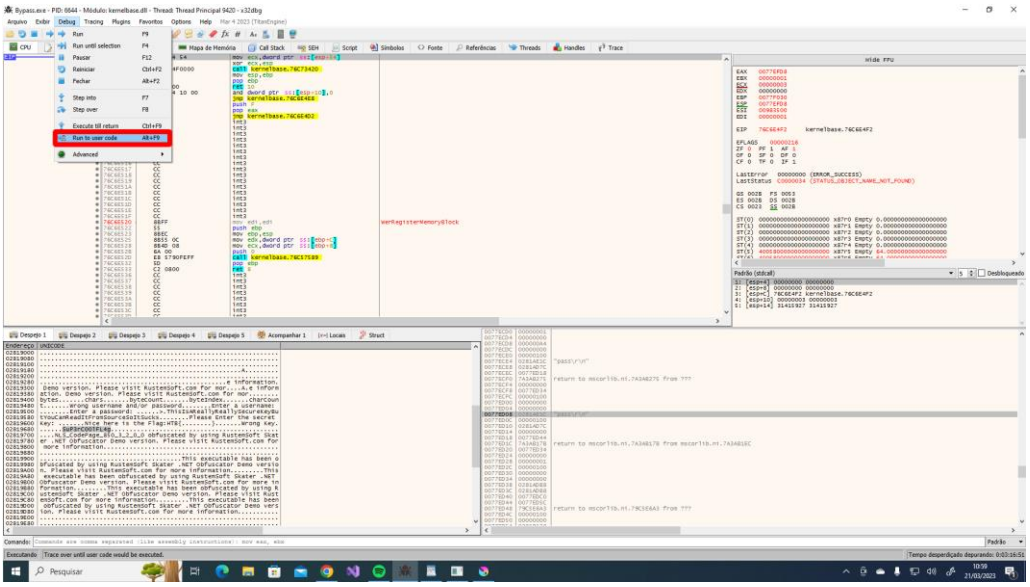
Bypass Write up

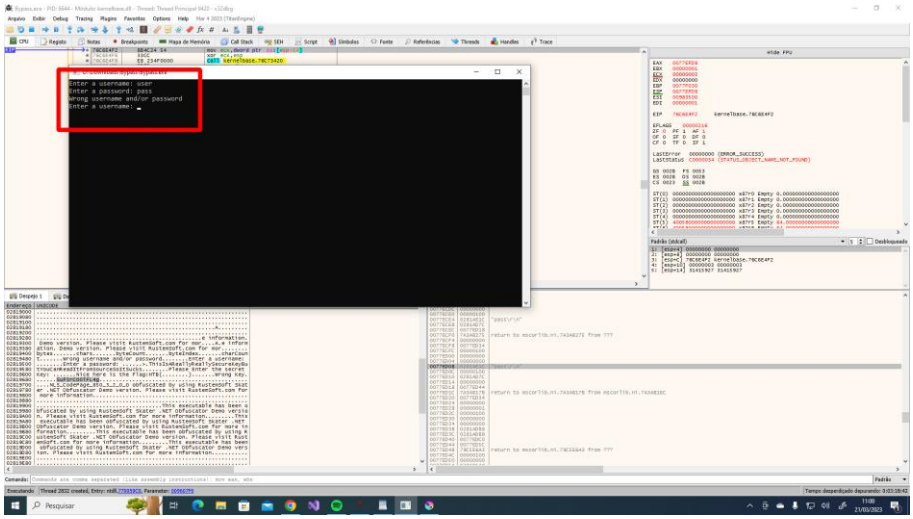
Esse CTF nos faz olhar para um sistema simples de usuário e senha, onde teremos que passar uma chave secreta após para obter a flag.

Minha Solução:

1. Em um primeiro momento me assustei com a quantidade de informações que o x32dbg passava para fazermos a análise do executável, após duas pesquisas de como o programa funcionava em si e não de como resolver esse ctf, percebi uma opção na caixa de Debug chamada Run to user code.



2. Após executar o programa normalmente, com usuários e senhas errados, pude mapear a execução do programa, e como a memória se comportava ao passar esses parâmetros errôneos.



3. Fui filtrando na memória, essas operações com minha palavra "pass" que apareciam na gravação do programa, jogando as pro despejo, até que na última operação que o programa

utilizava-a, no unicode, possui-a a mensagem de senha incorreta, porém ao mesmo tempo passava a flag como se fosse um condicional em high level.
Ao notar a frase "Nice here is the Flag:HTB{....}, possuía as opções de chave incorreta e a SuP3rC00lFL4G, deduzi então que essa seria a palavra da flag desejada pelo CTF.