Passphrase

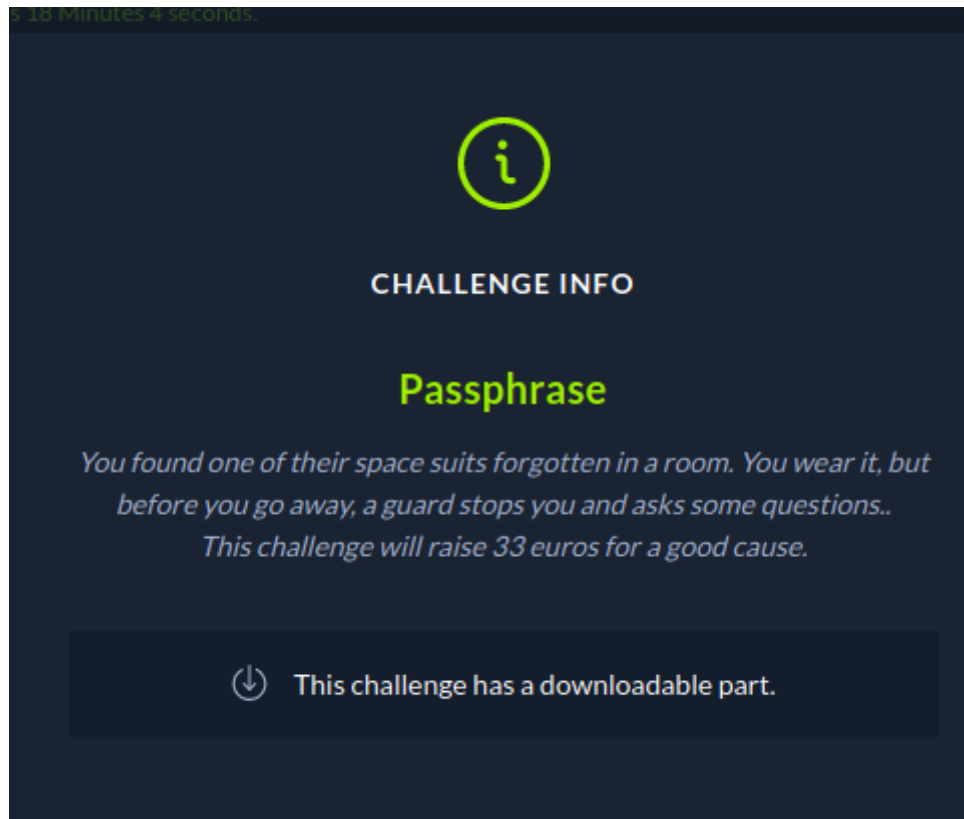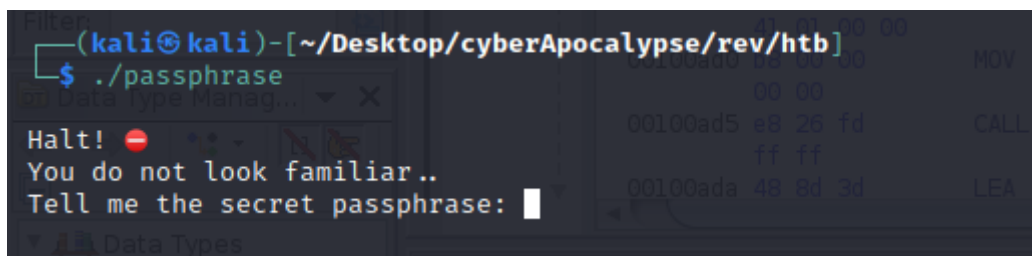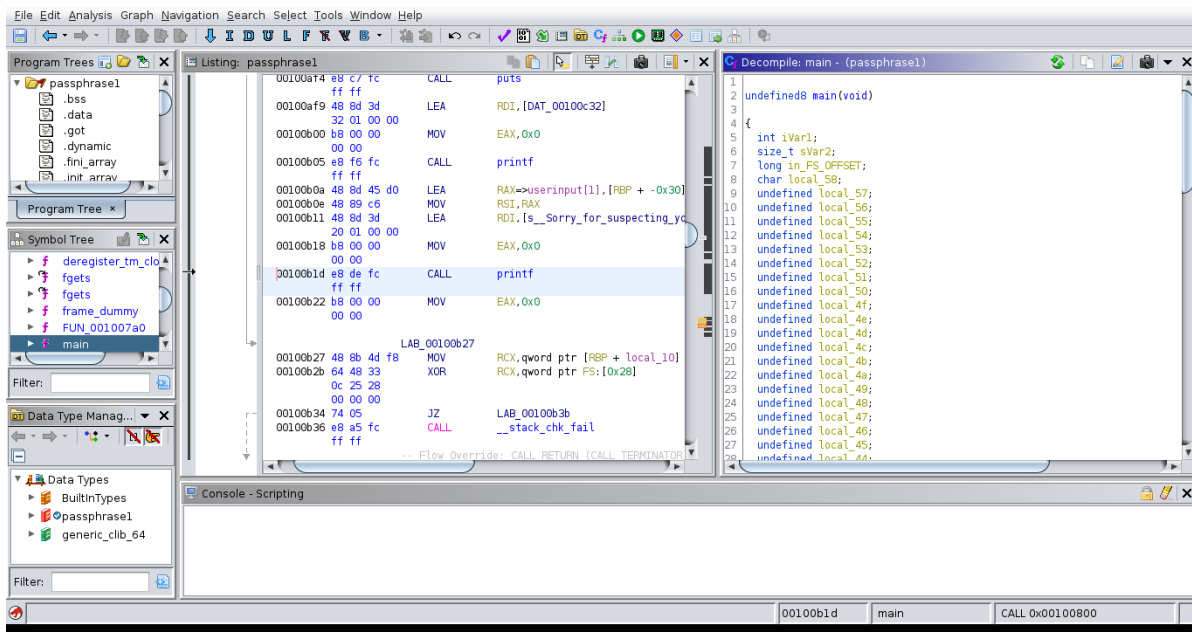## Solution

