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。而为了较好的支持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。

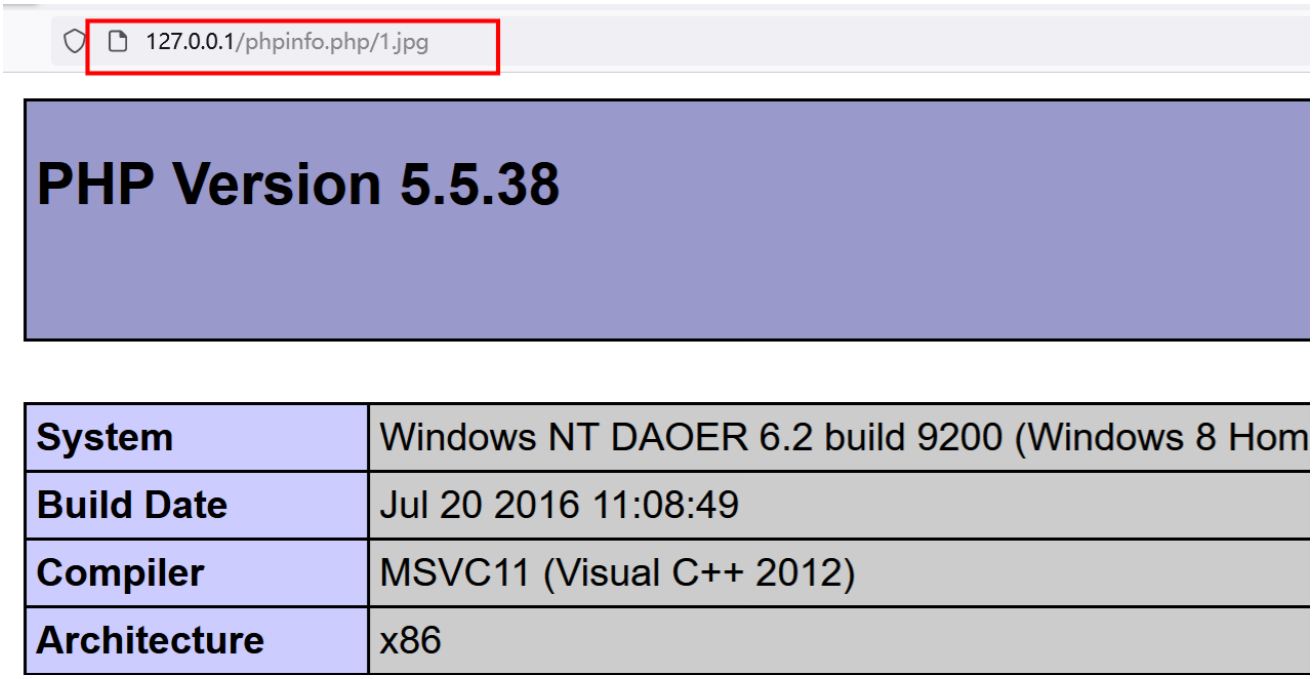
漏洞复现

1、打开php.ini文件设置cgi.fix_pathinfo=1

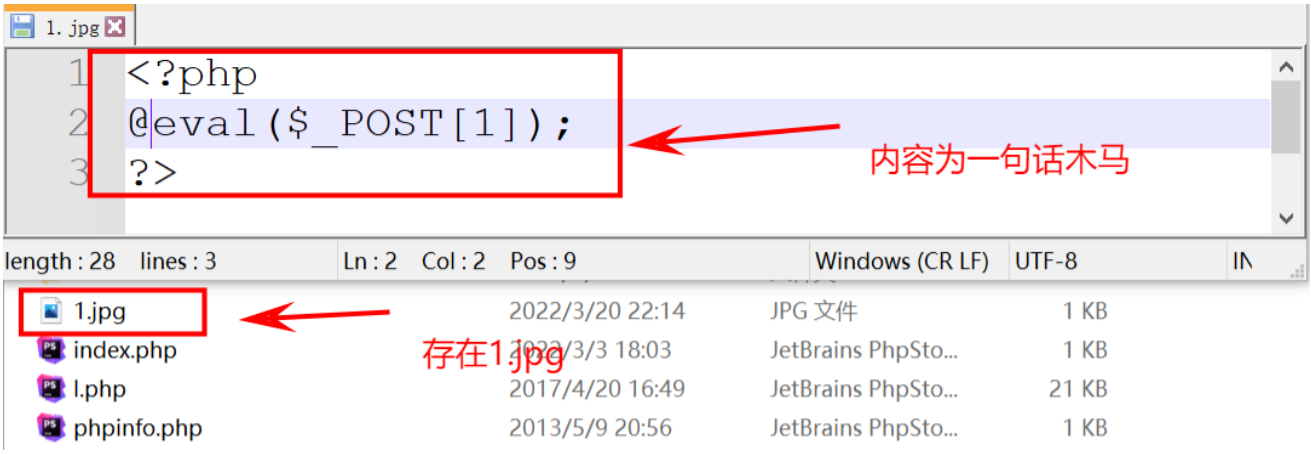
```
; cgi.fix_pathinfo provides *real* PATH_INFO/PATH_TRANSLATED support for CGI.  PHP's
; previous behaviour was to set PATH_TRANSLATED to SCRIPT_FILENAME, and to not grok
