M10915027 石成峰 HW7

[Going Crazy]

1. 先使用Go寫一個hello world，再使用GDB看main的大約位置。
2. 使用GDB將gogo中大概是main附近的asm全部打開來看後，找出像是main的區段。
3. 找出main後trace asm發現除了golang的函數以外，還有其餘3個函數。
4. 在main中發現輸入長度必須>4並且頭尾需要有x，還有發現像是會將輸入split的函數，查看register後確定是會用,將字串切割的函數。
5. 在第二個check\_input中發現一個會執行36次的回圈，並且每次都需要將bezu得結果與某個資料進行比對是否相等，以及撈出填入切割後陣列的索引值範圍為0~35，判斷出切割後的陣列長度需要36。
6. 繼續trace register後發現會將切割後的每個字串轉成數值後送入

bezu中並且會在rchvf中進行遞迴，將回傳值根據某區段資料比對是否符合。

1. 透過trace asm直接用C++重建出bezu和rchvf，並多次比對輸入及輸出無誤。
2. 將要比對的某區段資料撈出來後，用C++從0往上暴力搜尋相等的輸入值。
3. 找到36個最小的符合值後轉回字串重建出可以通過check\_input的輸入payload為x70,76,65,71,123,103,111,103,111,95,112,48,119,101,114,114,52,110,103,51,114,33,121,111,117,95,100,105,100,95,73,84,33,33,33,125x。
4. 發現所有數值都小於256，並且依照main的做法將頭尾x去掉並依照,切割成ascii陣列後，得到字串FLAG{gogo\_p0werr4ng3r!you\_did\_IT!!!}，送出後確認為flag。