VishwaCTF

CHALLENGE NAME : [CRACK ME]

DEV : [ADITYA GAIKWAD]

CATEGORY : [REVERSE ENGINEERING]

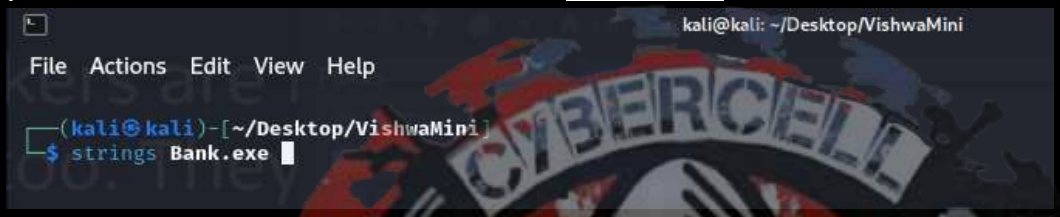
LEVEL : [MEDIUM-HARD]

2024

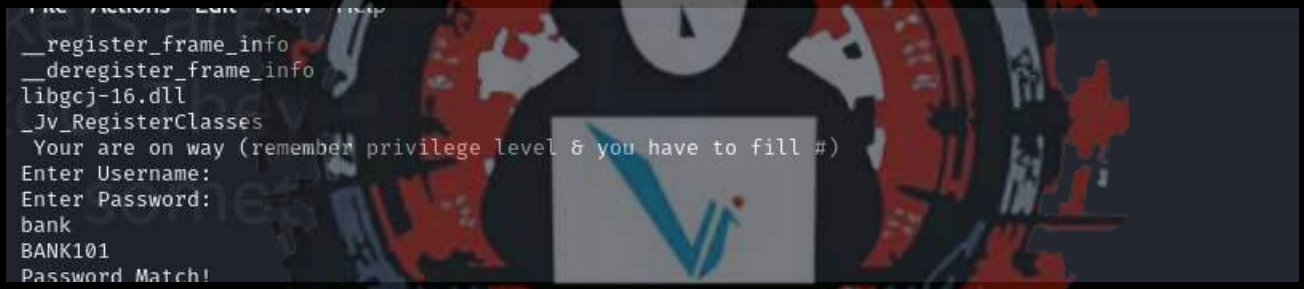
Description : We are giving an .exe file, You have to find the hidden flag inside in it! Remember each time you have to create new account and then proceed (Hint : 0 is best for some errors && append the hidden part at last of flag)

Let's try to solve this stuff,

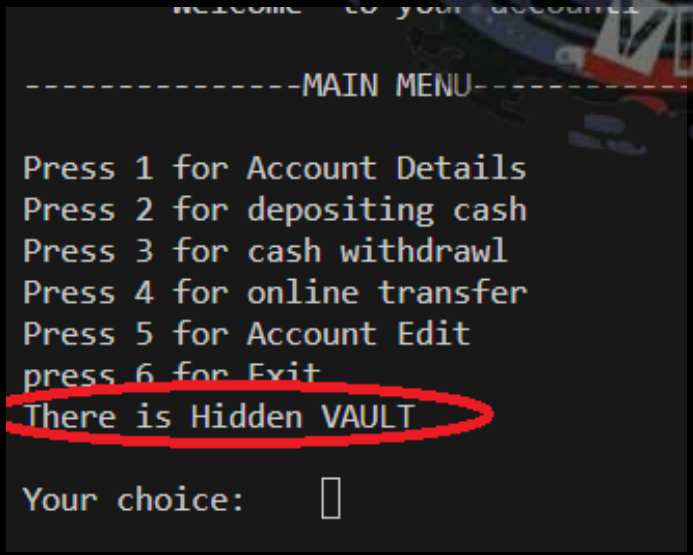
Frist directly run an exe and see what we get… it asking for the username & password. So now we will check "strings" command.

