

ThinkCMF 框架上的任意内容包含漏洞

2019-10-21 17:08 ThinkCMF (/?tag=thinkcmf) WEB安全 (/?tag=web%E5%B9%A5%E5%B8%A8) 漏洞分析 (/?tag=%E6%BC%8F%E6%B4%B9%E5%B8%86%E6%9E%90)

- 一、背景
- 二、影响版本
- 三、漏洞危害
- 四、漏洞挖掘
- 五、影响范围
- 六、修复方法
- 七、自定义后门

一、背景

ThinkCMF是一款基于PHP+MYSQL开发的中文内容管理框架，底层采用ThinkPHP3.2.3构建。
ThinkCMF提出灵活的应用机制，框架自身提供基础的管理功能，而开发者可以根据自身的需求以应用的形式进行扩展。
每个应用都能独立的完成自己的任务，也可通过系统调用其他应用进行协同工作。在这种运行机制下，开发商场应用的用户无需关心开发SNS应用时如何工作的，但他们之间又可通过系统本身进行协调，大大的降低了开发成本和沟通成本。
官网: http://www.thinkcmf.com

二、影响版本

ThinkCMF X1.6.0
ThinkCMF X2.1.0
ThinkCMF X2.2.0
ThinkCMF X2.2.1
ThinkCMF X2.2.2

三、漏洞危害

远程攻击者在无需任何权限情况下，通过构造特定的请求包即可在远程服务器上执行任意代码。

四、漏洞挖掘

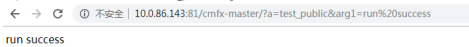
根据index.php中的配置，他的项目路径为application，打开 Portal 下的 Controller 目录，选择一个控制类文件。

```
namespace Portal\Controller;
use Common\Controller\HomebaseController;
/**
 * 首页
 */
class IndexController extends HomebaseController {
    //首页 小夏是老猫除外最帅的男人了
    public function index() {
        $this->display(":index");
    }
}
```

发现他的父类为Common\Controller\HomebaseController，
在HomeBaseController中加入如下测试代码

```
public function test_public($arg1='') {
    echo $arg1;
    die();
}
```

ThinkPHP是一套基于MVC的应用程序框架，被分成三个核心部件：模型（M）、视图（V）、控制器（C）。
由于添加的代码在控制器中，根据ThinkPHP框架约定可以通过a参数来指定对应的函数名，但是该函数的修饰符必须为Public，而添加的代码正好符合该条件。
可以通过如下URL进行访问，并且可以添加GET参数arg1传递给函数。
http://127.0.0.1/cmfx-master/?a=test_public&arg1=run%20success



HomeBaseController类中有一些访问权限为public的函数。

```
/**
 * 加载模板和页面输出 可以返回输出内容
 * @access public
 * @param string $templateFile 模板文件名
 * @param string $charset 模板输出字符集
 * @param string $contentType 输出类型
 * @param string $content 模板输出内容
 * @return mixed
 */
public function display($templateFile = '', $charset =
    {
        parent::display($this->parseTemplate($templateFile))
    }

/**=
public function fetch($templateFile='', $content='', $pre

/**=|
public function parseTemplate($template='') {=

/**
 * 设置错误，成功跳转页面
```

重点关注display函数 看描述就是可以自定义加载模版，通过
\$this->parseTemplate 函数根据约定确定模版路径，如果不符合原先的约定将会从当前目录开始匹配。
然后调用Thinkphp Controller 函数的display方法

