[hw0x00] writeup

莊翔旭, woolniesun, b04902083

Buffer Overflow

objdump 觀察後發現有 `hidden`(0x400566) 和 `gets` 的使用，buffer 長度為 16，把 payload 構造出來送過去就拿到 shell 了。

Pusheeeeen

因為在 debugger network 有開啟 preserve log，所以有發現 302 redirects，curl location 的 kaibro_big_gg.php 就可以拿到 FLAG 了。

MdRsRcXt

把 `MdRsRcXt.py` 的 A 反過來重構回去，就會出現 FLAG 了 (其中 pow(m, 65537, b) 的部分是看網路上的文章解出來的)。

babystego

使用 Stegsolve.jar 在 blue plane0 中發現 CS.2018.Fall 的提示，存成二進制檔案用 file 去看觀察，發現他是一個 MPEG 檔，再使用 exiftool 去看是哪一種 MPEG 檔，確認是 mp3 檔案後播放來聽聽 (然後就卡關了，最後是別人提示下知道要先反轉 mp3 檔案...) 。把 mp3 反轉後會聽到一串字符，轉成 ascii 就是 FLAG 了...

notbabyjava

直接用線上的 decomplier 去反組譯 jar 裡面的 main.java 檔，觀察反組譯後的程式碼，把陣列裡面的數字反過來按照程式碼重構回去，就會出現 FLAG 了。