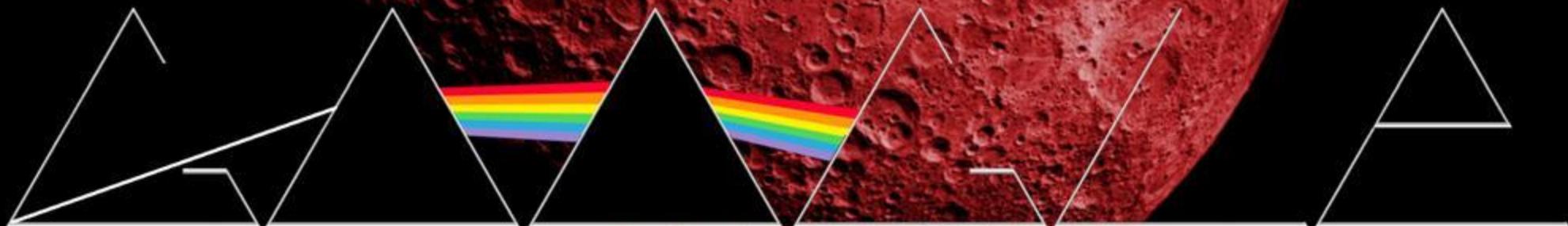
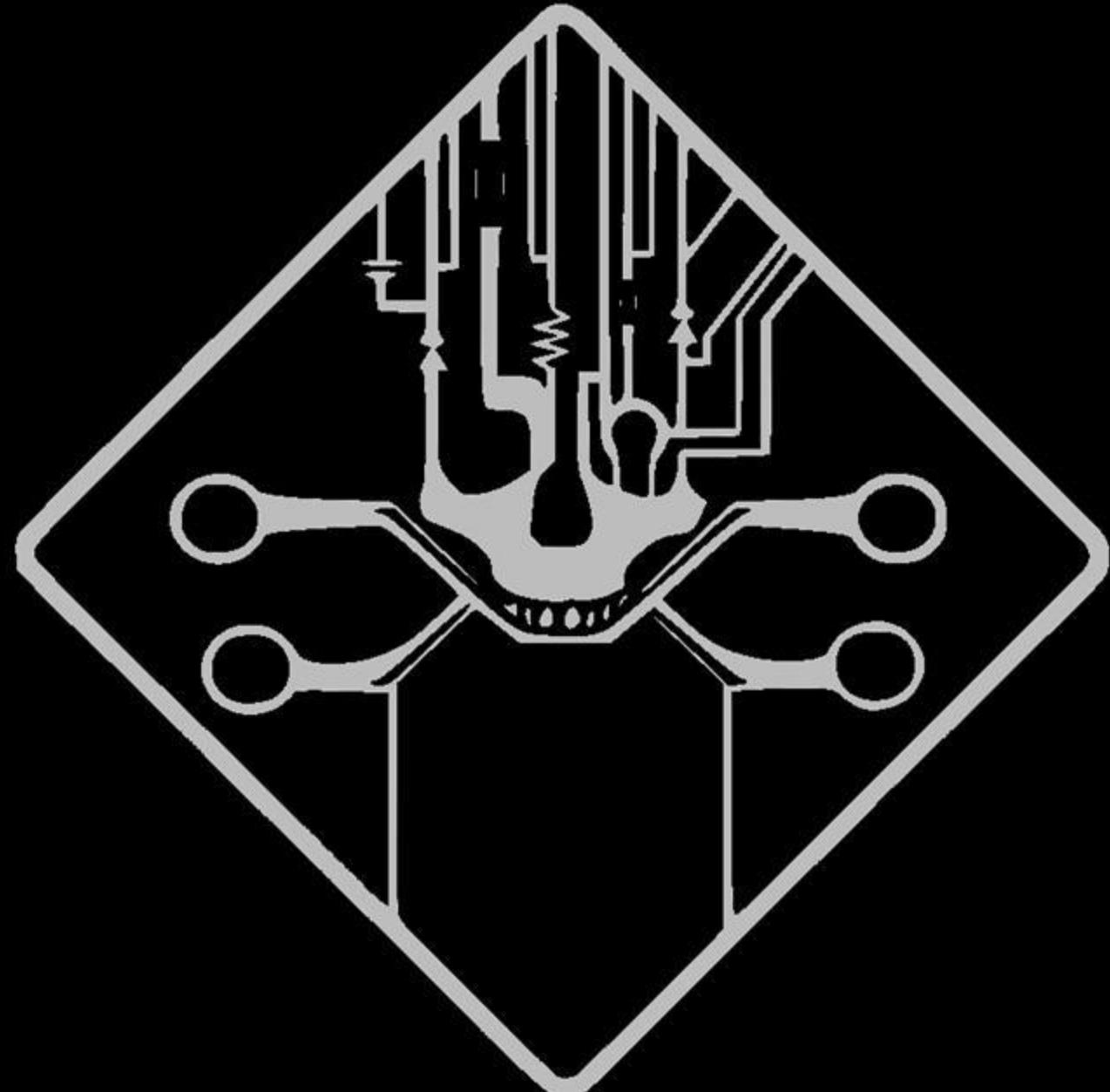




'THE' DORK

SIDE OF



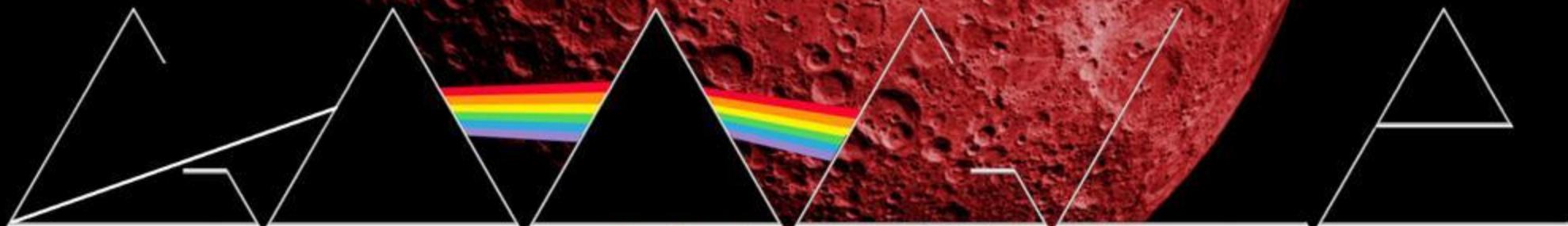


mes3hacKlab



'THE' DORK

SIDE OF



THE DORK SIDE OF GOOGLE



Principali funzioni di ricerca utilizzate:

Site	Specifica il sito da filtrare.
Inurl	Specifica cosa deve contenere l'URL.
Intext	Specifica le parole chiave nel body della pagina.
Intitle	Specifica le parole chiave da cercare nel titolo della pagina.
Filetype	Specifica il tipo di file (dal estensione).

Simboli:

-
|
~
.

OR
Specifica una parola da cercare nel body.
Sostituisce un qualsiasi valore tra due parole.



THE DORK SIDE OF GOOGLE

Le shell

THE DORK SIDE OF GOOGLE



C99Shell v. 1.0 pre-release build #9

Software: Apache/2.2.15 (CentOS). PHP/5.3.3

uname -a:

Safe-mode: OFF (not secure)

/var/www/clients/ drwxr-xr-x

Free 46.09 GB of 50 GB (92.18%)

[Home](#) [←](#) [→](#) [File](#) [Encoder](#) [Tools](#) [Proc.](#) [FTP brute](#) [Sec.](#) [SQL](#) [PHP-code](#) [Update](#) [Feedback](#) [Self remove](#) [Logout](#)

Listing folder (0 files and 2 folders):

Name	Size	Modify	Owner/Group	Perms	Action
..	LINK	05.06.2012 00:07:02	0/0	drwxr-xr-x	? ■
.	LINK	03.06.2012 23:24:01	0/0	drwxr-xr-x	? ■
[client1]	DIR	20.05.2012 08:05:01	0/0	drwxr-xr-x	? ■
[client2]	DIR	03.06.2012 23:24:02	0/0	drwxr-xr-x	? ■

[Select all](#)

[Unselect all](#)

[With selected: ▾](#)

[Confirm](#)

:: Command execute ::

Enter:

[Execute](#)

Select:

[Execute](#)

:: Search ::

- regexp [Search](#)

:: Upload ::

[Seleccionar archivo](#) [No se eli... archivo](#) [Upload](#)

[Read-Only]

:: Make Dir ::

/var/www/dlients/ [Create](#)
[Read-Only]

:: Make File ::

/var/www/dlients/ [Create](#)
[Read-Only]

THE DORK SIDE OF GOOGLE



C99Shell v. 1.0 pre-release build #9

Software: Apache/2.2.15 (CentOS). PHP/5.3.3

uname -a:

Safe-mode: OFF (not secure)

/var/www/clients/ drwxr-xr-x

Free 46.09 GB of 50 GB (92.18%)



Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

Listing folder (0 files and 2 folders):

Name	Size	Modify	Owner/Group	Perms	Action
..	LINK	05.06.2012 00:07:02	0/0	drwxr-xr-x	
.	LINK	03.06.2012 23:24:01	0/0	drwxr-xr-x	
[client1]	DIR	20.05.2012 08:05:01	0/0	drwxr-xr-x	
[client2]	DIR	03.06.2012 23:24:02	0/0	drwxr-xr-x	

Select all

Unselect all

With selected:

Confirm

:: Command execute ::

Enter:

Execute

Select:

Execute

:: Search ::

(*)

- regexp

Search

:: Make Dir ::

/var/www/clients/

Create

[Read-Only]

:: Upload ::

Cosa fanno le shell?

- Accedere ad informazioni riservate.
- Caricare / Scaricare / Modificare file
- Tools DDoS, Mail, Proxy, ...
- Eseguire comandi sul server.

THE DORK SIDE OF GOOGLE



http://dsl.ebay.com/wp-includes/Text/Diff/Engine/shell.php

Most Visited Getting Started ► Ellie Goulding - Beat...

