**XSS姿势——文件上传XSS**

<http://static.hx99.net/static/drops/tips-14915.html>

### 姿势一：文件名方式

### 姿势二：Metadata

使用[exiftool](http://www.sno.phy.queensu.ca/%7Ephil/exiftool/)这个工具可以通过改变EXIF  metadata进而一定几率引起某处反射：

$ exiftool -field = XSS FILE

### 姿势三：Content

如果应用允许上传SVG格式的文件（其实就是一个图像类型的），那么带有以下content的文件可以被用来触发XSS：

<svg xmlns="http://www.w3.org/2000/svg" onload="alert(document.domain)"/>

### 姿势四：Source

建立一个携带有JavaScript payload的GIF图像用作一个脚本的源。这对绕过CSP（内容安全策略）保护“script-src ‘self’”（即不允许使用示例的这种xss方式进行攻击<script>alert(1)</script>）是很有用的，但前提是我们能够成功地在相同的域注入，如下所示。

要创建这样的图像需要这个作为content 和 name，并使用.gif扩展名：

GIF89a/\*<svg/onload=alert(1)>\*/=alert(document.domain)//;

这个GIF的图片头——GIF89a，作为alert function的变量分配给alert function。但是他们之间，还有一个被标注的XSS变量用来防止图片被恢复为text/HTML MIME文件类型，因此只需发送一个对这个文件的请求payload 就可以被执行。