 09:40	3.2M	

Apache/2.4.10 (Debian) Server at www.urbackup.org Port 443

Index o

Name			
Parent Dire			
app.js			
app/			
config/			
data/			
gulpfile.js			
images/			
node_modu			
package.json	2016-12-12 14:46	1.3K	
public/	2016-12-12 14:46	-	
readme.md	2016-12-12 14:46	2.9K	
views/	2016-12-12 14:46	-	

Apache/2.4.7 (Ubuntu) Server at mnj.io Port 80

Index of /extra

Name	Last modified	Size	D
Parent Directory		-	
CHANGELOG.TXT	2011-06-08 16:55	53K	
FAQ.TXT	2011-06-08 16:55	2.5K	
Group-Office.php	2011-06-08 16:55	5.8K	
HtmlEditorSpellCheck.php	2011-06-08 16:55	3.7K	
INSTALL.TXT	2011-06-08 16:55	2.8	
LICENSE.AGPL	2011-06-08 16:55	34	
LICENSE.TXT	2011-06-08 16:55	1.5	
RELEASE.TXT	2011-06-08 16:55	17	
about.php	2011-06-08 16:55	1.8	
action.php	2011-06-08 16:55	10	
change_lost_password.php	2011-06-08 16:55	1.8	
classes/	2011-06-08 17:00	-	
cli-functions.inc.php	2011-06-08 16:55	9?	
compress.php	2011-06-08 16:55	1.2	
config.php	2017-12-13 08:54	2.7	
config.php.bak	2017-12-13 08:54	2.7	

Name	Last modified	Size	Description
Parent Directory		-	
TMP6balyviq87.htm	2017-06-02 09:36	17K	
TMP6balyviq87.htm.bak	2015-09-30 14:15	17K	
TMP9omu8v201x.htm	2017-06-02 09:33	17K	
TMP9omu8v201x.htm.bak	2015-09-30 14:15	17K	
TMP9wpdm6qa2e.htm	2017-06-02 09:36	20K	
TMP9wpdm6qa2e.htm.bak	2015-09-30 14:15	20K	
TMPaeznlvivjm.htm	2017-06-02 09:33	11K	
TMPaeznlvivjm.htm.bak	2015-09-30 14:15	11K	
TMPjro2xuaqi1.htm	2017-06-02 09:33	16K	
TMPjro2xuaqi1.htm.bak	2015-09-30 14:15	16K	
mm/	2015-09-24 10:24	-	
admin/	2015-09-30 14:16	-	

Index of /blog

Name	Last modified	Size	Description
Parent Directory		-	
admin/	2007-02-13 17:58	-	
archive.php	2007-02-13 17:57	1.4K	
blog_images/	2010-04-01 09:27	-	
comments_form.php	2007-02-13 17:57	2.1K	
index.php.bak	2007-02-13 17:58	9.8K	
recent.php	2007-02-13 17:58	1.3K	

Index of /alumni

Name	Last modified	Size	Description
Parent Directory		-	
Alumchg.htm	2016-01-01 10:13	45K	
Alumdece.htm	2016-01-01 10:13	11K	
Meeting98.html	2016-01-01 10:13	5.5K	
aboutal.htm	2016-01-01 10:13	901	
adovbs.inc	2016-01-01 10:13	9.8K	
alumemai.htm	2016-01-01 10:13	191K	
alumform.htm	2016-01-01 10:13	4.6K	
alumsearch-test.asp	2016-01-01 10:13	3.0K	
nsearch.asp	2016-01-01 10:13	2.9K	
nsearch.php.bak	2016-01-01 10:13	3.5K	
aws.htm	2016-01-01 10:13	11K	
p.htm	2016-01-01 10:13	12K	
mit.htm	2016-01-01 10:13	1.6K	
h.gif	2016-01-01 10:13	1.3K	
r_log	2016-01-01 10:13	72K	
nt.htm	2016-01-01 10:13	2.6K	
n.htm	2016-01-01 10:13	2.5K	
ctions.php.bak	2016-01-01 10:13	9.6K	
ex.php.bak	2016-01-01 10:13	3.4K	
.htm	2016-01-01 10:13	1.4K	

intitle:index.of inurl:0001

Index of /reps/rep-0001

Name	Last modified	Size	Description
Parent Directory		–	
rep-0001-1.png	31-May-2019 23:06	20K	

