教育部先進資通安全實務人才培育計畫

111年度新型態資安實務暑期課程

Advanced Information Security Summer School

軟體安全-第三組 DFF一站式漏洞檢測工具箱

組員：曾厚荃 林祐丞 鄭帆修 吳柏宏

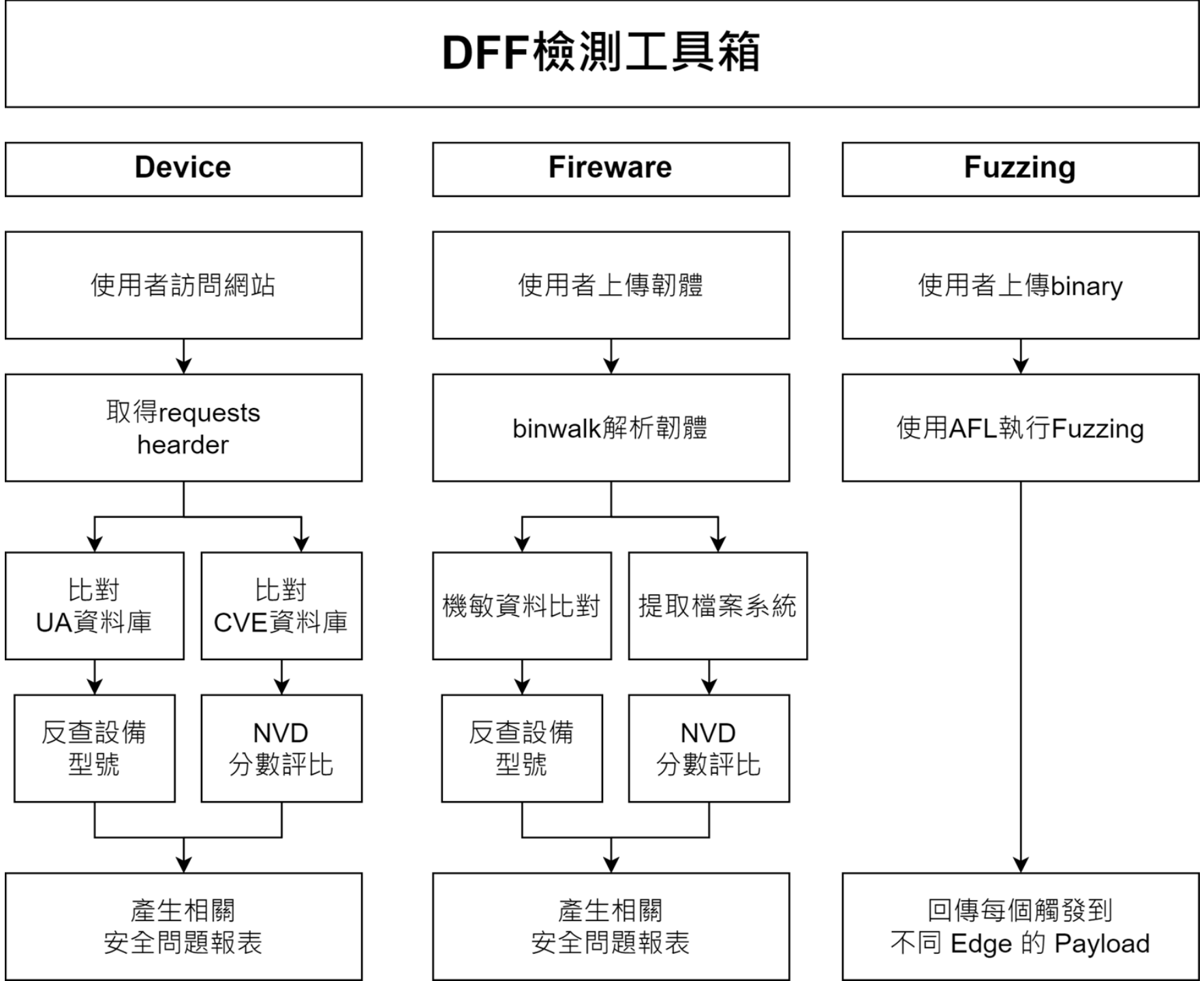
目錄

專題介紹——DFF檢測工具箱

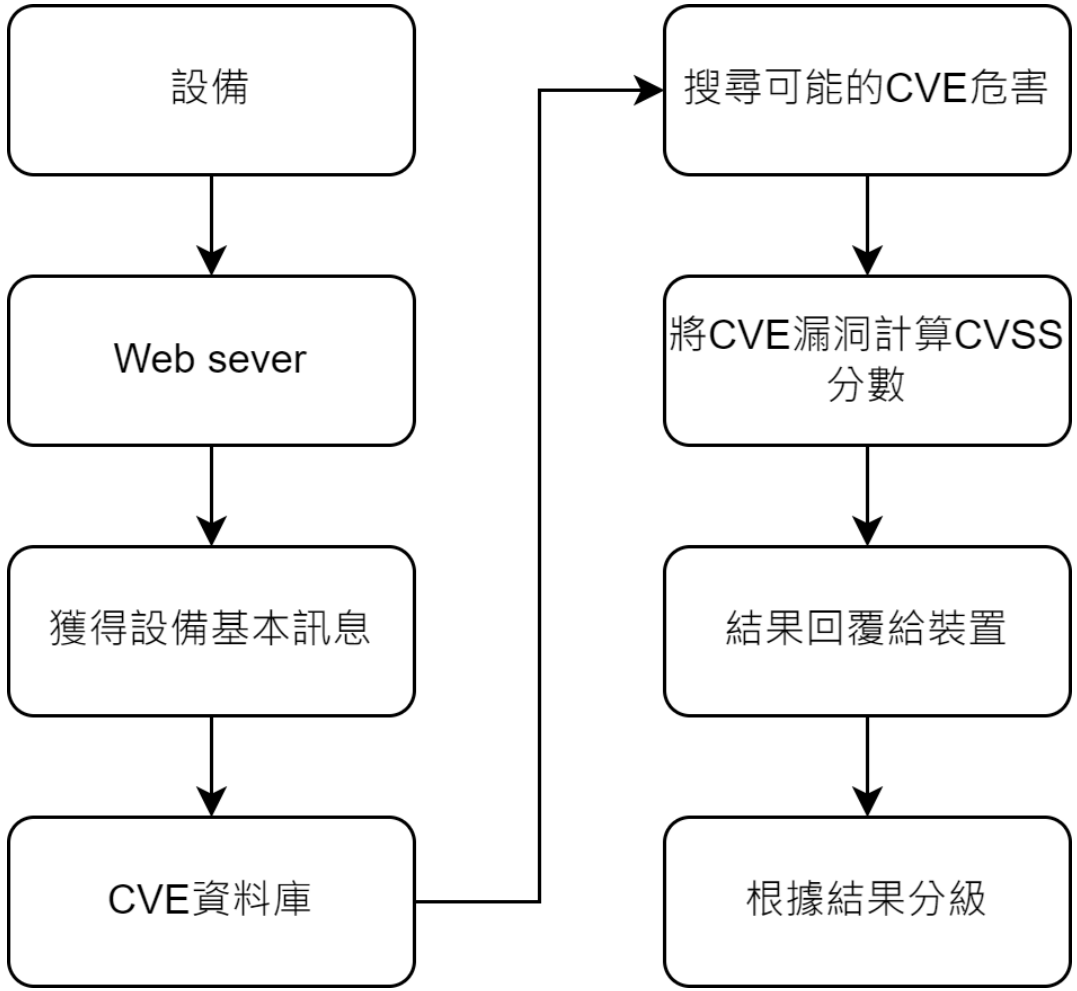
