CVE-2013-4547 漏洞复现

漏洞原因

phpstudy 采用了符合漏洞范围版本的 Nginx

Nginx 漏洞影响到范围：Nginx 0.8.41~1.4.3 / 1.5.0~1.5.7

漏洞复现

0x01 测试环境:

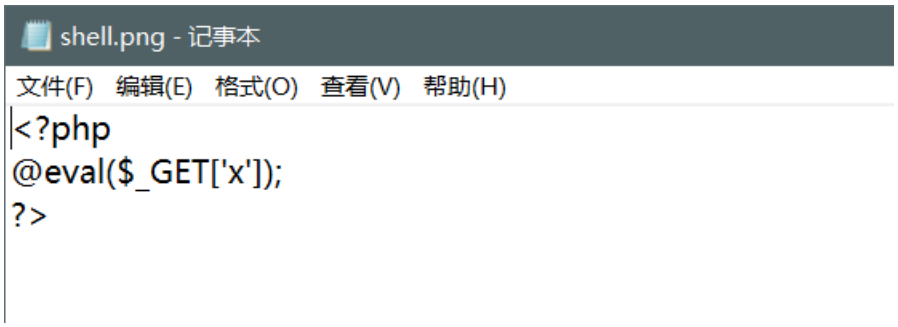
Windows 10 专业版

Phpstudy：8.1.0.7

Nginx：

php：7.3.4

0x02 准备一个图片马

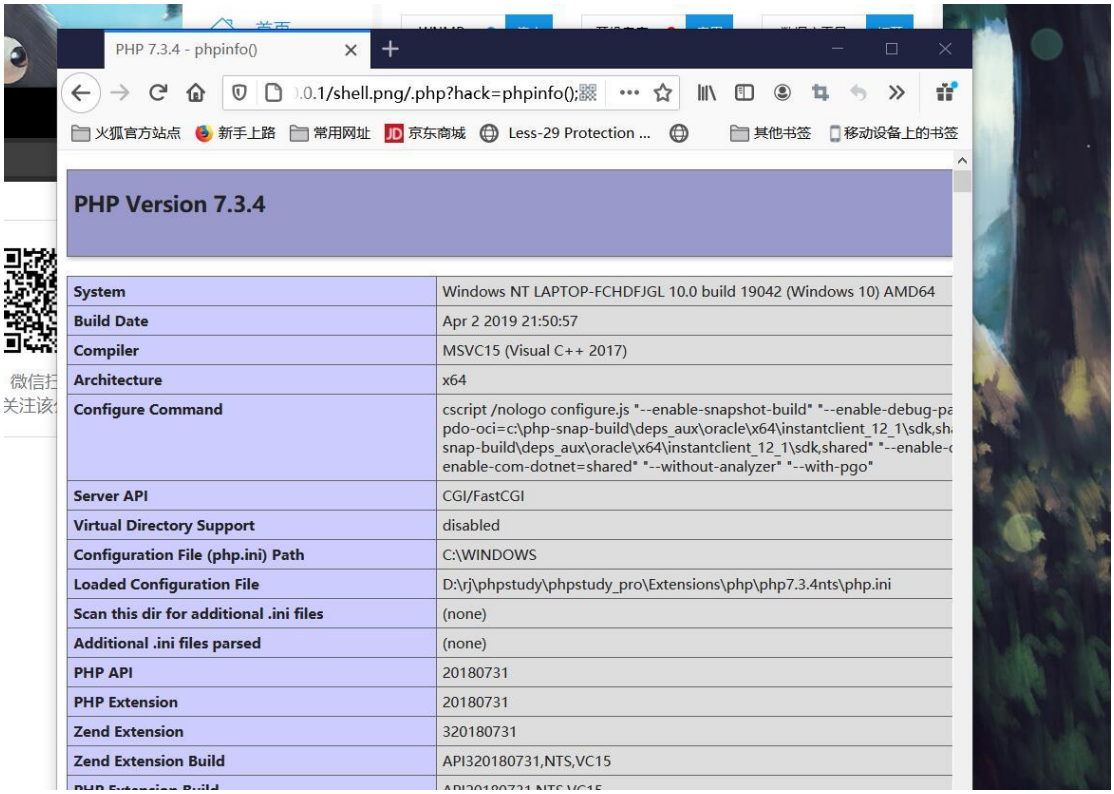


上传该图片马，获得保存路径

0x03 访问图片马

/upload/shell.png/.php?x=phpinfo();

成功将上传的 png 文件 解析成 php 文件



分析漏洞

1、 该漏洞主要因为 Nginx，由于 nginx.conf 的配置问题，导致 Nginx 把以 “.php” 结尾的文件交给 fastcgi 处理。例如我们可以构造出的非 php 后

缀文件并让 Nginx 交给 fastcgi

2、 当 fastcgi 在处理“.php”的文件时发现文件并不存在，例如我们这里 URL 里的“/.php”（url 结尾不一定是“.php”，任何服务器端不存在的 php 文件均可，比如'a.php'）这时 php.ini 配置文件中 cgi.fix_pathinfo=1 就发挥作用

3、 cgi.fix_pathinfo 这项配置是用于修复路径，如果当前路径下不存在则采用上层路径。为此 fastcgi 处理的文件就变成了“./shell.png”

4、 最重要的一点，php-fpm.conf 中的 security.limit_extensions 配置项限制了 fastcgi 解析文件的类型（即指定什么类型的文档当作代码解析），这项设置为空时才允许 fastcgi 将“.png”等文件当作代码解析。

漏洞修复

修复的关键就是把 php.ini 文件中 cgi.fix_pathinfo 的值设置为 0，即未找到的文件就返回 404 页面，同时把 php-fpm.conf 中的 security.limit_extensions 后面的值设置为“.php“