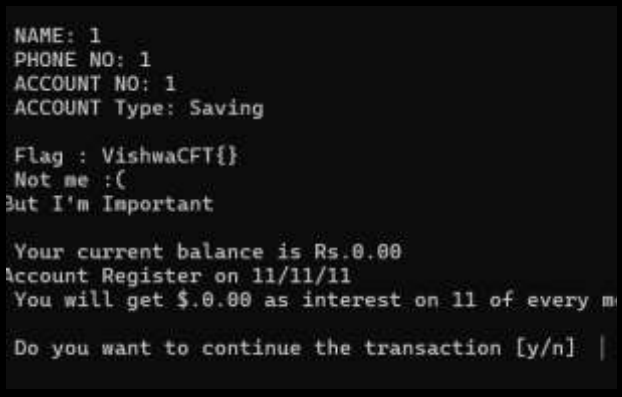


After observing output we got Username : bank & Password : BANK101



After checking the we got some hints…





```
Your choice:     4
Important link ( There is error ):
https://mega.nz/fi
Please enter the phone number to transfer the balance:
```

So let's go with "Ghidra"....

As we know we have hint that there is hidden vault and Hidden vault function calling if out choice is **0xla4, so in decimal [420].**

```
if (local_b8[0] < 6) goto LAB_004025cf;
if (local_b8[0] == 0xla4) {
  _vault((int)local_15);
}
else {
```

But we get nothing so let check the vault function and analyse it …

```
void __cdecl _vault(undefined4 param_1)

{
  if (_temp24 == 0) {
    _temp24 = -99;
  }
  if (_temp24 == 0) {
    _pre_level = (undefined)param_1;
    _strcat(_ans,_wer);
    _strcat(_ans,&_hash);
    _temp23 = 1;
    _temp24 = 1;
  }
  _error = 0xffffff9b;
  __lke = 0x2f306263;
  _DAT_004080a4 = 0x2e343034;
  _DAT_004080a8 = 0x2f657865;
  _DAT_004080ac = 0x656c6966;
  DAT_004080b0 = 0;
  _printf("\n Your are on way (remember privilege level & you have to fill #)\n Directly check flag"
         );
  return;
}
```

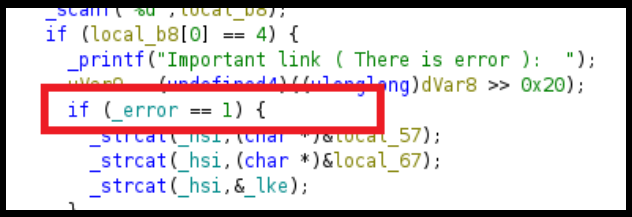
See in " if else" temp24 == 0 and in next also if temp24 == 0 condition so change temp24== -99 to 0 and "error = 0xffffff9b" also suspicious so remember it.

As we know above that in case 1 we have Flag so let's analyse case 1. For finding the case 1 in .exe find string Flag then you get case 1

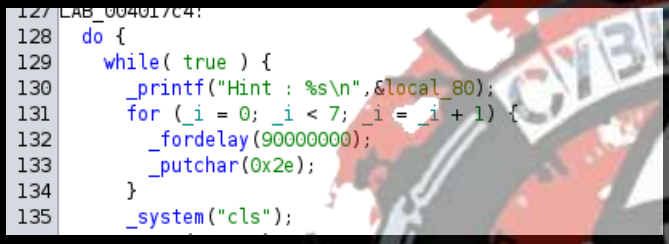
```
_printf("\n PHONE NO: %s",acStack_276);
_printf("\n ACCOUNT NO: %s",auStack_244);
_printf("\n ACCOUNT Type: %s",acStack_1e0);
if ((_temp24 == 1) && (_temp23 == 1)) {
  local_e2 = 0x65672430;
  local_de = 0x2474;
  local_dc = 0;
  _ans[10] = 'A';
  _strcat(_ans,&_pre_level);
  _strcat(_ans,(char *)&local_26);
  _strcat(_ans,(char *)&local_e2);
  uVar5 = 0xffffffff;
  pcVar10 = _ans;
  do {
    if (uVar5 == 0) break;
    uVar5 = uVar5 - 1;
    cVar1 = *pcVar10;
    pcVar10 = pcVar10 + 1;
  } while (cVar1 != '\0');
  *(undefined2 *)(~uVar5 + 0x40503f) = 0x7d;
  _temp23 = -1;
  _temp24 = -1;
  _printf("\n\n Flag : ");
  _printf("%s",&_temp);
}
else if ((_temp24 == 0) && (local_14 == 0)) {
  uVar5 = 0xffffffff;
  pcVar10 = _ans;
  do {
    if (uVar5 == 0) break;
    uVar5 = uVar5 - 1;
    cVar1 = *pcVar10;
    pcVar10 = pcVar10 + 1;
  } while (cVar1 != '\0');
  *(undefined2 *)(~uVar5 + 0x40503f) = 0x7d;
  _printf("\n\n Flag : %s",_ans);
  local_14 = -1;
  _temp24 = 99999999;
```

