Práctica 4: Bomba

contraseña:hplaryos
pincode:2789

- Resolución de la contraseña:

  Iniciar la ejecución con br*main y entonces observas que hay un bucle usando password y metiendo en otra variable(variable del main) el valor final de password y al seguir la estructura del main llegas a la conclusión de que va desde el final de password hasta el inicio y lo mete en otra variable con la que compara lo que has introducido, comparando entonces con la variable puesta del revés.

- Resolución del pin:

  Pones un br*main+273 que es donde te pide introducir el pin y sigues la ejecución con ni, observas que estas dentro de un bucle que va hasta la 4 iteración y lo que hace dentro es sumarle al valor del pin introducido por el usuario($rsp+0x0c),entonces si el pin con el que compara es 2799 y te suma 10, será necesario que el valor que tu introduzcas sea 2789 para que al sumar 10 valga 2799, ves que br *main+336 es despues de ese bucle y ahora si, al imprimir $rsp+0x0c tienes el valor del pin tras sumarle dentro de un bucle el indice desde 0 hasta 4.

- Pasos que he seguido con el archivo de bomba-gdb.gdb:

```
layout asm
layout regs
run < <(echo -e hplaryos\\n2789\\n)
br *main      #observas que hay un bucle usando password y metiendo en otra
#variable
cont
br *main+67 #sale del for y compara strcmp con otra variable que no es password
cont
br *main+138
info regs
p(char*) $rsi #tenemos la contraseña
set $rdi="hplaryos"
br *main+273          #te pide introducir el pin
cont
br  *main+336         #despues del bucle de sumarle a la contraseña
```