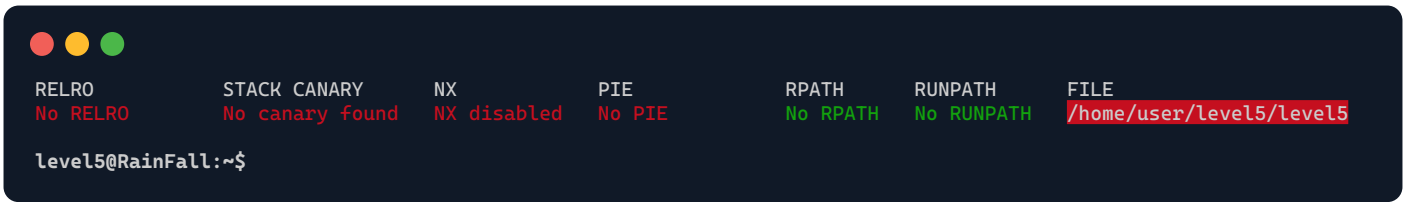
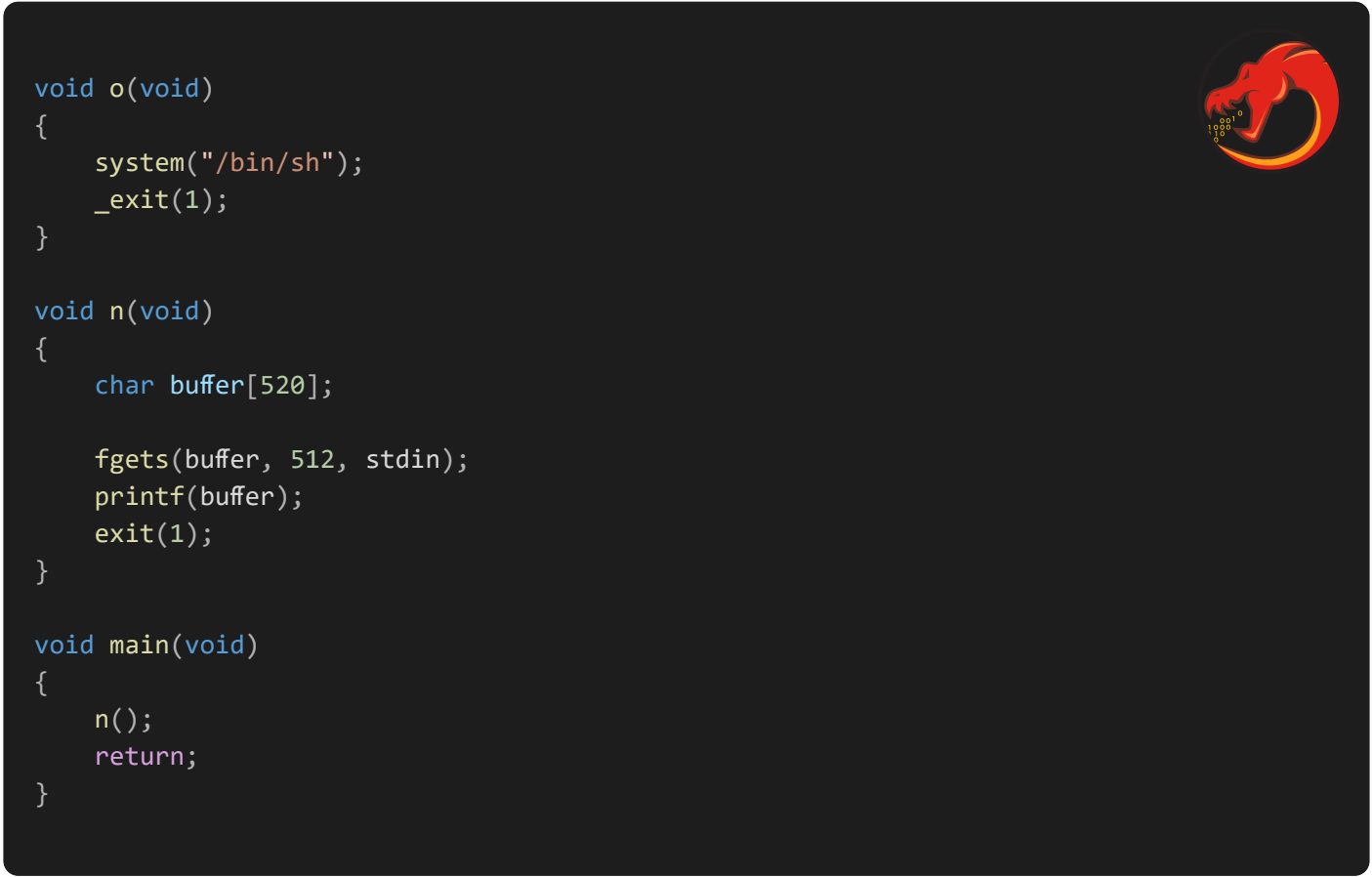


# ./level5



Decompiled file with *Ghidra*:



This level closely resembles the previous two, always featuring a vulnerability with **printf(buffer)**.

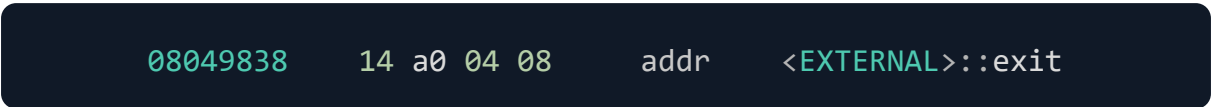
This time, we need to access the function **o(void)**, which provides us with a **shell**. We can't alter the **return** address of the **n** function through an **overflow** since it uses **exit()** instead of a **return**.

So, we must modify the behavior of **exit** to redirect us to the **o** function.

To achieve this, we will target the **Global Offset Table (GOT)**. The **GOT** is a table used in compiled programs to store addresses of dynamic functions that a program may call. By manipulating entries in the **GOT**, we can redirect function calls to our desired location.

In this case, we aim to alter the address associated with **exit()** in the **GOT**, so that it points to the **o** function instead. This way, when the program attempts to **exit**, it will inadvertently call our desired function, granting us access to the shell.

Using Ghidra, we found the GOT entry for **exit** as:



Using the same technique as the last exercise, we'll overwrite the **GOT** entry for **exit** at **0x08049838** with the address of the **o** function, **0x080484a4**.

