

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
- 動機
- DFF檢測工具箱
- 心得結論
- 未來工作

#### 專題介紹——DFF檢測工具箱

**Device** 

**F**irmware

Fuzzing

版本健檢

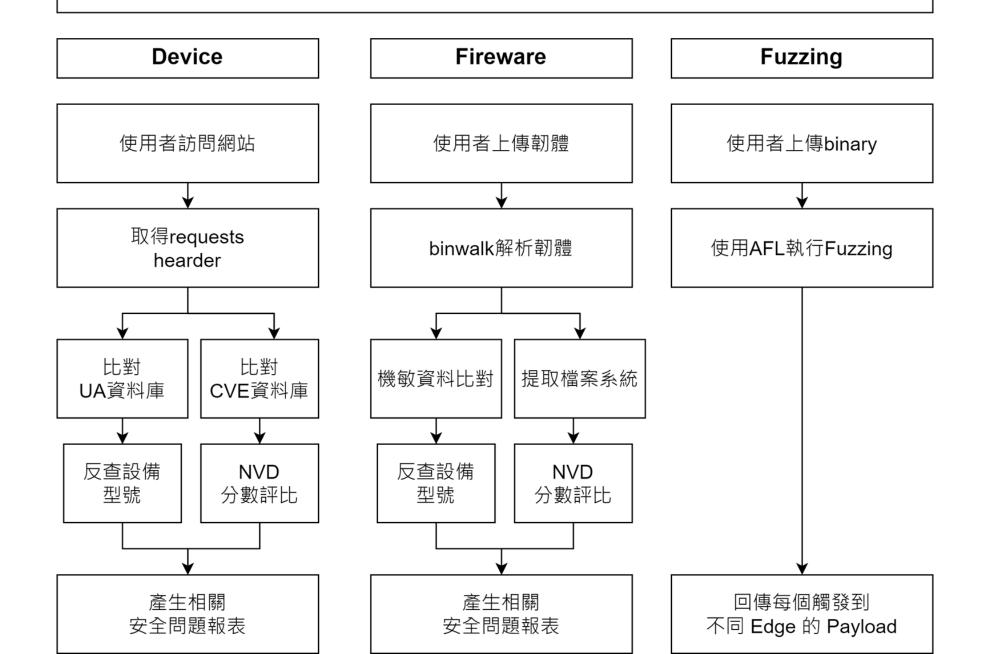
線上拆解

線上執行

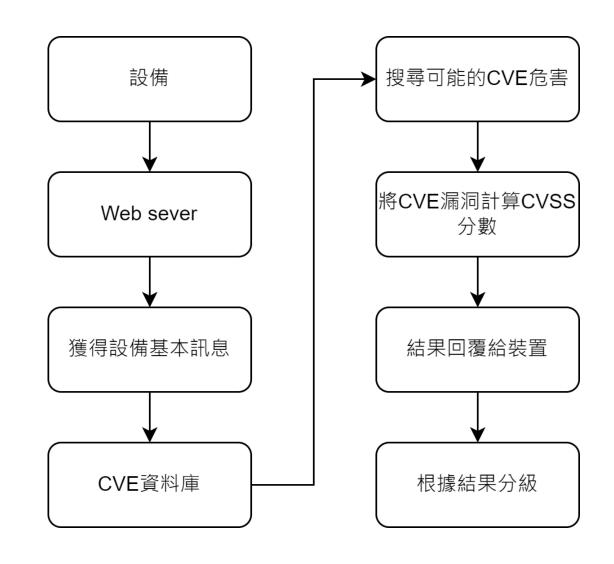
## 動機

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

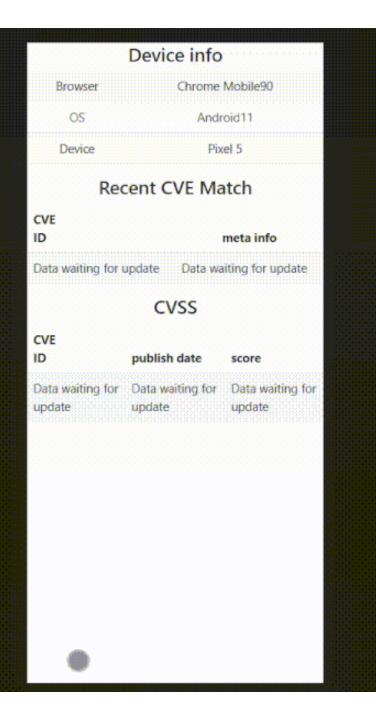
#### DFF檢測工具箱



#### Device版本健檢



## 實作



## IOT Device Firmware線上拆解

#### 概念設計

```
2022-07-29 02:02:10
Scan Time:
Target File:
               /home/ubuntu/_ddwrt-linksys-wrt1200ac-webflash.bin.extracted/5CC0
MD5 Checksum: 823cb7af09c80319faea337d7bea8469
              391
Signatures:
DECIMAL
              HEXADECIMAL
                             DESCRIPTION
608
              0x260
                             device tree image (dtb)
1125248
                             SHA256 hash constants, little endian
             0x112B80
                             Certificate in DER format (x509 v3), header length: 4, sequence length: 1332
1407037
             0x15783D
                             Certificate in DER format (x509 v3), header length: 4, sequence length: 5376
4085317
             0x3E5645
                             Certificate in DER format (x509 v3), header length: 4, sequence length: 5384
4267401
             0x411D89
4579129
             0x45DF39
                             Certificate in DER format (x509 v3), header length: 4, sequence length: 1432
6336576
             0x60B040
                             CRC32 polynomial table, little endian
