M10915027 石成峰 HW8

[Guess]

1. 使用IDA將程式打開後，根據magic number以及會輸出固定長度的字串推斷出是在進行MD5加密。
2. 將hash檔案裡的字串切成4段長度32字元的hash值丟去網路上的MD5暴力解密。
3. 將解密後的結果組成flag。

[Uroboros]

1. 將程式反編譯後得到是將輸入對某個資料結構進行操作後，比對是否符合某個預設的答案。
2. 根據結構的特性判斷為link list，並將其視為等效長度314的陣列A。
3. 得出輸入對陣列A的操作為，A[輸入的字元ascii\*7%314] << 6 + 輸入的字元位置。
4. 將預設的答案撈出來進行反向操作後得到flag。

[SecureContainProtect]

1. 先使用程式解出數獨完輸入後發現需要有Action code。
2. 發現最後判斷的部分為將某段資料^數獨解答^輸入後加總要等於257498則輸入是正確的，並會顯示出ascii art的解答。
3. 首先某段資料^數獨解答這部分可以預先計算好，因此只要將算好的答案和輸入進行xor sum後得到257498就是正確輸入了。
4. 由於進行完xor後會是ascii art，因此合理推斷應該會有許多空白字元(32)的部分才會容易看懂。
5. 將某段資料^數獨解答不進行互斥或直接顯示出來可以發現有一個出現頻率異常高的magic string: DECRYPT THE DOCUMENT OF scp，中間空白部分字元值為127，並且2個magic string開頭的最短間隔為32。
6. 由於最後的輸入長度最多為39，因此合理推斷正確輸入的長度應該是32並且根據可能出現大量空白推斷出前綴為magic string和整串空白的xor為decrypt\_the\_document\_of\_SCP。
7. 在透過最後一個字元必須要能構造出換行來排版，得出最後一個字元必為1。
8. 剩下位置27~30的可以根據輸入及xor完都是ascii(32~127)以及xor sum為257498的條件暴力求出唯一解。
9. 將唯一解: decrypt\_the\_document\_of\_SCP-2521輸入後得到ascii art的flag。