

Image Names Gone Bad ha.ckers.org web application security lab

Image Names Gone Bad ha.ckers.org web application security lab - Author not stated, ha.ckers.org.

- Published: date not stated
- Original: <<http://ha.ckers.org/blog/20070209/image-names-gone-bad/>>
- Preserved from: <http://ha.ckers.org/blog/20070209/image-names-gone-bad/> (stored) on 2026-08-17
- Capture timestamp: 20081121152246
- Licence: unknown

Rights remain with the original author and publisher. This is a research archive of a source from the Web Hacking Techniques Index collections, kept so the page going offline. To read the original, follow the link above.

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.

Image Names Gone Bad ha.ckers.org web application security lab

[[image: image]](<http://ha.ckers.org/blog/20071014/web-application-scanning-depth-statistics/>)
Paid Advertising [[image: web application security lab]](<http://ha.ckers.org/>)

Image Names Gone Bad

I was having a thought today, which has probably occurred to someone along the way but this is the first time I've heard of this. There are a number of systems out in the wild that will let you upload images and will keep them named whatever you choose. Further, once they appear on the page, they have to be called by something (JavaScript or an IMG tag generally). What if we were to name the images something bad? What if we were to turn the name into an XSS vector? Well here are some for you to try out if you like:

I bet there are some systems out there that are otherwise hardened that have this issue. The first one above is simply trying to break out of an image tag. The next two are taking a guess that they may be inside a JavaScript tag. Either way, you get the idea. Could be bad, who knows?

This entry was posted on Friday, February 9th, 2007 at 5:06 pm and is filed under [XSS](#), [Webappsec](#). You can leave a response as well.

Respond here or Discuss [On the Forums](#)

Your Name *

E-Mail (will be hidden) *

URL

Archived from <http://ha.ckers.org/blog/20070209/image-names-gone-bad/>. Rendered offline from the local Markdown copy.