unzip downloaded file and run

binary asking for an password

Decompileing

> open this file in **ghidra**

decompiled **main** function looks like this

```
undefined8 main(void)

{
  int iVar1;
  size_t sVar2;
  long in_FS_OFFSET;
  char local_58;
  undefined local_57;
  undefined local_56;
  undefined local_55;
  undefined local_54;
  undefined local_53;
  undefined local_52;
  undefined local_51;
  undefined local_50;
  undefined local_4f;
  undefined local_4e;
  undefined local_4d;
  undefined local_4c;
  undefined local_4b;
  undefined local_4a;
  undefined local_49;
  undefined local_48;
  undefined local_47;
  undefined local_46;
  undefined local_45;
  undefined local_44;
  undefined local_43;
  undefined local_42;
  undefined local_41;
  undefined local_40;
  undefined local_3f;
  undefined local_3e;
  undefined local_3d;
  char userinput [41];
  long local_10;
```

```
  local_10 = *(long *)(in_FS_OFFSET + 0x28);
  setbuf(stdout,(char *)0x0);
  local_58 = '3';
  local_57 = 0x78;
  local_56 = 0x74;
  local_55 = 0x72;
  local_54 = 0x34;
  local_53 = 0x74;
  local_52 = 0x33;
  local_51 = 0x72;
  local_50 = 0x52;
  local_4f = 0x33;
  printstr(&DAT_00100bc8);
  printstr("\nYou do not look familiar..");
  printstr("\nTell me the secret passphrase: ");
  local_4e = 0x73;
  local_4d = 0x74;
  local_4c = 0x52;
  local_4b = 0x31;
  local_4a = 0x34;
  local_49 = 0x4c;
  local_48 = 0x35;
  local_47 = 0x5f;
  local_46 = 0x56;
  fgets(userinput + 1,0x28,stdin);
  local_45 = 0x53;
  local_44 = 0x5f;
  local_43 = 0x68;
  local_42 = 0x75;
  sVar2 = strlen(userinput + 1);
  userinput[sVar2] = '\0';
  local_41 = 0x6d;
  local_40 = 0x34;
  local_3f = 0x6e;
  local_3e = 0x35;
  local_3d = 0;
  iVar1 = strcmp(&local_58,userinput + 1);
  if (iVar1 == 0) {
    puts(&DAT_00100c2e);
    printf("\x1b[32m");
    printf(
           "\nSorry for suspecting you, please transfer this important message to
the chief:CHTB{%s}\n\n"
           ,userinput + 1);
  }
  else {
    printf("\x1b[31m");
    printstr(&DAT_00100c17);
  }
  if (local_10 != *(long *)(in_FS_OFFSET + 0x28)) {
                    /* WARNING: Subroutine does not return */
    __stack_chk_fail();
  }
  return 0;
}
```

when user input secret +1 its compare with `&local_58` .if true then prints the flag.

`&local_58` is a [reference](#)

local_3e to **local_57** holds some hex values.

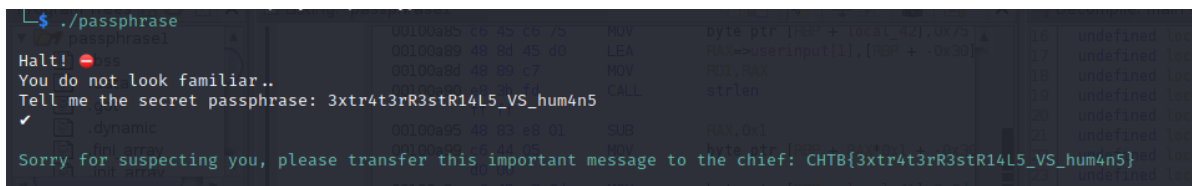- our goal is to convert this to ascii

for that i wrote python code.

```python
hexs =
[0x78,0x74,0x72,0x34,0x74,0x33,0x72,0x52,0x33,0x73,0x74,0x52,0x31,0x34,0x4c,0x35,
0x5f,0x56,0x53,0x5f,0x68,0x75,0x6d,0x34,0x6e,0x35]
out =[]
for hx in hexs:
    out.append(chr(hx))
print(''.join(out))
```

> Output
>
>   xtr4t3rR3stR14L5_VS_hum4n5

finally append loacl_58 value 3 to the start of the secret

>   3xtr4t3rR3stR14L5_VS_hum4n5