vishwaCTF

CHALLENGE NAME: [FIGHT FIGHT FIGHT]

DEV : [Pushkar]

CATEGORY: [Reverse Engineering]

LEVEL: [Hard]

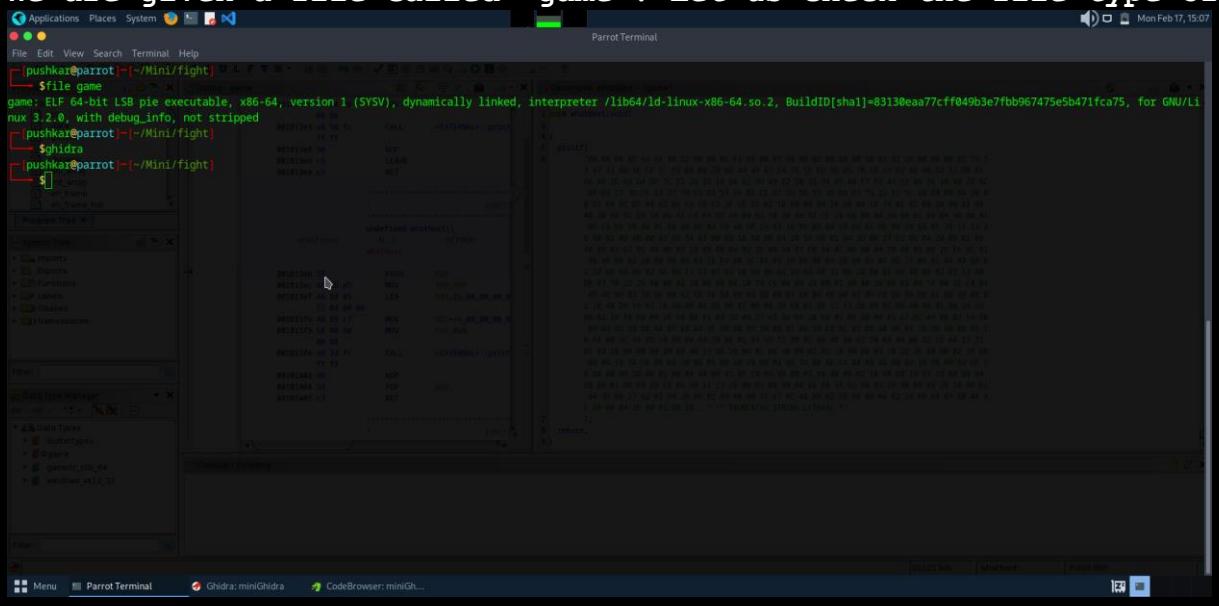
2025

Challenge Description:

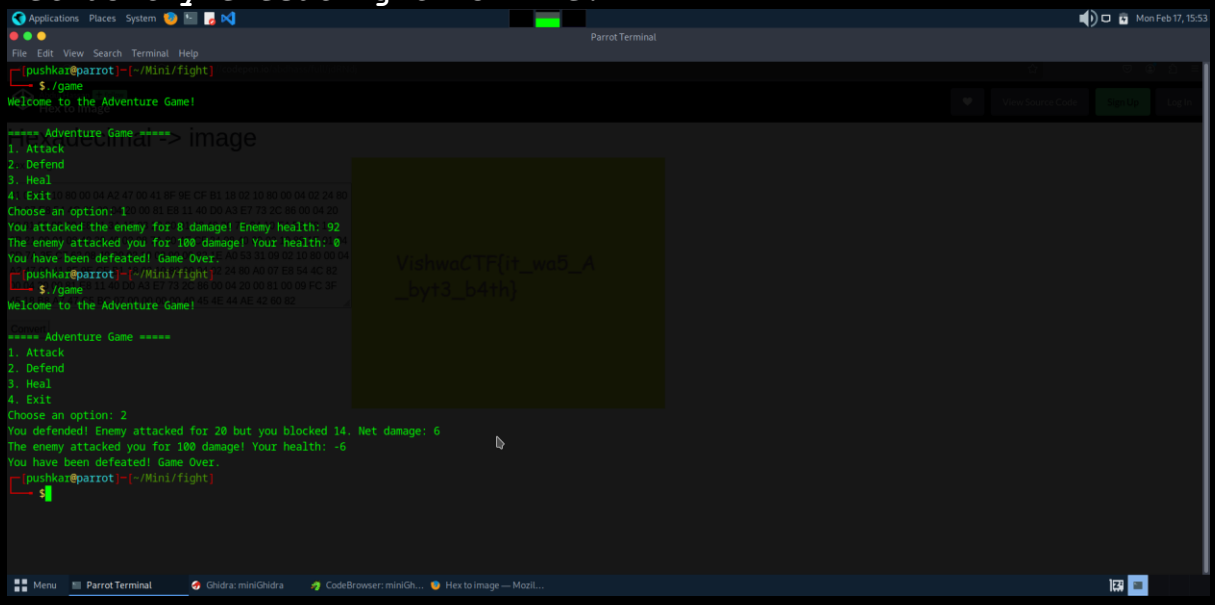
Win this game, by hook or by crook.

