Writeup

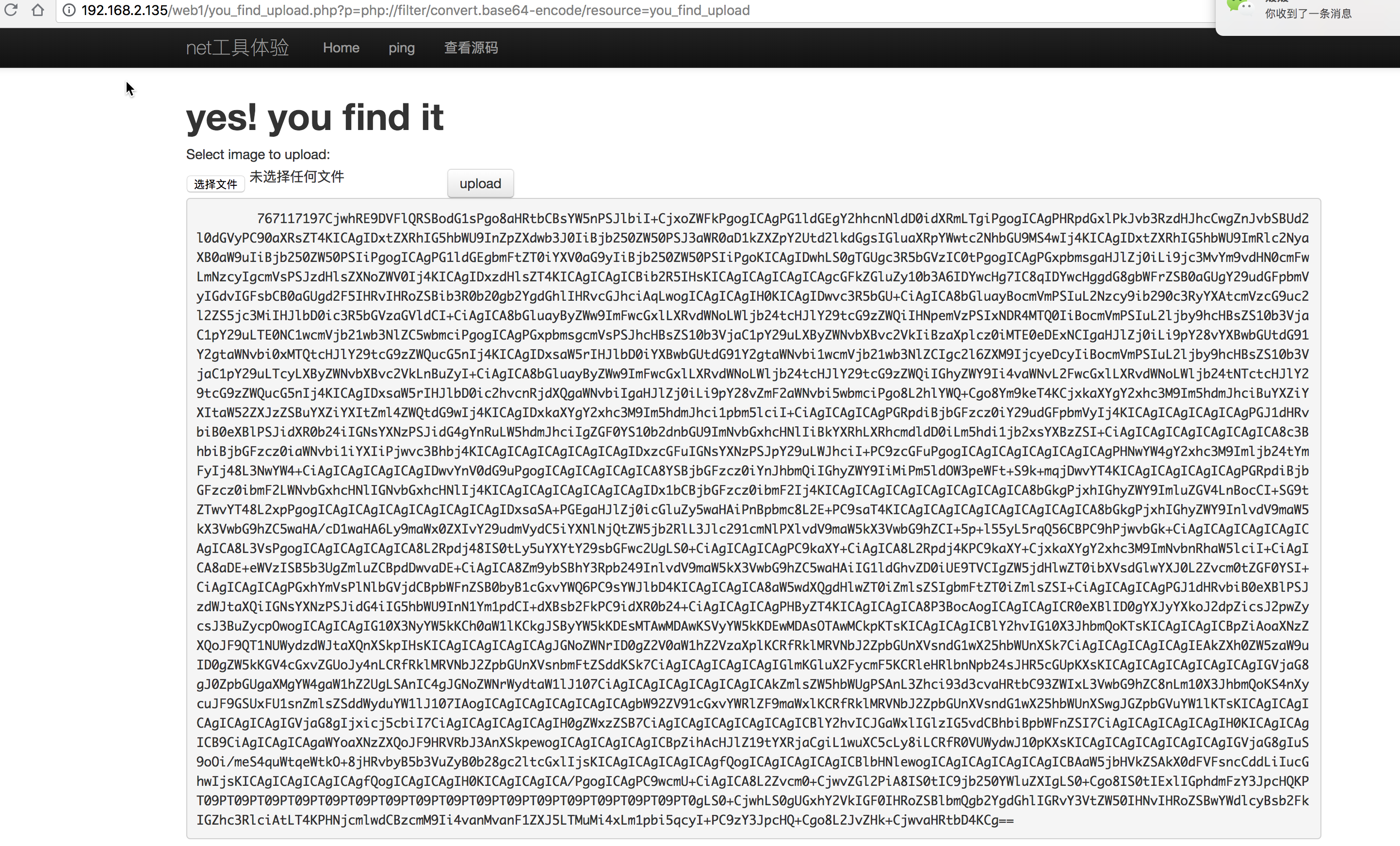
Net工具体验

Flag:upload目录下的f14g\_saikjmld98401294.php文件

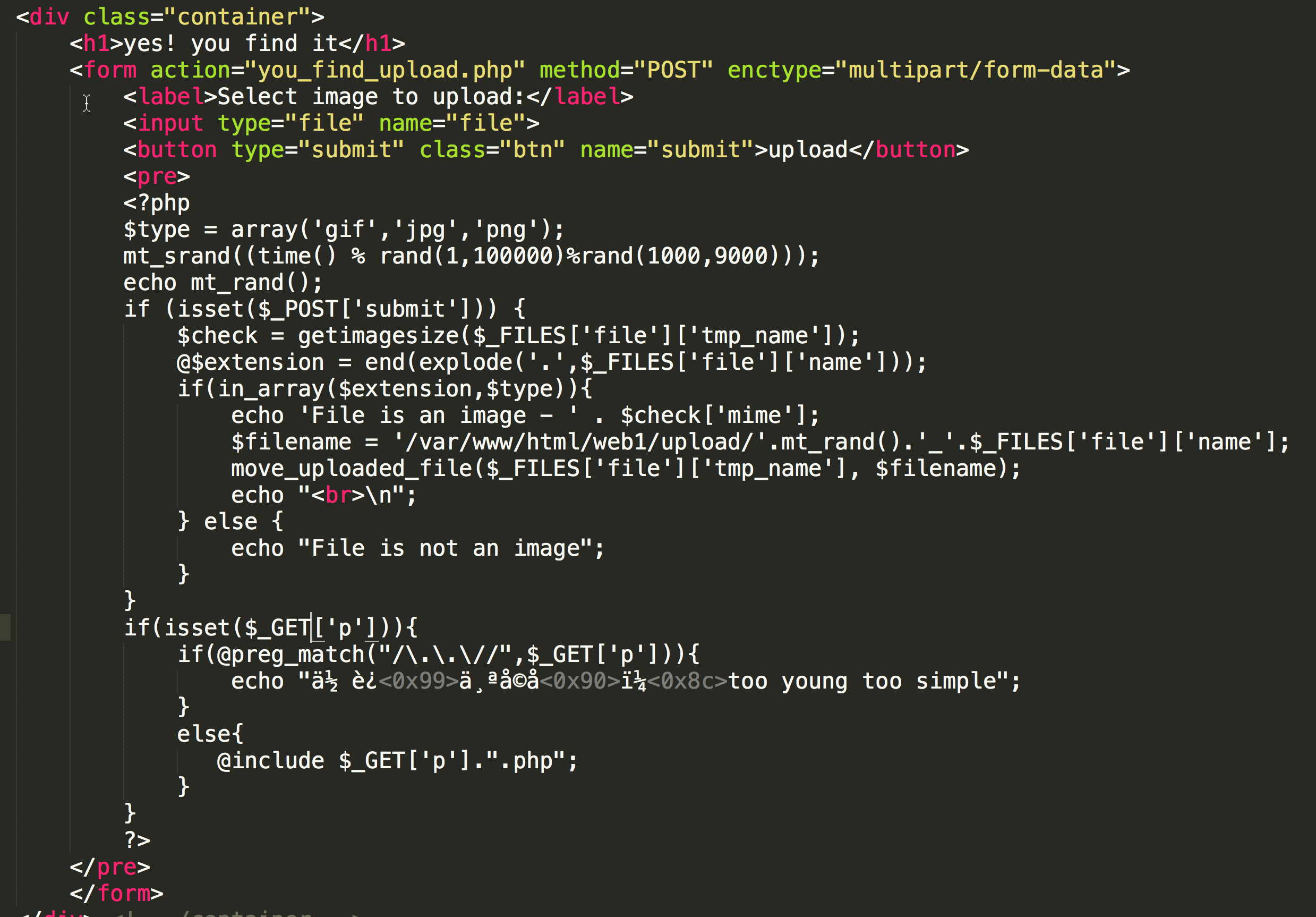
1. 使用127.0.0.1&&ls进行命令执行，找到you\_find\_upload.php文件



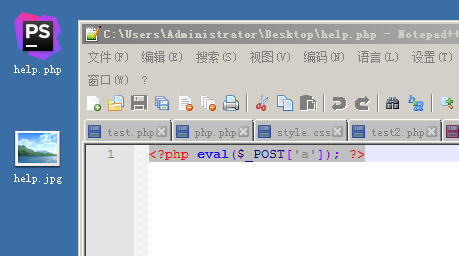
1. 该文件存在一个上传点和一个文件包含，点击查看源码可以查看文件的源码的base64编码文件



