Reversing the Sins

Question :

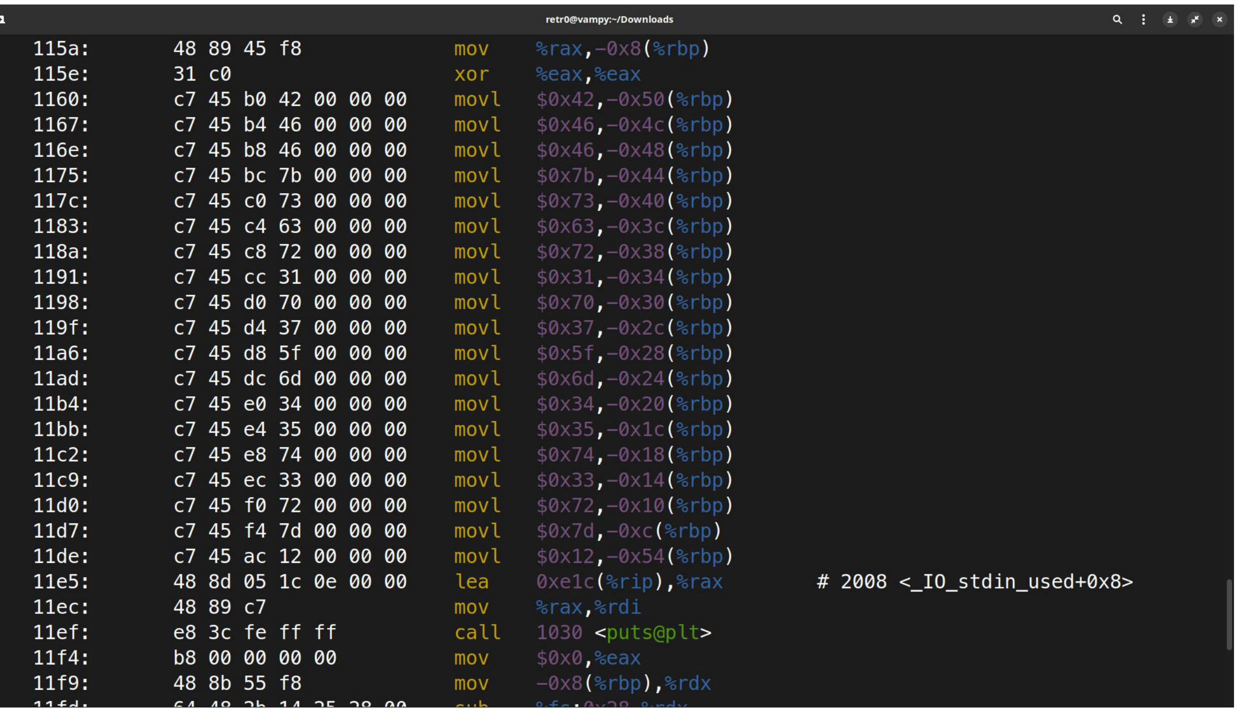
- A Wich cast a spell on the program written by the Princess Indumati of Dholakpur. She asked you to find a hidden text somewhere in this executable. Can you find it for her ?

Hint :

- axb, cxd, exf

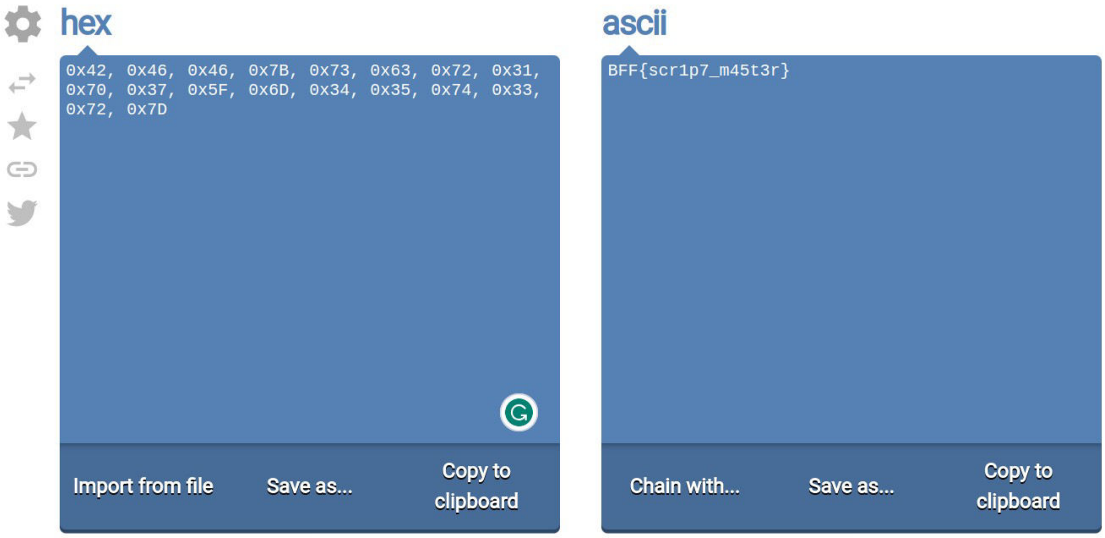
Solution :

