[pwnable.kr WriteUp]

이태규(ltg2030)

[Toddler's Bottle] blackjack 1PT

문제 설명

Hey! check out this C implementation of blackjack game!
I found it online
*
http://cboard.cprogramming.com/c-programming/114023-simple-blackjack-program.html

I like to give my flags to millionares.
how much money you got?

Running at : nc pwnable.kr 9009

문제 풀이(이론)

1. 먼저 백만장자가 되는 목표를 해결하기 위해 문제에서 주어진 소스 파일을 분석했다.

2. 소스 파일은 간단한 블랙잭 게임이며 betting 이라는 함수에서 취약점이 발생한다.

3.

```
int betting() //Asks user amount to bet
{
 printf("\n\nEnter Bet: $");
 scanf("%d", &bet);

 if (bet > cash) //If player tries to bet more money than player has
 {
          printf("\nYou cannot bet more money than you have.");
          printf("\nEnter Bet: ");
          scanf("%d", &bet);
          return bet;
 }
 else return bet;
}
```

이 함수에서 입력한 값으로 베팅을 하여 이기면 그 만큼 주고 지면 그만큼 뺏긴다. 하지만 이 함수에서 베팅금액의 제한을 cash보다 작거나 갖게 입력하는지 확인을 한번만 하고 그 다음 입력에 대해서는 제한을 확인하지 않는다. 따라서 cash가 500일 때 베팅을 1000000 하면 다시 입력하라는 얘기가 나올 것이고 그 때 다시 1000000을 입력하면 백만 달러가 베팅이 되어 한판만 이기면 백만장자가 되어 flag를 얻을 수 있다.

문제 풀이(실습)

[pwnable.kr WriteUp]

이태규(ltg2030)

```
YaY_I_AM_A_MILLIONARE_LOL


Cash: $1000500
-------
|C    |
|  9  |
|    C|
-------

Your Total is 9

The Dealer Has a Total of 6

Enter Bet: $
```

500달러가 있는 상태에서 백만달러를 걸고 게임에서 한판 승리한 결과 Cash가 1000500이 되었고 YaY_I_AM_A_MILLIONARE_LOL 이라는 flag를 얻었다.

실행화면