Solution:

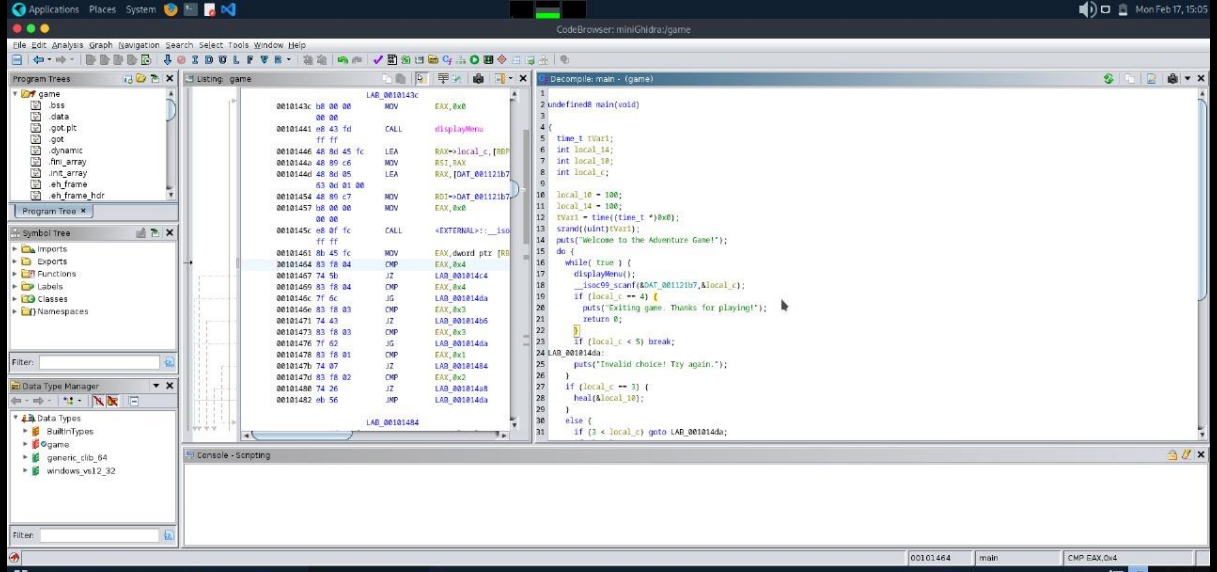
- **We are given a file called "game". Let us check the file type of "game".**