! CEHSecurity

Encoder Bind Proc. FTP brute Sec. SQL

SECURITY BY Jordan

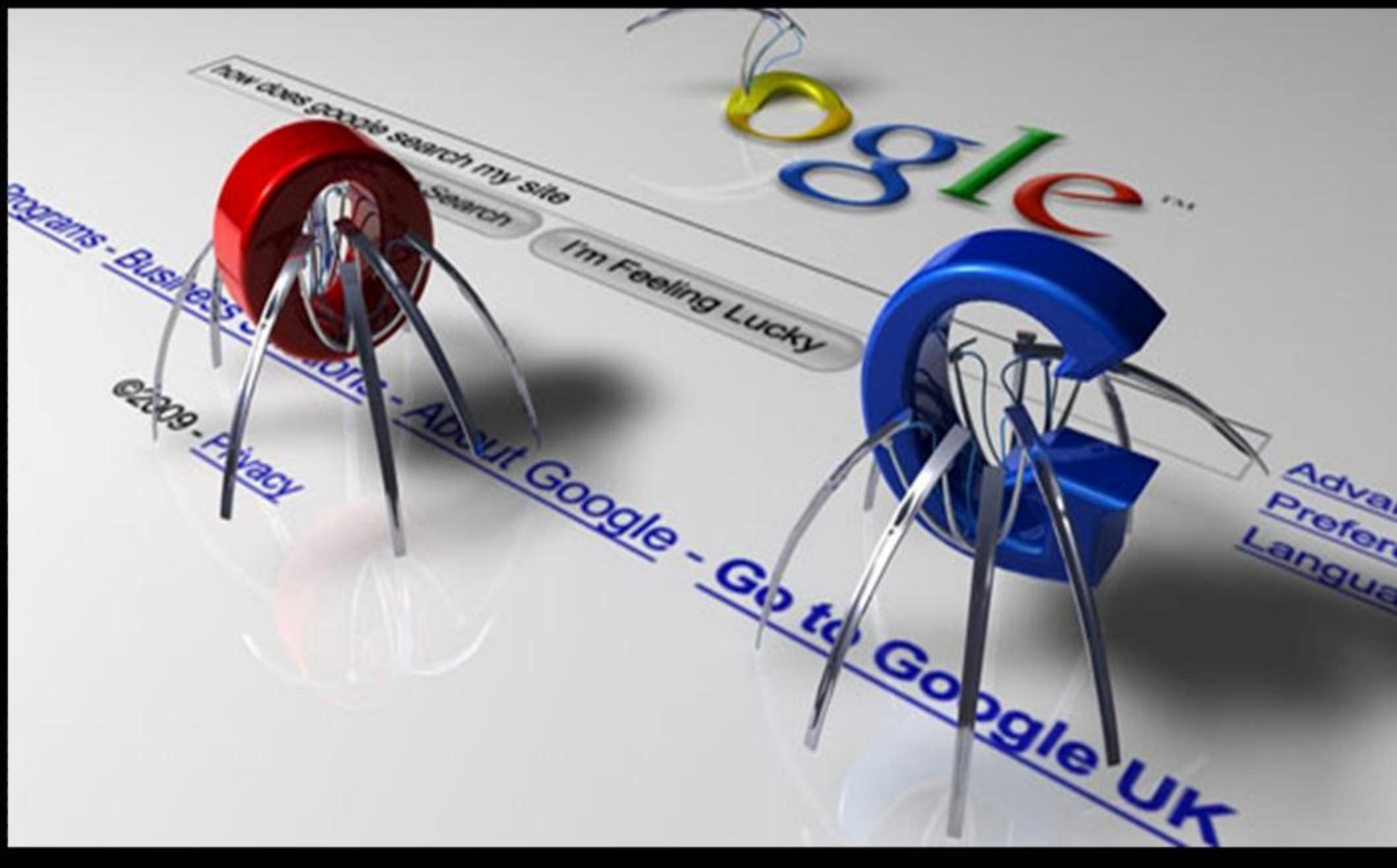
Listing directory (39 fi

Name	Size	Modify
active.php	LINK	
string.php	LINK	
diff.php	DIR 28 B 41 B 546 B	

THE DARK SIDE OF GOOGLE



Come funziona il crawler di Google?



THE DORK SIDE OF GOOGLE



Seguiamolo ...

THE DORK SIDE OF GOOGLE



Cosa fa google per ogni URL:

`http://example.org/dir1/dir2/index.html`

Cerca le parole chiave...

`http://example.org/dir1/dir2/`

Cerca index...

`http://example.org/dir1/`

Cerca index...

`http://example.org/`

Cerca index...

THE DORK SIDE OF GOOGLE



Index of /nginx/apk/

..		
root/		
ADV Honeycomb Theme (1.0).apk	28-Mar-2011 04:32	-
App Drawer Icon Pack (1.2.3).apk	07-Mar-2011 08:24	1005429
Contact2SimPro_v1.6.apk	07-Mar-2011 08:26	547460
Contact2Sim_1.17.apk	09-Mar-2011 02:31	23873
SMS Unread Count (1.5.7).apk	09-Mar-2011 02:32	123269
ZDbox_1.4.77.Android.apk	07-Mar-2011 09:07	187762
apk	06-Apr-2011 05:29	1576205
athan.apk	07-Apr-2011 03:09	26
com.funfoneapps.speedboostota.apk	09-Mar-2011 02:43	4695080
com.stylem.wallpapersota.apk	10-Mar-2011 03:03	376202
iptables	10-Mar-2011 03:04	122466
lv.n3o.swapper_0.2.7.apk	24-Mar-2011 02:17	109020
organizer-widget.apk	07-Apr-2011 03:08	84365
root.rar	09-Mar-2011 06:14	152944
signed-dream_devnphone_userdebug-img-14731.zip	28-Mar-2011 04:32	581923
silverexplorer.apk	04-Apr-2011 03:54	40118457
smsbackup.apk	09-Mar-2011 02:39	326796
space_ota.apk	09-Mar-2011 02:36	145363
speak_text_ota.apk	10-Mar-2011 03:08	2915939
streetracing5pp_ota.apk	10-Mar-2011 03:05	135738
su	10-Mar-2011 03:01	3102867
su.zip	01-Aug-2009 02:08	76232
ymet.android.fxcameraota.apk	28-Mar-2011 04:22	48224
z4root_1.3.0.apk	10-Mar-2011 03:06	1451385
zdbox_1.3.71_2020000007_xda-developers.apk	18-Mar-2011 02:28	978414
	05-Apr-2011 04:16	1989013

Autoindex



THE DORK SIDE OF GOOGLE



Name	Last modified	Size	Description
Parent Directory		-	
ATT2.doc	08-Jul-2010 06:49	20K	
ATT2.pdf	15-Jul-2010 14:37	260K	
ATT3.pdf	08-Jul-2010 06:49	1.8M	
ATT7.pdf	08-Jul-2010 06:49	1.3M	
ATT8.htm	08-Jul-2010 06:49	1.9K	
Advanced Java Programming.pdf	08-Jul-2010 06:49	1.2M	
Chapter 1-2-3-4 CSCE 337-IP Lecture Note.pdf	08-Jul-2010 06:49	1.1M	
IDL1.pdf	28-Oct-2010 16:00	859K	
IDL3.doc	28-Oct-2010 16:01	29K	
IDL3.pdf	17-May-2011 02:12	3.2M	
IDL5.php	02-Mar-2014 03:29	52	
IDL11.php	02-Mar-2014 03:33	52	
Niussie Tadesse.pdf	08-Jul-2010 06:49	177K	
cost mesi.doc	08-Jul-2010 06:49	41K	

SHELL



'THE DORK

SIDE OF



COME TROVARE LE SHELL

THE DORK SIDE OF GOOGLE



Microsoft-IIS/6.0. PHP/4.4.7

Kernel: Windows NT HOSTER8-3 5.2 build 3790 (Microsoft Windows [Version 5.2.3790])

Safe-Mode: OFF (not secure)

Running As: IUSR_iscgov

Disabled PHP Functions: NONE

Free 100.27 GB of 441.4 GB (22.72%)

cURL: ON

Server IP: 205.139.130.14 • Your IP: 66.249.79.100

F:\inetpub\vhosts\www.g00g1e.net\httpdocs\ drwxrwxrwx

Detected drives: [A:] [C:] [D:] [F:]

[Home] [Back] [Forward] [Up] [Refresh] [Search] [Buffer]

[String/Hash Tools] [Processes] [Users] [System Information] [SQL Manager] [Reverse IP] [Kernel Exploit Search] [Execute PHP Code] [PHP Info]

[PHP Tools] [Bind Shell Backdoor] [Back-Connection] [Mass Code Injection] [Exploits] [cPanel Finder] [RFI/LFI Finder] [Install IP:Port Proxy] [Install PHP Proxy] [Suicide Script]

Listing folder (61 files and 9 folders):

Name	Size	Modify	Perms	Action
.	LINK	13.03.2014 09:34:43	drwxrwxrwx	[info] []
..	LINK	01.01.1970 02:00:00	?-----	[info] [change] [download] []
[App_Data]	DIR	05.07.2013 01:01:11	drwxrwxrwx	[info] []
[_notes]	DIR	26.02.2012 14:47:46	drwxrwxrwx	[info] []
[aspnet_client]	DIR	26.02.2012 14:47:38	drwxrwxrwx	[info] []
[index2007]	DIR	26.02.2012 14:47:40	drwxrwxrwx	[info] []
[index2008]	DIR	26.02.2012 14:47:41	drwxrwxrwx	[info] []
[index2009]	DIR	26.02.2012 14:47:42	drwxrwxrwx	[info] []
[picture_library]	DIR	26.02.2012 14:43:10	drwxrwxrwx	[info] []
[previouses2009]	DIR	26.02.2012 14:47:46	drwxrwxrwx	[info] []

THE DORK SIDE OF GOOGLE



Microsoft-IIS/6.0. PHP/4.4.7

Kernel: Windows NT HOSTER8-3 5.2 build 3790 (Microsoft Windows [Version 5.2.3790])

