CS: hw4 - profile_manager

學號：b04902053 姓名：鄭淵仁

flag: `FLAG{I_HAVE_N0_1DEA}`

script

- 可以取得 shell 的 python3 檔案： `profile_manager.py`

  (requirements: `pwntools`)

write-up

程式的漏洞

`profile_manager` 有兩個漏洞：

- `add_profile` 在 `calloc` `desc` 的時候，如果大小不是 8 的倍數，他會自動「 7 捨 8 入 」到 16 的倍數。所以如果選擇 `0x92` 的大小的 `desc` 時， `calloc` 只會開一個 `0x90` 大小的 chunk，卻會 `read` `0x91` 個 byte，這樣就有少量的 heap overflow 的問題可以利用。
- `edit_profile` 在 `realloc` `name` 的時候，如果 `realloc` 的大小是 0 的話，會變成 `free` 掉 `name` ，然後直接 `return` 。也就是說，這樣一來只會 `free` 掉 `name` ，而且 pointer 沒有設成 `NULL` ，還有 use after free 的問題。

主要思路

可以利用第 2 個漏洞來達到在任意位置 `malloc` 的效果，這樣一來就可以 `malloc` 在想要改的 chunk header 的位置，然後隨自己開心的改寫 chunk header，然後就可以用上課教的 unlink 的技巧去改掉 `profile` array 裡面的值，就可以 leak GOT 和改寫 GOT了。

但是為了要能 `malloc` 在想要改的 chunk header 的地方，要先知道 heap 的 address，所以我先 leak 出 heap 的 address，接下來就可以依照剛剛說的方法去取得 shell。

leak 出 heap 的 address

所以首先製造 2 個 `profile` ，再利用第 2 個漏洞 `free` 掉這 2 個 `profile` 的 `name` ，這時候 `profile[1].name` 的值就會是 `profile[0].name` 的 address 。

接下來再 edit `profile[1].name` 的最後 1 個 byte ，讓 `profile[1].name` 的最後 1 個 byte 不是 `NULL` ，這樣就可以用 `show_profile(1)` 來取得 `profile[0].name` 的 address ，也就可以推算出 heap 的 address 。

製造 fake chunk

算出 heap 的 address 之後，就可以透過修改 `profile[1].name` 來讓下下一次的 `malloc` 的位置變成是 `profile[2].desc` 的 chunk header 的後 8 個 byte。再利用第 1 個漏洞 (heap overflow) 把 `profile[2].desc` 的 chunk header 的 `prev_size` 的 byte 改成 `0x20` 來騙過下下一次 `malloc` 的 size 的檢查。

這樣一來，下下一次 `malloc` 的時候就會 `malloc` 在 `profile[2].desc` 的 chunk header 的後 8 個 byte ，也就可以把這個 chunk header 的 `prev_inuse` 的 bit 設為 0。

最後再利用一次第 1 個漏洞去把 `profile[2].desc` 的 chunk header 的 `prev_size` 改為 `0x90` ，同時順便在 `profile[1].desc` 裡面寫入假的 chunk 的 header。

這樣一來再 `delete_profile(2)` ，就會把 `profile[1].desc` 的 address 從指向 heap 變成指向 `profile[0].desc` 。就可以用來編輯 `profile[0].desc` 的 address 了。

leak 出 `system` 的 address 並蓋掉 `atoi@GOT`

最後，就可以利用改寫 `profile[1].desc` 來把 `profile[0].desc` 的 address 改成 `atoi@GOT` ，再 `show_profile(0)` 就可以 leak 出 `atoi` 的 address ，並推算出 `system` 的 address。

接著再 `edit_profile(0)` 來把 `atoi@GOT` 的值改成 `system` ，最後再 choice 的時候送出 `';/bin/sh';` 就可以取得 shell 了。