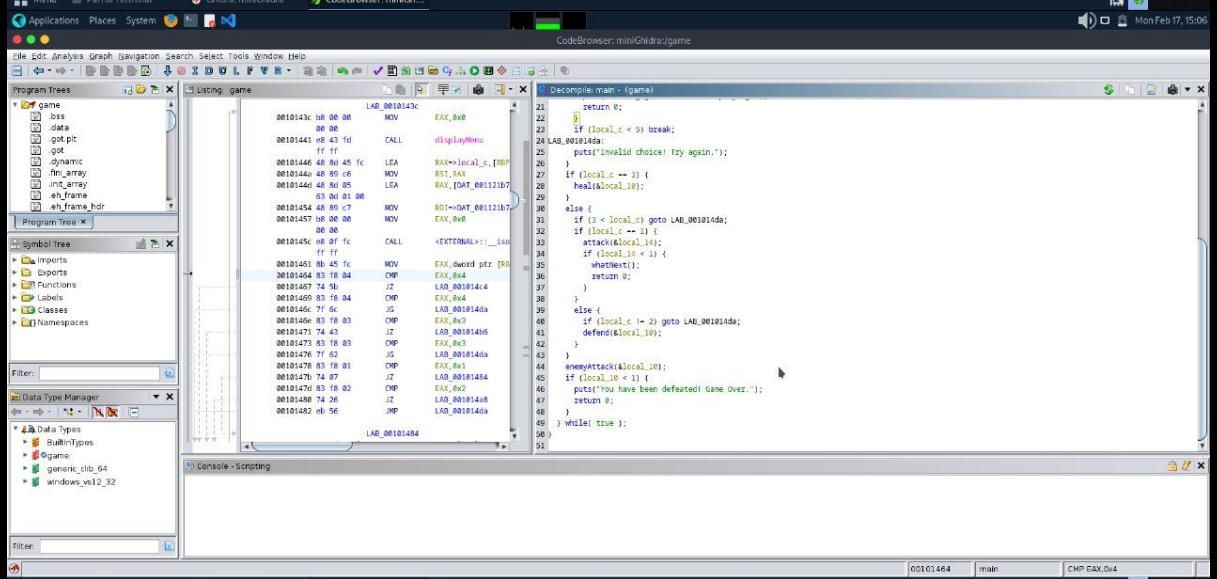


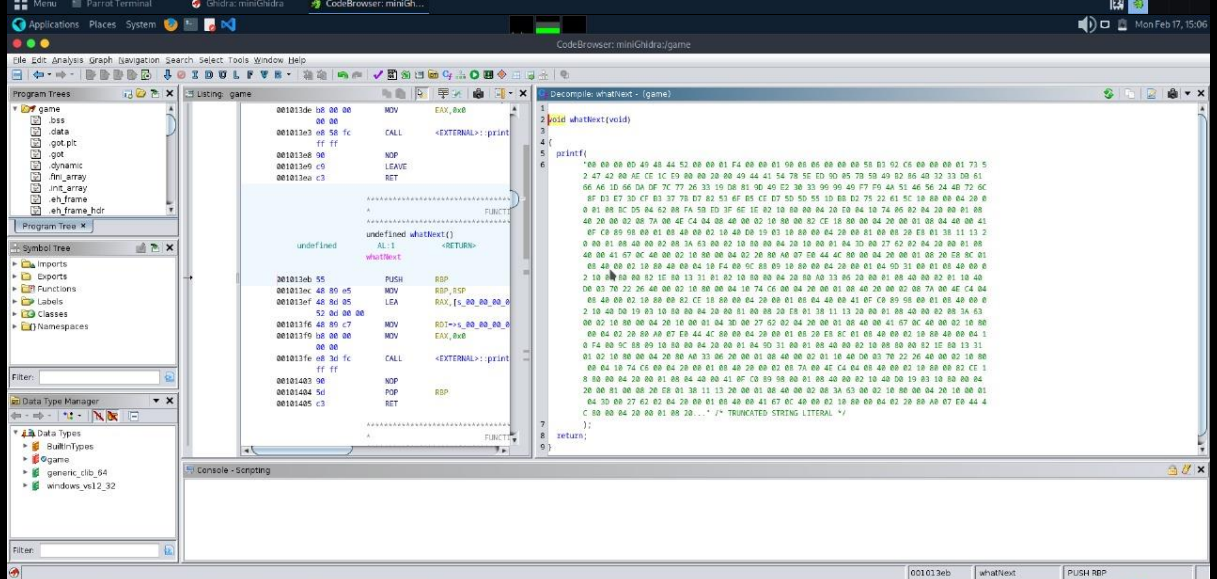
- **This is an ELF file which is fortunately not stripped.**
- **Let us try executing this file.**