Device	版本健檢
Firmware	線上拆解
Fuzzing	線上執行

動機

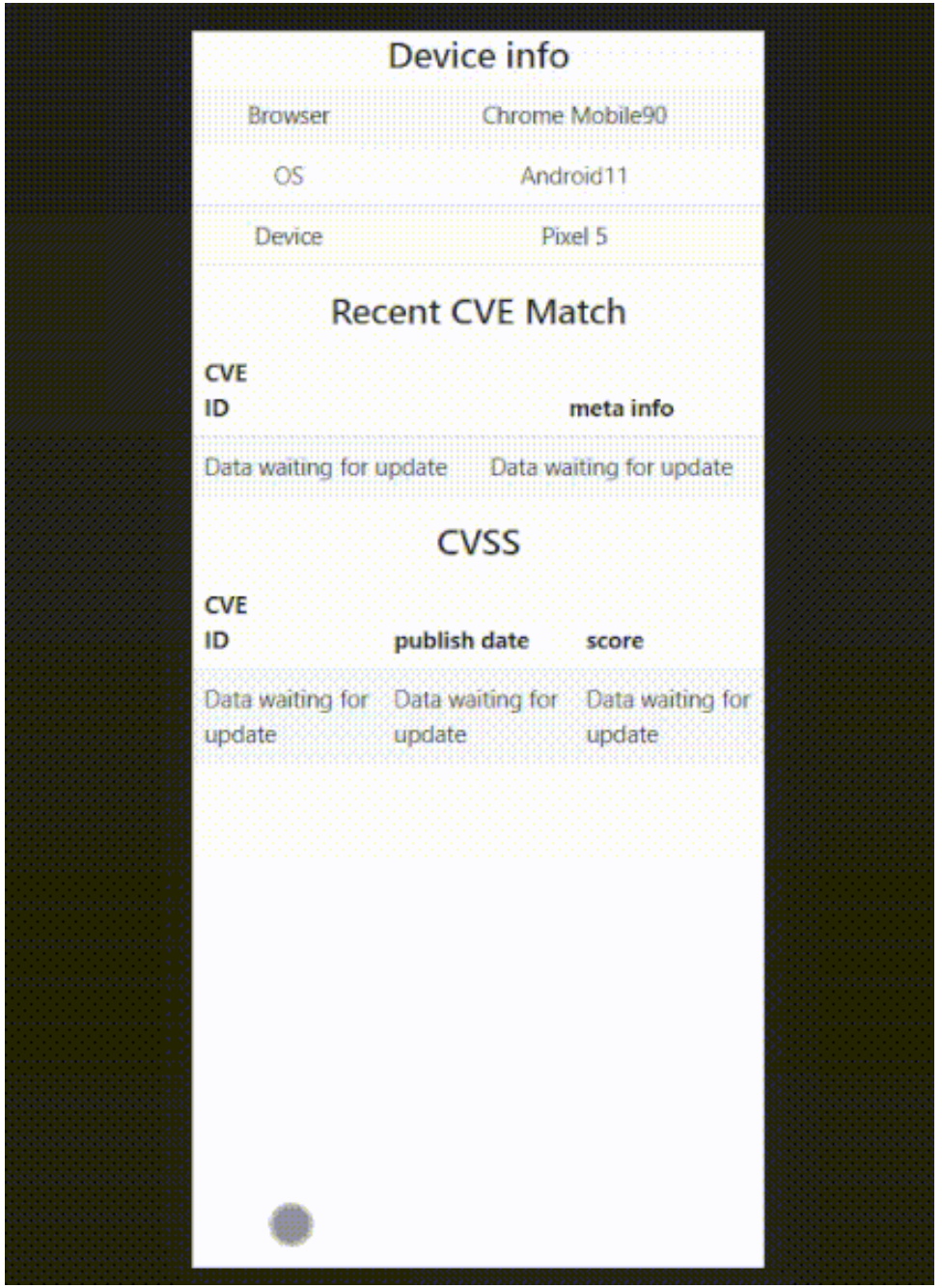
Device	"Had I been pwned" 啟發自個資外洩事件 裝置資訊與CVE的資料庫比對
Firmware	藉由WebService將環境交給後端 實現在任何地方都可以拆韌體
Fuzzing	課程中使用白箱進行Fuzzing 延伸應用在黑箱下解決Fuzzing Fuzzing運算資源適合於雲端主機運行


DFF檢測工具箱
Device
使用者訪問網站
取得requests hearder
比對 UA資料庫
比對 CVE資料庫
反查設備 型號
NVD 分數評比
產生相關 安全問題報表
Fireware
使用者上傳韌體
binwalk解析韌體
機敏資料比對
提取檔案系統
反查設備 型號
NVD 分數評比
產生相關 安全問題報表
Fuzzing
使用者上傳binary
使用AFL執行Fuzzing
回傳每個觸發到 不同 Edge 的 Payload

