

Over The Edge

by [Davidpb](#) / [Davidpb](#)

Tags: [pwn](#) [underflow](#)

Rating:

1337UP LIVE CTF 2023

Over The Edge

Numbers are fun!! ?

Author: [kavigihan](#)

`over_the_edge.py`

Tags: [pwn](#)

Solution

We get a small python script for this challenge. The interesting bit is in `process_input`.

```
def process_input(input_value):
    num1 = np.array([0], dtype=np.uint64)
    num2 = np.array([0], dtype=np.uint64)
    num2[0] = 0
    a = input_value
    if a < 0:
        return "Exiting..."
    num1[0] = (a + 65)
    if (num2[0] - num1[0]) == 1337:
        return 'You won!\n'
    return 'Try again.\n'
```

This obviously is a buffer underflow. `num1` and `num2` are both `uint64` values, whereas `num2` always is `0`. We basically need to find a number that gives us `0 - (x+65) = 1337`. We can calculate this like `(1<<64)-1402` (as `1337+65 = 1402`), which gives us `18446744073709550214`. If we enter this as input the value will underflow and we will get the flag.

Flag `INTIGRITI{fUn_w1th_1nt3g3r_0v3rf10w_11}`

[Original writeup](https://github.com/D13David/ctf-writeups/blob/main/1337uplive/pwn/over_the_edge/README.md) (https://github.com/D13David/ctf-writeups/blob/main/1337uplive/pwn/over_the_edge/README.md).

Comments

All tasks and writeups are copyrighted by their respective authors. [Privacy Policy](#).

Hosting provided by [Transdata](#).