- **Turns out, this is a game but we are losing no matter what.**
- **Let us understand how this game is working in order to play it better. Let us open this file in Ghidra.**

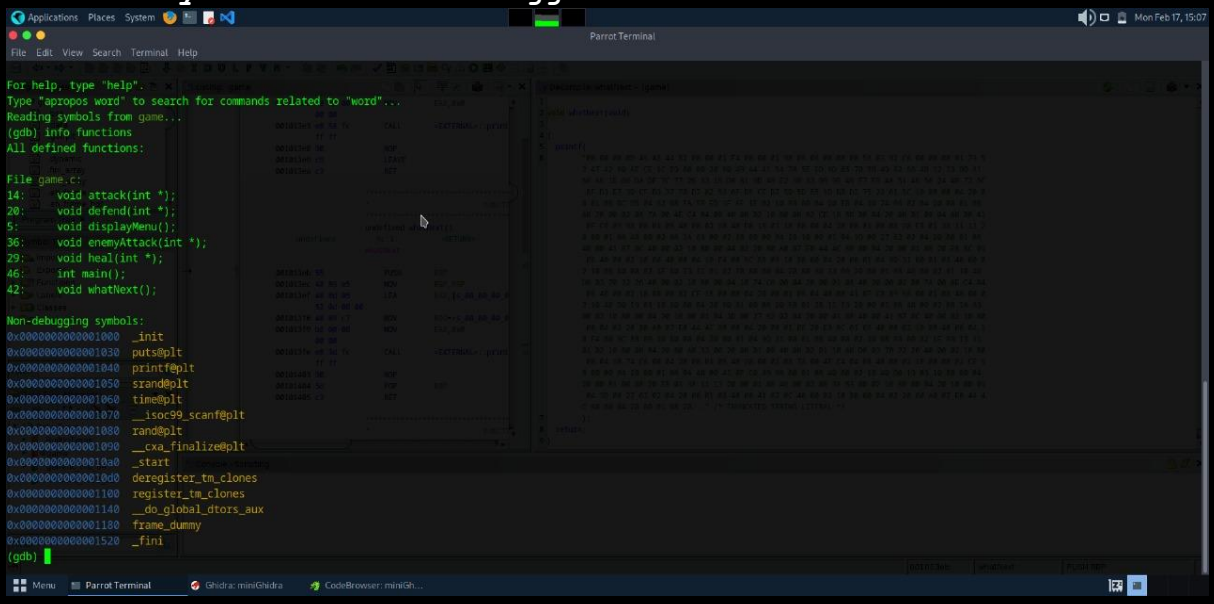




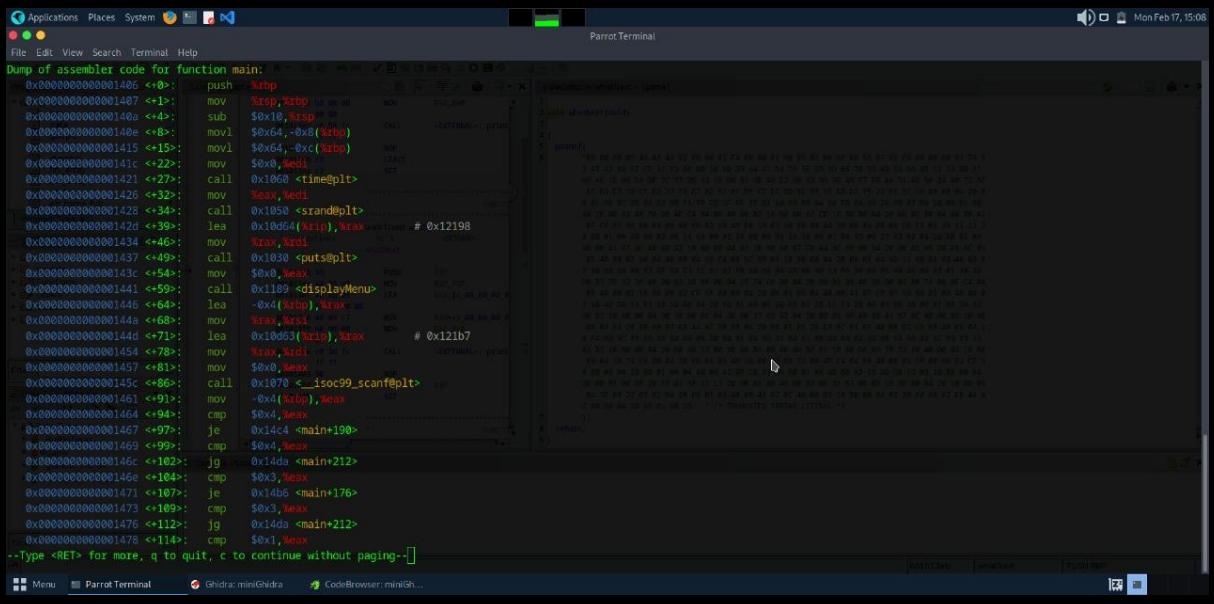


- Here we can see there are two variables which are initialized to 100, local_10 and local_14.
- Maybe it can be the player health and enemy health but we are not sure.
- In the attack function, we can observe that the local_14 variable is passed, we can assume that it is enemy health but we are still not sure.
- In the enemy attack function, we can observe that local_10 variable is passed, again an assumption can be this is the player's health.