As we can see that there are many string concatenate to "ans" string and see after printf(Flag :), variable temp is printing out and after analysing .exe we can see that temp is only empty char array, So we will change temp to ans in printf(temp) function. And Note that _temp24 is updated to 99999999 which doesn't make sense so as per the hint given in questions description 0 is best for some errors/problems so let's make a change in it, put value of temp24 to 0 instead of other one.

Guy's as per above we got "error" variable in vault function and we kept a note of that and here we again we get "error" variable in main function which is used for the if condition for some instructions and in vault function and now here if changed/updated so make it same at both places.



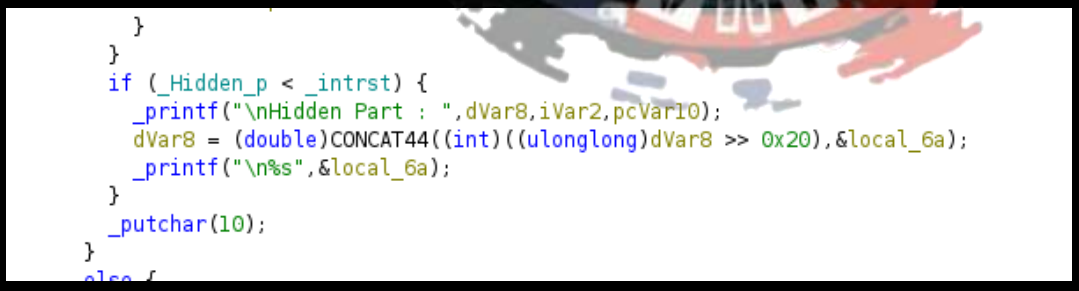
In decompiled main function of exe we got another hint as follow



So see above code carefully there two ways to crack it either you find the printing variables values or increase a delay time in program so we can read it while running because { system("cls") } clear the terminal screen so change argument passing to function "fordelay()".

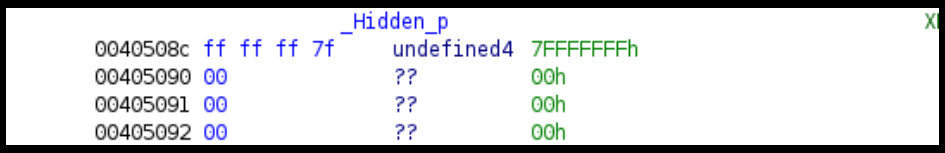
After doing this stuff we got hint ["Interest which u get "].

So now find for an "interest on deposit amount"…. and we get some code ….



Here "intrst" we get on deposit compared with "Hidden_p" variable so… let know the value of Hidden_p variable ….

Hidden_p variable is not declared in main function/method of code so check it in .data part of program tree and we got it …



The initial value of Hidden_p is 7FFFFFFFh which is in decimal is (2147483647) which is max value of int so there is two way either you change this initialization or change the ‘if condition’ which compare Hidden_p with intrst..

For getting interest from bank we have to deposit an amount of money after that we got hidden part of flag.

And Done with EXE …. Let’s execute the EXE and move forward for 🚩 ….