Apache Server at www.ros.org Port 80

Index of /reps

Name	Last modified	Size	Description
Parent Directory		–	
README.txt	31-May-2019 23:06	633	
mermaid.css	31-May-2019 23:06	3.9K	
mermaid.js	31-May-2019 23:06	1.4M	
rep-0000.html	31-May-2019 23:06	21K	
rep-0000.rst	31-May-2019 23:06	11K	
rep-0001.html	31-May-2019 23:06	33K	
rep-0001/	31-May-2019 23:06	–	
rep-0002.html	31-May-2019 23:06	15K	
rep-0003.html	31-May-2019 23:06	30K	
rep-0008.html	31-May-2019 23:06	26K	
rep-0009.html	31-May-2019 23:06	19K	
rep-0010.html	31-May-2019 23:06	9.7K	
rep-0012.html	31-May-2019 23:06	39K	
rep-0100.html	31-May-2019 23:06	28K	
rep-0101.html	31-May-2019 23:06	16K	
rep-0102.html	31-May-2019 23:06	29K	
rep-0103.html	31-May-2019 23:06	18K	

filetype:cfg mrtg "target[*]" -sample -cvs -example

```
# Created by
# /usr/local/mrtg-2/bin/cfgmaker --global "WorkDir: /var/www/mrtg" --global "Options[_]
zsladmin@150.254.151.120


### Global Config Options

#   for UNIX
# WorkDir: /home/http/mrtg

#   or for NT
# WorkDir: c:\mrtgdata

### Global Defaults

#   to get bits instead of bytes and graphs growing to the right
# Options[ ]: growright, bits
```

```
WorkDir: /usr/people/glenn/ircache/mrtg
IconDir: /usr/people/glenn/ircache/mrtg
Options[^]: perhour

Target[cacheServerRequests]: cacheServerRequests&cacheServerRequests:public@localhost:3401
MaxBytes[cacheServerRequests]: 100000
Title[cacheServerRequests]: cacheServerRequests
Options[cacheServerRequests]: gauge, growright
PageTop[cacheServerRequests]: <h1>cacheServerRequests @ localhost</h1>
YLegend[cacheServerRequests]:
LegendI[cacheServerRequests]: cacheServerRequests
LegendO[cacheServerRequests]:
Legend1[cacheServerRequests]: cacheServerRequests
Legend2[cacheServerRequests]:

Target[cacheServerErrors]: cacheServerErrors&cacheServerErrors:public@localhost:3401
MaxBytes[cacheServerErrors]: 100000
Title[cacheServerErrors]: cacheServerErrors
Options[cacheServerErrors]: gauge, growright
PageTop[cacheServerErrors]: <h1>cacheServerErrors @ localhost</h1>
YLegend[cacheServerErrors]:
LegendI[cacheServerErrors]: cacheServerErrors
LegendO[cacheServerErrors]:
Legend1[cacheServerErrors]: cacheServerErrors
Legend2[cacheServerErrors]:

Target[cacheServerInKb]: cacheServerInKb&cacheServerInKb:public@localhost:3401
MaxBytes[cacheServerInKb]: 100000000
Title[cacheServerInKb]: cacheServerInKb
Options[cacheServerInKb]: gauge, growright
```

```
PageTop[submitted-messages]: <H1>This page shows the number of messages have been submitted</H1>
Options[submitted-messages]: integer,nopercent,perminute
LegendI[submitted-messages]: Submitted Messages
LegendO[submitted-messages]:
YLegend[submitted-messages]: Messages/Minute
ShortLegend[submitted-messages]: msgs/m
Legend1[submitted-messages]: The Number of Submitted Messages per Minute
Legend2[submitted-messages]:
Target[submitted-messages]: 1.3.6.1.4.1.5678.2.1.2.3.0&.1.3.6.1.4.1.5678.2.1.2.3.0:<community>@<ip>

PageTop[delivered-messages]: <H1>This page shows the number of successfully delivered and failed recipients</H1>
Options[delivered-messages]: integer,nopercent,perminute
LegendI[delivered-messages]: Delivered Recipients
LegendO[delivered-messages]: Failed Recipients
YLegend[delivered-messages]: Recipients/Minute
ShortLegend[delivered-messages]: msgs/m
Legend1[delivered-messages]: The Number of Delivered Recipients per Minute
Legend2[delivered-messages]: The Number of Failed Recipients per Minute
Target[delivered-messages]: 1.3.6.1.4.1.5678.2.1.2.22.0&.1.3.6.1.4.1.5678.2.1.2.20.0:<community>@<ip>
```