; what PATH_INFO is.  For more information on PATH_INFO, see the cgi specs.  Setting
; this to 1 will cause PHP CGI to fix its paths 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
```

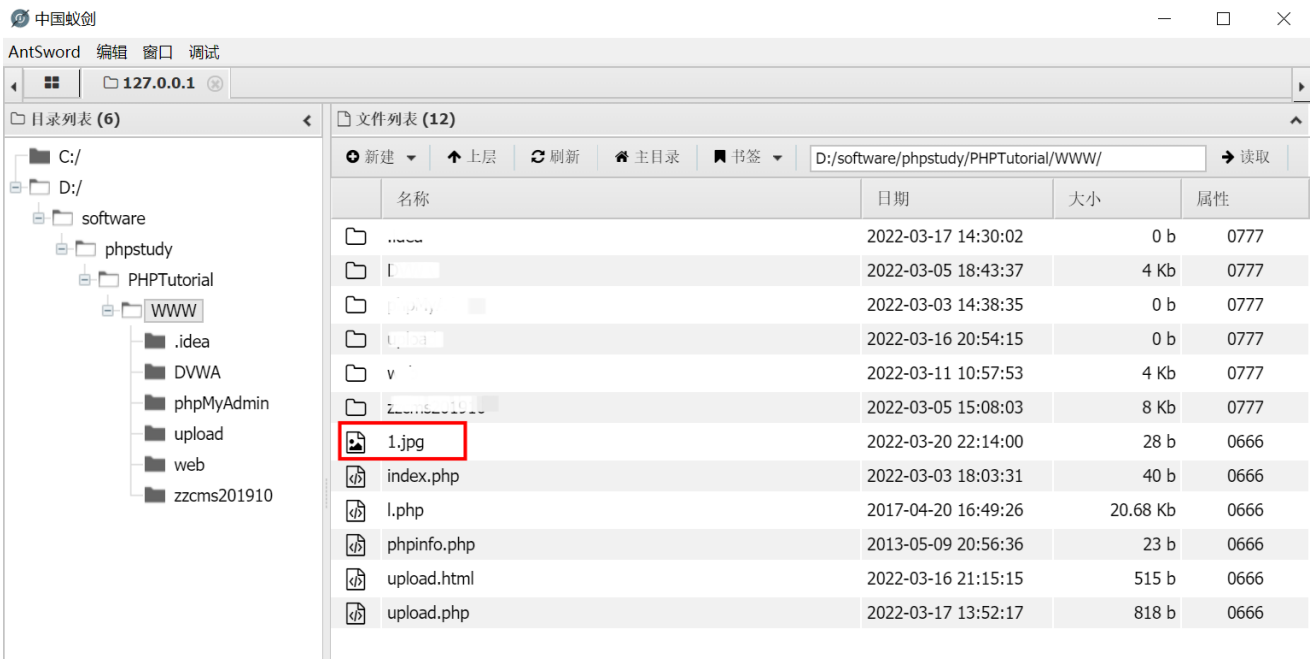
2、在此目录下phpinfo.php文件存在，因为1.jpg不存在所以php就会向前解析，导致漏洞

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



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





漏洞修复

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