- We can confirm this by checking the if statement in attack function where local_14 value is being checked in order to see whether we win or not. Therefore it is safe to assume that local_14 is enemy health and local_10 is player health.

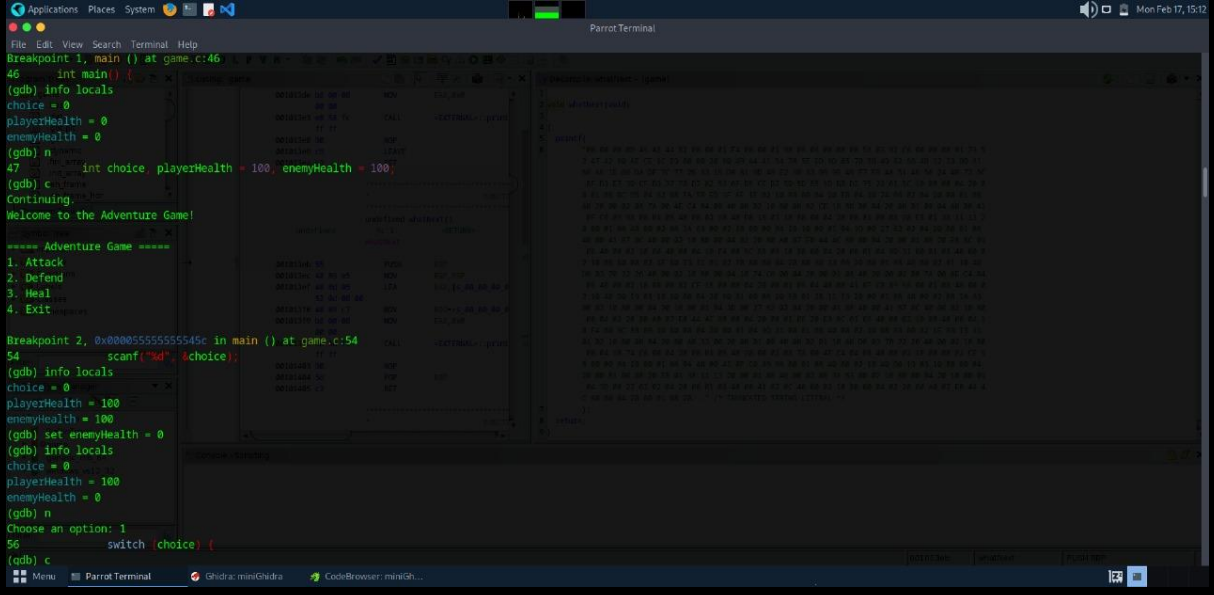
- Also, every time the enemy attack function is called, it makes the player health 0 causing us losing the game no matter what we choose.
- Therefore, we must attack the enemy and make its health 0 before it attacks us.
- In order to this, we must be able to magically pause time and make enemy health 0.
- Let us try it with GDB debugger.



