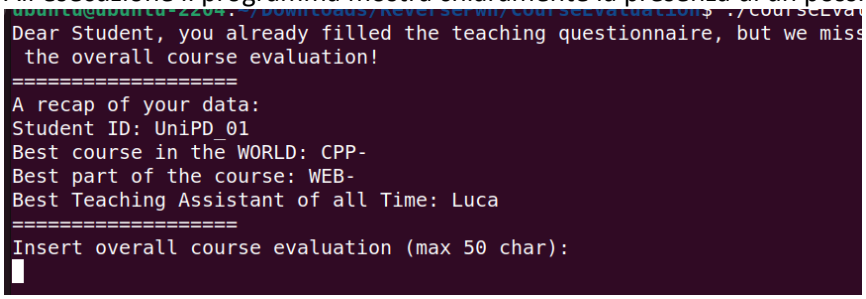
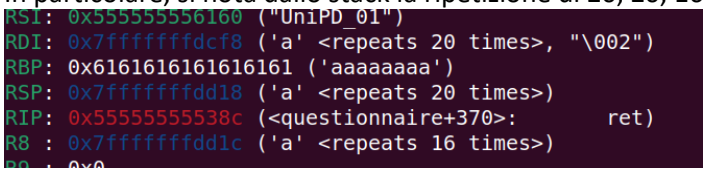
Soluzione

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



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:



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"))
```