Running As: IUSR_iscgov

Free 100.27 GB of 441.4 GB (22.72%)

Safe-Mode: OFF (not secure)

Disabled PHP Functions: NONE

cURL: ON

Server IP:

Your IP:

F:\inetpub\vhosts\www.gov.ru\httpdocs\ drwxrwxrwx

Detected drives: [A:] [C:] [D:] [F:]

[Home] [Back] [Forward] [Up] [Refresh] [Search] [Buffer]

[String/Hash Tools] [Processes] [Users] [System Information] [SQL Manager] [Reverse IP] [Kernel Exploit Search] [Execute PHP Code] [PHP Info]

[PHP Tools] [Bind Shell Backdoor] [Back-Connection] [Mass Code Injection] [Exploits] [cPanel Finder] [RFI/LFI Finder] [Install IP:Port Proxy] [Install PHP Proxy] [Suicide Script]

Listing folder (61 files and 9 folders):

Name	Size	Modify	Perms	Action
.	LINK	13.03.2014 09:34:43	drwxrwxrwx	[info] <input type="checkbox"/>
..	LINK	01.01.1970 02:00:00	?-----	[info] [change] [download] <input type="checkbox"/>
[App_Data]	DIR	05.07.2013 01:01:11	drwxrwxrwx	[info] <input type="checkbox"/>
[_notes]	DIR	26.02.2012 14:47:46	drwxrwxrwx	[info] <input type="checkbox"/>
[aspnet_client]	DIR	26.02.2012 14:47:38	drwxrwxrwx	[info] <input type="checkbox"/>
[index2007]	DIR	26.02.2012 14:47:40	drwxrwxrwx	[info] <input type="checkbox"/>
[index2008]	DIR	26.02.2012 14:47:41	drwxrwxrwx	[info] <input type="checkbox"/>
[index2009]	DIR	26.02.2012 14:47:42	drwxrwxrwx	[info] <input type="checkbox"/>
[picture_library]	DIR	26.02.2012 14:43:10	drwxrwxrwx	[info] <input type="checkbox"/>
[previouses209]	DIR	26.02.2012 14:47:46	drwxrwxrwx	[info] <input type="checkbox"/>

THE DORK SIDE OF GOOGLE



permit for foreign insurance company 2008.doc	53.5 KB	26.02.2012 14:47:38	-rw-rw-rw-	[info] [change] [download]	<input type="checkbox"/>
regulation 9812.doc	324 KB	26.02.2012 14:47:38	-rw-rw-rw-	[info] [change] [download]	<input type="checkbox"/>
				<input type="checkbox"/> Select all <input type="checkbox"/> Unselect all <input type="checkbox"/> With selected: <input type="button" value="Confirm"/>	

Enter: <input type="text"/>	<input type="button" value="Execute"/>	Kernel Info: Windows NT HOSTER8-3 5.2 build 3790	<input type="button" value="Google!"/>
-----------------------------	--	---	--

Functions <input checked="" type="checkbox"/> Wipe Logs Using zap2 (*nix) <input type="button" value="Execute"/>	Make Dir <input type="text" value="f:\inetpub\vhosts\httpdocs"/> <input type="button" value="Create"/> <input type="button" value="ok"/>	Go Dir <input type="text" value="f:\inetpub\vhosts\httpdocs"/> <input type="button" value="Go"/>
Aliases <input checked="" type="checkbox"/> <input type="button" value="Execute"/>	Make File <input type="text" value="f:\inetpub\vhosts\httpdocs"/> <input type="button" value="Create"/> <input type="button" value="ok"/>	Go File <input type="text" value="f:\inetpub\vhosts\httpdocs"/> <input type="button" value="Go"/>

PHP Safe-Mode Bypass (Read File) File: <input type="text"/> e.g.: /etc/passwd or C:\WINDOWS\system32\.SAM	PHP Safe-Mode Bypass (Directory Listing) Dir: <input type="text"/> e.g.: /etc/ or C:\
---	---

Search <input type="text" value="(*)"/> <input checked="" type="checkbox"/> - regexp <input type="button" value="Search"/>	Upload <input type="button" value="Browse..."/> No file selected. <input type="button" value="Upload"/> <input type="button" value="ok"/>
---	---

THE DORK SIDE OF GOOGLE



permit for foreign insurance company 2008.doc	53.5 KB	26.02.2012 14:47:38	-rw-rw-rw-	[info] [change] [download]	<input type="checkbox"/>
regulation 9812.doc	324 KB	26.02.2012 14:47:38	-rw-rw-rw-	[info] [change] [download]	<input type="checkbox"/>
				Select all	Unselect all

With selected: Confirm

Enter:

Execute

Kernel Info:

Windows NT HOSTER8-3 5.2 build 3790

Google!

Functions

Wipe Logs Using zap2 (*nix)

Execute

Make Dir

f:\inetpub\vhosts\ \httpdocs\

Create [ok]

Go Dir

f:\inetpub\vhosts\ \httpdocs\

Go

Aliases

Execute

Make File

f:\inetpub\vhosts\ \httpdocs\

Create [ok]

Go File

f:\inetpub\vhosts\ \httpdocs\

Go

PHP Safe-Mode Bypass (Read File)

File Read File

e.g.: /etc/passwd or C:\WINDOWS\system32\.SAM

PHP Safe-Mode Bypass (Directory Listing)

Dir: List Directory

e.g.: /etc/ or C:\

Search - regexp Search

Upload Browse... No file selected. Upload
[ok]

THE DORK SIDE OF GOOGLE



Applications Places System Fri Apr 11, 10:52 PM

inurl:php intext:free | gb intext:space | disk "your.ip" "server.ip" "gb" "on" "off" - Google Search - Tor Browser

File Edit View History Bookmarks Tools Help

<https://encrypted.google.com/search?output=search&sclient=psy-ab&q=ir> Startpage HTTPS

Google

Web Videos Shopping Images News More

About 2,010 results (0.31 seconds)

Free - r57shell
www.lomadelgallo.com.mx/index.php?free ▾
r57shell 1.40, 09-04-2014 00:36:28 Your IP: [66.249.66.105] Server IP: [74.63.154.105]
PHP version: 5.2.17 cURL: ON MySQL: ON MSSQL: OFF PostgreSQL: OFF Oracle:
OFF Safe_mode: OFF ... Free space : 7.66 GB Total space: 34.02 GB

realise2 - r57shell
www.lomadelgallo.com.mx/index.php?realise2 ▾
r57shell 1.40, 09-04-2014 01:03:24 Your IP: [66.249.67.98] Server IP: [74.63.154.105]
PHP version: 5.2.17 cURL: ON MySQL: ON MSSQL: OFF PostgreSQL: OFF Oracle:
OFF Safe_mode: OFF ... Free space : 7.66 GB Total space: 34.02 GB

resolv - r57shell
www.lomadelgallo.com.mx/index.php?resolv ▾
r57shell 1.40, 09-04-2014 04:43:08 Your IP: [66.249.65.130] Server IP: [74.63.154.105]
PHP version: 5.2.17 cURL: ON MySQL: ON MSSQL: OFF PostgreSQL: OFF Oracle:
OFF Safe_mode: OFF ... Free space : 7.65 GB Total space: 34.02 GB

hosts - r57shell
www.lomadelgallo.com.mx/index.php?hosts ▾
r57shell 1.40, 09-04-2014 04:42:14 Your IP: [66.249.65.98] Server IP: [74.63.154.105]
PHP version: 5.2.17 cURL: ON MySQL: ON MSSQL: OFF PostgreSQL: OFF Oracle:

inurl:php intext:free | ...

THE DORK SIDE OF GOOGLE



Applications Places System

Fri Apr 11, 10:53 PM

r57shell - Tor Browser

File Edit View History Bookmarks Tools Help

g inurl:php intext:free | gb inte... g r57shell

https://webcache.googleusercontent.com/search?q=cache:l3kp08QKb8EJ:w Startpage HTTPS

This is Google's cache of <http://www.lomadelgallo.com.mx/index.php?realise2>. It is a snapshot of the page as it appeared on 9 Apr 2014 07:03:26 GMT. The [current page](#) could have changed in the meantime. [Learn more](#)

Tip: To quickly find your search term on this page, press **Ctrl+F** or **⌘-F** (Mac) and use the find bar.

[Text-only version](#)

! r57shell 1.40

```
09-04-2014 01:03:24 Your IP: [66.249.67.98] Server IP: [74.63.154.105]
PHP version: 5.2.17 curl: ON MySQL: ON MSSQL: OFF PostgreSQL: OFF Oracle: OFF
Safe mode: OFF Open basedir: NONE Safe mode_exec_dir: NONE Safe mode_include_dir: NONE
Disable functions: NONE
Free space : 7.66 GB Total space: 34.02 GB
Useful: gcc,cc,ld,php,perl,python,ruby,make,tar,netcat,locate,
Dangerous: iptables,logwatch,
[ phpinfo ] [ php.ini ] [ cpu ] [ mem ] [ syslog ] [ resolv ] [ hosts ] [ shadow ] [ passwd ] [ tmp ] [ delete ]
[ procinfo ] [ version ] [ free ] [ dmesg ] [ vmstat ] [ lspci ] [ lsdev ] [ interrupts ] [ realise1 ] [ realise2 ] [ lsattr ]
[ w ] [ who ] [ uptime ] [ last ] [ ps aux ] [ service ] [ ifconfig ] [ netstat ] [ fstab ] [ fdisk ] [ df -h ]
```

uname -a :	Linux cp03.cloud.viawest.net 2.6.18-194.17.1.el5 #1 SMP Wed Sep 29 12:50:31 EDT 2010 x86_64 x86_64 x86_64 GNU/Linux
sysctl :	Linux 2.6.18-194.17.1.el5
\$OSTYPE :	linux-gnu
Server :	Apache
id :	uid=99(nobody) gid=99(nobody) groups=99(nobody)
pwd :	/home/soldadur/public_html (0)