Device版本健檢


設備
Web sever
獲得設備基本訊息
CVE資料庫
搜尋可能的CVE危害
將CVE漏洞計算CVSS分數
結果回覆給裝置
根據結果分級

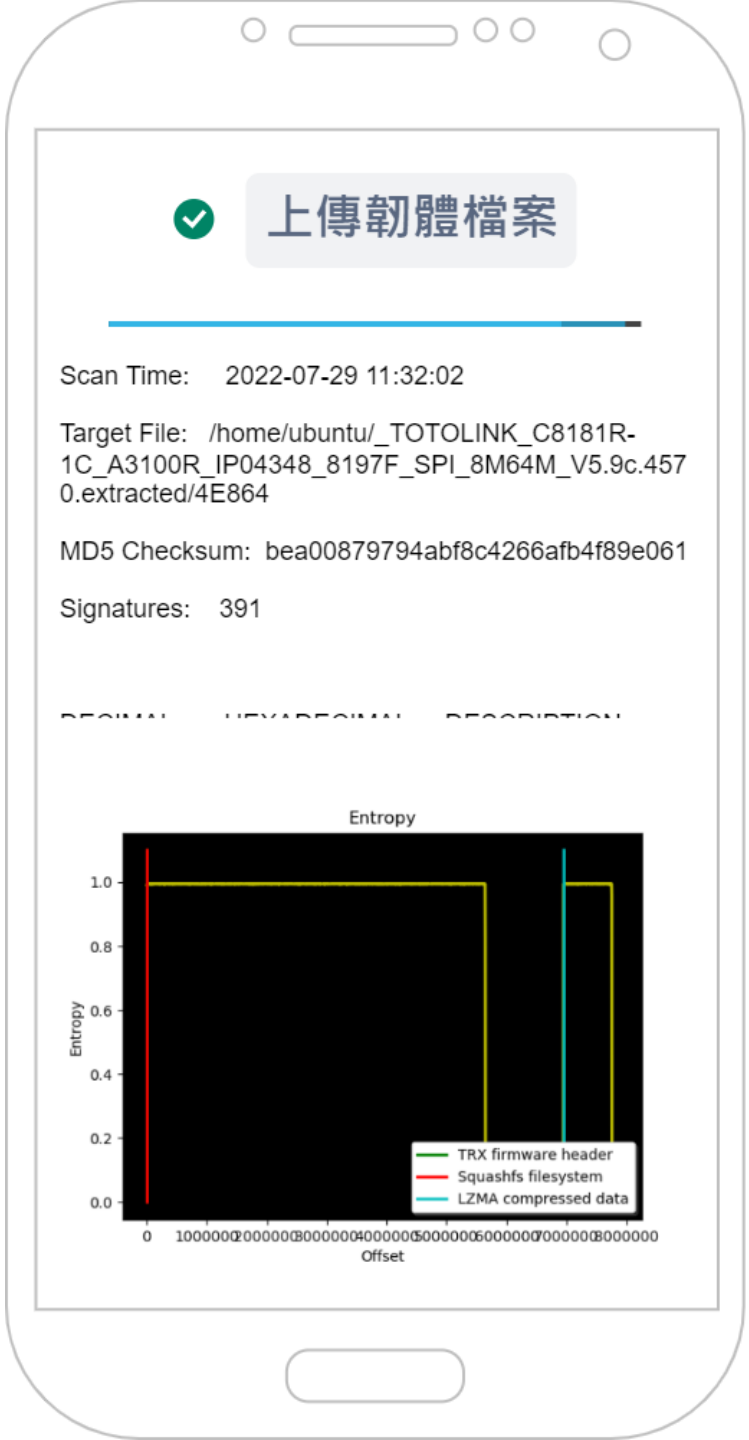
實作


Device info
Browser
Chrome Mobile90
OS
Android11
Device
Pixel 5
Recent CVE Match
CVE ID
meta info
Data waiting for update
Data waiting for update
CVSS
CVE ID
publish date
score
Data waiting for update
Data waiting for update
Data waiting for update

