ThinkPHP5.0.x 远程代码执行漏洞

安全威胁通告

综述

ThinkPHP 是一个快速、兼容而且简单的轻量级国产 PHP 开发框架。ThinkPHP 从诞生以来一直秉承简洁实用的设计原则，在保持出色的性能和至简的代码的同时，也注重易用性。并且拥有众多原创功能和特性，在社区团队的积极参与下，在易用性、扩展性和性能方面不断优化和改进。1 月 11 日，ThinkPHP 官方发布了安全更新，其中修复了存在 ThinkPHP5.0.0~5.0.23 版本中的远程代码执行漏洞

相关链接：https://blog.thinkphp.cn/910675

漏洞利用评估

在 ThinkPHP5.0.x 在 5.0.24 之前的所有版本，由于 Request 类 method 方法对用户可控的数据处理不当，攻击者可以通过发送精心构造的恶意请求，即可在服务端执行任意代码，利用方式简单，影响面广。

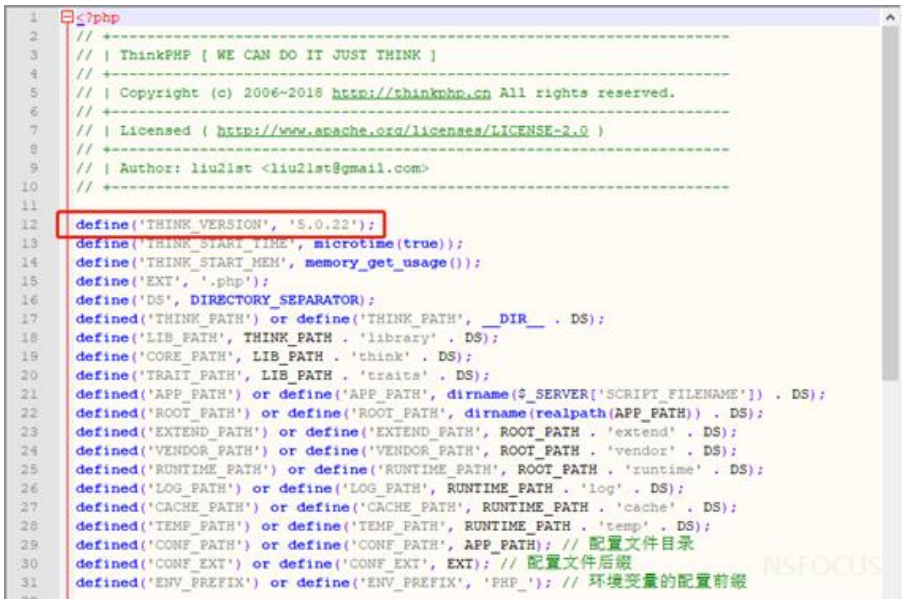
受影响的版本

ThinkPHP5.0.x 在 5.0.24 之前的所有版本

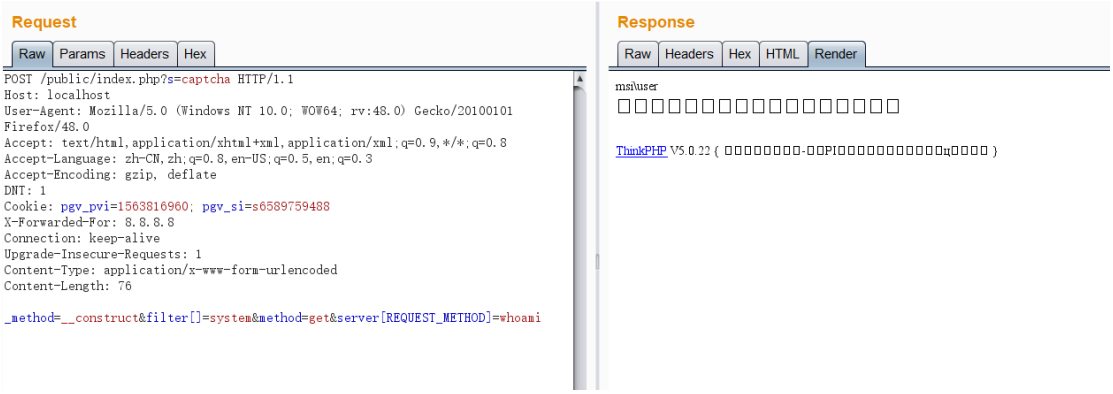
检测方法

- 检查 ThinkPHP5.0.x 是否为受影响版本：5.0.24 之前的所有版本

  使用文本编辑器打开 thinkphp\base.php 文件，在常量定义的代码中即可获取当前框架的版本：



- 以 ThinkPHP5.0.22 为例进行测试，构造如下数据包：



解决方案

- 版本升级：更新 ThinkPHP 到 5.0.24

  ThinkPHP5 支持使用 Composer 来安装升级，建议先备份 application 和修改过的目录，在网站根目录下打开 cmd，执行如下命令之一：

```
composerupdatetopthink/framework5.0.24
composerupdatetopthink/framework=5.0.24
composerupdatetopthink/framework:5.0.24
```

注：若用户使用的为早期 ThinkPHP5 版本，在升级过程中可能存在兼容性问题，用户可参考官方手册的升级指导章节进行升级。参考链接如下：

https://www.kancloud.cn/manual/thinkphp5/163239

- 如果不能更新到最新版本，建议直接参考最新版本的 Request 类的 method 方法进行手动修复。

  该漏洞存在于 ThinkPHP 处理请求的关键类 Request 中。用户也可通过改进 Request 类，对此漏洞进行修复，具体代码修复方案可参考下列链接：

  https://github.com/top-think/framework/commit/4a4b5e64fa4c46f851b4004005bff5f3196de003

使用编辑器打开\thinkphp\library\think\Request.php，找到第 525、526 行代码：

```
$this->method=strtoupper($_POST[Config::get('var_method')]);
$this->{$this->method}($_POST);
```

将其修改为如下代码：

```
$method=strtoupper($_POST[Config::get('var_method')]);
if(in_array($method,['GET','POST','DELETE','PUT','PATCH'])){
    $this->method=$method;
    $this->{$this->method}($_POST);
}
```

保存即可。