/etc/issue.net

```
This computer system is for authorized users only. Individuals using this
system without authority or in excess of their authority are subject to
having all their activities on this system monitored and recorded or
examined by any authorized person, including law enforcement, as system
personnel deem appropriate. In the course of monitoring individuals
improperly using the system or in the course of system maintenance, the
activities of authorized users may also be monitored and recorded. Any
material so recorded may be disclosed as appropriate. Anyone using this
system consents to these terms.
```

r57shell - Tor Browser

THE DORK SIDE OF GOOGLE



Applications Places System

Fri Apr 11, 10:56 PM

inurl:php intext:free | gb intext:space | disk "your.ip" "server.ip" "gb" "on" "off" "php" intext:mysql | mssql | postgres

File Edit View History Bookmarks Tools Help

inurl:php intext:free | gb intext:... +

https://encrypted.google.com/search?biw=1000&bih=600&noj=1&sclient= Startpage HTTPS

Google "gb" "on" "off" "php" intext:mysql | mssql | postgresql | oracle intext:windows | linux

Sign in

Web Videos Shopping Images News More Search tools

About 800 results (0.52 seconds)

ipays - exploit - web1.muirfield-h.schools.nsw.edu.au
web1.muirfield-h.schools.nsw.edu.au.../sdd/.../coksu.php?act... ▾
OS : Linux utapau 3.11.0-15-generic #25-Ubuntu SMP Thu Jan 30 17:22:01 UTC 2014
x86_64 ... Freespace : 1723.17 GB of 2003.93 GB (85.99%). MySQL: ON MSSQL:
OFF Oracle: OFF MSSQL: OFF PostgreSQL: OFF Name Flags %2d %2s Free
Space free; unknown scsi dac960 cpqarray file ataraid PHP Filesystem:

[+] 1n73ct10n Shell V3.3 [+]
www.parassoftware.com/suntix.php?y=/sbin/&edit=/sbin/parted ▾
Feb 11, 2014 - System OS : Linux lnx7sg-u.securehostdns.com ... PHP Version :
5.4.26 ON cgi-fcgi. Server ip : 216.245.206.162 | Your ip Surving : 66.249.65.43 | Your
... Free Disk: 458.69 GB / 1.76 TB Safemode: OFF Disabled Functions: NONE MySQL:
ON | MSSQL: OFF | Oracle: OFF | Perl: ON | Python: ON | Ruby: OFF ...

bulldog4you.com -
bulldog4you.com/wp-login.php?x...f...%2Fdev%2Fdisk%2Flocal ▾
Mar 15, 2014 - PHP/5.4.26 - php.ini ... Uname -a : Linux rsj12.rhostjh.com
3.4.83-20140315.1.bh6.x86_64 #1 SMP ... Server IP : 173.254.58.41 - Your IP :
66.249.67.87. Freespace : 15.67 GB of 15.67 GB (100%). MySQL: ON MSSQL: OFF
Oracle: OFF MSSQL: OFF PostgreSQL: ON ... Changing file-mode (/dev/disk
/local/.) ...

inurl:php intext:free | ...

THE DORK SIDE OF GOOGLE



Applications Places System [+] 1n73ct10n Shell V3.3 [+] - Tor Browser Fri Apr 11, 10:57 PM

File Edit View History Bookmarks Tools Help

[inurl:php intext:free | gb int...] [+] 1n73ct10n Shell V3.3 [...] +

https://webcache.googleusercontent.com/search?q=cache:uGg1_kjYO5Yjw Startpage HTTPS

This is Google's cache of <http://www.parassoftware.com/suntix.php?y=/sbin&edit=/sbin/parted>. It is a snapshot of the page as it appeared on 24 Mar 2014 21:15:39 GMT. The [current page](#) could have changed in the meantime. [Learn more](#)

Tip: To quickly find your search term on this page, press **Ctrl+F** or **⌘-F** (Mac) and use the find bar.

[Text-only version](#)

Software : Apache
System OS : Linux lnx7sg-u.securehostdns.com 2.6.32-431.5.1.el6.centos.plus.x86_64 #1 SMP Tue Feb 11 21:21:23 UTC 2014 x86_64 | [Google]
| [milw0rm]
ID : uid=593(parassof) gid=604(parassof) groups=604(parassof)
PHP Version : 5.4.26 ON cgi-fcgi
Server ip : 216.245.206.162 | Your ip Surving : 66.249.65.43 | Your Real ip : 66.249.65.43 | Admin : webmaster@parassoftware.com
Free Disk: 458.69 GB / 1.76 TB
Safemode: OFF
Disabled Functions: NONE
MySQL: ON | MSSQL: OFF | Oracle: OFF | PL/SQL: ON | Python: ON | Ruby: OFF | Java: OFF | GCC: OFF | cURL: ON | WGet: ON
> /sbin /

1n73ction Shell V3.3 [Special Edition]

File Shell Eval Mysql DB Dump Phn Info NetSploit Upload Mail Port Scan

Tools Ddos Symlink Multi Config Fucker Multi Bypass Exploit Multi Index Changer Mass Deface

Zone-H

Multi Reset password Wordpress BruteForce Joomla BruteForce Cpanel BruteForce Hash Hash ID Whois

Bypass CloudFlare Script Encode Joomla Server Scan Admin Finder Tutorial & Ebook About Log-Out

```
d
Q      Y      +      I

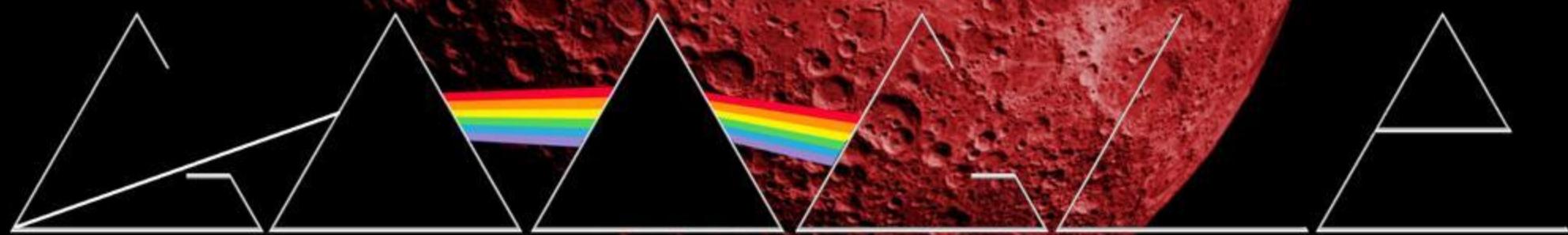
%5
%6c--25.25s %s
Unit? Partition number? Flag to Invert? New state? New device? parted.c start_dist >= 0 end_dist >= 0 start <= end resize Start? End? searching for file systems No device found devices free
list all Minor: %d
Flags: %s
File System: %s
Size: Minimum size: Maximum size: unknown scsi ide dac960 cpqarray file ata raid i2o ubd viodasd sx8 dm xvd sd/mmc virtblk CHS: CYL: BYT: %s:%s;%s;%ld;%ld;%s;%s;
Model: %s (%s)
Disk %s: %s
%d:%d;%d:%s;
Partition Table: %s
```

[+] 1n73ct10n Shell ...



'THE DORK

SIDE OF



COME TROVARE DELLE SHELL SPECIFICHE

THE DORK SIDE OF GOOGLE



Applications Places System

Fri Apr 11, 11:01 PM

inurl:php "disk.free" "gb" "yer_ip" - Google Search - Tor Browser

File Edit View History Bookmarks Tools Help

inurl:php "disk.free" "gb" "yer_ip" +

https://encrypted.google.com/search?biw=1000&bih=600&noj=1&sclient= Startpage HTTPS

Google inurl:php "disk.free" "gb" "yer_ip" Sign in

Web Shopping Videos Images News More Search tools

3 results (0.30 seconds)

Did you mean: inurl:php "disk.free" "gb" "your ip"

PHP - Hardcom-Service
hardcom-service.com/sigescaweb/ex1.php?&dxmode=PHP ▾
Disk free: 1006.82 GB / 1833.27 GB ; OS: Nix () ; Yer_IP: 66.249.68.208 () ; Own/U/G/Pid/Inode:hardcoms / 2644 / 2642 / 19646 / 49946190 ; MySQL : ; Apache ...

Modes - AVNIET...
www.avniel.ac.in/adminpanel/material/2.php?&dxmode=SQL ▾
Disk free: 1132.75 GB / 1833.41 GB ; OS: Nix () ; Yer_IP: 66.249.66.3 () ; Own/U/G/Pid/Inode:shineits / 1748 / 1746 / 21912 / 79694253 ; MySQL : ; Apache ...

public tennc / webshell Octocat-spinner-32 - GitHub
https://github.com/tennc/webshell/blob/master/.../DxShell_hk.php.txt ▾
This a share webshell. Contribute to webshell development by creating an account on GitHub.

*In order to show you the most relevant results, we have omitted some entries very similar to the 3 already displayed.
If you like, you can repeat the search with the omitted results included.*

DxShell

THE DORK SIDE OF GOOGLE



Applications Places System Fri Apr 11, 11:03 PM

hardcom-service.com -- DxShell 1.0 - by o_O Tync == :: PHP COnsole - Tor Browser

File Edit View History Bookmarks Tools Help

8 inurl:php "disk.free" "gb" "ye... x hardcom-service.com -- Dx... x +

https://webcache.googleusercontent.com/search?q=cache:H-RCg_ULAmMJ Startpage HTTPS

This is Google's cache of <http://hardcom-service.com/sigescaweb/ex1.php?&dxmode=PHP>. It is a snapshot of the page as it appeared on 19 Mar 2014 20:26:17 GMT. The [current page](#) could have changed in the meantime. [Learn more](#)

Tip: To quickly find your search term on this page, press **Ctrl+F** or **⌘-F** (Mac) and use the find bar.