IOT Device Firmware線上拆解

概念設計

```
Scan Time:     2022-07-29 02:02:10
Target File:   /home/ubuntu/_ddwrt-linksys-wrt1200ac-webflash.bin.extracted/5CC0
MD5 Checksum:  823cb7af09c80319faea337d7bea8469
Signatures:    391

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
608           0x260           device tree image (dtb)
1125248       0x112B80        SHA256 hash constants, little endian
1407037       0x15783D        Certificate in DER format (x509 v3), header length: 4, sequence length: 1332
4085317       0x3E5645        Certificate in DER format (x509 v3), header length: 4, sequence length: 5376
4267401       0x411D89        Certificate in DER format (x509 v3), header length: 4, sequence length: 5384
4579129       0x45DF39        Certificate in DER format (x509 v3), header length: 4, sequence length: 1432
6336576       0x60B040        CRC32 polynomial table, little endian
6390035       0x618113        Intel x86 or x64 microcode, sig 0x03000000, pf_mask 0x01, 20C0-18-20, rev 0x6aa56c00, size 192
6871376       0x68D950        xz compressed data
6917700       0x698E44        Unix path: /lib/firmware/updates/4.9.54
6995948       0x6ABFEC        Unix path: /sys/firmware/devicetree/base
6996836       0x6AC364        Unix path: /sys/firmware/fdt': CRC check failed
7004825       0x6AE299        Neighborly text, "neighbor table overflow!is %x"
7034318       0x6B55CE        Neighborly text, "neighbor %.2x%.2x.%pM lost rename link %s to %s"
7041024       0x6B7000        ELF, 32-bit LSB shared object, ARM, version 1 (SYSV)
8573455       0x82D20F        LZMA compressed data, properties: 0xC0, dictionary size: 0 bytes, uncompressed size: 64 bytes


Scan Time:     2022-07-29 02:02:13
Target File:   /home/ubuntu/_ddwrt-linksys-wrt1200ac-webflash.bin.extracted/_5CC0.extracted/82D20F
MD5 Checksum:  3b5d3c7d207e37dceeedd301e35e2e58
Signatures:    391

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
```