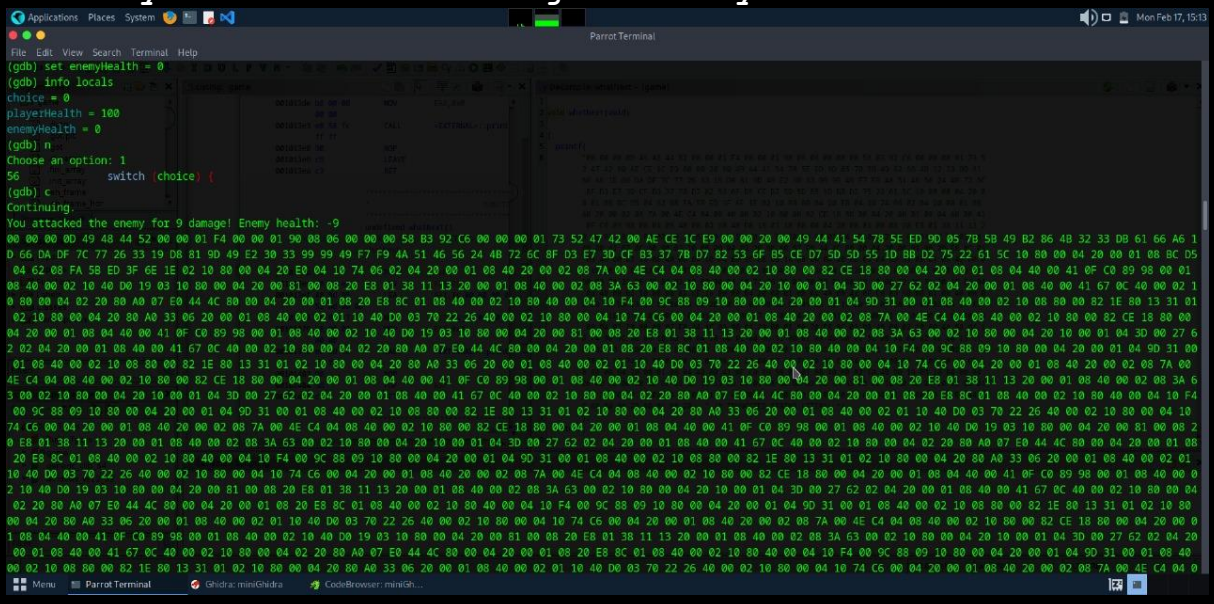
- These are the functions available to us.
- Let us disassemble main.



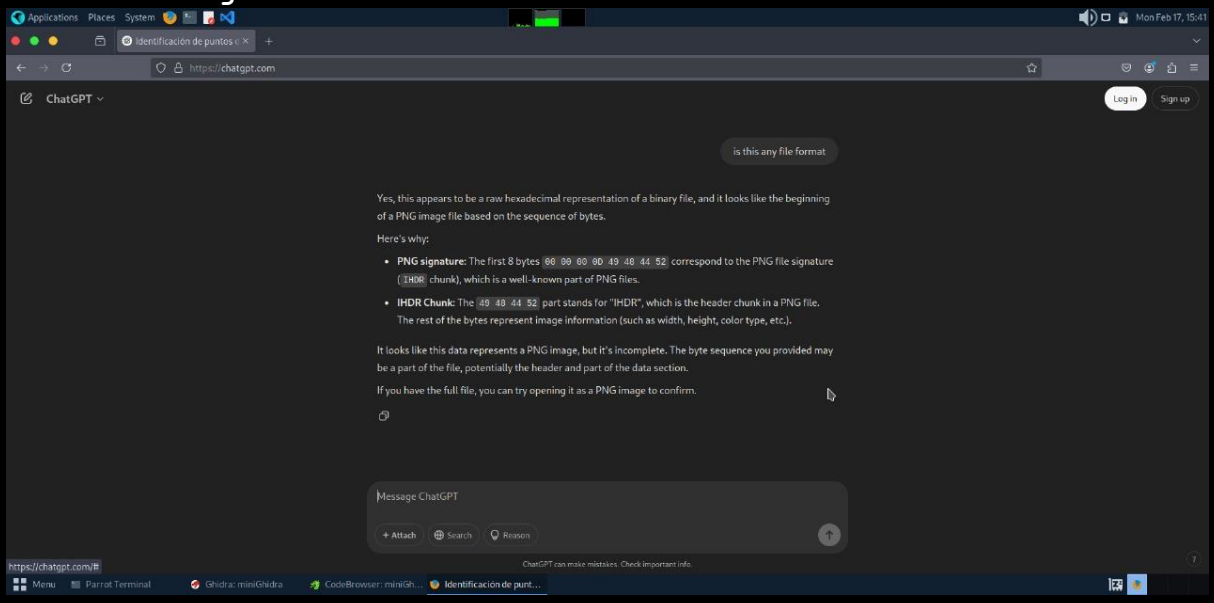
- Here, we have a scanf@plt function. This must be the point where the game asks us for our input like attack, defense, etc.
- We must make the enemy health 0 before it attacks us.
- Let us add breakpoints at required points and then run.



