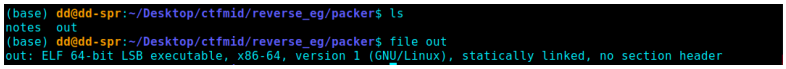
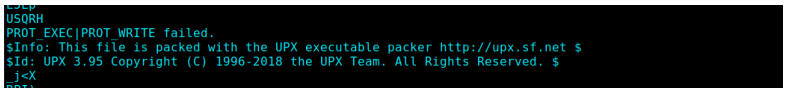
the binary itself. However, upon closer inspection, I noticed the binary lacked section headers, which made it challenging to analyze initially.



Step 3: Checking Strings

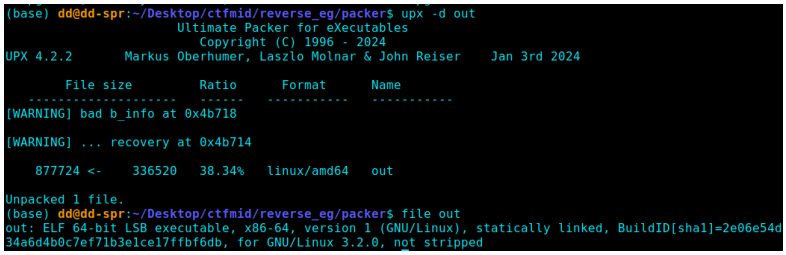
Next, I used the `strings` command on the binary. This revealed that the binary was packed using the **UPX packer**. UPX (Ultimate Packer for Executables) compresses binaries and includes decompression stubs to restore them during execution.

For more details about UPX, you can check their official website.



Step 4: Initial Debugging

I loaded the binary into `gdb`, but due to the UPX compression, I couldn't retrieve any valuable information. At this stage, the packed binary was still obfuscated.



Step 5: Unpacking the Binary

After some research, I discovered that UPX offers a built-in unpacking feature. Using the `upx` package, I unpacked the binary with the following command:

```
upx -d <binary_name>
```

This process successfully restored the binary's section headers, making it much easier to analyze.