[Text-only version](#)

DxShell v1.0

php_ver : 5.4.26 ; php_Safe_Mode : OFF ; magic_quotes : OFF ; gZip : ON ; cURL : ON ; MySQL : ON ; MsSQL : OFF ; PostgreSQL : ON ; Oracle : OFF ; Disabled functions: NONE

Disk free: 1006.82 GB / 1833.27 GB ; OS: Nix () ; Yer_IP: 66.249.68.208 () ; Own/U/G/Pid/Inode:hardcoms / 2644 / 2642 / 19646 / 49946190 ; MySQL : ; Apache :

Modes DIR | VIEW | FTP || SQL | PHP | COOKIE | CMD || MAIL | STR | PORTSCAN | SOCK | PROXY

@MODE: PHP COnsole

Do [phpinfo] [GLOBALS] [php_ini] [extensions]

hardcom-service.com...

THE DORK SIDE OF GOOGLE



Applications Places System

Fri Apr 11, 11:06 PM

inurl:php "GNY.Shell" "Edition" "Generated.in" "server.ip" "your.ip" - Google Search - Tor Browser

File Edit View History Bookmarks Tools Help

inurl:php "GNY.Shell" "Edition" ...

https://encrypted.google.com/search?biw=1000&bih=600&noj=1&sclient= Startpage HTTPS

Google inurl:php "GNY.Shell" "Edition" "Generated.in" "server.ip" "your.ip" Sign in

Web Videos Shopping Images News More ▾ Search tools

9 results (0.30 seconds)

Install IP:Port Proxy
www.imobialianca.com.br/images/imoveis/6134/root.php?act=proxy ▾
cURL: ON. Free 555.6 GB of 707.08 GB (78.58%), Server IP: 187.45.210.97 - Your IP: 66.249.75.36 ... [GNY.Shell | Standard Edition | Generated In: 0.0789]:

Social working - Google Search - CIFlorestas
www.ciflorestas.com.br/arquivos/anuncio_16848.php?act=phpproxy ▾
cURL: ON. Free 233.9 GB of 399.99 GB (58.48%), Server IP: 200.234.196.214 - Your IP: 66.249.67.162 ... [GNY.Shell | Standard Edition | Generated In: 0.0242]:

Reverse IP - Social working - Google Search
www.isc.gov.lb/gny.php?act=rip ▾
cURL: ON. Free 8.23 GB of 441.4 GB (1.86%), Server IP: 92.62.167.10 - Your IP: 66.249.76.2 ... [GNY.Shell | Standard Edition | Generated In: 0.0442]:

GNY.Shell.v1.1.txt - GitHub
<https://github.com/nikicat/web-malware.../PHP/GNY.Shell.v1.1.txt> ▾
web-malware-collection / Backdoors / PHP / GNY.Shell.v1.1.txt. Fetching contributors... free_percent.%)'. } echo '</td><td align=right>Server IP:
<a ... a> - Your IP: Stand@rd
Edition | Generated In: <?php echo round(getmicrotime()-starttime,4); ?>].
'.
.

GnyShell

inurl:php "GNYShell" "E..."

THE DORK SIDE OF GOOGLE



Social working - Google Search - Tor Browser

File Edit View History Bookmarks Tools Help

8 inurl:php "GNY.Shell" "Editio... 8 Social working - Google Sear... +

https://webcache.googleusercontent.com/search?q=cache:KMQmeuwRXa4 Startpage HTTPS

This is Google's cache of <http://www.imobialianca.com.br/images/imoveis/6134/root.php?act=proxy>. It is a snapshot of the page as it appeared on 18 Feb 2014 14:12:03 GMT. The [current page](#) could have changed in the meantime. [Learn more](#)

Tip: To quickly find your search term on this page, press **Ctrl+F** or **⌘-F** (Mac) and use the find bar.

[Text-only version](#)



Apache. PHP/5.2.17
Kernel: Linux plesk65.hospedagemdesites.ws 2.6.18-348.12.1.el5 #1 SMP Wed Jul 10 05:28:41 EDT 2013
x86_64
Safe-Mo...
Disal...
exec

uid=48(apache) gid=48(apache) groups=48(apache),2523(psaserv)

Free 555.6 GB of 707.08 GB (78.58%) Server IP: 187.45.210.97 - V

/home/httpd/vhosts/imobialianca.com.br/httpdocs/images/imoveis/6134/ drwxrwxrwx
[Home] [Back] [Forward] [Up] [Refresh] [Search] [Buffer]

[String/Hash Tools] [Processes] [Users] [System Information] [SQL Manager] [Reverse IP] [Kernel Exploit Search] [Execute PHP Code]
[PHP Tools] [Bind Shell Backdoor] [Back-Connection] [Mass Code Injection] [Exploits] [cPanel Finder] [RFI/LFI Finder] [Install IP:Port Proxy] [Suicide Script]

Are you sure you want to install an IP:Port proxy on this website/server?
Please note, some servers with firewalls or other security features may not be compatible with this, even if the proxy appears to be installed.

Yes || No

Social working - Googl...

THE DORK SIDE OF GOOGLE



GnyShell

THE DORK SIDE OF GOOGLE



THE DORK SIDE OF GOOGLE



Applications Places System

Fri Apr 11, 11:12 PM

inurl:php "enter" "kernel.info" "functions" "make" "dir" "aliases" "your.ip" - Google Search - Tor Browser

File Edit View History Bookmarks Tools Help

inurl:php "enter" "kernel.info" ...

https://encrypted.google.com/search?biw=1000&bih=600&noj=1&sclient= Startpage HTTPS

Google inurl:php "enter" "kernel.info" "functions" "make" "dir" "aliases" "your.ip" Sign in

Web Videos Shopping Images News More Search tools

About 163,000 results (0.36 seconds)

Social working - Google Search
[www.imobialianca.com.br/images/imoveis/6134/root.php?...phpinfo... ▾](http://www.imobialianca.com.br/images/imoveis/6134/root.php?...phpinfo...)
cURL: ON. Free 554.71 GB of 707.08 GB (78.45%), Server IP: 187.45.210.97 - Your IP: 66.249.75.36 ... Enter: Kernel Info: Functions. Make Dir ... Aliases ...

Social working - Google Search - CIFlorestas
[www.ciflorestas.com.br/arquivos/anuncio_16848.php?act=phpinfo&d... ▾](http://www.ciflorestas.com.br/arquivos/anuncio_16848.php?act=phpinfo&d...)
Running As: IUSR_HM1259_241, Disabled PHP Functions: escapeshellarg ... cURL: ON. Free 0 B of 0 B (0%), Server IP: 200.234.196.214 - Your IP: 66.249.64.37 ... Enter: Kernel Info: Functions. Make Dir. Go Dir ... Aliases. Make File ...

www.uniodontomaceio.com.br - Storm7Shell
[www.uniodontomaceio.com.br/swf/grilo.php?act=ls&d=%2F ▾](http://www.uniodontomaceio.com.br/swf/grilo.php?act=ls&d=%2F)
uid=48(apache) gid=48(apache) groups=48(apache), Disabled PHP Functions: NONE. Free 7.33 GB of 57.15 GB (12.82%), Server IP: 127.0.0.1 - Your IP: ...

www.voizmax.com - Storm7Shell
[www.voizmax.com/admin/up_lesson/.../strom.php?...phpsess... ▾](http://www.voizmax.com/admin/up_lesson/.../strom.php?...phpsess...)
... Functions: NONE. Free 9.39 GB of 97.74 GB (9.61%), Server IP: 203.78.99.109 - Your IP: 66.249.77.54 ... Enter: Kernel Info: Functions. Make Dir ... Aliases ...

- Storm7Shell

GnyShell

THE DORK SIDE OF GOOGLE



Social working - Google Search - Tor Browser

File Edit View History Bookmarks Tools Help

inurl:php "enter" "kernel.info..." Social working - Google Sear... Social working - Google Sear... +

https://webcache.googleusercontent.com/search?q=cache:F47kEPBgzlUJ:w Startpage HTTPS

Tip: To quickly find your search term on this page, press **Ctrl+F** or **⌘-F** (Mac) and use the find bar.

Text-only version



Apache. [PHP/5.3.17](#)

Kernel: Linux plesk63.hospedagemdesites.ws 2.6.18-348.12.1.el5 #1 SMP Wed Jul 10 05:28:41 EDT 2013
x86_64

Safe-Mod
Disal
exec

uid=48(apache) gid=48(apache) groups=48(apache),2523(psaserv)

Free 554.71 GB of 707.08 GB (78.45%)

Server IP: 187.45.210.97 - Y

/home/httpd/vhosts/imobialianca.com.br/httpdocs/images/imovelis/3698/ drwxrwxrwx

[Home] [Back] [Forward] [Up] [Refresh] [Search] [Buffer]

[String/Hash Tools] [Processes] [Users] [System Information] [SQL Manager] [Reverse IP] [Kernel Exploit Search] [Execute PHP Code]
[PHP Tools] [Bind Shell Backdoor] [Back-Connection] [Mass Code Injection] [Exploits] [cPanel Finder] [RFI/LFI Finder] [Install (P)Port Prox
Proxy] [Suicide Script]

Waiting for www.imobialianca.com.br...

Social working - Googl...

THE DORK SIDE OF GOOGLE



Applications Places System

Fri Apr 11, 11:18 PM

inurl:php "* safe.mode bypass" "read file" "directory listing" - Google Search - Tor Browser

File Edit View History Bookmarks Tools Help

inurl:php "* safe.mode bypass" ...

https://encrypted.google.com/search?noj=1&biw=1000&bih=600&q=inurl:php%20%22*%20safe.mode%20bypass%22%20%22read%20file%22%20%22directory%20listing%22

Startpage HTTPS

Sign in

Google inurl:php "* safe.mode bypass" "read file" "directory listing"

Web Videos Shopping News Images More Search tools

About 2,010,000 results (0.33 seconds)

[great-rock.co.uk](#) -
great-rock.co.uk/tag/mountain-bike-holiday/?x=f&f=wp...php&d... ▾
PHP Safe-Mode Bypass (Read File). File: e.g.: /etc/passwd or C:\WINDOWS\system32\SAM. PHP Safe-Mode Bypass (Directory Listing). Dir: e.g.: /etc/ or C:\.