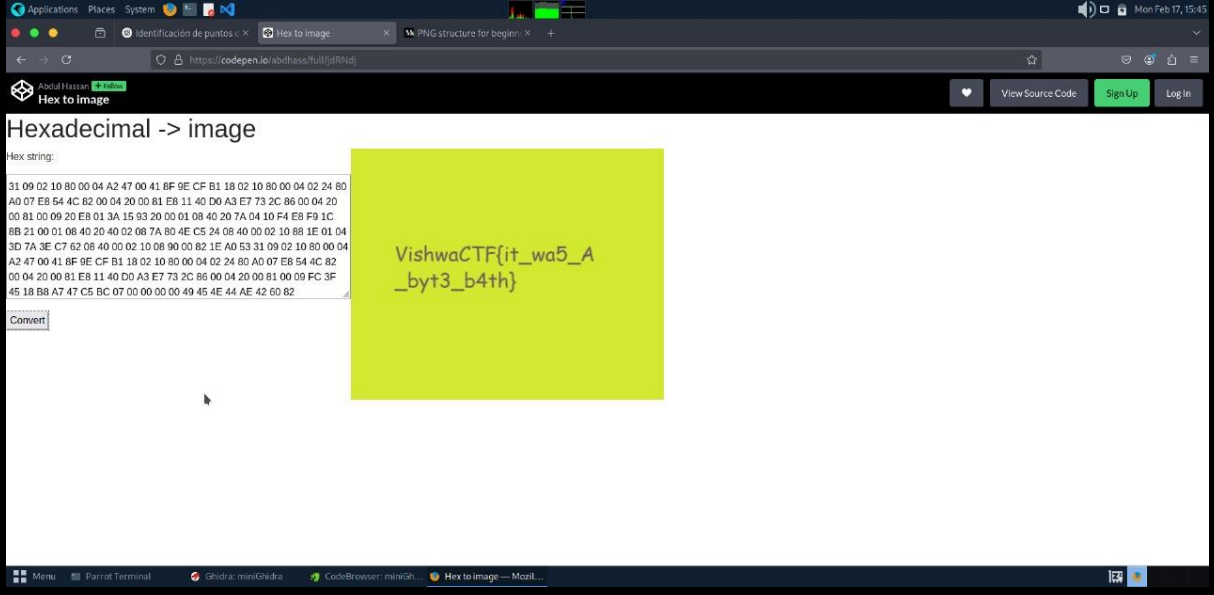
- Now that we have made the enemy health 0, let us attack now because that is the only time we are checking the enemy health value to be 0.



- We get a big hex dump with a message that we won.
- If we put some part of it on ChatGPT, it tells us this is a PNG dump with some missing headers.



- 89 50 4E 47 0D 0A 1A 0A is the missing header.
- Now let us put it at the start of the hex dump and try to convert it.



-
- **Voila! We get back our flag.**

  - **Flag: VishwaCTF{it_wa5_A_byt3_b4th}**