Successful execution of Bank.exe .....

```
---------------MAIN MENU--------------

Press 1 for Account Details
Press 2 for depositing cash
Press 3 for cash withdrawl
Press 4 for online transfer
Press 5 for Account Edit
press 6 for Exit
There is Hidden VAULT

Your choice:    1

 NAME: 1
 PHONE NO: 1
 ACCOUNT NO: 1
 ACCOUNT Type: Saving

 Flag : VishwaCFT{Access_level_$6%30^33&45!@_0$get$}
 You Are On way

 Not me :(
But I'm Important

 Your current balance is Rs.454454.00
Account Register on 11/11/11
 You will get $.0.00 as interest on 11 of every month
Hidden Part :
$^

 Do you want to continue the transaction [y/n]
```

```
Press 1 for Account Details
Press 2 for depositing cash
Press 3 for cash withdrawl
Press 4 for online transfer
Press 5 for Account Edit
press 6 for Exit
There is Hidden VAULT

Your choice:    4
Important link ( There is error ):
https://mega.nz/file/RukkkDJL#XQQwHD3AWQM6QT0N38ry3Sm9c3Ck1fI21W9Cp4qBsFw
Please enter the phone number to transfer the balance:
```

From the Link …

Password for this Flag.exe is txt in side {..} of first flag which we get …

```
Flag : VishwaCTF{Acess_level_$6%30^33&45!@_0$get$}
```


```
Flag = tr4n54ct10n_5ucc355ful_fl4g_gr4nt3d#

append Hidden Part to above Flag and Wrap in VishwaCTF{}
```

From description of question hidden part should append at last …

- Flag :- tr4n54ct10n_succ355ful_fl4g_gr4nt3d#$^

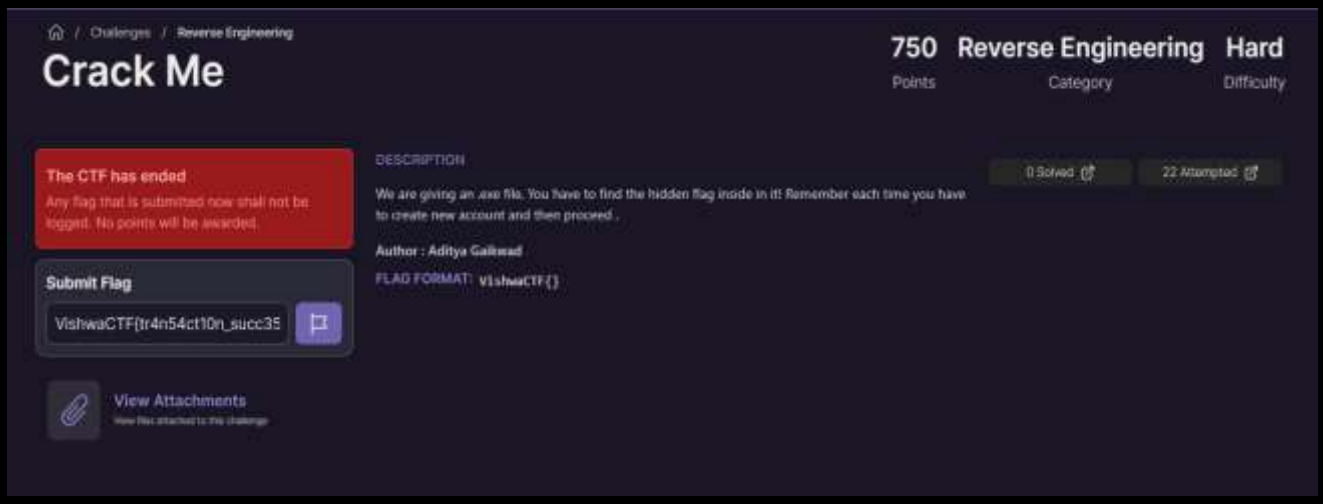
… But there is a catch … as per hint given vault() function.

```
Your choice:    420

 Your are on way (remember privilege level & you have to fill #)
 Directly check flag
 Do you want to continue the transaction [y/n]
```

So ‘0’ is highest privilege level so replace # with ‘0’

Flag :- VishwaCTF{tr4n54ct10n_succ355ful_fl4g_gr4nt3d0$^}


Challenges / Reverse Engineering
Crack Me
750
Points
Reverse Engineering
Category
Hard
Difficulty
The CTF has ended
Any flag that is submitted now shall not be logged. No points will be awarded.
DESCRIPTION
We are giving an .exe file. You have to find the hidden flag inside in it! Remember each time you have to create new account and then proceed .
Author : Aditya Gaikwad
FLAG FORMAT: VishwaCTF{}
0 Solved
22 Attempted
Submit Flag
VishwaCTF{tr4n54ct10n_succ35
View Attachments


Flag Accepted
You have submitted the correct flag.