

राश्मिCTF

CHALLENGE NAME : [HUNGRY FRIENDS]

DEV : [ABHINAV MEHTA]

CATEGORY : [REVERSE ENGINEERING]

LEVEL : [MEDIUM]



2025


```
Windows PowerShell
PS D:\Downloads> gdb ./snakes.exe
GNU gdb (GDB) 7.6.1
Copyright (C) 2013 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "mingw32".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from D:\Downloads\snakes.exe...done.
(gdb) disass main
Dump of assembler code for function main:
0x00401b42 <+0>: lea    0x4(%esp),%ecx
0x00401b46 <+4>: and    $0xffffffff0,%esp
0x00401b49 <+7>: pushl  -0x4(%ecx)
0x00401b4c <+10>: push   %ebp
0x00401b4d <+11>: mov    %esp,%ebp
0x00401b4f <+13>: push   %ebx
0x00401b50 <+14>: push   %ecx
0x00401b51 <+15>: sub    $0x10,%esp
0x00401b54 <+18>: call   0x402360 <_main>
0x00401b59 <+23>: movl   $0x0,(%esp)
0x00401b60 <+30>: call   0x4043f8 <time>
0x00401b65 <+35>: mov    %eax,(%esp)
0x00401b68 <+38>: call   0x404410 <srand>
0x00401b6d <+43>: call   0x4015e5 <_Z11HIDE_CURSORv>
0x00401b72 <+48>: call   0x401659 <_Z9INIT_GAMEv>
0x00401b77 <+53>: call   0x4016b1 <_Z10SPAWN_FOODv>
0x00401b7c <+58>: movzbl 0x40c024,%eax
0x00401b83 <+65>: test   %al,%al
0x00401b85 <+67>: jne    0x401c3f <main+253>
0x00401b8b <+73>: call   0x404498 <_kbhit>
0x00401b90 <+78>: test   %eax,%eax
0x00401b92 <+80>: setne  %al
0x00401b95 <+83>: test   %al,%al
0x00401b97 <+85>: je     0x401c10 <main+206>
0x00401b99 <+87>: call   0x404498 <_getch>
0x00401b9e <+92>: cmp    $0x64,%eax
0x00401ba1 <+95>: je     0x401bfb <main+185>
0x00401ba3 <+97>: cmp    $0x64,%eax
```

After disassembling main, we find various functions.

```
Windows PowerShell
0x00401b95 <+83>: test   %al,%al
0x00401b97 <+85>: je     0x401c10 <main+206>
0x00401b99 <+87>: call   0x404498 <_getch>
0x00401b9e <+92>: cmp    $0x64,%eax
0x00401ba1 <+95>: je     0x401bfb <main+185>
0x00401ba3 <+97>: cmp    $0x64,%eax
0x00401ba6 <+100>: jg     0x401baf <main+109>
0x00401ba8 <+102>: cmp    $0x61,%eax
0x00401bab <+105>: je     0x401be5 <main+163>
0x00401bad <+107>: jmp    0x401c10 <main+206>
0x00401baf <+109>: cmp    $0x73,%eax
0x00401bb2 <+112>: je     0x401bcf <main+141>
0x00401bb4 <+114>: cmp    $0x77,%eax
0x00401bb7 <+117>: jne    0x401c10 <main+206>
0x00401bb9 <+119>: movl   $0x0,0x40c03c
0x00401bbc <+129>: movl   $0xffffffff,0x407004
0x00401bcd <+139>: jmp    0x401c10 <main+206>
0x00401bce <+141>: movl   $0x0,0x40c03c
0x00401bd9 <+151>: movl   $0x1,0x407004
0x00401be3 <+161>: jmp    0x401c10 <main+206>
0x00401be5 <+163>: movl   $0xffffffff,0x40c03c
0x00401bef <+173>: movl   $0x0,0x407004
0x00401bf9 <+183>: jmp    0x401c10 <main+206>
0x00401bfb <+185>: movl   $0x1,0x40c03c
0x00401c05 <+195>: movl   $0x0,0x407004
0x00401c0f <+205>: nop
0x00401c10 <+206>: call   0x401a18 <_Z10MOVE_SNAKEv>
0x00401c15 <+211>: call   0x40179b <_Z9DRAW_GAMEv>
0x00401c1a <+216>: mov    0x40c020,%eax
0x00401c1f <+221>: cmp    $0x270f,%eax
0x00401c24 <+226>: jne    0x401c2b <main+233>
0x00401c26 <+228>: call   0x4019a1 <_Z9SHOW_FLAGv>
0x00401c2b <+233>: movl   $0x64,(%esp)
0x00401c32 <+240>: call   0x4044e8 <Sleep@4>
0x00401c37 <+245>: sub    $0x4,%esp
0x00401c3a <+248>: jmp    0x401b7c <main+58>
0x00401c3f <+253>: mov    0x40c020,%ebx
0x00401c45 <+259>: movl   $0x4080b7,0x4(%esp)
0x00401c4d <+267>: movl   $0x40d324,(%esp)

End of assembler dump.
(gdb) |
```

