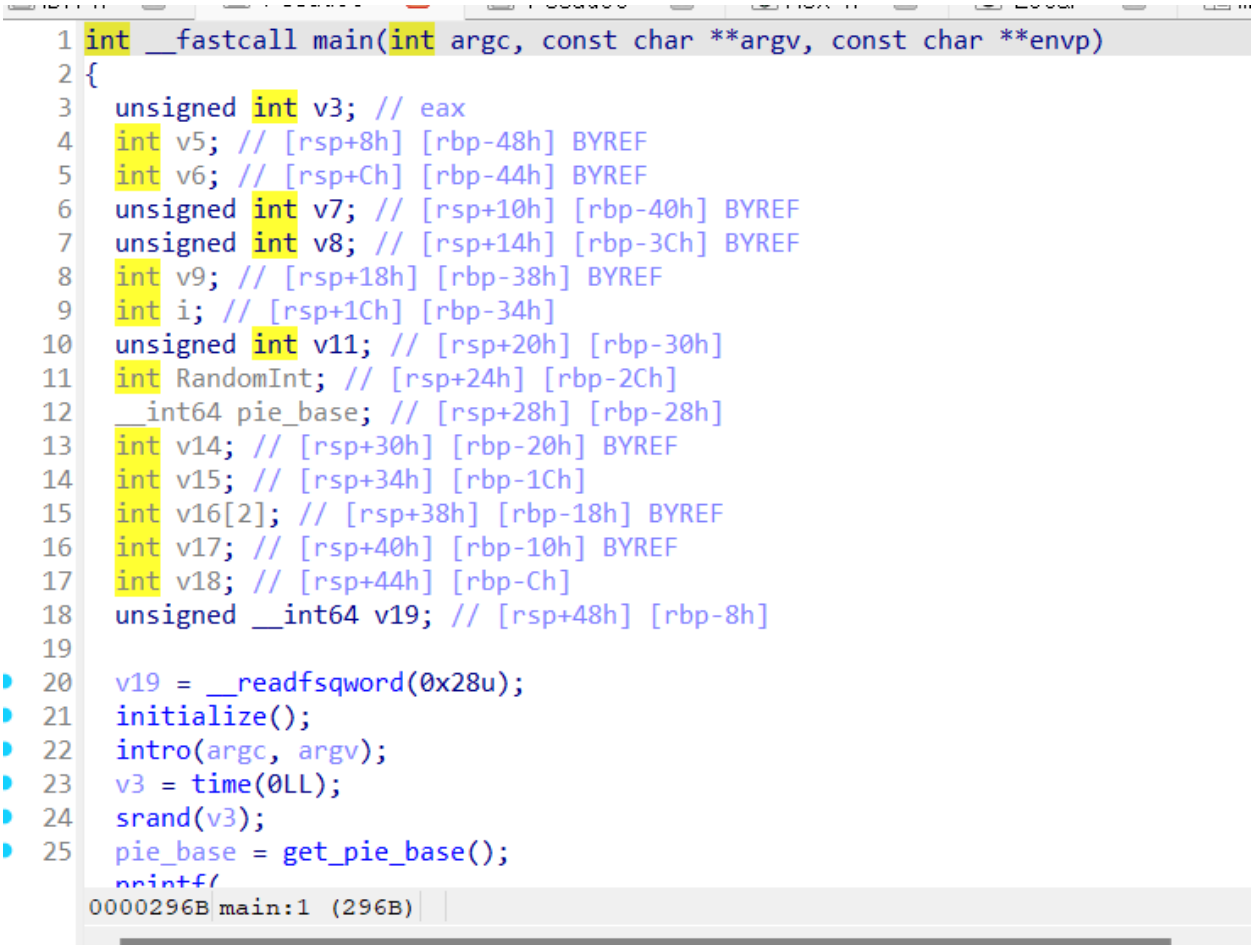
PokWemoN

태그	포너블
상태	진행 중



```
int __fastcall main(int argc, const char **argv, const char **envp)
{
  unsigned int v3; // eax
  int v5; // [rsp+8h] [rbp-48h] BYREF
  int v6; // [rsp+Ch] [rbp-44h] BYREF
  unsigned int v7; // [rsp+10h] [rbp-40h] BYREF
  unsigned int v8; // [rsp+14h] [rbp-3Ch] BYREF
  int v9; // [rsp+18h] [rbp-38h] BYREF
  int i; // [rsp+1Ch] [rbp-34h]
  unsigned int v11; // [rsp+20h] [rbp-30h]
  int RandomInt; // [rsp+24h] [rbp-2Ch]
  __int64 pie_base; // [rsp+28h] [rbp-28h]
  int v14; // [rsp+30h] [rbp-20h] BYREF
  int v15; // [rsp+34h] [rbp-1Ch]
  int v16[2]; // [rsp+38h] [rbp-18h] BYREF
  int v17; // [rsp+40h] [rbp-10h] BYREF
  int v18; // [rsp+44h] [rbp-Ch]
  unsigned __int64 v19; // [rsp+48h] [rbp-8h]

  v19 = __readfsqword(0x28u);
  initialize();
  intro(argc, argv);
  v3 = time(0LL);
  srand(v3);
  pie_base = get_pie_base();
  printf(
0000296B main:1 (296B)
```