Fuzzing線上執行

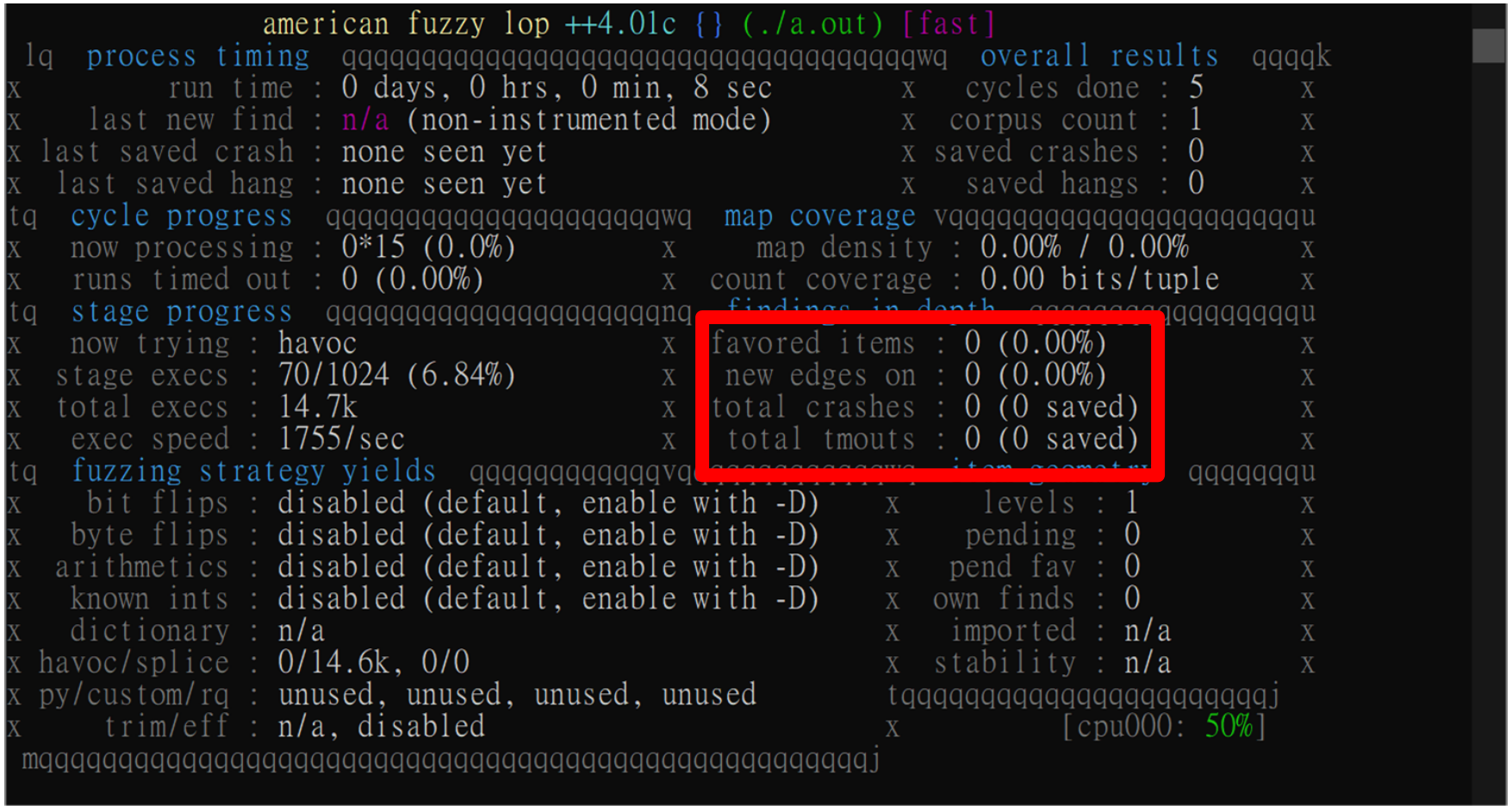
實驗結果

```c
// 1.c
int foo(char *buf) {

    if (buf[2] == 'A') {
        if (buf[3] != 'G')
            return 0;
        else {
            strtok("BOOOOM", "O"); // Crash
            return 1;
        }
    }
}
```

```c
int main() {

    char buf[20]

    scanf("%20s", buf);

    if (buf[0] == 'F') {
        if (buf[1] == 'L')
            return foo(buf);
        else
            return 0;
    } else
        return 0;
}
```

