1) Many websites expose their ".git" files, please show how it could be dangerous.

Ans: If you leave the. git folder accessible to the public, it gives access to your source code to everyone on the internet who may be able to fetch your intellectual property built into the code, hardcoded credentials if there is any, and discover other logical flaws.

An attacker may retrieve your database credentials. He may also extract your API keys, among other sensitive data from the source code if they are hardcoded. Besides these, the attacker may also use this information to discover even more vulnerabilities which may escalate to more dangerous attacks, which may be unknown to the attacker since the source code wasn't accessible. These may include database takeovers and even Remote Code Execution, etc.

2) Imagine that we have 248 text files. Explain how can we find which files are the same.**

Ans: One of interesting ideas that crossed my mind is to hash the text files with one of hashing algorithms such as SHA-256 and then compare the hashed files with each other (It is by far easier to compare hashed files compared to the files themselves). This approach will work since we know that hashing algorithms will produce different hashes for different inputs (even they are different in tiny details).

3) Write a hello-world C program and explain how we can dump its binary code with radare2.

Ans: To create hello-world C program we have (figure 1) (I also added the version that I wrote in visual studio in the repository with the name of Source.c):

In order to dump program's binary code, we can enter following instruction in Figure 2 (after installing radare2).

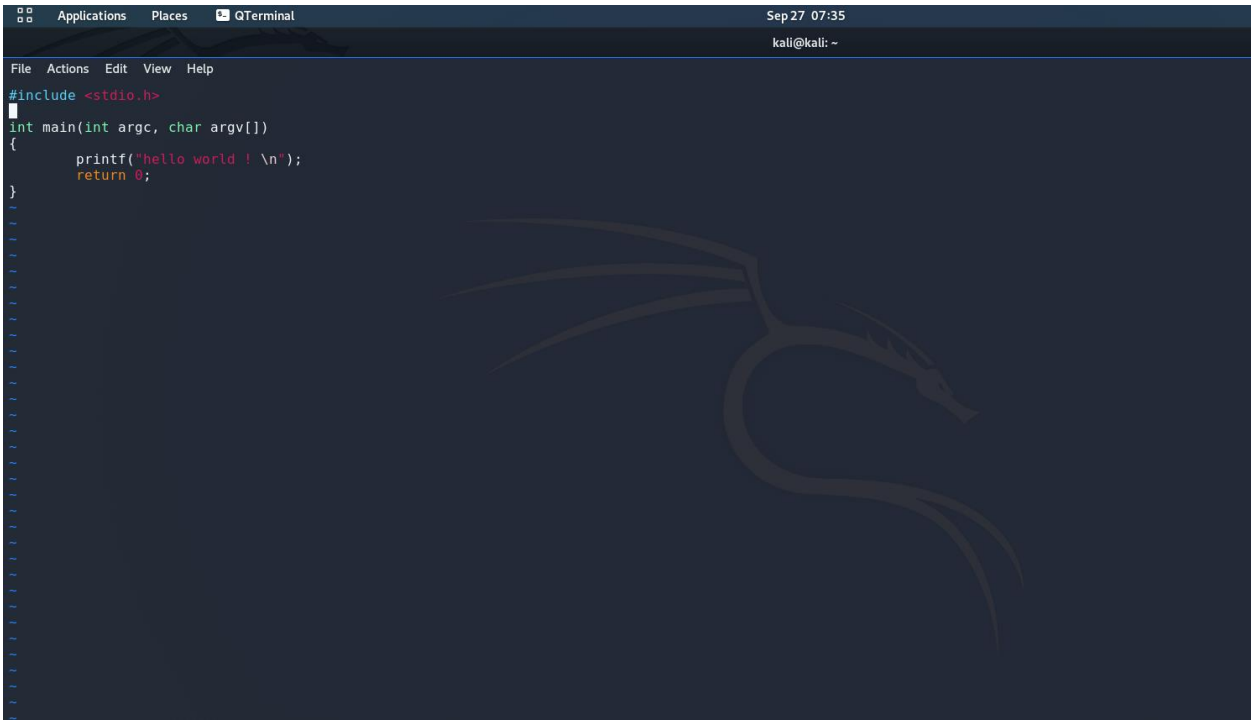

Figure 1.

Figure 2.