IDA로 메인함수 디컴파일.

```
for ( i = 1; i <= 10; ++i )
{
  RandomInt = getRandomInt(0LL, 17LL);
  v16[0] = RandomInt;
  v16[1] = 10 * i;
  printf("\n================ Battle %d ================\n", (unsigned int)i);
  if ( i == 5 )
  {
    puts("\nMIDDLE BOSS: DRAGON FRUIT PIE");
    v17 = 14;
    v18 = 120;
    dragon_fruit_pie(&v14, &v17, &v7, &v9);
    puts("\n\nChoose the item(1.damage increase 2.health increase 3.opponent damage decrease 4. goods)");
    __isoc99_scanf("%d", &v6);
```

배틀 10 사이클 반복.

5번째에 보스전이 나온다.

```
__isoc99_scanf("%d", &v6);
switch ( v6 )
{
  case 1:
    v11 = getRandomInt(8LL, 13LL);
    v9 += v11;
    printf("%d Damage increase\n", v11);
    break;
  case 2:
    v8 = getRandomInt(10LL, 15LL);
    printf("%d Health increase\n", v8);
    break;
  case 3:
    v7 = getRandomInt(3LL, 5LL);
    printf("%d Opponent Damage Decrease\n", v7);
    break;
  case 4:
    puts("\n --------------");
    printf("|0x%lx|\n", pie_base);
    puts(" --------------\n");
    break;
}
```

보스전 승리 시 선택(입력값)에 따라 보상 증정.

4번 “goods”의 경우만 무언가 출력문이 복잡하다.

```
else if ( i == 10 )
{
  puts("\nFINAL BOSS: POISON BIRD");
  v17 = 7;
  v18 = 200;
  simulateBattle(&v14, &v17, &v7, &v9, &v8);
  record();
```

10턴에 최종보스전.

승리시 record();가 호출된다.

record();

```
unsigned __int64 record()
{
  char buf[40]; // [rsp+0h] [rbp-30h] BYREF
  unsigned __int64 v2; // [rsp+28h] [rbp-8h]

  v2 = __readfsqword(0x28u);
  puts("CONGRATUATION!!!!!");
  puts("YOU ARE THE PokWemoN CHAMPION");
  puts("________RANK________");
  puts("|1. KIM          9  |");
  puts("|2. MIN          9  |");
  puts("|3. ROKAF        9  |");
  puts("|4. GivMeInJ     8  |");
  puts("|5. JUN          7  |");
  puts("|                   |");
  puts("|___________________|");
  puts("ENTER YOUR NAME:");
  getchar();
  read(0, buf, 0x50uLL);
  puts("________RANK________");
  printf("|1.%s10|\n", buf);
  puts("|2. KIM          9  |");
  puts("|3. MIN          9  |");
  puts("|4. ROKAF        9  |");
  puts("|5. GivMeInJ     8  |");
  puts("|6. JUN          7  |");
  puts("|___________________|");
  puts("ENTER YOUR NAME:");
  getchar();
  return v2 - __readfsqword(0x28u);
}
```

입력받은 문자를 buf에 저장하고 랭킹에 출력. 다만 출력 뒤에도 이름을 묻는 입력문이 한번 더 나오는데, 그 이유는 모르겠다.

```
-0000000000000030
-0000000000000030 buf             db ?
-000000000000002F                 db ? ; undefined
-000000000000002E                 db ? ; undefined
-000000000000002D                 db ? ; undefined
```

```
-0000000000000009                db ? ; undefined
-0000000000000008 var_8          dq ?
+0000000000000000  s              db 8 dup(?)
+0000000000000008  r              db 8 dup(?)
+0000000000000010
+0000000000000010 ; end of stack variables
```

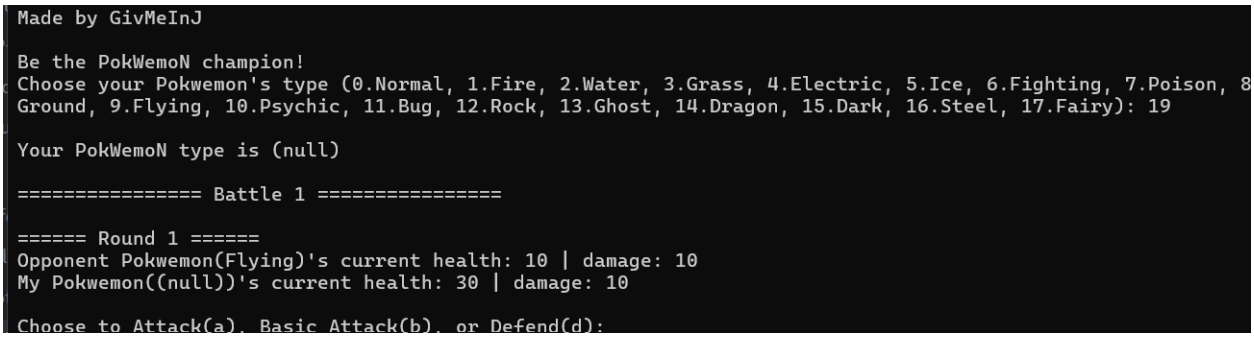
이름을 입력받는 버프의 용량은 여기까지. 혹시 버퍼오버플로우 공격을 하면 플래그가 출력이 될까?

