vishwaCTF

CHALLENGE NAME : [STACK HACK]

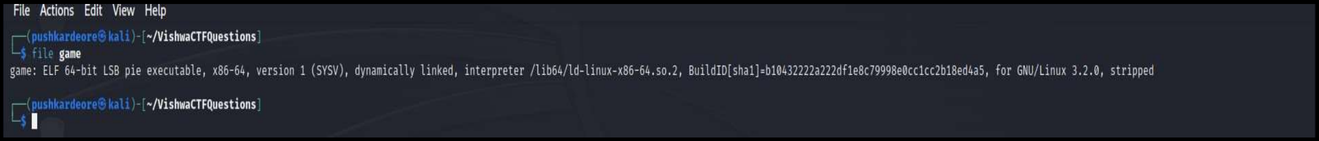
DEV : [PUSHKAR DEORE]

CATEGORY : [REVERSE ENGINEERING]

LEVEL : [EASY]

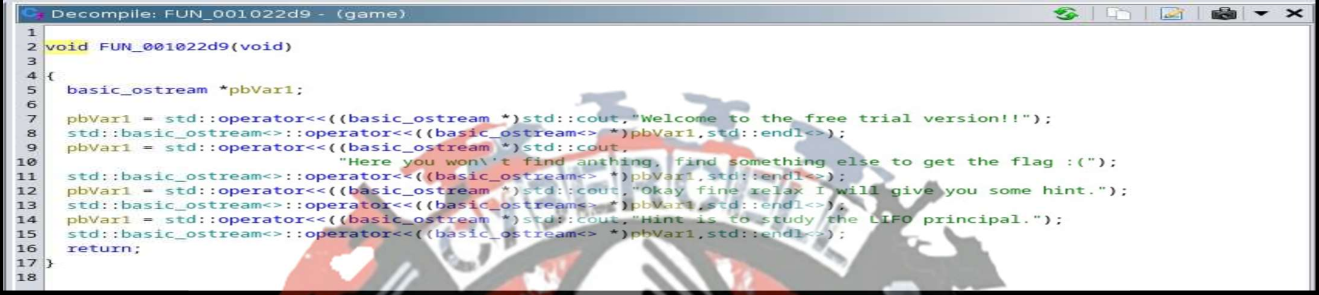
2024

In this question, you have been given a stripped ELF file.



```
File  Actions  Edit  View  Help
┌──(pushkardeore㉿kali)-[~/VishwaCTFQuestions]
└─$ file game
game: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=b10432222a222df1e8c79998e0cc1cc2b18ed4a5, for GNU/Linux 3.2.0, stripped

┌──(pushkardeore㉿kali)-[~/VishwaCTFQuestions]
└─$ ▌
```

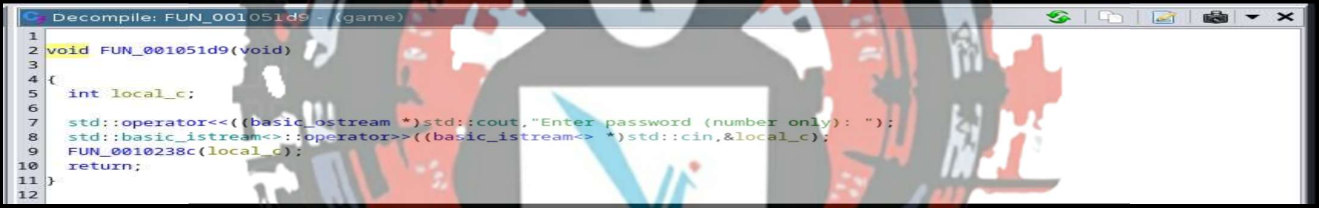
Here, if we open this question in a software like Ghidra or IDA, you will find that there is a function associated with free version. When you open this question, you will find a statement that you should study LIFO principal. This gives a hint that stack data structure is used here, hence Stack Hack.



