



# Getting Hacked via An Image Gallery, Sucks

By E.Kasey Kasemodel • apin.com

Lessons learned the hard way. I'm writing this for all you webmasters out there who have ever installed an image gallery. As you're likely well aware, any software that's designed to upload files by the public is a hackcident waiting to happen. A few things to remember:

1. **Keep it current.** Coppermine and every other open source project has had security issues. If you install software for someone, it's a really good idea to keep track of this so that when you become aware of an update, you can at least recommend they upgrade. Sure, this is CYA, but it's also the right thing to do.
2. **Do not allow open uploads,** comments, or even open contact forms for that matter. Spam robots are all too common now and any open system will get spammed, hacked or both. Force users to register and validate. Even that's not foolproof, but it's way better than leaving it open to anonymous visitors from the Ukraine. (Sorry to all the good people from the Ukraine, but most of our recent attacks came from that neighborhood)
3. **Do not load non-essential software to a production domain.** In other words, if a company uses their website to conduct business, don't plop an image gallery on there just because it's easy to do. Spend the \$9/year and get a separate domain. You're going to theme the gallery/forum to match their site anyway, so sending them to another domain -- it's likely they'll never notice they've left. If the gallery does get hacked, the production site never misses a beat.

I wanted to contribute something beyond these three simple reminders, so here's a hack (the good kind) that we did recently to add a simple CAPTCHA to a contact form. While this one is for Coppermine, the same steps would apply in just about any open source CMS... well, except that all the file names would change :)

## Adding a Spam Resistent Contact Form to Coppermine

### Step 1 - Upload contact.php

Upload contact.php into the root directory, remember to change the to: email address first. (A copy of contact.php is included on the last page of this doc)

### Step 2 - Modify include/themes.inc

search for this

```
// HTML template for template sys_menu buttons
if (!isset($sys_menu_buttons)) { //{THEMES}
```

add this:

```
addbutton($sys_menu_buttons, '{CONTACT_LNK}', '{CONTACT_TITLE}', '{CONTACT_TGT}', 'contact', '');
```

then about halfway down the file, look for

```
$param = array(
```

and add these:

```
'{CONTACT_TGT}' => "contact.php?referer=$REFERER", // your_name_date
'{CONTACT_TITLE}' => $lang_main_menu['contact_title'], // your_name_date
'{CONTACT_LNK}' => $lang_main_menu['contact_lnk'], // your_name_date
```

The // **your\_name\_date** is to remind you that any file you modify should include your name, the date and even some contact info near the lines you touch, especially if you're doing this for someone else.

Remember, when you upgrade, you will need to do this all over again, so leaving some breadcrumbs behind is always a good idea.

One more thing: Before you modify a core file, make a copy of it called whatever.php1 so that it's clear that file has been changed.

### Step 3 - Modify include/functions.inc.php (optional)

This is not really part of the hack to install a CAPTCHA contact form. This is optional but I am including it here because I used it in the last project and if I didn't write it down somewhere, I would never remember. The below change will remove the credit line "Powered by Coppermine" from all pages.

**Now the important part:** Developers deserve all the credit they can get, so the only way you should do this is if you give credit back that's bigger/better than this single line. We did this for cosmetic reasons, not to remove their much earned recognition. If you do this, please add a separate page giving them their due.

```
// $template = str_replace($tmpl_loc['l'], $tmpl_loc['s'], $template);  
replace with  
$template = str_replace($tmpl_loc['l'], '' , $template);
```

Here's a snapshot of the credit page we inserted after we removed their powered by line:



*This is what  
we used as a  
replacement  
for their  
"powered by"  
line*

#### Powered By ... Coppermine!



This portion of SnappyVeronica is powered by Coppermine, the best open source image gallery out there! We've got nothing but love for these folks and encourage you to visit them at [coppermine-gallery.net](http://coppermine-gallery.net) Yes, we did hack the code to remove the location of where they had their *Powered by* -- but we did this only for cosmetic reasons. (we artist types do that) This is not a violation of GPL license agreement, but we think it's very reasonable they want recognition for such a fantastic product -- so on every page, over there on the right, you'll see Powered by Coppermine!.

#### Just so you know...

Coppermine is a multi-purpose fully-featured and integrated web picture gallery script written in PHP using GD or ImageMagick as image library with a MySQL backend. Coppermine is free software which you can download and install on your webspace.

Check em out -- and tell 'em Veronica sent ya!

#### Also, a big *You Rock!* to ...

This very excellent theme ([I feel dirty](#)) was crafted by [studio ST](#) and then elegantly ported to Coppermine by none other than [Billy Bullock](#) Thanks Billy, you're awesome!

All this stuff (Coppermine, Wordpress, Joomla) was installed, hosted and supported by those clever and crafty guys at [API Network](#) in Dexter, Michigan.