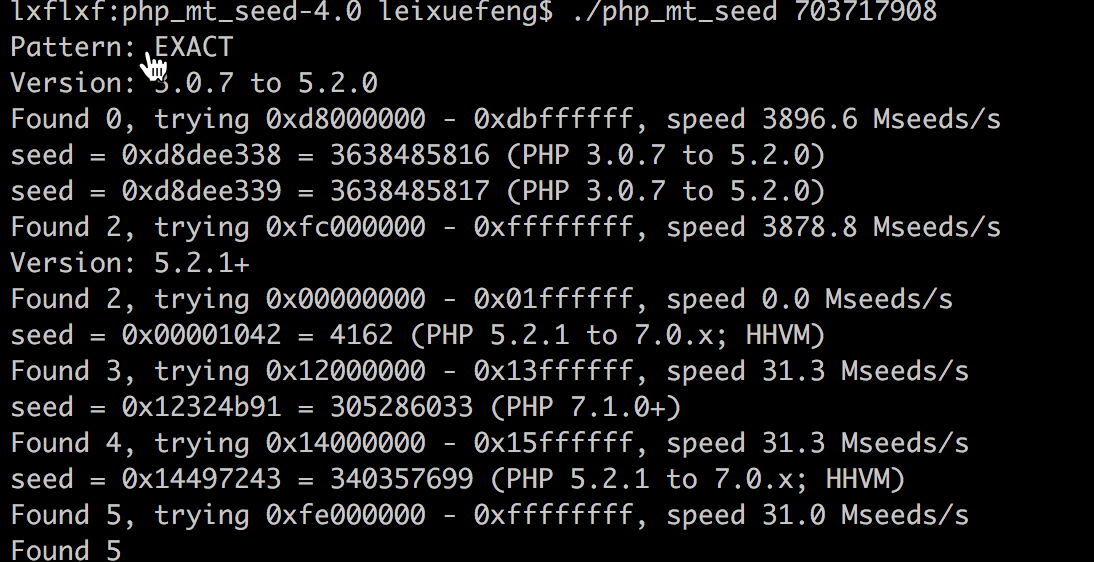
1. 解码出来后是you\_find\_upload.php的源代码文件。



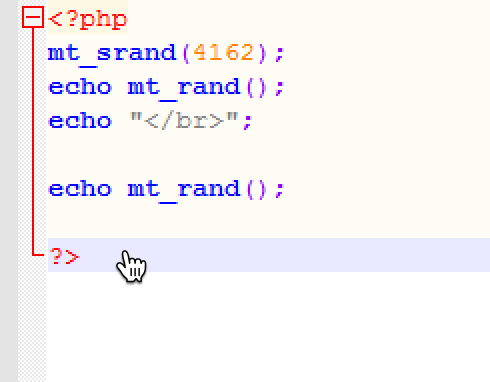
1. 可通过phar协议进行包含文件，制作一个包含一句话木马的zip压缩包，压缩完后将后缀改成jpg

