M10915027 石成峰 HW0

[Web]

1. 使用後綴為true或false的字串可以繞過!cute.match("(true|false)$")的檢查。
2. 可以將cute參數以字串形式直接加入userInfo的字串中並填入api的字串中。
3. 後面的參數可以覆蓋掉前面的值。
4. url中%22表示”、%23表示&、%26表示#。
5. 總和以上資訊，可以得出一個將admin覆蓋為true並且新增givemeflag=yes，再用#將後面的givemeflag無效化並且後綴為true的網址，前往後可以得到flag。

[Pwn]

1. 使用gdb測試後得出buffer長度為24，之後便可覆蓋到return address。
2. Disas後可以看出在func1中0x4011a1的位置可以get shell
3. 使用pwntool連線後送出24個字元+ p64(0x4011a1)即可get shell
4. 使用linux指令在/home/Cafeoverflow/中找到flag的檔案打開後取得flag。

[Misc]

1. 查看原始碼後可得知需透過浮點計算誤差得到小於-3000的數值才能得到超過3000的balance。
2. 使用C在範圍i:0~ 100000000、j:0~127中計算i \* BASE - j \* BASE - (i - j) \* BASE、BASE = 88.88，可以得到i = 96646659、j = 87時有最小值-2048。
3. 連線後輸入2組的96646659、-87、- 96646572讓balance增加到4096後可以得到flag。

[Cryptography]

1. 查看原始碼後可以得知加密法為TEA，可以在維基上獲得透過密文及金鑰和delta解密的程式。
2. 已知密文和delta只差金鑰，Python的rand在set相同的seed後取出的亂數序列都一樣，因此找出金鑰等同於找出當時的rand seed。
3. 從output.txt的檔案修改時間推斷，rand seed的時間只會更早，因此從修改時間遞減後進行解密。
4. 第一個解密後出現前綴為flag的明文即是flag。

[Reversing Engineering]

1. 先將Exe檔用ILSpy打開後可以看到原始碼即圖片。
2. 找到輸出flag的原始碼函數，發現需要每張圖片(66,99)像素的R值。
3. 將每張圖片的R值取出後填入函數中，再使用C#編譯執行，即可得到輸出為flag。