- Disassemble the executable: Use a disassembler tool like objdump or a debugger like gdb to disassemble the compiled executable.
- use this command : **objdump -d xor2 > xor2.asm**
- This command will create a file named "xor2.asm" containing the disassembled code.
- Analyse the assembly code using **cat xor2.asm** and check for text in the format as per hint “axb, cxd” in the main function. Locate the flag-related code.
- Search for code segments that access or manipulate data similar to the flag array contents as per the hint **“axb, cxd”**



```
    115a:	48 89 45 f8          	mov    %rax,-0x8(%rbp)
    115e:	31 c0                	xor    %eax,%eax
    1160:	c7 45 b0 42 00 00 00 	movl   $0x42,-0x50(%rbp)
    1167:	c7 45 b4 46 00 00 00 	movl   $0x46,-0x4c(%rbp)
    116e:	c7 45 b8 46 00 00 00 	movl   $0x46,-0x48(%rbp)
    1175:	c7 45 bc 7b 00 00 00 	movl   $0x7b,-0x44(%rbp)
    117c:	c7 45 c0 73 00 00 00 	movl   $0x73,-0x40(%rbp)
    1183:	c7 45 c4 63 00 00 00 	movl   $0x63,-0x3c(%rbp)
    118a:	c7 45 c8 72 00 00 00 	movl   $0x72,-0x38(%rbp)
    1191:	c7 45 cc 31 00 00 00 	movl   $0x31,-0x34(%rbp)
    1198:	c7 45 d0 70 00 00 00 	movl   $0x70,-0x30(%rbp)
    119f:	c7 45 d4 37 00 00 00 	movl   $0x37,-0x2c(%rbp)
    11a6:	c7 45 d8 5f 00 00 00 	movl   $0x5f,-0x28(%rbp)
    11ad:	c7 45 dc 6d 00 00 00 	movl   $0x6d,-0x24(%rbp)
    11b4:	c7 45 e0 34 00 00 00 	movl   $0x34,-0x20(%rbp)
    11bb:	c7 45 e4 35 00 00 00 	movl   $0x35,-0x1c(%rbp)
    11c2:	c7 45 e8 74 00 00 00 	movl   $0x74,-0x18(%rbp)
    11c9:	c7 45 ec 33 00 00 00 	movl   $0x33,-0x14(%rbp)
    11d0:	c7 45 f0 72 00 00 00 	movl   $0x72,-0x10(%rbp)
    11d7:	c7 45 f4 7d 00 00 00 	movl   $0x7d,-0xc(%rbp)
    11de:	c7 45 ac 12 00 00 00 	movl   $0x12,-0x54(%rbp)
    11e5:	48 8d 05 1c 0e 00 00 	lea    0xe1c(%rip),%rax        # 2008 <_IO_stdin_used+0x8>
    11ec:	48 89 c7             	mov    %rax,%rdi
    11ef:	e8 3c fe ff ff       	call   1030 <puts@plt>
    11f4:	b8 00 00 00 00       	mov    $0x0,%eax
    11f9:	48 8b 55 f8          	mov    -0x8(%rbp),%rdx
    11fd:	64 48 2b 14 25 28 00 	sub    %fs:0x28,%rdx
```

- You will find these in the main function.
- (0x42, 0x46, 0x46, 0x7B, 0x73, 0x63, 0x72, 0x31, 0x70, 0x37, 0x5F, 0x6D, 0x34, 0x35, 0x74, 0x33, 0x72, 0x7D). These values represent the hidden flag.
- Convert each hexadecimal value to its corresponding ASCII character. You can use an online tool



```
0x42, 0x46, 0x46, 0x7B, 0x73, 0x63, 0x72, 0x31,
0x70, 0x37, 0x5F, 0x6D, 0x34, 0x35, 0x74, 0x33,
0x72, 0x7D
```

```
BFF{scr1p7_m45t3r}
```

- From the above screenshot, you can view the highlighted flag..... Happy capturing.
- Flag: BFF{scr1p7_m45t3r}