filetype:xls username password email

PORTAL LOGIN DETAILS

S.No.	Site	Login Id	Password	Email
1	WWW.createspace.com		Findresume	vijethak_____com
2	www.resume-india.com		Resume123#	jobs_____com
3	www.A2Zjobs.in		Sunshine1	Vijethau_____il.com
4	Babajobs.com		Wintersale	Vijethau_____il.com
5	OLX.com		London	Vijethau_____l.com
6	Quikr		Mangofruity	vijethau_____l.com
7	PlacementIndia.com		Orange123	Vijetha_____
8	Job is Job		Studentwin	Vijetha_____
9	ClickJobs.com		Urogulfjobs	Vijetha_____l.com
10	WiseStep.com		january144@u	bestj_____om
11	CareerBuilder		India123	bestj_____om
12	Iconjob.com		North123	vijethau_____il.com
13	Jobsindia.com		Recruiter	vijeth_____
14	Vivastreet	vijethau____@gmail.com	Vivastreet	vijetha_____l.com
15	Jobsviewer.com	vijethaurogul@gmail.com	Wonderful	vijethau_____
16	FreshersWorld.com		Freshers	vijethau_____
17	Jobsomega.com	Vijetha	BUILDING(B is small letter)	vijethaur_____
18	Keralajobfair.com		Wipro123	vijethaur_____
19	Topindiajobs.com		Capital123	Resum_____.com
20	Placementpoint.com		intexbadyear42	vijethau_____mail.com
21	Naukari2000		Naukari2000	Resum_____f.com
22	AlljobsHome.com		Satelite5	vijet_____
23	Adoos.in		Careerjobs1#	res_____
24	Jobs-bank.com		Placement123	vijet_____mail.com
25	Careesma		Strength123	_____

Information collection framework

abhishek@gmail.com->abhishekatgmaildotcom->"abhishek at gmail dot com"

abhishek@gmail.com->"abhishek gmail com" ->"abhishek@gmail.com"

Steps for email verification:-
      $host -t mx gmail.com
      $telnet gmail-smtp-in.l.google.com 25
      HELO test
      abhishekpandey1103@gmail.com
      quite

Exploits

"#include<stdio.h>" usage exploit

"#include<stdio.h>" usage exploit telnet   🔍

All   News   Videos   Images   Maps   More   Settings   Tools

About 17,800 results (0.45 seconds)

How to write remote exploits – OUAH
www.ouah.org/readmeneu.htm ▾
We want to exploit a vulnerable server program (vulnerable.c). We want to get a … #include
<stdio.h> #include <netdb.h> … Here's how you must compile and use the program. … Trying ::1…
telnet: connect to address ::1: Connection refused.

