可以先透過 `checksec pwntools` 來確認有哪些安全選項有開啟

```
root@kali:~/chang6# checksec pwntools
[*] '/root/chang6/pwntools'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
root@kali:~/chang6#
```

發現到 `PIE` 是關的

嘗試執行後發現有 1 次輸入

```
File  Edit  View  Search  Terminal  Help
root@kali:~/chang6# socat TCP-LISTEN:20000,fork EXEC:'./pwntools'
```

```
root@kali:~/chang6# nc 127.0.0.1 20000
Give me the magic :)
abc
Bye!
root@kali:~/chang6#
```

執行 objdump 後發現到 main 在 read 後有一次 cmp

```
objdump -M intel -d pwntools
```

```
 40094c:       e8 df fd ff ff          call   400730 <read@plt>
 400951:       8b 45 dc                mov    eax,DWORD PTR [rbp-0x24]
 400954:       3d ff 87 94 07          cmp    eax,0x79487ff
```

先嘗試輸入 `0x79487ff` 給程式看結果，這裡使用 pwntools send

```
40093a:       ba 04 00 00 00          mov    edx,0x4
40093f:       48 89 c6                mov    rsi,rax
400942:       bf 00 00 00 00          mov    edi,0x0
400947:       b8 00 00 00 00          mov    eax,0x0
40094c:       e8 df fd ff ff          call   400730 <read@plt>
```

在這裡可以發現到 read 只收 4 bytes，因此 python 使用 p32 傳送 4bytes 的訊息。

```python
from pwn import *
r = remote('127.0.0.1',20000)
r.recvuntil(':)')
r.sendline(p32(0x79487FF))
r.interactive()
```

```
root@kali:~/chang6# python3 send.py
[+] Opening connection to 127.0.0.1 on port 20000: Done
send.py:3: BytesWarning: Text is not bytes; assuming ASCII, no gu
  r.recvuntil(':)')
[*] Switching to interactive mode

Hacker can complete 1000 math problems in 60s, prove yourself.
23579 * 5863 = ?$
```

發現到後面有 1000 道數學題目，格式為 數字 運算符 數字 = ?

exploit.py

```python
from pwn import *
r = remote('127.0.0.1', 20000)
r.recvuntil(':)')
r.sendline(p32(0x79487FF))

r.recvline()
r.recvline()
cnt = 0
while(cnt!=1000):
        cnt += 1
        s = r.recvuntil('?')
        print(s)
        arr = s.split(b' ')
        a = int(arr[0])
        b = int(arr[2])
        op = arr[1]
        res = 0
        if(op == b'+'):
                res = a+b
        elif(op == b'-'):
                res = a-b
        elif(op == b'*'):
                res = a*b
        r.sendline(str(res))
r.interactive()
```

```
root@kali:~/chang6# python3 exploit.py
[+] Opening connection to 127.0.0.1 on port 20000: Done
exploit.py:3: BytesWarning: Text is not bytes; assuming ASCII,
  r.recvuntil(':)')
exploit.py:11: BytesWarning: Text is not bytes; assuming ASCII,
  s = r.recvuntil('?')
b'27688 - 12020 = ?'
exploit.py:24: BytesWarning: Text is not bytes; assuming ASCII,
  r.sendline(str(res))
b'7122 * 25307 = ?'
b'16463 + 26773 = ?'
b'6816 * 29590 = ?'
b'24471 - 7893 = ?'
b'27435 + 35281 = ?'
```

```
b'38557 + 13650 = ?'
b'39619 - 29215 = ?'
b'10126 * 29296 = ?'
b'35263 + 2586 = ?'
b'38469 + 1167 = ?'
[*] Switching to interactive mode
Welcome hacker!
$
```