# Buffer Overflow with server side execution of payloads

## Hack The Box – You know 0xDiablos

We are given an instance to start with a URL and a port, as well as the binary.

When executing the binary it allows us to input text and the outcome is the text printed back

The idea behind this challenge is to buffer overflow the executable.

Before this however I ran the binary through gdb and looked at the how it worked. I then decompiled the binary in Ghidra. By breaking the program down like this I can see all the functions and function calls the program makes.

What I noticed when breaking the program down was that there is a function called flag. When this is called it does some sort of check and then reads a text file.

I want to find this address in memory and get the EIP to point to this.

Putting the binary through …….. it tells me what protections the stack has. In this case it has none, so I need to just find the offset and point to the flag function.

I need to do this server side now in order to exploit the weakness in the code. I will use netcat to do this. To overflow I need to pass through some parameters alongside the overflow code this will be achieved through a payload.