                             Intel x86 or x64 microcode, sig 0x03000000, pf mask 0x01, 20C0-18-20, rev 0x6aa56c00, size 192
6390035
             0x618113
6871376
              0x68D950
                             xz compressed data
6917700
             0x698E44
                             Unix path: /lib/firmware/updates/4.9.54
6995948
             0x6ABFEC
                             Unix path: /sys/firmware/devicetree/base
6996836
                             Unix path: /sys/firmware/fdt': CRC check failed
              0x6AC364
              0x6AE299
                             Neighborly text, "neighbor table overflow!is %x"
7004825
                             Neighborly text, "neighbor %.2x%.2x.%pM lost rename link %s to %s"
7034318
              0x6B55CE
                             ELF, 32-bit LSB shared object, ARM, version 1 (SYSV)
7041024
              0x6B7000
                             LZMA compressed data, properties: 0xC0, dictionary size: 0 bytes, uncompressed size: 64 bytes
8573455
              0x82D20F
Scan Time:
               2022-07-29 02:02:13
Target File:
              /home/ubuntu/_ddwrt-linksys-wrt1200ac-webflash.bin.extracted/_5CCO.extracted/82D20F
MD5 Checksum:
              3b5d3c7d207e37dceeedd301e35e2e58
Signatures:
              391
              HEXADECIMAL DESCRIPTION
```



#### 上傳韌體檔案

Scan Time: 2022-07-29 11:32:02

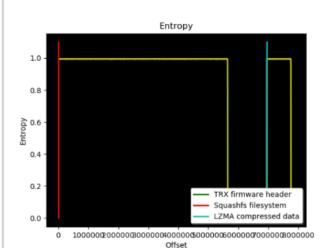
Target File: /home/ubuntu/\_TOTOLINK\_C8181R-1C\_A3100R\_IP04348\_8197F\_SPI\_8M64M\_V5.9c.457

0.extracted/4E864

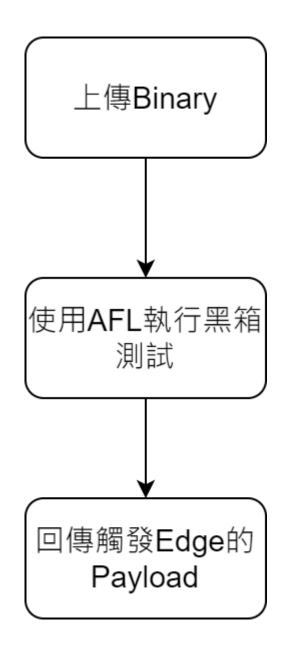
MD5 Checksum: bea00879794abf8c4266afb4f89e061