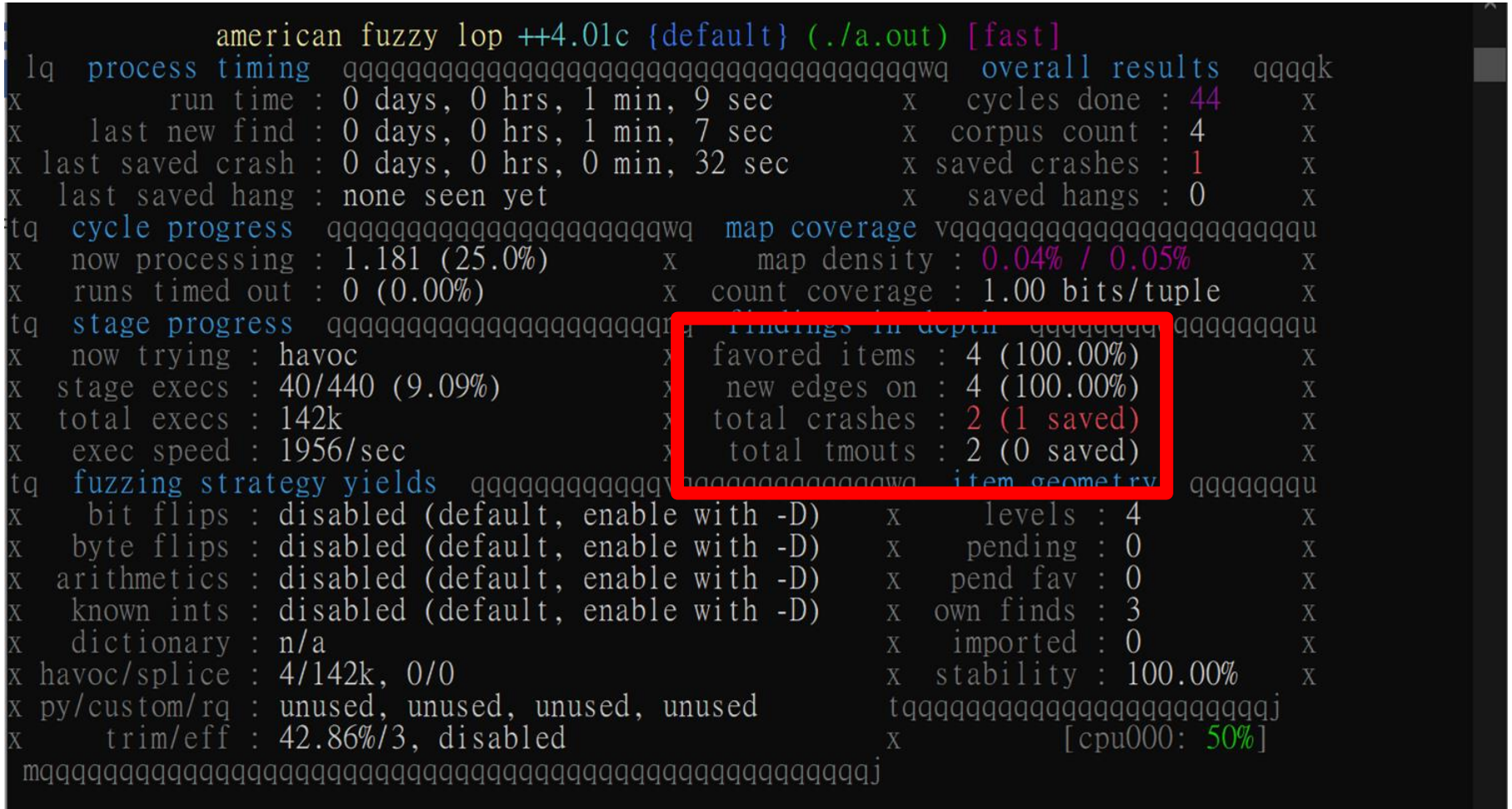
實驗結果

```
afl-fuzz -n -i input/ -o output -- ./a.out
-n              - fuzz without instrumentation (non-instrumented mode)
```

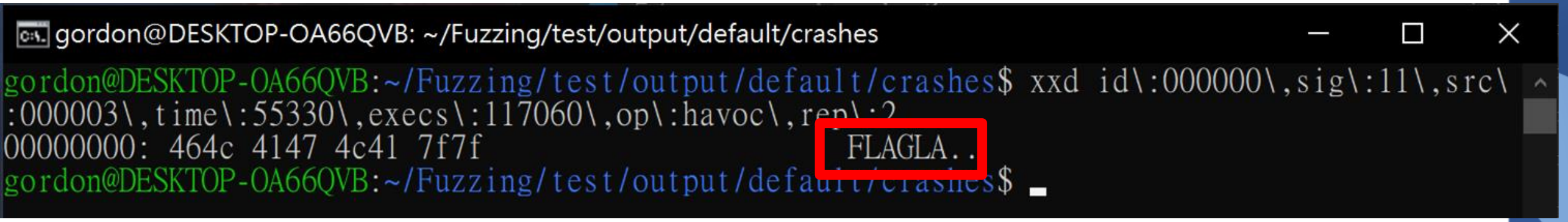


實驗結果

```
afl-fuzz -Q -i input/ -o output -- ./a.out
```



實驗結果


gordon@DESKTOP-OA66QVB: ~/Fuzzing/test/output/default/crashes
gordon@DESKTOP-OA66QVB:~/Fuzzing/test/output/default/crashes$ xxd id\:000000\,sig\:11\,src\
:000003\,time\:55330\,execs\:117060\,op\:havoc\,rep\:2
00000000: 464c 4147 4c41 7f7f FLAGLA..
gordon@DESKTOP-OA66QVB:~/Fuzzing/test/output/default/crashes$

心得結論

- 藉由專案實作回顧課程
- 找尋資料發想延伸應用
- 嘗試在一天內完成PoC

未來工作

Device

增強cve搜尋能力

串接第三方資料庫取得更多裝置特徵

Firmware

能適用更多環境的韌體,如arm64等

Fuzzing

完善自動化流程

Thanks For Listening

Q & A