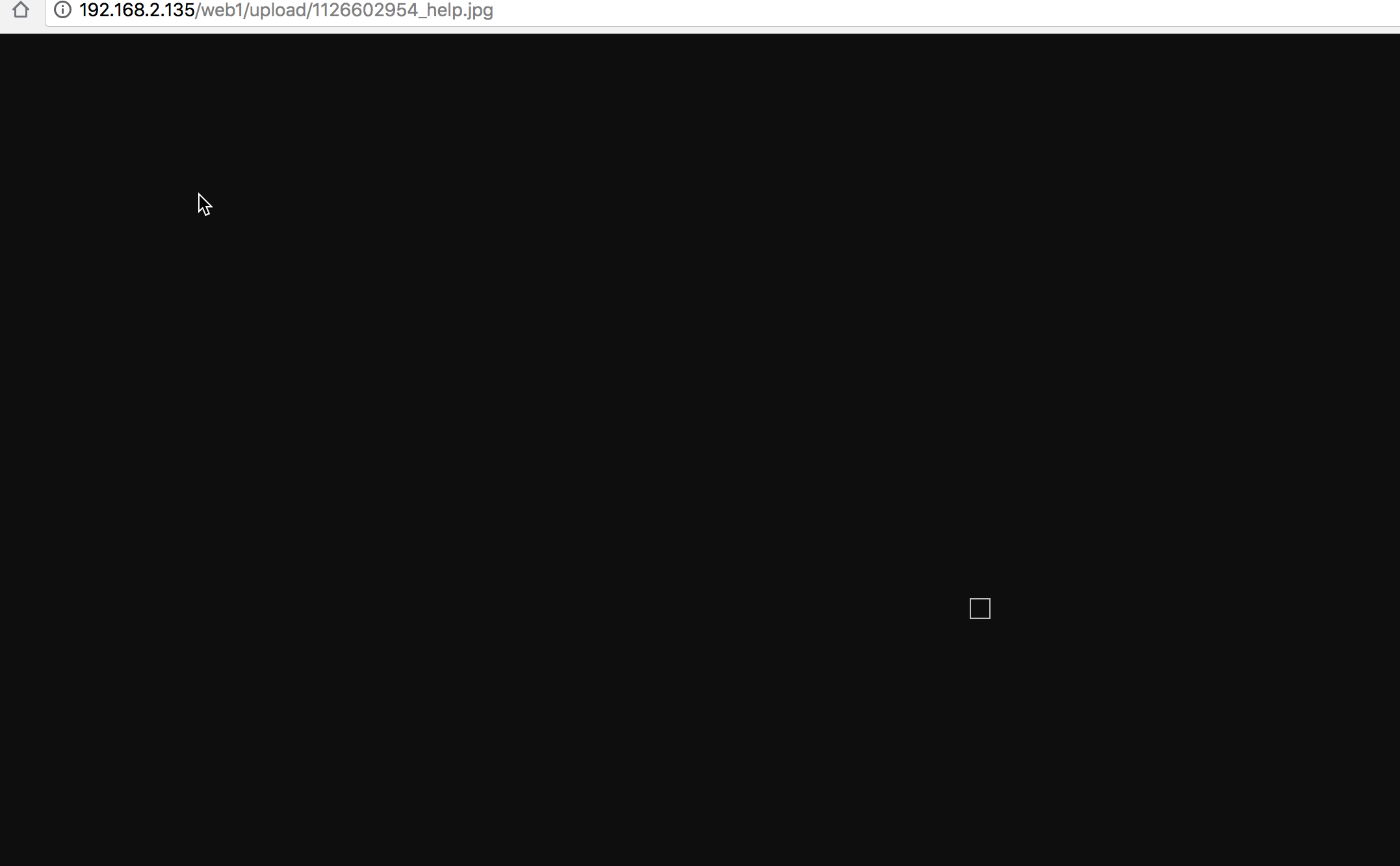


1. 上传该文件，会生成一个随机数，通过php\_mt\_seed进行爆破。找到随机数种子



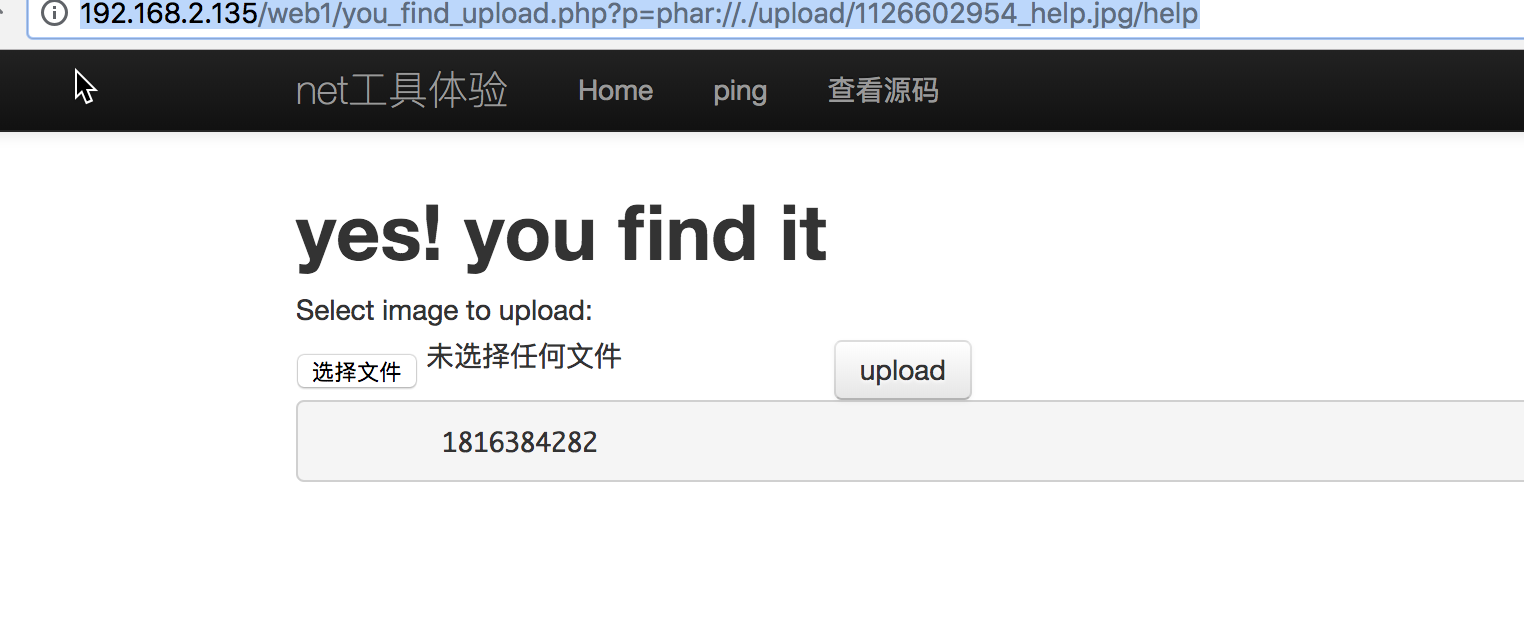
1. 写代码，找到第二次生成的随机数，并找到上传的文件





1. 通过phar协议进行包含

<http://192.168.2.135/web1/you_find_upload.php?p=phar://./upload/1126602954_help.jpg/help>



1. 菜刀连接

