

計算機安全 HW8 Writeup

- Real name: 張瀚文
- Nickname on course website: Hwww
- Student ID: b07505027.

wishMachine

解法

雖然這題沒有debug資訊，但慢慢找可以找到幾個主要的函數，其中主要的檢查函數，慢慢讀的話可以發現，程式會將輸入進去的serial (長度為70)，檢查 $f(\text{serial}[\text{num2} + j]) == (\text{num3或num4})$ ， f 是函數，可能有五種：

1. 費波納契
2. 某種累加
3. 乘135
4. xor 1383424633
5. 0xFAC0B00C累減0x7788或0x78

根據已經存好的表決定f要用什麼函數

通過檢查後，會讓已經存好的flag ^= serial，重複1000個serial後就可解密為正確的flag，

上述的num2, num3, num4, flag, f都是存好的東西，可以從記憶體或stack撈出來

也就是說我們已經可以自行算出serial了，因為 $\text{serial}[\text{num2} + j] = \text{invf}(\text{num3或num4})$ ，所以只要自己寫出五種函數相對應的反函數invf就可以得到flag了～

程式碼可參考 code/wishMachine/ 底下的：

1. wish.py：主程式
2. fib 跟 fib.cpp：費波納契表。原本是用Python寫，但中間發現因為C會overflow，算出來的答案會跟Python不同，只好用C先建表
3. facebook 跟 facebook.cpp：因為一直出問題，怕跟fib一樣所以用C寫一下表
4. bur, flag：存num2, num3, num4, f, flag等資料

Curse

解法

根據提示 (或自己慢慢猜)，先找到原本在data中，被寫入的code是在哪裡被執行的，發現是在 `.text:00401A8E call eax` 這行，

而跟進去eax後 (假設叫他 `bad()` 函數)，因為ida不會解析得很漂亮，甚至要等ida跑完hex才會被解析成指令，或是要自己手動將他轉為指令，因此只能慢慢尋找程式的關鍵點，而且麻煩的是每次寫入的code的記憶體Base不一樣，如果忘記紀錄Base就可能要重來...但只要乖乖花時間跟著跑就會找到bad中最關鍵的地方，bad會在位移為13DE的地方呼叫位移1573的函數 (假設叫 `real_main()`)，如 `006413DE call near ptr unk_641573`

找到 `real_main()` 後就輕鬆多了，研究一下後知道，`real_main()` 裡面包含了輸入、將輸入做某種轉換、一段疑似跟flag有關的奇怪的字串 `"^cm1;Fo]Zb..."`、最後輸出一段裝飾用的文字。這裡把printable ascii丟進去測試一下輸入的轉換是什麼，結果發現這個轉是可以直接用輸入跟輸出建對照表的，然後根據其他題的解法，猜測輸入應該就是flag，flag會被程式轉換成 `"^cm1;Fo]Zb..."`，所以建好表後把他反轉換就會得到flag拉～

程式碼可參考：

1. `code/Curse/solve.py`
2. `code/Curse/note`：一些過程記錄

SecureContainProtect

解法

這題可以先解出數獨，存成一個陣列ans，送出finish後，需要輸入一個action_code，用ida看按下finish後會進的這個函數 (假設叫finish函數) 非常的簡單易懂，可以很明顯的看出finish函數會把兩個存好的陣列s1, s2分別跟ans做xor之後輸出，而這就是我們可以看到的TOP SECRET等字。

接下來就是重點部分，他會把一個存好的encoded_flag跟ans跟我們要輸入的action_code做xor ($flag = encoded_flag \oplus ans \oplus action_code$)，然後檢查是否正確並輸出。其中encoded_flag跟ans是已知，所以我們可以先把它們做一次xor (變成 $flag = encoded_flag \oplus action_code$)，也就是說剩下只要找到action_code這個密鑰就好。

