Báo cáo thực hành nhóm 11

Yêu cầu 1:

Ta dùng phím F5 để chuyển sang xem mã giả

```
1 int hardCode()
2 {
3   int result; // eax@2
4   char s1; // [sp+8h] [bp-3F0h]@1
5
6   getchar();
7   puts("Enter the hard-coded password (option 1):");
8   __isoc99_scanf("%[^\n]", &s1);
9   printf("Your input hard-coded password: %s\n", &s1);
0   if ( !strcmp(&s1, "Never offer to teach fish to swim") )
1     result = success_1();
2   else
3     result = failed();
4   return result;
5 }
```

Input là s1

Ở câu lệnh if nếu s1 giống chuỗi đó thì sẽ trả về thành công, ngược lại là thất bại

Suy ra pass: **Never offer to teach fish to swim**

Ta thử nhập pass là chuỗi trên và xem kết quả

```
thaont@ubuntu:~/Documents$ ./basic-reverse
Supported authentication methods:
1. Hard-coded password
2. A pair of 2 numbers
3. Username/password
Enter your choice: 1
Enter the hard-coded password (option 1):
Never offer to teach fish to swim
Your input hard-coded password: Never offer to teach fish to swim
Congrats! You found the hard-coded secret, good job :).
thaont@ubuntu:~/Documents$
```

Yêu cầu 2:

Dùng f5 chuyển sang mã giả

```
int otherhardCode()
{
  int v0; // edx@2
  int result; // eax@3
  int v2; // [sp+4h] [bp-14h]@1
  int v3; // [sp+8h] [bp-10h]@1
  int v4; // [sp+Ch] [bp-Ch]@1

  getchar();
  puts("Enter your 2 numbers (separated by space) (option 2):");
  __isoc99_scanf("%d %d", &v3, &v2);
  printf("Your input: %d %d\n", v3, v2);
  v4 = 7;
  if ( v3 == 7 )
  {
    v0 = funny_func(7, funny_seq[7]);
    if ( v0 == v2 )
      result = success_2();
    else
      result = failed();
  }
  else
  {
    result = failed();
  }
  return result;
}
```

```
int __cdecl funny_func(int a1, int a2)
{
  return a1 * (a1 + a2) + a2;
}
```

```
.rodata:08048B60 ; int funny_seq[10]
.rodata:08048B60 funny_seq       dd 0Ah
.rodata:08048B64                 db    3
.rodata:08048B65                 db    0
.rodata:08048B66                 db    0
.rodata:08048B67                 db    0
.rodata:08048B68                 db    6
.rodata:08048B69                 db    0
.rodata:08048B6A                 db    0
.rodata:08048B6B                 db    0
.rodata:08048B6C                 db    9
.rodata:08048B6D                 db    0
.rodata:08048B6E                 db    0
.rodata:08048B6F                 db    0
.rodata:08048B70                 db    1
.rodata:08048B71                 db    0
.rodata:08048B72                 db    0
.rodata:08048B73                 db    0
.rodata:08048B74                 db    4
.rodata:08048B75                 db    0
.rodata:08048B76                 db    0
.rodata:08048B77                 db    0
.rodata:08048B78                 db    7
.rodata:08048B79                 db    0
.rodata:08048B7A                 db    0
.rodata:08048B7B                 db    0
```

```
.rodata:08048B7C                 db    2
.rodata:08048B7D                 db    0
.rodata:08048B7E                 db    0
.rodata:08048B7F                 db    0
.rodata:08048B80                 db    5
.rodata:08048B81                 db    0
.rodata:08048B82                 db    0
.rodata:08048B83                 db    0
.rodata:08048B84                 db    8
.rodata:08048B85                 db    0
.rodata:08048B86                 db    0
.rodata:08048B87                 db    0
```

Ta có hai số cần tìm là v3 và v2. Ở câu lệnh if đầu tiên, nếu v3 != 7 thì chương tình trả về failed. Vậy suy ra input đầu tiên là **7**.
Tiếp theo ta có funny_seq[7]. Vì 1 phần tử là một số nguyên 4 byte, db là 1 byte, vậy ta đọc một lần 4 byte, vậy tại vị trí thứ 7 sẽ là 2000. Mà nó lưu dưới dạng Little Endian nên ta cần chuyển ngược lại là 0002. Vậy funny_seq[7] = 0002 = 2

Do đó 2 tham số truyền vào funny_func sẽ là 7 và 2. Từ đó ta tính được v0 = 7 * (7 + 2) + 2 = 65

Nêu v2 = v0 thì sẽ trả về thành công, từ đó suy ra v2 = 65.