그외 poison_bird 등 서브 함수들도 살펴봤는데, 특이점을 발견하진 못 하겠다.

실행 화면.

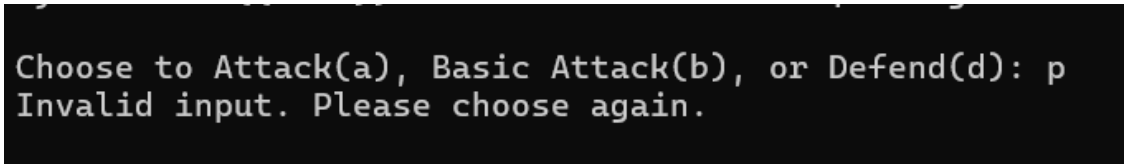
```
================ Battle 4 ================

====== Round 1 ======
Opponent Pokwemon(Fairy)'s current health: 40 | damage: 10
My Pokwemon(Dragon)'s current health: 18 | damage: 26

Choose to Attack(a), Basic Attack(b), or Defend(d): a

DAMAGE IS CRITICAL!!!!
Opponent Pokwemon attacked my Pokwemon! Damage: 20

NO DAMAGE...
My Pokwemon attacked the opponent Pokwemon! Damage: 0

== Health Bars ==
Opponent Pokwemon(Fairy): ========================================
My Pokwemon(Dragon):
```

플레이할 경우 정상적으로 플레이된다. 그러나 대부분의 경우 “드래곤”전인 5단계까지 도달하지 못 한다. 랜덤으로 배정되는 데미지/체력이 불리하게 설정된 것으로 추측.

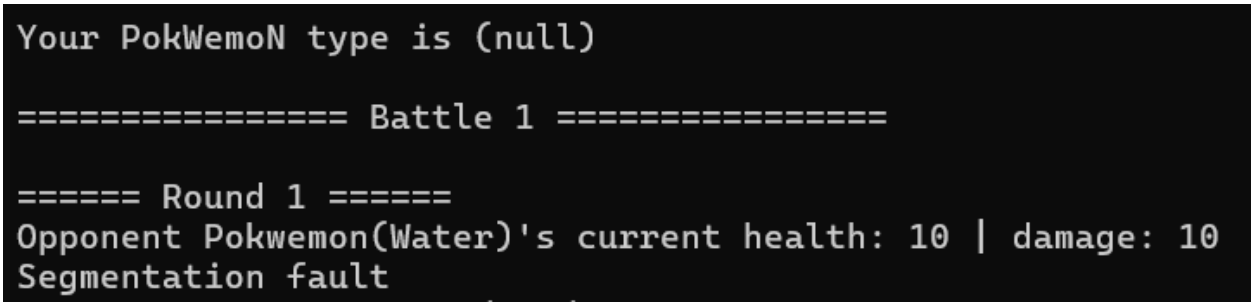


?

영역 밖의 포켓몬을 설정하자 null로 설정이 됐다.



잘못된 알파벳은 시정된다.

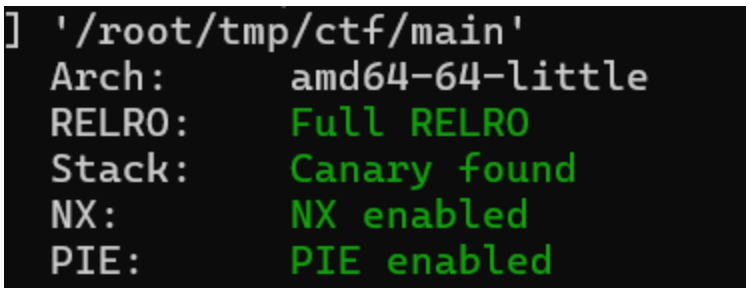


포켓몬 타입을 “-1”로 설정할 경우 segmentation fault 출력.

(할당 받지 못한 메모리 접근)

https://c0wb3ll.tistory.com/entry/메모리-보호-기법-NX-Bit

💡 checksec



stack canary found.

→ 스택 오버플로우 방지기법 감지.

full relro

→ 메모리 보호기법(read-only)

nx/pie 활성화

가능한 모든 메모리 보호기법이 활성화되어있다. 스택 오버플로우는 힘들지 않을까?