Decompile: FUN_001022d9 - (game)

```

void FUN_001022d9(void)

{
  basic_ostream *pbVar1;

  pbVar1 = std::operator<<((basic_ostream *)std::cout,"Welcome to the free trial version!!");
  std::basic_ostream<>::operator<<((basic_ostream<> *)pbVar1,std::endl<>);
  pbVar1 = std::operator<<((basic_ostream *)std::cout,
                           "Here you won\'t find anthing, find something else to get the flag :(");
  std::basic_ostream<>::operator<<((basic_ostream<> *)pbVar1,std::endl<>);
  pbVar1 = std::operator<<((basic_ostream *)std::cout,"Okay fine relax I will give you some hint.");
  std::basic_ostream<>::operator<<((basic_ostream<> *)pbVar1,std::endl<>);
  pbVar1 = std::operator<<((basic_ostream *)std::cout,"Hint is to study the LIFO principal.");
  std::basic_ostream<>::operator<<((basic_ostream<> *)pbVar1,std::endl<>);
  return;
}

```

If we go to the function associated with the premium version, you will be asked for password.



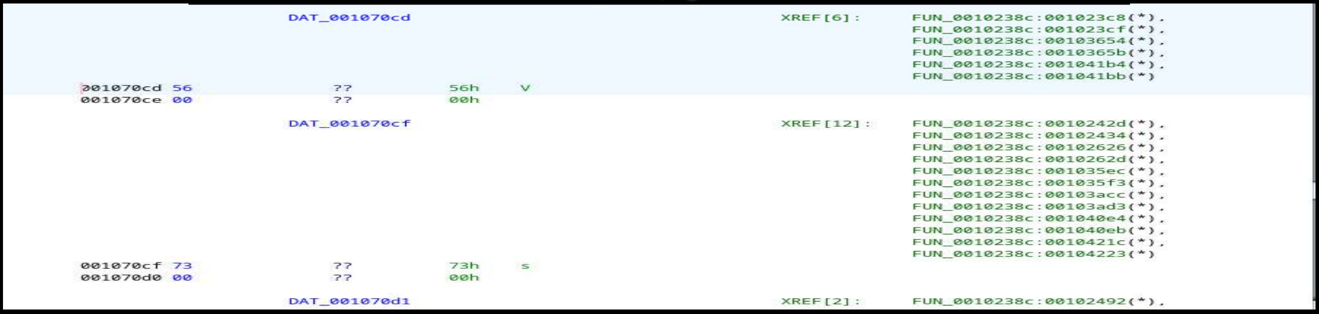
Decompile: FUN_001051d9 - (game)

```

void FUN_001051d9(void)

{
  int local_c;

  std::operator<<((basic_ostream *)std::cout,"Enter password (number only): ");
  std::basic_istream<>::operator>>((basic_istream<> *)std::cin,&local_c);
  FUN_0010238c(local_c);
  return;
}

```

And in the password checker function, your numerical password will be passed as a parameter to another function.

In this function, you will find that there are a lot of random symbols and alphabets pushed on a stack. At the end of the function, you will find a loop to which prints every Nth element from the stack if N is the integer passed as password.

If you study the elements on the stack, you will find that every 3rd element is part of the flag in VishwaCTF{} format.



```
                     DAT_001070cd                    XREF[6]:     FUN_0010238c:001023c8(*),
                                                                  FUN_0010238c:001023cf(*),
                                                                  FUN_0010238c:00103654(*),
                                                                  FUN_0010238c:0010365b(*),
                                                                  FUN_0010238c:001041b4(*),
                                                                  FUN_0010238c:001041bb(*)
    001070cd 56          ??         56h    V
    001070ce 00          ??         00h
                     DAT_001070cf                    XREF[12]:    FUN_0010238c:0010242d(*),
                                                                  FUN_0010238c:00102434(*),
                                                                  FUN_0010238c:00102626(*),
                                                                  FUN_0010238c:0010262d(*),
                                                                  FUN_0010238c:001035ec(*),
                                                                  FUN_0010238c:001035f3(*),
                                                                  FUN_0010238c:00103acc(*),
                                                                  FUN_0010238c:00103ad3(*),
                                                                  FUN_0010238c:001040e4(*),
                                                                  FUN_0010238c:001040eb(*),
                                                                  FUN_0010238c:0010421c(*),
                                                                  FUN_0010238c:00104223(*)
    001070cf 73          ??         73h    s
    001070d0 00          ??         00h
                     DAT_001070d1                    XREF[2]:     FUN_0010238c:00102492(*),
```

Hence if you input password as 3, you will get your flag printed but in reverse format.

FLAG: VishwaCTF{reversal_success}