[procoffee.by](#) -
procoffee.by/?x=f&f=wp-config.php&ft=info&d...html ▾
PHP Safe-Mode Bypass (Read File). File: e.g.: /etc/passwd or C:\WINDOWS\system32\SAM. PHP Safe-Mode Bypass (Directory Listing). Dir: e.g.: /etc/ or C:\.

[Social working - Google Search](#)
www.imobialianca.com.br/images/imoveis/6134/root.php?act=eval... ▾
PHP Safe-Mode Bypass (Read File). File: e.g.: /etc/passwd or C:\WINDOWS\system32\SAM. PHP Safe-Mode Bypass (Directory Listing). Dir: e.g.: /etc/ or C:\ ...

[tabalongkab.go.id - indocaderlink06](#)
tabalongkab.go.id/dishub/aka.php?x=eval&d... ▾
Feb 12, 2014 - PHP Safe-Mode Bypass (Read File). File: e.g.: /etc/passwd or C:\WINDOWS\system32\SAM. PHP Safe-Mode Bypass (Directory Listing). Dir:

[peelpgs.ca - CYBERIRC](#)

GnuShell

THE DORK SIDE OF GOOGLE



Social working - Google Search - Tor Browser

This is Google's cache of <http://www.isc.gov.lb/gny.php?act=phptools>. It is a snapshot of the page as it appeared on 21 Mar 2014 20:22:09 GMT. The [current page](#) could have changed in the meantime. [Learn more](#)

Tip: To quickly find your search term on this page, press **Ctrl+F** or **⌘-F** (Mac) and use the find bar.

[Text-only version](#)

FUD by albowz

Microsoft-IIS/6.0. [PHP/4.4.7](#)

Kernel: Windows NT HOSTER8-3 5.2 build 3790 (Microsoft Windows [Version 5.2.3790])

Safe-Mode: **OFF (not**

Disabled PHP Functions

cU

Running As: IUSR_iscgov

Server IP: 92.62.167.10 - Your IP: 60.241

Free 106.51 GB of 441.4 GB (24.13%)

f:\inetpub\wwwroot\isc.gov.lb\httpdocs drwxrwxrwx

Detected drives: [A:] [C:] [D:] [F:]

[Home] [Back] [Forward] [Up] [Refresh] [Search] [Buffer]

[String/Hash Tools] [Processes] [Users] [System Information] [SQL Manager] [Reverse IP] [Kernel Exploit Search] [Execute PHP Code] [PHP Tools] [Bind Shell Backdoor] [Back-Connection] [Mass Code Injection] [Exploits] [cPanel Finder] [RFI/LFI Finder] [Install IP:Port Proxy] [PHP Proxy] [Suicide Script]

Mailer

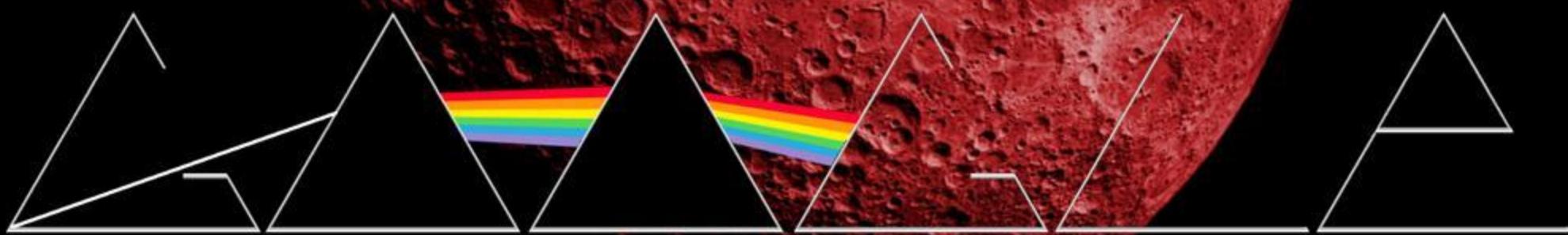
to
from
subject
body

Social working - Google...



'THE DORK

SIDE OF



COME TROVARE DELLE SHILL UNIVERSITARIE

THE DORK SIDE OF GOOGLE



Applications Places System

Fri Apr 11, 10:46 PM

inurl:edu "your.ip" "server.ip" "gb" - Google Search - Tor Browser

File Edit View History Bookmarks Tools Help

inurl:edu "your.ip" "server.ip" "gb"

https://encrypted.google.com/search?noj=1&sclient=psy-ab&q=inurl%3Ae... Startpage HTTPS

Google Sign in

Web Videos Shopping Images More Search tools

About 134,000 results (0.27 seconds)

ipays - exploit - web1.muirfield-h.schools.nsw.edu.au
web1.muirfield-h.schools.nsw.edu.au/.../sdd/.../coksu.php?act... ▾
Jan 30, 2014 - Server IP : 10.29.4.30 - Your IP : 153.107.32.14. Freespace : 1723.15
GB of 2003.93 GB (85.99%). MySQL: ON MSSQL: OFF Oracle: OFF ...

ipays - exploit - web1.muirfield-h.schools.nsw.edu.au
web1.muirfield-h.schools.nsw.edu.au/.../sdd/.../coksu.php?... ▾
Jan 30, 2014 - Server IP : 10.29.4.30 - Your IP : 153.107.32.13. Freespace : 1723.13
GB of 2003.93 GB (85.99%). MySQL: ON MSSQL: OFF Oracle: OFF ...

ipays - exploit - web1.muirfield-h.schools.nsw.edu.au
web1.muirfield-h.schools.nsw.edu.au/.../sdd/.../coksu.php?act... ▾
Jan 30, 2014 - Server IP : 10.29.4.30 - Your IP : 153.107.32.13. Freespace : 1723.15
GB of 2003.93 GB (85.99%). MySQL: ON MSSQL: OFF Oracle: OFF ...

Social working - Google Search
www.mec.edu.ma/.../photo_link_12photo_config.php?... ▾
... pcntl_exec, pcntl_getpriority, pcntl_setpriority, cURL: ON. Free 23.73 GB of 29.53 GB
(80.38%). Server IP: 107.170.241.109 - Your IP: 66.249.73.93 ...

Chairman of the Group of Saudi security - Mr.KsA
moon.cse.yzu.edu.tw/~s981443/upload//1/21/upload.php?act...d... ▾

inurl:edu "your.ip" "ser..."

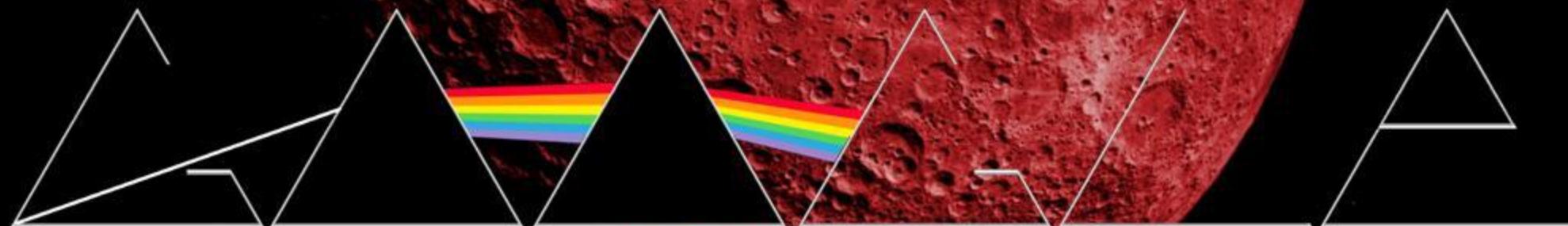
THE DORK SIDE OF GOOGLE





'TETE D'ORAK

THE SIDE OF



COME OTTENERE LE PAGINE GIALLE DELLE
shell governative

THE DORK SIDE OF GOOGLE



Applications Places System Access documents, folders and network places jb - Google Search - Tor Browser Fri Apr 11, 9:37 PM

File Edit View History Bookmarks Tools Help

inurl:gov "your.ip" "server.ip..." www.seplan.mt.gov.br [Gh0...]

https://encrypted.google.com/search?output=search&sclient=psy-ab&q=ir Startpage HTTPS

Google inurl:gov "your.ip" "server.ip" "gb"

Web Shopping Videos Images More Search tools Sign in

About 146,000 results (0.13 seconds)

[www.seplan.mt.gov.br \[Gh0st SheLL\]](#)
www.seplan.mt.gov.br/~seplan/.../gr.php?d=...1...gov%20silval...
Time at this server : 07:32:57 | Free Space in dir: 139.11 Gb ... Your IP: [66.249.68.157] Server IP: [201.49.164.155]. [Back] [Home] [Shell (1) (2)] [Upload] [Tools] ...

[www.seplan.mt.gov.br \[Gh0st SheLL\]](#)
www.seplan.mt.gov.br/~seplan/arquivos/gr.php?...msg%20gov...
Time at this server : 07:11:11 | Free Space in dir: 139.11 Gb ... Your IP: [66.249.68.189] Server IP: [201.49.164.155]. [Back] [Home] [Shell (1) (2)] [Upload] [Tools] ...

[www.seplan.mt.gov.br \[Gh0st SheLL\]](#)
www.seplan.mt.gov.br/~seplan/.../gr.php?d=...del...gov%20stn...
Time at this server : 07:11:14 | Free Space in dir: 139.11 Gb ... Your IP: [66.249.68.157] Server IP: [201.49.164.155]. [Back] [Home] [Shell (1) (2)] [Upload] [Tools] ...

[vito- Rawckerhead - www.kai.gov.kz](#)
www.kai.gov.kz/images/stories/wp-images.php?act=feedback
Sep 30, 2013 - Server IP : 212.154.192.250 - Your IP : 66.249.78.191. Freespace : 4.4 GB of 29.3 GB (15.01%). MySQL: ON MSSQL: OFF Oracle: OFF MSSQL: ...

[Feria Agropecuaria del Valle - Municipalidad de Gaiman](#)
www.gaiman.gov.ar/en/?start=36

inurl:gov "your.ip" "ser...

