網安實務 Hw3

網工所碩一 309552005 吳偉誠

用到的工具:angr(該HW的練習工具、版本: 8.20.1.7)、python3.8

Question2

1

exploit.py的code:

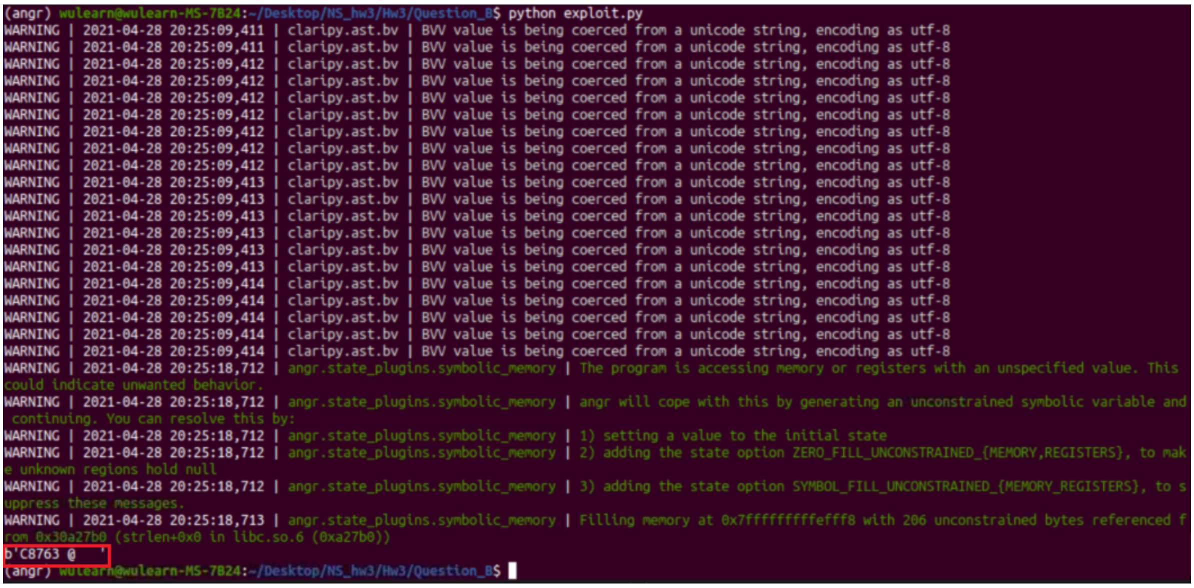
```
import angr
import claripy

proj = angr.Project("./example")
argv1 = claripy.BVS("argv1", 10 * 8)
initial_state = proj.factory.full_init_state(args=["./abc",argv1],
add_options=angr.options.unicorn)
for byte in argv1.chop(8):
    initial_state.add_constraints(byte >= '\x20')# ' '
    initial_state.add_constraints(byte <= '\x7e')# '~'
sm = proj.factory.simulation_manager(initial_state)
sm.explore(find=0x400b0e)
found = sm.found[0]
print(found.solver.eval(argv1, cast_to=bytes))
```

> 基本上跟原本的solve.py大同小異
> 差別在於第六行與第九行的迴圈
> 第六行:使用unicorn引擎來幫助我們執行許多的concrete execution工作
> 第八行:將argv1限制在typical char範圍裡(限制在ascii字元裡、可避免其它怪怪的字元)

改的代碼是參考angr的doc裡的:https://github.com/angr/angr-doc/blob/master/CHEATSHEET.md

2



```
(angr) wulearn@wulearn-MS-7B24:~/Desktop/NS_hw3/Hw3/Question_B$ python exploit.py
WARNING | 2021-04-28 20:25:09,411 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:25:09,411 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:25:09,412 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:25:09,412 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:25:09,412 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:25:09,412 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:25:09,412 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:25:09,412 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:25:09,412 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:25:09,413 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:25:09,413 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:25:09,413 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:25:09,413 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:25:09,413 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:25:09,413 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:25:09,414 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:25:09,414 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:25:09,414 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:25:09,414 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:25:09,414 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:25:18,712 | angr.state_plugins.symbolic_memory | The program is accessing memory or registers with an unspecified value. This
could indicate unwanted behavior.
WARNING | 2021-04-28 20:25:18,712 | angr.state_plugins.symbolic_memory | angr will cope with this by generating an unconstrained symbolic variable and
 continuing. You can resolve this by:
WARNING | 2021-04-28 20:25:18,712 | angr.state_plugins.symbolic_memory | 1) setting a value to the initial state
WARNING | 2021-04-28 20:25:18,712 | angr.state_plugins.symbolic_memory | 2) adding the state option ZERO_FILL_UNCONSTRAINED_{MEMORY,REGISTERS}, to mak
e unknown regions hold null
WARNING | 2021-04-28 20:25:18,712 | angr.state_plugins.symbolic_memory | 3) adding the state option SYMBOL_FILL_UNCONSTRAINED_{MEMORY_REGISTERS}, to s
uppress these messages.
WARNING | 2021-04-28 20:25:18,713 | angr.state_plugins.symbolic_memory | Filling memory at 0x7ffffffffefff8 with 206 unconstrained bytes referenced f
rom 0x30a27b0 (strlen+0x0 in libc.so.6 (0xa27b0))
b'C8763 @   '
(angr) wulearn@wulearn-MS-7B24:~/Desktop/NS_hw3/Hw3/Question_B$
```