Signatures: 391

SECULAL LIEVABEOUAL BECODIETION



## Fuzzing線上執行



```
// 1.c
                                                     int main() {
int foo(char *buf) {
                                                         char buf[20]
    if (buf[2] == 'A') {
        if (buf[3] != 'G')
                                                          scanf("%20s", buf);
            return 0;
        else {
                                                         if (buf[0] == 'F') {
                                                             if (buf[1] == 'L')
            strtok("B0000M", "0"); // Crash
            return 1;
                                                                 return foo(buf);
                                                              else
                                                                 return 0;
                                                         } else
                                                              return 0;
```

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

```
american fuzzy lop ++4.01c {} (./a.out)
run time: 0 days, 0 hrs, 0 min, 8 sec
                                               cycles done: 5
   last new find : n/a (non-instrumented mode)
                                            x corpus count: 1
last saved crash: none seen yet
 last saved hang: none seen yet
                                               saved hangs: 0
 now processing: 0*15 (0.0%)
                                    map density : 0.00% / 0.00%
                                  count coverage : 0.00 bits/tuple
  runs timed out : 0 (0.00\%)
 stage progress qqqqqqqqqqqqqqqqqqqqqqq
  now trying: havoc
                                   favored items : 0 (0.00%)
 stage execs: 70/1024 (6.84%)
                                  new edges on : 0 (0.00\%)
 total execs: 14.7k
                                  total crashes : 0 (0 saved)
  exec speed: 1755/sec
                                   total tmouts: 0 (0 saved)
 fuzzing strategy yields qqqqqqqqqqqqqq
                                                           qqqqqqu
  bit flips: disabled (default, enable with -D)
                                                levels : 1
  byte flips: disabled (default, enable with -D)
                                           x pending: 0
 arithmetics: disabled (default, enable with -D)
                                              pend fav : 0
  known ints: disabled (default, enable with -D)
                                           x own finds: 0
  dictionary: n/a
                                              imported: n/a
havoc/splice : 0/14.6k, 0/0
                                           x stability: n/a
py/custom/rq: unused, unused, unused, unused
                                            tqqqqqqqqqqqqqqqqqqqqq
    trim/eff: n/a, disabled
                                                     [cpu000: 50%]
```

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

```
american fuzzy lop ++4.01c {default} (./a.out) [fast]
       run time: 0 days, 0 hrs, 1 min, 9 sec x cycles done: 44
   last new find: 0 days, 0 hrs, 1 min, 7 sec x corpus count: 4
 last saved crash: 0 days, 0 hrs, 0 min, 32 sec x saved crashes: 1
 last saved hang: none seen yet
                                        x saved hangs: 0
 now processing: 1.181 (25.0%) x map density: 0.04% / 0.05%
  runs timed out : 0 (0.00%) x count coverage : 1.00 bits/tuple
qqqqqqqu
                    mew edges on: 4 (100.00%)
total crashes: 2 (1 saved)
 stage execs: 40/440 (9.09%)
 total execs: 142k
  exec speed: 1956/sec
                                total tmouts : 2 (0 saved)
 qqqqqqqu
   bit flips : disabled (default, enable with -D)
  byte flips: disabled (default, enable with -D)
                                     x pending: 0
 arithmetics: disabled (default, enable with -D)
                                           pend fav : 0
  known ints: disabled (default, enable with -D)
                                       x own finds: 3
  dictionary: n/a
                                       x imported: 0
 havoc/splice : 4/142k, 0/0
                                       x stability: 100.00%
 py/custom/rq: unused, unused, unused, unused
                                        tagagagagagagagagagag
    trim/eff: 42.86%/3, disabled
                                                [cpu000: 50%]
```

```
gordon@DESKTOP-OA66QVB: ~/Fuzzing/test/output/default/crashes$ xxd id\:000000\,sig\:11\,src\ \cdot \:0000003\,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