畸形解析漏洞

在IIS7.0中，在默认开启Fast-CGI开启的情况下，我们在与片中写入代码

')?>

这是一个XXS语句，当然你也可以修改为其他代码，然后保存为 kk.png 格式，假设其服务器目录为/update，然后我们这句话是生成一段shell.php木马的，之后你就会发想，当我们访问/update/kk.png/shell.php的时候，畸形解析开始发挥作用。

kk.png会将图片当成一个Php文件进行解析，所以我们里面插入的代码也会被执行。

临时解决方法是将cgi.fix_pathinfo 为 0