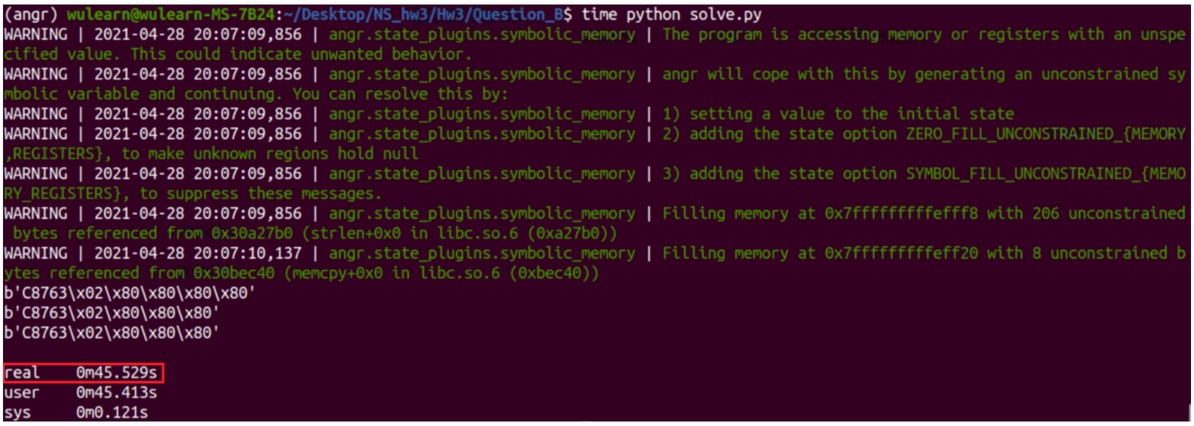
> 得到: `C8763`

並將該輸入餵給example(記得先改成可執行: `chmod +x example`):

```
(angr) wulearn@wulearn-MS-7B24:~/Desktop/NS_hw3/Hw3/Question_B$ ./example C8763
You got it!!
```

3

原本助教提供的腳本運行時間:

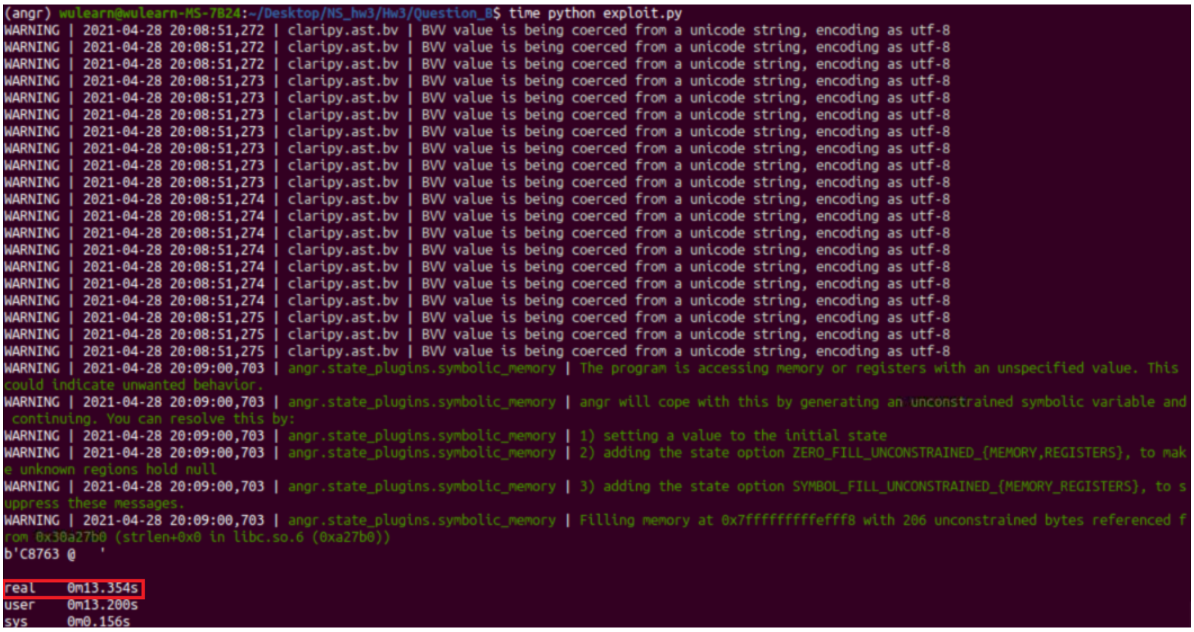


```
(angr) wulearn@wulearn-MS-7B24:~/Desktop/NS_hw3/Hw3/Question_B$ time python solve.py
WARNING | 2021-04-28 20:07:09,856 | angr.state_plugins.symbolic_memory | The program is accessing memory or registers with an unspe
cified value. This could indicate unwanted behavior.
WARNING | 2021-04-28 20:07:09,856 | angr.state_plugins.symbolic_memory | angr will cope with this by generating an unconstrained sy
mbolic variable and continuing. You can resolve this by:
WARNING | 2021-04-28 20:07:09,856 | angr.state_plugins.symbolic_memory | 1) setting a value to the initial state
WARNING | 2021-04-28 20:07:09,856 | angr.state_plugins.symbolic_memory | 2) adding the state option ZERO_FILL_UNCONSTRAINED_{MEMORY
,REGISTERS}, to make unknown regions hold null
WARNING | 2021-04-28 20:07:09,856 | angr.state_plugins.symbolic_memory | 3) adding the state option SYMBOL_FILL_UNCONSTRAINED_{MEMO
RY_REGISTERS}, to suppress these messages.
WARNING | 2021-04-28 20:07:09,856 | angr.state_plugins.symbolic_memory | Filling memory at 0x7ffffffffefff8 with 206 unconstrained
 bytes referenced from 0x30a27b0 (strlen+0x0 in libc.so.6 (0xa27b0))
WARNING | 2021-04-28 20:07:10,137 | angr.state_plugins.symbolic_memory | Filling memory at 0x7fffffffffeff20 with 8 unconstrained b
ytes referenced from 0x30bec40 (memcpy+0x0 in libc.so.6 (0xbec40))
b'C8763\x02\x80\x80\x80\x80'
b'C8763\x02\x80\x80\x80'
b'C8763\x02\x80\x80\x80'

real    0m45.529s
user    0m45.413s
sys     0m0.121s
```

> 都是大概約45秒

改良後的時間:



```
(angr) wulearn@wulearn-MS-7B24:~/Desktop/NS_hw3/Hw3/Question_B$ time python exploit.py
WARNING | 2021-04-28 20:08:51,272 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:08:51,272 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:08:51,272 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:08:51,273 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:08:51,273 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:08:51,273 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:08:51,273 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:08:51,273 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:08:51,273 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:08:51,273 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:08:51,274 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:08:51,274 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:08:51,274 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:08:51,274 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:08:51,274 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:08:51,274 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:08:51,274 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:08:51,275 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:08:51,275 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:08:51,275 | claripy.ast.bv | BVV value is being coerced from a unicode string, encoding as utf-8
WARNING | 2021-04-28 20:09:00,703 | angr.state_plugins.symbolic_memory | The program is accessing memory or registers with an unspecified value. This
could indicate unwanted behavior.
WARNING | 2021-04-28 20:09:00,703 | angr.state_plugins.symbolic_memory | angr will cope with this by generating an unconstrained symbolic variable and
 continuing. You can resolve this by:
WARNING | 2021-04-28 20:09:00,703 | angr.state_plugins.symbolic_memory | 1) setting a value to the initial state
WARNING | 2021-04-28 20:09:00,703 | angr.state_plugins.symbolic_memory | 2) adding the state option ZERO_FILL_UNCONSTRAINED_{MEMORY,REGISTERS}, to mak
e unknown regions hold null
WARNING | 2021-04-28 20:09:00,703 | angr.state_plugins.symbolic_memory | 3) adding the state option SYMBOL_FILL_UNCONSTRAINED_{MEMORY_REGISTERS}, to s
uppress these messages.
WARNING | 2021-04-28 20:09:00,703 | angr.state_plugins.symbolic_memory | Filling memory at 0x7ffffffffefff8 with 206 unconstrained bytes referenced f
rom 0x30a27b0 (strlen+0x0 in libc.so.6 (0xa27b0))
b'C8763 @   '

real    0m13.354s
user    0m13.200s
sys     0m0.156s
```

> 都是大概約13秒

將近快了3倍多