GENERICO

THE DORK SIDE OF GOOGLE



Applications Places System Browse and run installed applications Fri Apr 11, 9:37 PM

File Edit View History Bookmarks Tools Help

inurl:gov "your.ip" "server.ip..." www.seplan.mt.gov.br [Gh0st SheLL] - Tor Browser

www.seplan.mt.gov.br [Gh0st SheLL] - Tor Browser

https://webcache.googleusercontent.com/search?q=cache:AczyTe7aRpqjw Startpage HTTPS

Tip: To quickly find your search term on this page, press Ctrl+F or ⌘-F (Mac) and use the find bar.

Text-only version

0/home/seplan/public_html/arquivos/
id: uid=33(www-data) gid=33(www-data) groups=33(www-data),1001(seplan)

cat /proc/version || uname -a: Linux version 3.5.0-25-generic (buildd@komainu) (gcc version 4.7.2 (Ubuntu/Linaro 4.7.2-2ubuntu1)) #39-Ubuntu SMP Mon Feb 25 18:26:58 UTC 2013

Time at this server : 07:32:57 | Free Space in dir: 139.11 Gb

Your IP: [66.249.68.157] Server IP: [201.49.164.155]

[Back] [Home] [Shell (1) (2)] [Upload] [Tools] [Exploits (1) (2)] [IFRAME] [SQL] [DEL Folder] [Self Remover]

:: Create folder :: Create file :: Read file if safe mode is On :: PS table ::
CHMOD file /home/seplan/public_html/arquivos/gov silval.jpg

This file chmod is -rw-r--r--

CHMOD (File Permissions)			
Permission	Owner	Group	Other
Read	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Execute	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Octal:	<input type="text"/>	<input type="text"/>	<input type="text"/> = 777
Symbolic:	<input type="text"/>	<input type="text"/>	<input type="text"/> = <input type="text"/>

/home/seplan/public_html/arquivos/gov silval.jpg

BRASILE

THE DORK SIDE OF GOOGLE



The screenshot shows a Linux desktop interface with a top panel containing icons for Applications, Places, System, and a date/time indicator. A Tor Browser window is open, displaying a web page titled 'PLaTo- exploit - www.kai.gov.kz - Tor Browser'. The page content includes system details (Apache 2.2.14, PHP 5.3.2, MySQL 5.1.48, etc.), a menu bar with various exploit tools, and a file viewer for a JPEG image. The file viewer shows the image's EXIF data, which is heavily obfuscated.

KAZAKISTAN

THE DORK SIDE OF GOOGLE



FILIPPIINE

THE DORK SIDE OF GOOGLE



The screenshot shows a terminal window titled 'imdersincelejo.gov.co - FaTaLiSTiCz_Fx Fx29SheLL v1.5 06.2008 - Tor Browser'. The window contains a banner for 'FaTaLiSTiCz_Fx Fx29SheLL v1.5 06.2008' stating ': No System is Perfectly Safe :'. It displays system information: Software: Apache, PHP/5.2.17+php.ini; SAFE MODE is OFF (Not Secure); OS: Linux prosperidad1.diamex.co 2.6.18-274.7.1.el5 #1 SMP Thu Oct 20 16:21:01 EDT 2011 x86_64; User ID: popen Disabled!. It also shows network details: Server IP: imdersincelejo.gov.co - Your IP: 66.249.73.77, Freespace: 783.77 GB of 900.88 GB (87%). Below this, it lists MySQL, MSSQL, Oracle, MSSQL, PostgreSQL, cURL, WGet, Fetch, and Perl status. A section for 'Disabled Functions' lists show_source, system, shell_exec, passthru, exec, phpinfo, popen, proc_open, and allow_url_fopen. A navigation menu includes links like Enumerate, Security Info, Processes, MySQL, PHP-Code Encoder, Mailer, milw0rm.it!, Md5-Lookup, Word-Lists, Toolz, Self-Kill, Feedback, Update, About, FTP-Brute, Backdoor, and Back-Connect. Below the menu are links for Home, Back, Forward, Up, Search, and Buffer. The current directory is /home/imdersin/public_html/admin/. The main content area shows a file viewer for 'b_archivos2.php' (922 B) with permissions -rw-r--r--. It lists various file actions: Open (+), Copy (+), Paste (+), Code (+), Session (+), SDB (+), and several others. A 'Size' dropdown menu offers options 100, 50, and 20. At the bottom, there's a 'COMMANDS PANEL' with a 'Command:' input field and an 'Execute' button, followed by a 'Quick Commands:' dropdown and another 'Execute' button.

COLOMBIA

THE DORK SIDE OF GOOGLE



Social working - Google Search - Tor Browser

File Edit View History Bookmarks Tools Help

8 inurl:gov "your.ip" "server.ip..." 8 inurl:gov.lb "your.ip" "server..." 8 Social working - Google Sear... +

Go back one page
Right-click or pull down to show history antime. [Learn more](#)
Tip: To quickly find your search term on this page, press **Ctrl+F** or **⌘-F** (Mac) and use the find bar.

Text-only version

ENGLISH

FUD by alibabz

Microsoft-IIS/6.0 PHP/5.4.7

Kernel: Windows NT HOSTER8-3 5.2 build 3790 (Microsoft Windows [Version 5.2.3790])

Safe-Mode: OFF (not
Disabled PHP Functions
cU

Running As: IUSR_iscgov

Free 106.51 GB of 441.4 GB (24.13%)

Server IP: 92.62.167.10 - Your IP: 66.241.11.11

f:\inetpub\wwwroot\gov.lb\httpdocs\ drwxrwxrwx

Detected drives: [A:] [C:] [D:] [F:]

[Home] [Back] [Forward] [Up] [Refresh] [Search] [Buffer]

[String/Hash Tools] [Processes] [Users] [System Information] [SQL Manager] [Reverse IP] [Kernel Exploit Search] [Execute PHP Code] [PHP Tools] [Bind Shell Backdoor] [Back-Connection] [Mass Code Injection] [Exploits] [Panel Finder] [RFI/LFI Finder] [Install IP:Port Proxy] [PHP Proxy] [Suicide Script]

Mailer

to
from
subject
body

Submit

Social working - Googl...

LIBAN

THE DORK SIDE OF GOOGLE



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "r57 bypass shell | modified by h4cker.tr - Tor Browser". The terminal content displays a exploit shell on a Windows server, specifically a Plesk control panel. The output includes:

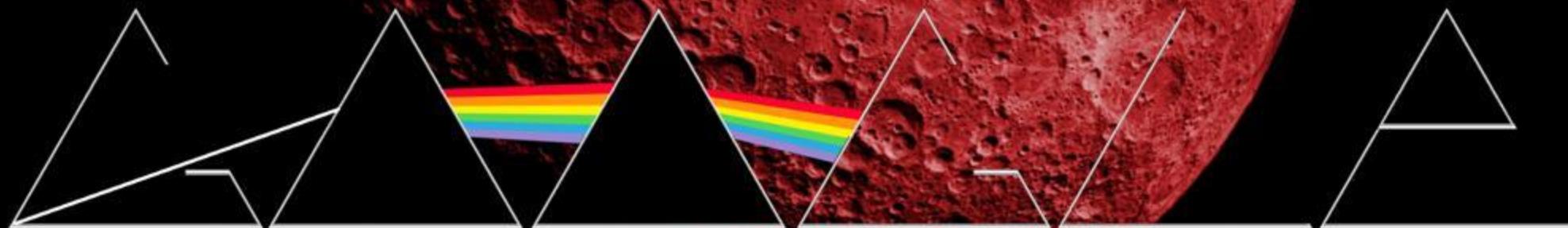
- System information: PHP version: 5.2.17, MySQL: ON, MSSQL: ON, PostgreSQL: Kapali, Oracle: Kapali.
- File system details: Safe mode: ON, Open basedir: C:/inetpub/vhosts/primocircolovicov.gov.lt;C:/Windows/Temp, Safe mode exec dir: NONE, Safe mode include dir: NONE.
- Disable functions: NONE.
- Free space: 67.85 GB Total space: 199.9 GB.
- Links: phpinfo, php.ini, cpu, mem, systeminfo, tmp, delete.
- Server details: OS: Windows NT BM-PLESKWIN 8.1 build 7601, Server: Microsoft-IIS/7.5, User: BM-PLESK-WINS, Path: C:/inetpub/vhosts/primocircolovicov.gov.lt/httpdocs/_pagine/Calendar_5099.
- Log entries (Komut Uygular: safe_dir):
 - 18.03.2014 14:10 196125 maxtor.php
 - 18.03.2014 14:09 24158 net.php
 - 18.03.2014 14:10 0 php.ini
- File operations:
 - Calisma Dizini: C:/inetpub/vhosts/primocircolovicov.gov.lt/httpdocs/_pagine/Calendar_5099
 - Dosya Duzenleme: C:/inetpub/vhosts/primocircolovicov.gov.lt/httpdocs/_pagine/Calendar_5099
 - Olustur/Sil Dosya/Dizin:

ITALIA



'THE DORK'

THE SIDE OF



ALCUNI TRUCCHI DA SAPERE
sulle shell governative

THE DORK SIDE OF GOOGLE



The screenshot shows a Google search results page within a Tor Browser window. The search query in the bar is 'inurl:gov.vn "your.ip" "server.ip" "gb"'. The results are as follows:

- b374k m1n1 1.01**
www.iwem.gov.vn/images/.../1392174101fr0g.phtml?...
server ip : 210.211.110.242 | your ip : 66.249.77.229 %NNY_0IM|uuB|]el>si>%igB_0V0jS%mp) 'Pmu'0 a "oCl h's {ÜÑÜoY È-C~Y,14_r0KR a3Äe)—EE‰ol.
- b374k m1n1 1.01**
www.iwem.gov.vn/images/.../1392174101fr0g.phtml?...
... gid=633(iwem) groups=633(iwem) server ip : 210.211.110.242 | your ip : 66.249.77.229 ... q < 7O}T) &c & gb)m U> 5iE8. 2l&K (2w:n0dw >. ýØýa JFIF ýÜ, ...
- b374k m1n1 1.01**
www.iwem.gov.vn/images/.../1392174101fr0g.phtml?...
uid=633(iwem) gid=633(iwem) groups=633(iwem) server ip : 210.211.110.242 | your ip : 66.249.77.229 safemode OFF > / home / iwem / public_html / images ...
- code**
www.iwem.gov.vn/images/prod/1392174101fr0g.phtml?...
server ip : 210.211.110.242 | your ip : 66.249.77.229 safemode \&\s-1CPAN\s0
stands for Comprehensive Perl Archive Network, a ~1.2Gb archive replicated ...