TelnetD encrypt_keyid – Function Pointer Overwrite – Exploit Database
https://www.exploit-db.com/exploits/18280 ▾
Dec 26, 2011 - CVE-2011-4862CVE-78020 . remote exploit for Linux platform. … #include <stdio.h>
#include <stdlib.h> #include <string.h> #include <unistd.h> …. NULL, NULL} }; /* Telnet commands
*/ static unsigned char tnet_init_enc[] …

BSD – 'TelnetD' Remote Command Execution (1) – Exploit Database
https://www.exploit-db.com/exploits/409 ▾
Jun 9, 2001 - CVE-6106CVE-2001-0093 . remote exploit for BSD platform. … #include <unistd.h>
#include <stdio.h> #include <stdlib.h> #include <string.h> … check telnetd only */ void usage (char
*progname); int xp_check (int fd); void …. tightly aligned and\n" "send 16/34mb of traffic to the remote
telnet daemon. it might …

"#include<stdio.h>" usage exploit telnet filetype:c

About 288 results (0.31 seconds)

exploits/apache-ex.c at master · perlancar/exploits · GitHub
https://github.com/perlancar/exploits/blob/master/apache/slapper/apache-ex.c ▾
Contribute to perlancar/**exploits** development by creating an account on … Then **use** another **exploit** to get r00t … **#include <stdio.h>** … #include <arpa/**telnet**.h>.

PacketStorm-Exploits/telnetd-encrypt_keyid.c at master · BuddhaLabs …
https://github.com/BuddhaLabs/PacketStorm-Exploits/…exploits/telnetd-encrypt_keyid.c
Usage: *. * $ gcc **exploit**.c -o **exploit**. *. * $ ./**exploit** 127.0.0.1 23 1. * [<] Succes … **Telnet** initial encryption mode and IV sent … **#include <stdio.h>**. #include …

un-D_0WNED.c ≈ Packet Storm
https://packetstormsecurity.com/files/41163/un-D_0WNED.c ▾
Nov 2, 2005 - if (argc < 2) { printf("\n\n 1337 0day D0S **exploit** for GoodTech **Telnet** Server for Windows NT/2000\n\n"); printf(" **usage**: %s <ip>\n\n", argv[0]);

About 113 results (0.33 seconds)

exploits/raptor_rlogin.c at master · 0xdea/exploits · GitHub
https://github.com/0xdea/exploits/blob/master/solaris/raptor_rlogin.c ▾
Dec 4, 2004 - of arguments through services such as **telnet** and rlogin (CVE-2001-0797). ... This remote root **exploit uses** the (old) System V based /bin/login.

exploitdb/16270.c at master · offensive-security/exploitdb · GitHub
https://github.com/offensive-security/exploitdb/blob/master/exploits/linux/.../16270.c ▾
exploitdb/**exploits**/linux/dos/16270.c ... **#include** <**stdio.h**>. #include <stdlib.h> ... Author: Maksymilian Arciemowicz. **Use**: ./vspoc232 127.0.0.1 21 user pass 1.

sbouncer004b.c
https://dl.packetstormsecurity.net/9903-exploits/sbouncer004b.c ▾
sbouncer 9999 wingate.blaha.com www.fbi.gov 23 ; **telnet** localhost 9999 * . ... Official distsite - http://www.c5.org * */ **#include** <**stdio.h**> #include <string.h> ... strlen (username)); **password**[strlen (**password**)] = 0; } else { printf ("**Usage**: %s ...

offensive-exploits/platforms/linux/remote/89.c at ... - GitBucket
https://git.coreitx.com/lwhite/offensive-exploits/blob/.../platforms/linux/remote/89.c ▾
Linux pam_lib_smb < 1.1.6 /bin/login **exploit**; * by vertex; *; * Tested on Redhat ... order to **use** pam_lib_smb_need_to_add_following_line_on_top; * of /etc/pam.d/login ... **#include** <**stdio.h**>; #include

filetype:reg HKEY_CURRENT_USER username ext:pwd inurl:_vti_pvt inurl:(Service | authors | administrators)

Other things that work:

error | warning | "not found" | "for more information"
login | login
username | userid | employee.id \"your user name is"
password | passcode | "your password is" reminder forgotten
Inurl:temp | inurl:tmp | inurl:backup | inurl:bak
Intranet | help.desk

?