Kết luận rằng 2 input sẽ là **7** và **65**
Ta thử kết quả:

```
thaont@ubuntu:~/Documents$ ./basic-reverse
Supported authentication methods:
1. Hard-coded password
2. A pair of 2 numbers
3. Username/password
Enter your choice: 2
Enter your 2 numbers (separated by space) (option 2):
7 65
Your input: 7 65
Congrats! You found a secret pair of numbers :).
thaont@ubuntu:~/Documents$
```

Yêu cầu 3:

Ta có mã giả

```
int userpass()
{
  size_t v0; // ebx@2
  int result; // eax@3
  long double v2; // fst7@13
  size_t v3; // eax@15
  size_t v4; // edx@16
  char v5[9]; // [sp+1Ah] [bp-2Eh]@6
  char v6[10]; // [sp+23h] [bp-25h]@1
  char s[10]; // [sp+2Dh] [bp-1Bh]@1
  char v8[5]; // [sp+37h] [bp-11h]@1
  unsigned int i; // [sp+3Ch] [bp-Ch]@4

  v8[0] = 33;
  v8[1] = 60;
  v8[2] = 55;
  v8[3] = 63;
  v8[4] = 97;
  getchar();
  puts("Enter your username:");
  __isoc99_scanf("%[^\n]", s);
  getchar();
  puts("Enter your password:");
  __isoc99_scanf("%[^\n]", v6);
  printf("Your input username: %s and password: %s\n", s, v6);
  if ( strlen(s) == 9 && (v0 = strlen(s), v0 == strlen(v6)) )
  {
    for ( i = 0; (signed int)i <= 8; ++i )
    {
      if ( (signed int)i > 1 )
      {
        if ( (signed int)i > 3 )
          v5[i] = v8[8 - i];
        else
          v5[i] = s[i + 2];
      }
      else
      {
        v5[i] = s[i + 5];
      }
    }
    for ( i = 0; ; ++i )
    {
      v3 = strlen(s);
      if ( v3 > i )
      {
        v2 = ceil((long double)((s[i] + v5[i]) / 2));
        if ( (long double)v6[i] == v2 )
          continue;
      }
      break;
    }
    v4 = strlen(s);
    if ( v4 == i )
      result = success_3();
    else
      result = failed();
  }
  else
  {
    result = failed();
  }
  return result;
}
```

3 thành viên nhóm có mssv lần lượt giảm dần là 22521371 - 22521190 - 22521181 vậy ta có username là **371190181**

Mã giả cho ta thấy được chương trình tính toán mảng v5 thông qua các giá trị của mảng v8 đã cho. Mã so sánh mật khẩu với v2 được tính toán thông qua công thức:

X = (giá trị của một phần tử v5 + giá trị của một phần tử username)/2

Sau đó trả về giá trị nhỏ nhất là lớn hơn X.
Từ mã giả ta có thể viết chương tình bằng ngôn ngữ C++ để tính toán được mật khẩu thuận tiện hơn.

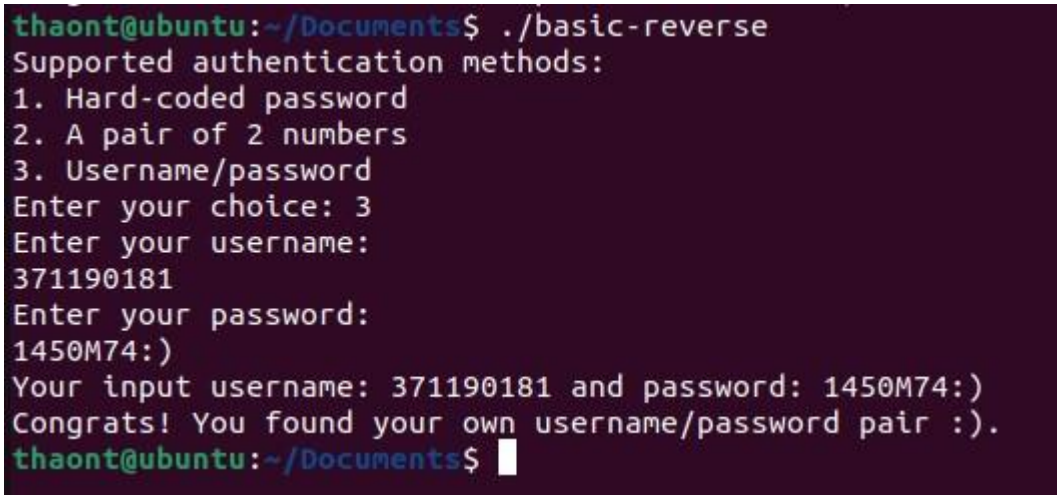
Source code

Password được tính: **1450M74:)**

```
Enter your username:371190181
1450M74:)
Process returned 0 (0x0)   execution time : 18.001 s
Press any key to continue.
```

Chạy code c++

Ta thử kết quả:


thaont@ubuntu:~/Documents$ ./basic-reverse
Supported authentication methods:
1. Hard-coded password
2. A pair of 2 numbers
3. Username/password
Enter your choice: 3
Enter your username:
371190181
Enter your password:
1450M74:)
Your input username: 371190181 and password: 1450M74:)
Congrats! You found your own username/password pair :).
thaont@ubuntu:~/Documents$