Here we find at instruction <+221> that a comparison is being done which results in equal, calls a function SHOW FLAG.

```
Windows PowerShell
0x00401bb2 <+112>: je 0x401bcf <main+141>
0x00401bb4 <+114>: cmp $0x77,%eax
0x00401bb7 <+117>: jne 0x401c10 <main+206>
0x00401bb9 <+119>: movl $0x0,0x40c03c
0x00401bc3 <+129>: movl $0xffffffff,0x407004
0x00401bcd <+139>: jmp 0x401c10 <main+206>
0x00401bef <+141>: movl $0x0,0x40c03c
0x00401bd9 <+151>: movl $0x1,0x407004
0x00401be3 <+161>: jmp 0x401c10 <main+206>
0x00401be5 <+163>: movl $0xffffffff,0x40c03c
0x00401bef <+173>: movl $0x0,0x407004
0x00401bf9 <+183>: jmp 0x401c10 <main+206>
0x00401bfb <+185>: movl $0x1,0x40c03c
0x00401c05 <+195>: movl $0x0,0x407004
0x00401c0f <+205>: nop
0x00401c10 <+206>: call 0x401a18 <_Z10MOVE_SNAKEv>
0x00401c15 <+211>: call 0x40179b <_Z9DRAW_GAMEv>
0x00401c1a <+216>: mov 0x40c020,%eax
0x00401c1f <+221>: cmp $0x270f,%eax
0x00401c24 <+226>: jne 0x401c2b <main+233>
0x00401c26 <+228>: call 0x4019a1 <_Z9SHOW_FLAGv>
0x00401c2b <+233>: movl $0x64,(&esp)
0x00401c32 <+240>: call 0x4044e8 <Sleep@4>
0x00401c37 <+245>: sub $0x4,%esp
0x00401c3a <+248>: jmp 0x401b7c <main+58>
0x00401c3f <+253>: mov 0x40c020,%ebx
0x00401c45 <+259>: movl $0x4080b7,0x4(&esp)
0x00401c4d <+267>: movl $0x40d324,(&esp)
End of assembler dump.
(gdb) break *main
Breakpoint 1 at 0x401b42
(gdb) run
Starting program: D:\Downloads\./snakes.exe
[New Thread 21676.0x5938]
[New Thread 21676.0x4a20]
[New Thread 21676.0x5bb8]
[New Thread 21676.0x4a24]

Breakpoint 1, 0x00401b42 in main ()
(gdb) set CHAKDE = 9999
(gdb) |
```

We have made necessary changes dynamically in the code. Now lets try to run it.

```
Windows PowerShell
##### jne 0x401c10 <main+206>
# movl $0x0,0x40c03c
# movl $0xffffffff,0x407004
# jmp 0x401c10 <main+206>
# movl $0x0,0x40c03c
# movl $0x1,0x407004
# jmp 0x401c10 <main+206>
# movl $0xffffffff,0x40c03c
# movl $0x0,0x407004
# jmp 0x401c10 <main+206>
# movl $0x1,0x40c03c
# movl $0x0,0x407004
# nop
# call 0x401a18 <_Z10MOVE_SNAKEv>
# call 0x40179b <_Z9DRAW_GAMEv>
# mov 0x40c020,%eax
# cmp $0x270f,%eax
# F jne 0x401c2b <main+233>
# call 0x4019a1 <_Z9SHOW_FLAGv>
# movl $0x64,(&esp)
# 0 call 0x4044e8 <Sleep@4>
##### sub $0x4,%esp
Score: 99993a <+248>: jmp 0x401b7c <main+58>
0x00401c3f <+253>: mov 0x40c020,%ebx
0x00401c45 <+259>: movl $0x4080b7,0x4(&esp)
Congratulations! Flag: VishwaCTF{th3r3_4r3_5n4k35_all_4r0und}
Game Over! Score: 9999
[Inferior 1 (process 21676) exited normally]
(gdb) oint 1 at 0x401b42
(gdb) run
Starting program: D:\Downloads\./snakes.exe
[New Thread 21676.0x5938]
[New Thread 21676.0x4a20]
[New Thread 21676.0x5bb8]
[New Thread 21676.0x4a24]

Breakpoint 1, 0x00401b42 in main ()
(gdb) set CHAKDE = 9999
(gdb) c
Continuing.
```

And there it is. We have the flag.

VishwaCTF{th3r3_4r3_5n4k35_all_4r0und}