稍微觀察一下encoded_flag，可以發現貌似有個規律，大致是由「大值字元 * 26 + 小值字元 * 6」組成，共32個字 (如下圖，\$是一些換行之類的特殊字元)，猜測action_code的長度應該跟32這個數字有關係，而這個數據也跟ida顯示的 `%39s` (action_code小於40個字) 吻合。


```
*,=6?;$;*%d,:*nt_of_SCP-2521j*mrypt_the_j,:*!z_of_S$5*221decrypt_t'*$+ument_of_SCP-2521decrypt_the_document_of_SCP-252$d
}{j~pt_th%Gd/(mubnt_of_SCP-252?)}{|ypt_the$|Sdum%$1$of_S$H55521decrypt_t({}G|ument_of_SCP-2521decrypt_the_document_of_SCP-252$d
}{jypt_the_d{ument_of_SCP-25<)}f{|jwpt_th}G|ument_of_S[H52521j*,=6?z_th}G|om:"knt_of_SCP-2521d*,=wpz$;fe_j,{men;$)_SCpb}z2$d
}{j62;$|he_d{ument_of_SCP-2;*6d%{j~t_th}G|ument_of_0[H-252u]}dr9h1$th}G|$a$u},t_of_SCP-2521d%{ja$&lp' /f$ {m/ent$w~QSC^5552$d
}{jypt_vhe_d{ument_of_SCP-<*~*{jahz_th}G|ocume!;$)_S[H5252]}|cryhlGth}G|ocuu}vt_of_SCP-2521de{japt_lp}_do{ument_/_~G|MH*252$d
}{jypt_the_d{ument_of_SCP#*221dec2ahlQth%G|acume`lGhf_S:H5<52)}|cryhlGth}G|ocuu}vt_of_SCP-2521de{japt_lp}_do{ument_o&GK[W-252$+
}{j6pt_the_d {mu*!;$ )$K$5*221dec=ah1G;he$w!:"!v$Xof_SC)5*;2q$;!-=h$Xt'})G| c:u}v;_ )$$$$b}z}~d*{ja?t$lp}$d {mu*nt_of_QKDP-252$d
ecrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-2521decrypt_the_documentz$ah/TCP-252$d
ecrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-2521decrypt_the_document4&w$XSCP-252$d
ecrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-252$d
ecrypt_the_document_of_SM$b}z<1decrypt_z'}_document_of_S$b}521decrypt_the_document_of_SCP#}z}~jencrypt_the_document_of_SCP-252$d
ecrypt_the_document_of_{$[ *rL*sdecrypt]lp}_document_of_S$H5*521decrypt_the_document_of_SC$5B2rH|'crypt_the_document_of_SCP-252$d
ecrypt_the_da,:*!;$ fGK[P-25*]|ec|6?;$lp}_document_of_SCH5*5<~&kcrypz$;*$jocuc*!;$ h_S[H52521]}{rypt_the_document_of_SCP-252$d
ecrypt_the_|w{rm%v1$ofGK[P-25*]|e'j~wt$lp}_document_of_SCH5*E0H|!ry4lGsh%G|-c1u}it$w~$S[H52521]}{rypt_the_document_of_SCP-252$d
ecrypt_the_|w{umev1GofGK[P-25*]|e{japt_lp}_document_of_SCH5*521|}{ryhlGtheg|wcmu}nt_w~GS[H52521]}{rypt_the_document_of_SCP-252$d
ecrypt_the_$w{7"!v$Xof$K[$-2q*)ce{japt_lp}_document_of_SCH5*521|}{ryhlGtheg|wcmu}nt_w~GS$H5p52u}|drypt_the_document_of_SCP-252$+
*,=6?;$;*%w,:*!;$Qof_$:Hov-B6de#$a2;$lp$|d,:*!;$ )$S$H5*2~|}{=y0$G6'!G$hc5$},;$w$XSC$T*~w}$brcrypt_the_document_of_SCP-252$d
ecrypt_the_mumen$;of_SCP-2521decrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-252$d
ecrypt_the_f$ {mu}v$Xof_SCP-2521decrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-252$d
ecrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-252$d
ecrypt_the_document_of_SCP-2521decrypt_the_da,mnen;G f_SCP-25<~|encrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-252$d
ecrypt_the_document_of_SCP-2521decrypt_the_fw{mmen4|hf_SCP-27*}|encrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-252$d
k,=6?;Qth*$+ c:"*!t_of$$$P-2521decrypt_z'*$+w{mme!;$ f_SM$b}z*)|encrypt_the_doc:"*!t_of$$$P-<z}~*mrypt_the_document_of_SCP-252$
}{uy0lG6he$|wmu-}vz_ohGTCp-2521decrypt$lpb_$w{mme.lGwf_$[H*2u*)|encrypt_the_docu-}vz_ohGTCpi*-51$}{0ypt_the_document_of_SCP-252$|
}{ryp1G1he_$w{{c$vlQa~XSCP-2521decryptG1pe_dw{mmen1Gwf_K[H-25*]|encrypt_the_docum%v1Qa~XSCP5*-21d}{jypt_the_document_of_SCP-252$|