关键字导航: 漏洞分析 (https://blog.riskivy.com/tag/%e6%bc%8f%e6%b4%9e%e5%88%86%e6%9e%00/) WEB安全 (https://blog.riskivy.com/tag/web%e5%ae%89%e5%85%a8/) 网络安全 (https://blog.riskivy.com/tag/%e7%bd%91%e7%bb%9c%e5%ae%89%e5%85%a8/) 智能合约 (https://blog.riskivy.com/tag/%e6%99%ba%e8%83%bd%e5%90%88%e7%ba%a6/) 区块链 (https://blog.riskivy.com/tag/%e5%8c%ba%e5%9d%97%e9%93%be/) 远程代码执行 (https://blog.riskivy.com/tag/%e8%b%9c%e7%a8%8b%e4%bb%a3%e7%a0%81%e6%89%a7%e8%a1%8c/) 反序列化 (https://blog.riskivy.com/tag/%e5%8f%8d%e5%ba%8f%e5%88%97%e5%8c%96/) 机器学习 (https://blog.riskivy.com/tag/%e6%9c%ba%e5%99%a8%e5%ad%e4%b9%a0/) ThinkPHP5 (https://blog.riskivy.com/tag/thinkphp5/) Confluence (https://blog.riskivy.com/tag/confluence/) 代码审计 (https://blog.riskivy.com/tag/%e4%bb%a3%e7%a0%81%e5%ae%a1%e8%ae%a1/) 渗透测试 (https://blog.riskivy.com/tag/%e6%b8%97%e9%80%8f%e6%b5%8b%e8%af%95/) 漏洞挖掘 (https://blog.riskivy.com/tag/%e6%bc%8f%e6%b4%9e%e6%8c%96%e6%8e%98/) WebLogic (https://blog.riskivy.com/tag/weblogic/) 逆向分析 (https://blog.riskivy.com/tag/%e9%80%86%e5%90%97%e5%88%86%e6%9e%90/) 内网渗透 (https://blog.riskivy.com/tag/%e5%86%65%e7%bd%97%e6%b8%97%e9%80%8f/) WebShell (https://blog.riskivy.com/tag/webshell/) IoT安全 (https://blog.riskivy.com/tag/iot%e5%ae%89%e5%85%a8/) 恶意文件 (https://blog.riskivy.com/tag/%e9%87%b6%e6%84%8d%e9%87%e4%b3%86/) Fastjson (https://blog.riskivy.com/tag/fastjson/) Jackson (https://blog.riskivy.com/tag/jackson/) 漏洞情报 (https://blog.riskivy.com/tag/%e6%bc%89%e6%84%9e%e9%85%e6%8a%5/) cve (https://blog.riskivy.com/tag/cve/) Shiro (https://blog.riskivy.com/tag/shiro/) 内网安全 (https://blog.riskivy.com/tag/%e5%86%85%e7%bd%97%e5%ae%89%e5%85%a8/) Nuexo (https://blog.riskivy.com/tag/nuxeo/) Kubernetes (https://blog.riskivy.com/tag/kubernetes/) 统计分析 (https://blog.riskivy.com/tag/%e7%bb%9f%e8%ae%a1%e5%88%86%e6%9e%90/) ICMP隧道 (https://blog.riskivy.com/tag/%e9%82%ae%e4%bb%b6%e6%9c%8d%e5%8a%a1/) DCshadow (https://blog.riskivy.com/tag/dcshadow/) DNS隧道 (https://blog.riskivy.com/tag/dns%e9%9a%7%e9%81%93/) 域控制侧 (https://blog.riskivy.com/tag/%e5%9f%9f%e6%8e%a7%e5%88%b6%e5%99%a8/) ECShop (https://blog.riskivy.com/tag/ecshop/) Spark (https://blog.riskivy.com/tag/spark/) Flask-admin (https://blog.riskivy.com/tag/flask-admin/) 移动安全 (https://blog.riskivy.com/tag/%e7%a7%bb%e5%8a%85%ae%89%e5%85%a8/)


相关推荐

Grafana 文件读取漏洞分析与汇总(CVE-2021-43798) (https://blog.riskivy.com/grafana-%e4%bb%bb%e6%84%8f%e6%96%87%e4%bb%b6%e8%a1%bb%e5%8f%96%e6%bc%8f%e6%b4%9e%e5%88%86%e6%9e%90%e4%b8%8e%e6%b1%87%e6%80%bbce-2021-43798/)
Weblogic CVE-2021-2394 RCE漏洞分析 (https://blog.riskivy.com/weblogic-cve-2021-2394-rce%e6%bc%8f%e6%b4%9e%e5%88%86%e6%9e%90/)
2021HVV期间披露的漏洞分析 (https://blog.riskivy.com/2021hvv%e6%9c%9f%e9%97%b4%e6%8a%b7%e9%9c%b2%e7%9a%84%e6%bc%8f%e6%b4%9e%e5%88%86%e6%9e%90%e6%8c%81%e7%bb%ad%e6%9b%b4%e6%96%b0/)
2021 攻防演练中需要关注的重点漏洞 (https://blog.riskivy.com/2021-%e6%94%bb%e9%98%b2%e6%bc%94%e7%bb%83%e4%b8%ad%e9%9c%80%e8%a6%81%e5%85%b3%e6%b3%a8%e7%9a%84%e9%8d%7%8d%e7%82%b2%9e%e6%bc%8f%e6%b4%9e/)
F5从认证绕过远程代码执行漏洞分析 (https://blog.riskivy.com/f5%e4%b8%e8%ae%a4%e8%81%e7%bb%95%e8%b8%7%e5%88%b0%e8%b4%9c%e7%a8%8b%e4%bb%a3%e7%a0%81%e6%89%a7%e8%bc%8f%e6%b4%9e%e5%88%86%e6%9e%90/)

评论 (0)

暂无评论

发表评论





邮箱: support@tophant.com
咨询: 400 156 9866 (7*24小时)

产品中心

PRS-NTA (https://www.riskivy.com/prs)
PRS-NXIDS (https://www.riskivy.com/prs-nxids)
PRS-MAC (https://www.riskivy.com/prs-mac)
ARS (https://www.riskivy.com/ars)
CRS (https://www.riskivy.com/crs)
ROT (https://www.riskivy.com/rot)
VMS (https://www.riskivy.com/vms)
ARL (https://www.riskivy.com/arl)

关注服务号



关于我们

最新动态 (https://www.riskivy.com/aboutUs/news)
关于斗象智能安全 (https://www.riskivy.com/aboutUs/about)
客户故事 (https://www.riskivy.com/aboutUs/partner)
联系我们 (https://www.riskivy.com/aboutUs/contact)
加入我们 (https://www.lagou.com/gongsi/j33219.html)

友情链接

斗象科技 (http://www.tophant.com)
FreeBuf (https://www.freebuf.com)
漏洞盒子 (http://www.vulbox.com)