[PDF] Ubuntu Server Administration (Network Professional's ...

Specificando il paese

THE DORK SIDE OF GOOGLE



Arcane Browser Cache :: Browse and run installed applications

File Edit View History Bookmarks Tools Help

g :: b374k mln1 1.01 ::

https://webcache.googleusercontent.com/search?q=cache:Y2THTtqM_iQj:w Startpage HTTPS

This is Google's cache of http://www.iwem.gov.vn/images/prod/1392174101fr0q.php?r=/home/iwem/public_html/images/prod/&view=/home/iwem/public_html/images/prod/12338896977.jpg&ttype=code. It is a snapshot of the page as it appeared on Feb 26, 2014 22:02:10 GMT. The [current page](#) could have changed in the meantime. [Learn more](#)

Tip: To quickly find your search term on this page, press **Ctrl+F** or **⌘+F** (Mac) and use the find bar.

[Text-only version](#)

b374k
mln1 1.01

Apache/2.2.23 (Unix) mod_ssl/2.2.23 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 mod_fcgid/2.3.6
Linux vps.210.211.110.242 2.6.32-vnh #1 SMP Wed Jul 10 09:13:36 ICT 2013 i686
uid=633(iwem) gid=633(iwem) groups=633(iwem)
server ip : 210.211.110.242 | your ip : 66.249.77.229
safemode OFF
> /home/iwem/public_html/images/prod/

explore shell eval mysql phpinfo netsploit upload mail

Filename /home/iwem/public_html/images/prod/12338896977.jpg
Size 8.17 kb
Permission rw-r--r--
Owner iwem : iwem
Create time 29-May-2013 15:23
Last modified 29-May-2013 15:23
Last accessed 27-Feb-2014 00:50
Actions edit | rename | delete | download (gzip)
View text | code | image

JFIF Ducky Adobe

Bb r3CSS 1AQa cs\$4 DJ"Q DJ"Q DJ"Q DJ"Q DJ"Q DJ"Q & &
DJ"Q DJ"Q DJ"Q {TMn-g r}[W]^>U & i#z Y
8FC-
5

Find: < Previous > Next Highlight all Match case

File Edit View History Bookmarks Tools Help

g :: b374k mln1 1.01 ::

VIEINAM



THE DORK SIDE OF GOOGLE

Applications Places System File Edit View History Bookmarks Tools Help

inurl:gov "your.ip" "server.ip" "gb" "mke" - Google Search - Tor Browser

File Edit View History Bookmarks Tools Help

inurl:gov "your.ip" "server.ip" ... +

https://encrypted.google.com/search?output=search&scclient=psy-ab&q=ir Startpage HTTPS

inurl:gov "your.ip" "server.ip" "gb" "mke"

Sign in

Web Shopping Videos Images More ▾ Search tools

9 results (0.26 seconds)

Code

[isc.gov.lb/Gny.php?act=f&f=InsuranceSectorReport2012...ft...gov...](#)
cURL: ON. Free 67.17 GB of 441.4 GB (15.22%), Server IP: 195.112.196.114 - Your IP: 66.249.75.224 WF\$2 & Gb/U%< w n / OwmOw o o / 2^U O] +> =LxeKx t&< / / } o|S)a & 6. h' i y 37;Z Y # 8 & e < p& 6 < u[MKE R9#R E /,P SSNE I/4K ...

Social working - Google Search

[isc.gov.lb/Gny.php?act=f&f=InsuranceSectorReport2011...gov...](#)
Running As: IUSR_Iscgov, Disabled PHP Functions: NONE cURL: ON. Free 65.91 GB of 441.4 GB (14.93%), Server IP: 195.112.196.114 - Your IP: 66.249.65.24 ...

fx0

[dprm.pids.gov.ph/wp-content/uploads/2014/01/1/2.php?x... ▾](#)
Jan 1, 2014 - Server IP : 203.167.111.155 - Your IP : 66.249.73.39. Freespace : 1705.7 GB of 1848.9 GB (92.25%). MySQL: ON MSSQL: OFF Oracle: OFF ...

fx0

[dprm.pids.gov.ph/wp-content/uploads/2014/01/1/2.php?x... ▾](#)
Jan 1, 2014 - Server IP : 203.167.111.155 - Your IP : 66.249.73.39. Freespace : 1705.99 GB of 1848.9 GB (92.27%). MySQL: ON MSSQL: OFF Oracle: OFF ...

Find: < Previous > Next Highlight all Match case

inurl:gov "your.ip" "ser...

Aggiungendo parole chiave



THE DORK SIDE OF GOOGLE

Applications Places System Fri Apr 11, 10:44 PM

inurl:gov "your.ip" "server.ip" "gb" "mke" - Google Search - Tor Browser

File Edit View History Bookmarks Tools Help

inurl:gov "your.ip" "server.ip" ...

https://encrypted.google.com/search?output=search&sclient=psy-ab&q=ir Startpage HTTPS

1706.83 GB of 1848.9 GB (92.32%). MySQL: ON MKE+
CjxVNTE0Nz4gPFU1MUY2Pgo8VTUxNDK+
IDxVNzA2RT47PFU3MDk3Pg08VTUxNEE+IDxVNTE0 ...

fx0
[dprm.pids.gov.ph/wp-content/uploads/.../2.php?x=f...](#)
Jan 1, 2014 - Server IP : 203.167.111.155 - Your IP : 66.249.67.48. Freespace : 1705.5
GB of 1848.9 GB (92.24%) +
YnDylgY2PQlmg05wZlwtqj2ZcZggAmBACbEBIBws46w6BCK6HEO6+nm5Qmi/
mKE/qu65cu+IVFk5kkakevQkk/+ ...

fx0
[dprm.pids.gov.ph/wp-content/uploads/2014/01/1/2.php?...](#)
Jan 1, 2014 - Server IP : 203.167.111.155 - Your IP : 66.249.67.48. Freespace :
1707.15 GB of 1848.9 GB (92.33%). MySQL: ON MSSQL: OFF Oracle: OFF ...

b374k m1n1 1.01
[www.msw.gov.bd/images/MOI/ht/fm.php?y=/home/www/...](#)
server ip : 114.130.54.109 | your ip : 66.249.79.110 safemode OFF ly+? Dt%K G<
N> UpSCh <s &a \$j7IP RoC 5^mW *n< \$f)gb g boQOjj <m ' B&k & p

code
[www.msw.gov.bd/images/MOI/ht/fm.php?y=/home/www/...](#)
server ip : 114.130.54.109 | your ip : 66.249.79.78 safemode OFF _L&'r_G<
%6lz"h2GKI MKe. OJ EVFS2 Qkf0 4J*a2]<o! Y <w x]%" E+gB '{ . ipfA u~/ K1oJ ...

In order to show you the most relevant results, we have omitted some entries very similar to the 9 already displayed.
If you like, you can repeat the search with the omitted results included.

Find: < Previous > Next Highlight all Match case

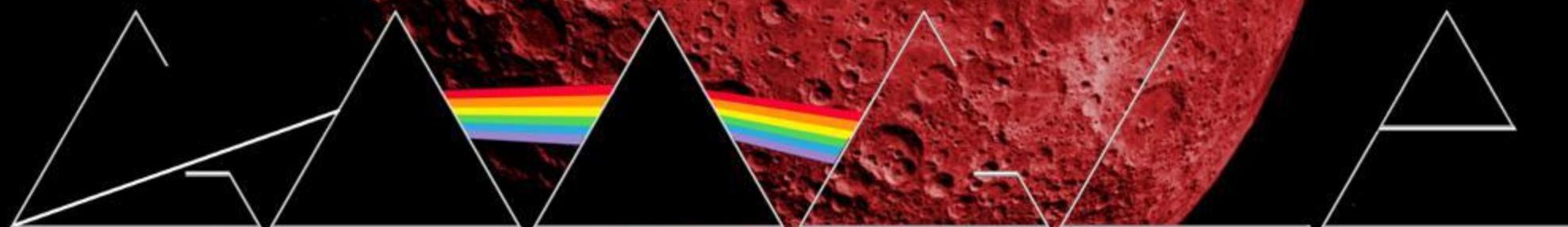
inurl:gov "your.ip" "ser...

BANGLADESH



'TETE D'ORAK

THE SIDE OF



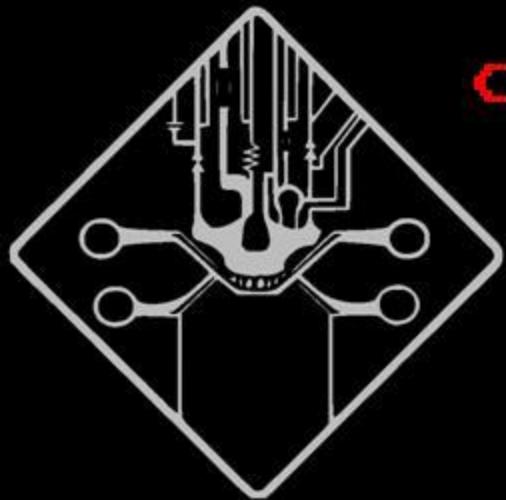
COME OTTENERE LE PAGINE GIALLE DELLE
shell governative



THE DORK SIDE OF GOOGLE



DOMANDA?



Contatti:

epto:

b3rito:
klez:

Site:

epto@mes3hacklab.org
b3rito@mes3hacklab.org
klez@mes3hacklab.org

<http://mes3hacklab.org>