1. How to find user id and password of pages that are not written in english language?

1. https://cse.google.com/

How to prevent this attack

1. SOFTWARE DEFAULT SETTINGS AND PROGRAMS
2. A Good Solid Security Policy
3. Web Server Safeguard
4. Directory Listings and Missing Index Files
5. Robots.txt: Preventing Caching
6. NOARCHIVE: The Cache "Killer"
7. Password-Protected Mechanisms
8. WIKTO by Sensepost

```
<META NAME="GOOGLEBOT" CONTENT="NOINDEX, NOFOLLOW">
```

```
<META NAME="ROBOTS" CONTENT="NOARCHIVE">
```

SHODAN

G

Say "OK Google" 🎤

Account	Maps	Gmail	Play	Contacts
Drive	Calender	Google+	Translate	Photos

📍 **Bangladesh** | Advertising   Business   About   Privacy   Terms

⚙

Shodan | Developers | Monitor | View All... | Show API Key | Help Center

SHODAN | Explore | Downloads | Reports | Pricing | Enterprise Access | My Account | Upgrade

The search engine for **Webcams**

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account | Getting Started

67.20.69.105
50.87.75.184
104.18.61.231

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

Explore

Discover the Internet using search queries shared by other users.

Featured Categories

Industrial Control Systems

Databases
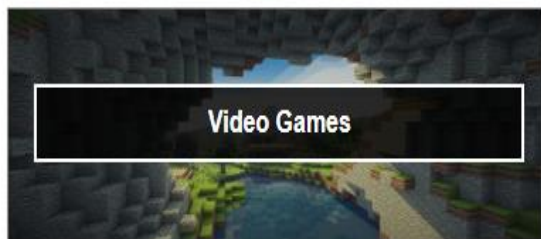
Video Games

Top Voted

11,072

Webcam
best ip cam search I have found yet.

webcam surveillance cams

2010-03-15

4,489

Cams
admin admin

cam webcam

2012-02-06

2,414

Netcam
Netcam

netcam

2012-01-13

Recently Shared

2

videogame
Suro

2019-06-04

1

Suro
Suro

2019-06-04

1

Laritta
Laritta

2019-06-04

Devices Vulnerable to Heartbleed

Search for vuln:cve-2014-0160 returned 237,539 results on 26-03-2016

Top Countries

1.	United States	57,598
2.	China	17,455
3.	Germany	17,273
4.	France	10,708
5.	India	9,427
6.	United Kingdom	9,268
7.	Russian Federation	7,897
8.	Korea, Republic of	7,525
9.	Brazil	7,095
10.	Japan	5,302

Filters:

1. city:"City name"
2. country:"country code"
3. port:port_number
4. os:"OS Name"
5. geo:longitud, latitude
6. net:ip_or_range
7. Hostname:host_name
8. before:DD/MM/YY
9. after:DD/MM/YY
10. What you want?

TOTAL RESULTS

3

TOP COUNTRIES

Pakistan   3

TOP CITIES

Karachi   2
Islamabad   1

TOP SERVICES

PPTP   2
FTP   1

TOP ORGANIZATIONS

LINKdotNET Telecom Limited   2
Pakistan Telecommunication C...   1

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

59.103.253.123

Pakistan Telecommunication Company Limited
Added on 2019-05-23 08:55:34 GMT
Pakistan, Islamabad

```
220 Wind River FTP server 6.5 ready.
530 Authorization failed
211- Command list:
 ABOR - Abort data transfer
 ACCT - Select account
 APPE - Append to file
 CDUP - Change to parent dir
  CWD - Change directory
 DELE - Delete file
 EPRT - Specify extended data port
 EPSV - Enter extended passive ...
```

202.61.42.115

static-host202-61-42-115.link.net.pk
LINKdotNET Telecom Limited
Added on 2019-05-28 09:54:05 GMT
Pakistan, Karachi

```
Firmware: 1
Hostname: GE-Wind-Master
Vendor: MikroTik
```

vpn

202.61.54.242

static-host202-61-54-242.link.net.pk
LINKdotNET Telecom Limited

```
Firmware: 1
```