*... and much thanks to Veronica  
at SnappyVeronica.com for allow-  
ing us to use her as an example.*

## Step 4 - Add to the language file - lang/english.php

You'll need to make two additions:

Search for this `$lang_main_menu = array(`

and add:

```
'contact_title' => 'Contact us',  
'contact_lnk' => 'Contact us',
```

Then add this block for the labels in the contact form:

```
// -----  
// File contact.php - your_name_date_contact_info  
// -----  
  
if (defined('CONTACT_PHP')) $lang_contact_php = array(  
    'contact' => 'Contact',  
    'required_fields' => 'All fields are required. I reply to all, so long as you can do  
the math :)',  
    'name' => 'Your Name',  
    'email' => 'Email Address',  
    'subject' => 'Subject',  
    'comment' => 'Comments',  
    'spam_prevention_answer' => ' plus ',  
    'spam_prevention_question' => 'Spammers be gone!',  
    'no_name' => 'But what is your name? ',  
    'no_email' => 'Hey! I need an email address',  
    'no_valid_email' => 'That email address smells fishy to me',  
    'no_subject' => 'Please tell me what this is about (e.g., enter a Subject)',  
    'no_comment' => 'I need details! So you must enter a comment.',  
    'no_spamprev' => 'You need to answer the math quiz!',  
    'no_valid_spamprev' => 'Sorry but you suck at math.',  
    'submit' => 'Submit',  
    'thank_you' => 'Thank you!',  
    'thank_you_email' => 'Thanks for your message!. I will get back to you soon.',  
    'contact_us' => 'Contact us',  
    'delivery_failed' => 'Darn. Message delivery failed...',  
    'cookie_warning' => 'Warning your browser does not accept script\'s cookies',  
);
```

## Step 5 - Add the link to your template page.

Depending on the theme, you can add this in `template.html`, or if you don't want to mess with native template code, you can do this via a `header.htm` inclusion.

If you want to add this as a `header.htm` inclusion, you would make a simple line of HTML, save it as `header.htm` then upload it to the `public_html` root. Then reference that file in the config settings.

Either way, here's what the code might look like:

```
<a href="contact.php?referer=index.php" title="Contact Me">Contact Me!</a>
```

**Voila!**

*... the finished product!*

*This is way better than those horrible LSD fonts!*



All fields are required. I reply to all, so long as you can do the math :)

Your Name \*

Email Address \*

Subject \*

Comments \*

23 plus 4 \*\*

Spammers be gone!

Submit

## contact.php

```
<?php
define('IN_COPPERMINE', true);
define('CONTACT_PHP', true);
require('include/init.inc.php');

$referer = $_GET['referer'] ? $_GET['referer'] : 'index.php';
if (strpos($referer, "http") !== false /*|| strpos($referer, "logout.php") !== false*/) {
    $referer = "index.php";
}
$cookie_warning = '';
if ($_REQUEST['submitted']=='yes') {
    $to = "yourname@yourdomain.com";
    $subject = addslashes($_POST['subject']);
    $body = addslashes($_POST['comment']);
    $headers = "From: ".addslashes($_POST['name'])."<".addslashes($_POST['email']).">\r\n";
    if (mail($to, $subject, $body,$headers)) {
        pageheader($lang_contact_php['thank_you'], "<META http-equiv=\`refresh\`"
content="\`3;url=$referer\`>");
        msg_box($lang_contact_php['thank_you'], $lang_contact_php['thank_you_email'], $lang_continue,
$referer);
        pagefooter();
        exit;
    } else {
        pageheader($lang_contact_php['thank_you'], "<META http-equiv=\`refresh\`"
content="\`3;url=$referer\`>");
        msg_box($lang_contact_php['contact_us'], $lang_contact_php['delivery_failed'],
$lang_continue, $referer);
        pagefooter();
        exit;
    }
}
if (!isset($_COOKIE[$CONFIG['cookie_name'] . '_data'])) {
    $cookie_warning = <<<EOT
        <tr>
            <td colspan="2" align="center" class="tableh2">
                <span style="color:red"><b>{$lang_contact_php['cookie_warning']}</b></span>
            </td>
        </tr>
    EOT;
}
```

edit this



## contact.php con't

```
<script language="javascript" type="text/javascript">
<!--
document.contactbox.name.focus();
function submitform()
{
    var spamanswer=eval(document.contactbox.firstnumber.value) +
eval(document.contactbox.secdnumber.value);

    if (document.contactbox.name.value=='')
    {
        alert('${lang_contact_php['no_name']}');
        document.contactbox.name.focus();
    }
    else if (document.contactbox.email.value=='')
    {
        alert('${lang_contact_php['no_email']}');
        document.contactbox.email.focus();
    }
    else if ( ( document.contactbox.email.value.search("@") == -1 ) || (
document.contactbox.email.value.search("[.*)" ) == -1 ) )
    {
        alert('${lang_contact_php['no_valid_email']}');
        document.contactbox.email.focus();
    }
    else if (document.contactbox.subject.value=='')
    {
        alert('${lang_contact_php['no_subject']}');
        document.contactbox.subject.focus();
    }
    else if (document.contactbox.comment.value=='')
    {
        alert('${lang_contact_php['no_comment']}');
        document.contactbox.comment.focus();
    }
    else if (document.contactbox.spamprev.value=='')
    {
        alert('${lang_contact_php['no_spamprev']}');
        document.contactbox.spamprev.focus();
    }
    else if (document.contactbox.spamprev.value!=spamanswer)
    {
        alert('${lang_contact_php['no_valid_spamprev']}');
        document.contactbox.spamprev.focus();
    }
    else
    {
        document.contactbox.action = "contact.php?submitted=yes";
        document.contactbox.submit();
    }
}
-->
</script>
EOT;
pagefooter();
ob_end_flush();
?>
```

In closing, asking to add two random numbers together is something a CAPTCHA cracking program could handle with ease, but the point is, not many hackers out there will spend the time to bypass this simple approach. Of course, now that I've said that, it's just a matter of time before someone writes one. In the meantime, if you have any questions about this, feel free to drop us an email at [support@apin.com](mailto:support@apin.com). To grab a copy of this document or the source for contact.php, go to <http://apin.com/help/captcha>