GIF/BMP Image - XSS

# How the image files are made:

Add a couple of lines of java script to source file of an image. (Attached the source file with javascript “jifjs.shinto”)

Compile the file using any gif compilers: I have used yasm (Works pretty well) yasm gifjs.shinto -o test.gif

# Test the file:

Let's test our GIF file. Create an HTML file with the following source.

<img src="img.gif">

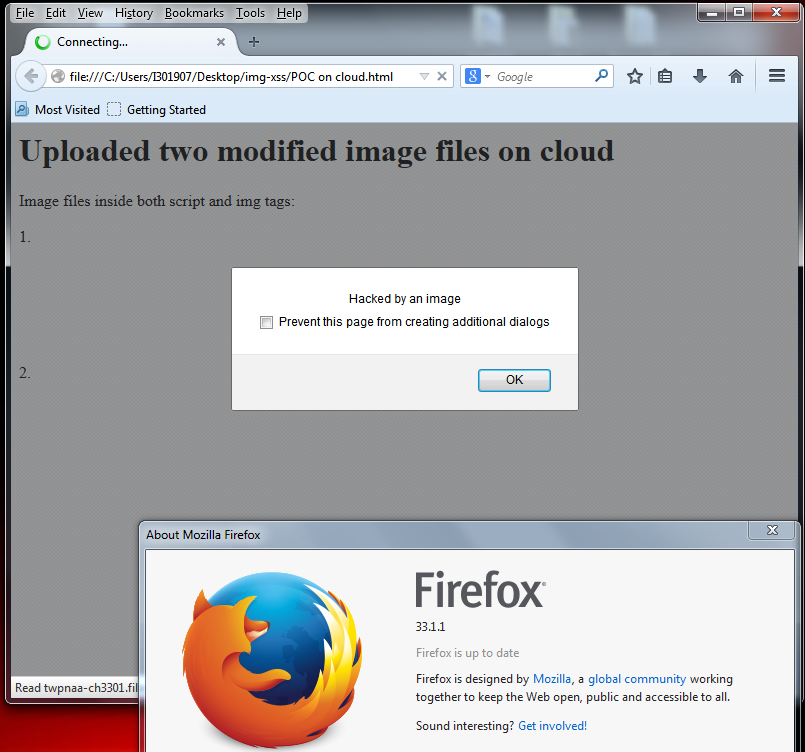
<script src="img.gif"></script>

You can upload these gif files in internet and can use those direct URLS as well.

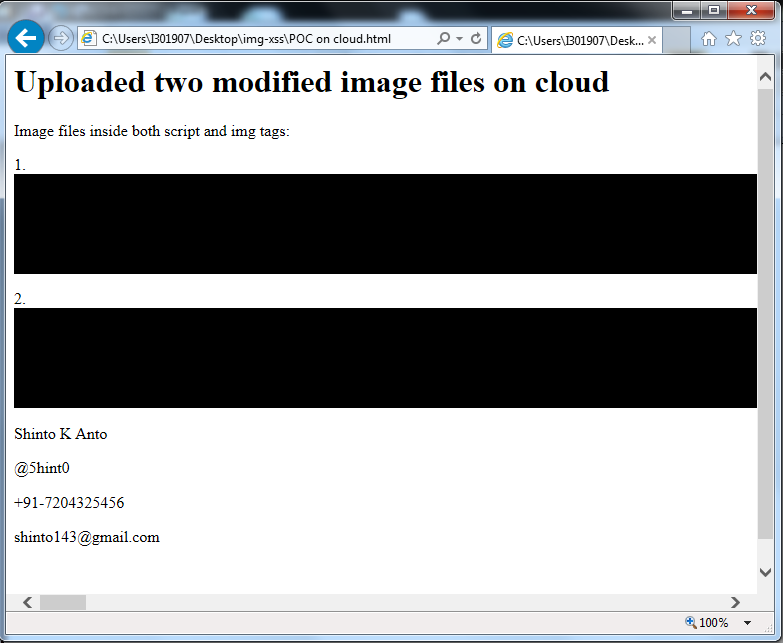
# Attachments

* Gifjs.shinto – source file of a gif image with JavaScript before compiling
* Test.gif – compiled gif image
* Sun.gif – Another modified gif image downloaded from <http://jklmnn.de/imagejs/>
* Img1.bmp – Modified BMP image downloaded from <http://jklmnn.de/imagejs/>
* POC on cloud.html
* POC on localhost.html

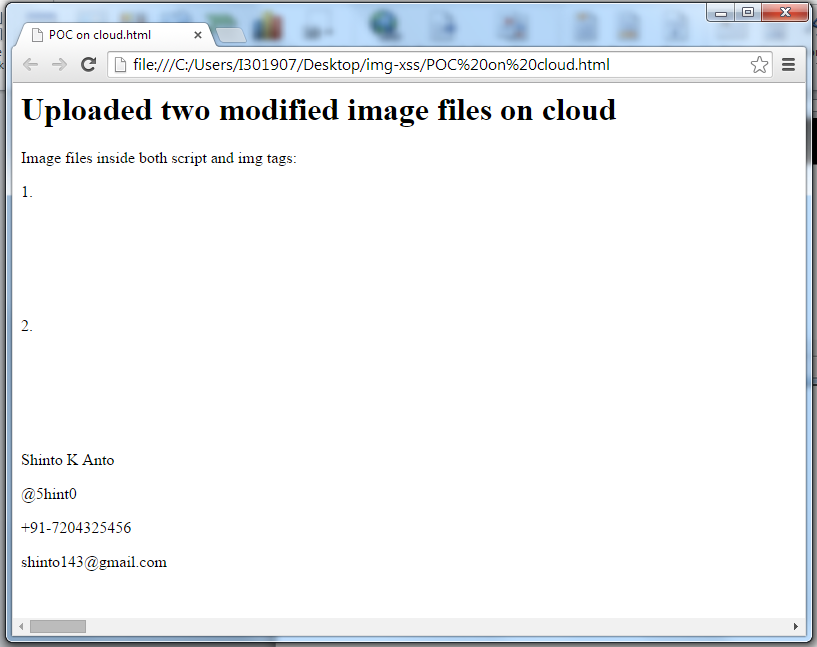
1. POC for scripts getting executed from an image file. (on cloude version.)



2. Behavior of Internet explorer 10 (It gives a warning but still even if we allow the warning the scripts won’t get executed.)



3. Chrome 39.0 will not load these images itself since these are manipulated. (Forget about script)



4. POC For images from localhost.