202.61.42.115 static-host202-61-42-115.link.net.pk View Raw Data

VPN

City	Karachi
Country	Pakistan
Organization	LINKdotNET Telecom Limited
ISP	LINKdotNET Telecom Limited
Last Update	2019-06-03T10:00:37.071418
Hostnames	static-host202-61-42-115.link.net.pk
ASN	AS23966

Ports

53	80	1723	2000

Services

53 tcp dns-tcp	Recursion: enabled

53 udp dns-udp	Recursion: enabled

80 tcp http	HTTP/1.1 200 OK
	Connection: Keep-Alive
	Content-Length: 7064
	Content-Type: text/html
	Date: Mon, 03 Jun 2019 10:00:35 GMT
	Expires: 0

⊕ 59.103.253.123 View Raw Data

City	Islamabad
Country	Pakistan
Organization	Pakistan Telecommunication Company Limited
ISP	PTCL
Last Update	2019-05-23T08:55:34.503110
ASN	AS17557

⊞ Ports

```
21    23
```

☰ Services

21
tcp
ftp
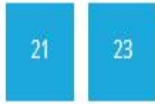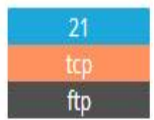
Wind River FTP server Version: 6.5

220 Wind River FTP server 6.5 ready.
530 Authorization failed

printer

🔧 Exploits   🔧 Maps   🎨 Images   🏷 Share Search   ⬇ Download Results   📊 Create Report

TOTAL RESULTS

116,700

TOP COUNTRIES
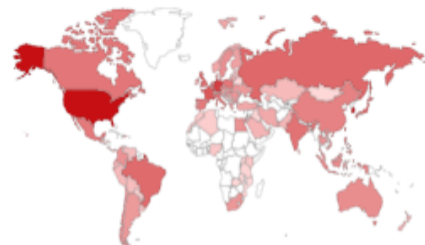
United States	24,524
Korea, Republic of	19,572
Germany	9,145
Taiwan	5,042
France	4,932

TOP SERVICES

Line Printer Daemon	61,009
SMB	47,847
SNMP	2,738
UPnP	1,213
Finger	753

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

180.201.23.17
Shandong University
Added on 2019-06-05 08:38:51 GMT
🇨🇳 China

Printer Name: printer
Jobs: No Jobs in Queue

61.40.137.56
LG DACOM Corporation
Added on 2019-06-05 08:40:15 GMT
🇰🇷 Korea, Republic of

Windows LPD ServerError: specified printer does not existnam

176.126.246.149
Windows 6.1
BHost Inc
Added on 2019-06-05 08:38:48 GMT
🇬🇧 United Kingdom, London

```
SMB Status
Authentication: disabled
SMB Version: 1
Capabilities: raw-mode,unicode,large-files,nt-smb,rpc-remote-api,nt-status,level2-oplocks,lock-and-read,nt-find,dfs,infolevel-
itex,unix,extended-security

Shares
```

```
                          Shares
                          Name              Type         Comments
                          ----------------------------------------------------------------

                          print$            Disk         Printer Drivers
                          IPC$              IPC          IPC Service (service10833 server (Samba, Ubuntu))
```

94.76.229.221

host.desatec.pt
Windows 6.1
Simply Transit Ltd
Added on 2019-06-05 08:39:00 GMT

🏴 United Kingdom

```
        SMB Status
        Authentication: disabled
        SMB Version: 1
        Capabilities: raw-mode,unicode,large-files,nt-smb,rpc-remote-api,nt-status,level2-oplocks,lock-and-read,nt-find,dfs,infolevel-pa
        itex,unix,extended-security


        Shares
        Name              Type         Comments
        ----------------------------------------------------------------

        print$            Disk         Printer Drivers
        IPC$              IPC          IPC Service (host server (Samba, Ubuntu))
```

