

Práctica 4: Desactivación de Bombas

Desactivación Bomba de Álvaro Rodríguez

Pablo Olivares Martínez

```
contraseña = "holamundo"
```

```
pin = 7974
```

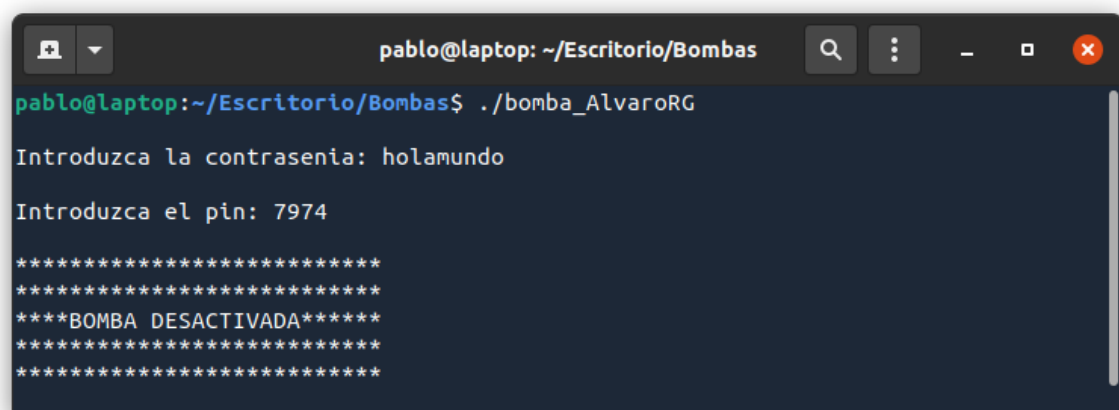
Para comenzar, ejecutaremos ltrace para ver con qué string compara nuestra cadena introducida. Vemos que compara con **holamundo**, así que como no parece tener ninguna modificación, probemos si es ésta la contraseña.

```
pablo@laptop:~/Bombas$ ltrace -i -S ./bomba_AlvaroRG

...

[0x7f155600f1e7] SYS_write(1, "Introduzca la contraseña: ", 27Introduzca la
contraseña: ) = 27
[0x7f155600f142] SYS_read(0holamundo
, "holamundo\n", 1024) = 10
[0x4007b1] <... fgets resumed> "holamundo\n", 100, 0x7f15560e9980) =
0x7fffbac81190
[0x4007cc] strncmp("holamundo\n", "holamundo\n", 11) = 0
```

Efectivamente, el valor es correcto. Ahora veamos cuál es el código. Para ello abramos gdb y analicemos el código. Vemos que hay dos identificadores: **# 0x601060 <codigo>** y **# 0x601068 <contrasenia>**. Comprobando los valores escribiendo **p(int) codigo** y **p(*char) contrasenia**, vemos que son **holamundo** y **7974** respectivamente. La contraseña ya sabemos que es esa. Ahora comprobemos el código. Al probarlo, vemos que efectivamente desactiva la bomba. Igualmente, fijándonos un poco vemos que el programa saca el valor de la pila e inmediatamente lo compara con la entrada almacenada en **\$eax**, la cual no es modificada en ningún momento. Por tanto de esta forma sería desactivada con éxito.



```
pablo@laptop: ~/Escritorio/Bombas
pablo@laptop:~/Escritorio/Bombas$ ./bomba_AlvaroRG
Introduzca la contraseña: holamundo
Introduzca el pin: 7974
*****
*****
***BOMBA DESACTIVADA***
*****
*****
```

