Gotta Catch Them All

Problem Type

Integer Overflow

Checksec

```
Arch:     amd64-64-little
RELRO:    Partial RELRO
Stack:    No canary found
NX:       NX enabled
PIE:      PIE enabled
```

Solution

Vulnerability

```
short enemy_health = 20000;
short player_health = 10000;
```

The enemy's health is declared as a `short` variable. `short` integers have a value range of -32,768 to 32,767. In the event where an arithmetic operation results in the program storing a value larger than the maximum value the variable can hold, this will result in an unexpected *wraparound* - the variable will wraparound to the minimum value. This is also known as **Integer Overflow**.

For example:

```
short enemy_health = 32767;
enemy_health = enemy_health+1;
printf("Enemy health is now %d", enemy_health);

OUTPUT: Enemy health is now -32768
```

- Expected `enemy_health` = 32768
- Actual `enemy_health` = -32768

`enemy_health` exceeded the maximum limit of what was allocated, and wrapped around to the minimum value of -32768.

Investigation

We note that when the enemy's health falls below 10000 HP, the enemy will heal for 12000 HP the next turn. This is controlled by the `heal_next_turn` variable.

```
if (enemy_health > 0){
    if (heal_next_turn){
         printf("Chikaphu is healing!!!\n");
         enemy_health += 12000;
         printf("This guy is unbeatable!\n");
         printf("Chikaphu Health: %d/20000\n", enemy_health);
         heal_next_turn = 0;
    }

    ...
```

```
        if (enemy_health < 10000){
            printf("Chikaphu begins to growl! Oh no!\n");
            heal_next_turn = 1;
            }
    }
```

We also note that we can heal Chikaphu by 2000 HP through the `playerFeed()` function.

```
void playerFeed()
{
    printf("You used Lighning Bolt!\n");
    printf("Chikaphu absorbs the lightning you shoot at it!\n");
    if (enemy_health != 20000){
        printf("Chikaphu eats the berries and heals for 4000 HP!!\n");
        printf("Shouldn't you be fighting it?\n");
        enemy_health += 2000;
    }
}
```

THe `playerFeed()` function ensures that we are not able to overheal the enemy_health past its maximum HP of 20000 under normal circumstances.

However, if we time it right, we will be able to heal Chikaphu when it is healing itself. This will result in Chikaphu having 8000+2000+12000 = 22000 HP, breaking past the `!= 20000` conditional. As such, we can continue to heal Chikaphu all the way till the maximum limit of the short variable (32767), which will result in integer overflow, and Chikaphu's HP will fall below 0.

Final Solution

1. Use Flamethrower 3 times (Chikaphu Health = 8000)
2. Heal Chikaphu with Thunderbolt (Chikaphu Health = 8000 + 2000 = 10000)
3. Chikaphu will heal himself over his max HP (Chikaphu Health = 10000 + 12000 = 22000)
4. Continue to Heal Chikaphu with Thunderbolt until its HP overflows into a negative value (Chikaphu Health = -31536)

Player Input: 3,3,3,4,4,4,4,4,4,4

Final Result

```
========================================
*************** Chikaphu Turn *************
----------------------------------------
Player Health: 1000/10000 HP
Chikaphu Health: -31536/20000 HP
----------------------------------------
========================================


Chikaphu fainted!
The flag is: CZ4067{1n7363r_0v3rfl0w_1n_p0k3m0n?}
```

Flag

CZ4067{1n7363r_0v3rfl0w_1n_p0k3m0n?}