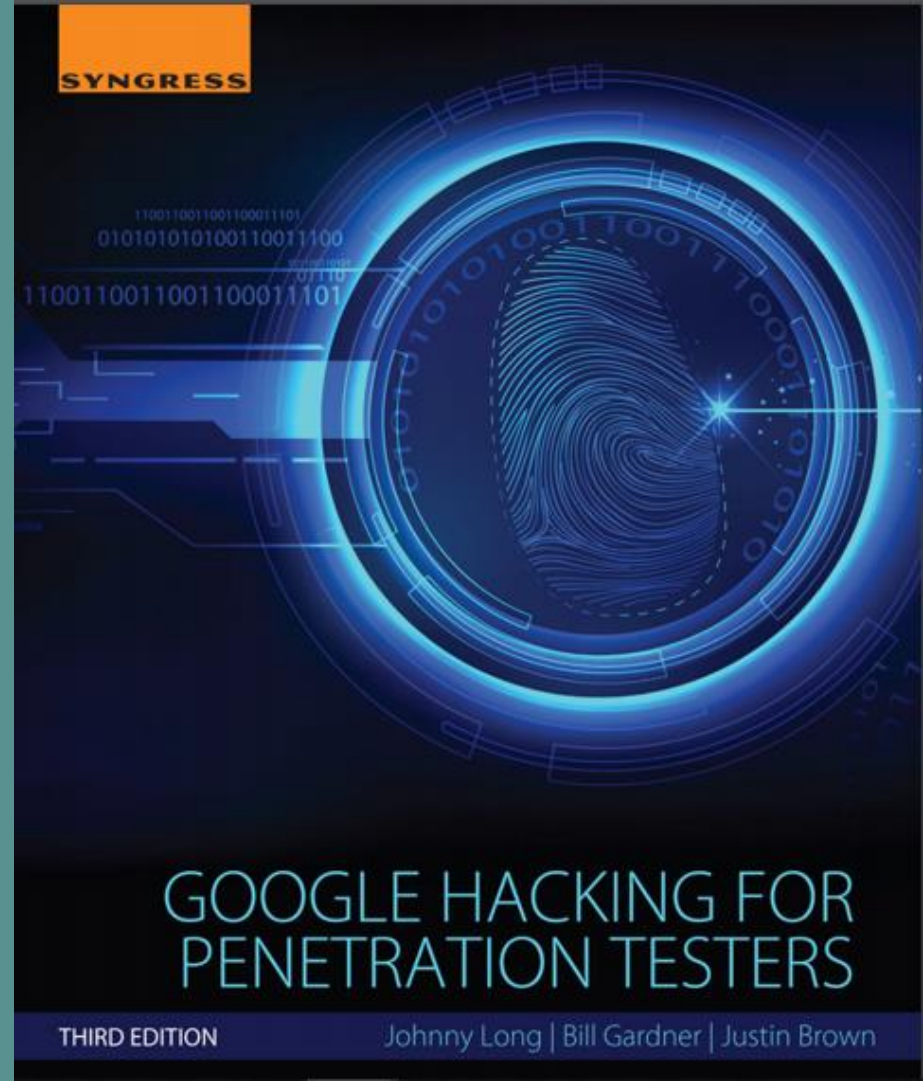## 136.24.3.61

61.3.24.136.in-addr.arpa
Webpass
Added on 2019-06-05 08:39:23 GMT

🇺🇸 United States, San Francisco

```
Windows LPD ServerError: specified printer does not existnamic
```

References:

https://www.exploit-db.com/google-hacking-database
ShodanDork GitHub

Future guidance

1. https://www.exploit-db.com/google-hacking-database
2. https://github.com/humblelad/Shodan-Dorks
3. https://github.com/techgaun/github-dorks
4. https://github.com/gwen001/github-search/blob/master/dorks.txt

Contact:
Pandeyabhishek1103@gmail.com

https://in.linkedin.com/in/abhishekpandey1103