}{ryp1G1he_d/{mub.lGwa_SCP-2521decryptG1pe_dw{mmen1Gwf_K[H-25*]|encrypt_the_docume.lGwa_SCP5*-21d}{jypt_the_document_of_SCP-252$d
$ {0641/she_d{mjen4Ghf_SCPb}z}~*~,=6?t$ $p'$ w{$oe!lGw)_$_{H0}q*)$gc=6?;$;*$+ cumenzGhf_SCPmK-p~ }$uypt_the_document_of_SCP-252$d
ecrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-2521decrypt_the_doc{'k'$Xof_SCP-2521decrypt_the_document_of_SCP-252$d
ecrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-2521decrypt_the_doc5$}$s_of_SCP-2521decrypt_the_document_of_SCP-252$d
ecrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-252$d
ecrypt_the_document_of_SCP-25<~|encrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP#2521decrypt_the_document_of_SCP-252$d
ecrypt_the_document_of_SCP-27*}|encrypt_the_document_of_SCP-2521decrypt_the_document_of_SM$52521decrypt_the_document_of_SCP-252$+
*,=yp;$;'e_document_of_SM$b}z*)|ecrw?;$;'k_dom:"*!;$Qof$$$$-v-p1+*,=ypt; '*+ m:"*!;$QofQ$[H5]z21decrypt_the_document_of_SCP-252$d
}{jyp4G1pe_document_of_{$[H*2u*)|ec6ahs_4p}$d+{mje.v&wf$K[H/0-B1d%{jwptQloe_dw{mje.lG-f_S[H52521decrypt_the_document_of_SCP-252$d
}{jyptG1pe_document_of_K[H-25*]|ecjah;$;p}Gdw{mmen4Ghf_S[H52521decrypt_the_document_of_SCP-252$d
}{jyptG1pe_document_of_K[H-25*]|ecjaht_thk$dw{mmenz$wf_K[H-2521dec2ahlXth_dw{mmen1Gwf_S[H52;21decrypt_the_document_of_SCP-252$d
%$ja$&v)}$b_+,:*!;$ )_$_{H0}q*)$gc2$H6$0p$Xd/$m/**1/hf$K[H02521dec2whs_the_dw{m/**1/hf_SAH5*721decrypt_the_document_of_SCP-252$d
ecrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-252$d
ecrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-2521$${~pt_the_+w{m"ent_of_SCP-2521decrypt_the_document_of_SCP-252$d
ecrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-2521decrypt_the_document_of_SCP-252$d
ecrypt_the_docuent$ )$SCP-2521d*{~ypt_the_docuc*!;$ )QSCP#}z}~*mrypz$;*$+acu-}v6_of_SCP-2521decrypt_the_document_of_SCP-252$d
ecrypt_the_dom:uent$w~GSCP-2521d%auypt_the_doc1$bnt_/$G$C$[5521$$(0y4$Xth$w$w!um%v1$of_SCP-2521decrypt_the_document_of_SCP-252$d
ecrypt_the_j {mu*!t_w~GSM$b<521+*,=yptQ;*$j cmu*nt_a"G#CH5)521j!{|$yhl$theQ w$umev1Gof_SCP-2521decrypt_the_document_of_SCP-252$d
ecrypt_the_d{ument_w~G#A)5*w21$}{jyp0G1`e_fwC5obnz$w$XSC$/55<u}|dry0vXtfg!$hcumen1Gqf_SCP-2521decrypt_the_document_of_SCP-252$d
ecrypt_the_d{ument_w~GSCP5*-21d}{jyp4|$p}$jocume.lGhf_SCP-2u*)cecrypt_4p}Xdocumev1Gof_SCP-2521decrypt_the_document_of_SCP-252$d
ecrypt_the_d{mue`t_w~GSCP5*-21d}{jyp;Qth1G|-cume';Qof_SCP-2;}}decrypt_z'k_documkv1/of_SCP-2521decrypt_the_document_of_SCP-252$+
*,=6?;$;*%doamu}lt$w~G$C$5*-}1+}{j6pl}vp}G$hcume1/of_SCP-2L*Adencrypt_$p$_docuc}v$ _of_SCP-2521decrypt_the_document_of_SCP-252
```

發現其中有很多很明顯的可讀字串，action_code: decrypt_the_document_of_SCP-2521 ，就可以解回flag了～

程式碼可參考 [code/SecureContainProtect/simply_find.py](#)

另解

因為程式最後會檢查 `sum(flag)` 有沒有等於257498，平均每個字元約43，而如果先把 `encoded_flag` 加總的話，會發現目前的sum非常大，所以先試著找到一個長度為w的 `action_code`，讓對應的flag可以最小，再由這個 `action_code` 往上暴搜，其中 `action_code` 跟flag要是printable ascii。結果發現在w = 32的時候，`action_code`的每一項讓相對應的flag值最小的解就恰巧是答案了><也不需要往上暴搜～

程式碼可參考 [code/SecureContainProtect/find_action_code.py](#)