Backdooring Images

Backdooring Images - pdp, gnucitizen.org.

- Published: date not stated
- Original: <https://www.gnucitizen.org/blog/backdooring-images/>
- Preserved from: https://www.gnucitizen.org/blog/backdooring-images/ (stored) on 2026-08-16
- 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.

Backdooring Images

Fri, 15 Dec 2006 04:57:22 GMT

by pdp

> An offensive move where a player cuts behind the defenders and receives a pass for a field-goal attempt. basketball-betting-college

OK, we've covered how to backdoor Flash, QuickTime, QuickTime Link, PDF and simple HTML files, but we haven't discussed how to backdoor images yet. In this post I am going to outline some of the techniques available for maliciously infecting Image (Picture) files with JavaScript code. I must worn you that what you are about to read is not intended to describe new issues but rather to clarify and provide scenarios where the discussed attack vectors can be implemented.

First of all I want to drag your attention to the infamous Internet Explorer GIF vulnerability which I believe was the first to bring a lot of attention on JavaScript inside images issue. The vulnerability was one of the most obscured ones and it was successfully used to compromise many bulletin boards and not only. Luckily, Microsoft came up with a patch for it some time ago and if you are on SP2 you are no affected any more. It is essential to understand that this was not the first one. In fact similar issues were found in Netscape and other popular browsers long before it but I will leave this research to you.

The essence of this GIF89 vulnerability is hidden inside the inner working of IE file detection engine. If a file starts with GIF89 header it will be threaded as gif, however if you append right after this header a html document with some malicious JavaScript, than you have a trojaned gif which will not display properly in the browser but will successfully exploit it.

This find was pretty good at the time it was discovered. Given the fact that Internet Explorer is the most popular browser (things are changing) on the planet, a lot of websites that allowed user

supplied content in a form of images were left open to many types of web related attacks. This, however, is not the end of the story because today, with IE6 and IE7 a very similar problem still occurs.

What types of other image file issues are still available today? There are a few that are ridiculously simple but also very, very dangerous. In fact, all of these techniques can be used to successfully recreate a worm, similar to the one that hit MySpace last week, to some extend.

You may not be aware of, but there is a bunch of insecure File Handling issues in Internet Explorer. That was discovered long time ago and it was outline in securityfocus here and here and a couple of other places. I don't know why nobody pays any attention on these and I guess I need cover this particular issue some other time.

If you read the BID references you will see that normal files like .jpg and .gif can contain HTML code which upon viewing will execute whatever it is inside, which may as well be a real image so that the user doesn't get too suspicious. Here is how to compose a malicious JPG file for IE.

```
<html>
  <body>
  <script>alert('backdoored');</script>
  </body>
</html>
```

Save that as .JPG and preview it in Internet Explorer. You need to put it on a web server first.

This is absolutely trivial but as I mentioned earlier it could be used for very destructive purposes. For example, if an attacker decides to hijack several MySpace accounts, he/she could simply put a link to a trojaned image on blogs found in MySpace. The image should be titled with an attractive name so users are more likely to click on it. Once an unaware user fells into the trap, the browser will redirect to the image location which in tern will ask for login credentials to preview the private content. That way, IMHO, attackers can phish many accounts.

I am not a MySpace fan and I don't have an account with them but if it is allowed to upload Image files the situation could get worse because the domain from where the images will come from is the same as the domain you want to exploit, imagine the possibilities.

Sometimes this scenario is quite easily achieved especially on various bulletin boards that don't verify that the user supplied avatar image is an actual image. You can create an account and upload backdoored JPG file. Then reference this file somewhere as a link. If an unaware user clicks on it, you will receive their session and you will be able to do all sorts of other stuff, as well. Here is a hint: attackers can post several other comments containing a link to the malicious JPG on behalf of you. This is how you do a malware infection on BB for example.

I know what you are thinking. This is so easy and virtually everyone can do it and there are so many web applications vulnerable to this issue that it is not even funny. But now you are thinking that Internet Explorer is the worst browser in the world. You are wrong. In fact, Internet Explorer is almost as vulnerable as Firefox and the rest of the browsers are. In fact, this is not even a browser related problem. It is a server side problem. People sanitize user supplied data but do they sanitize links to external or internal files,... nope. The reason for that is obvious: too much work and I don't

blame application vendors for not doing that. GMAIL does all of it the right way, though. I did spend some time testing this issue.

Firefox can also be made behave the same way like Internet Explorer. Simply we can change the mime type by composing the following htaccess file.

```
AddType text/html .jpg
```

If you put this file somewhere with your image, you will recreate the same effect. The only good thing about this approach is that it is less efficient..

I will leave this subject open because there is a lot one can say and I don't have much time. Has anyone tried Flicker yet?

Archived Comments