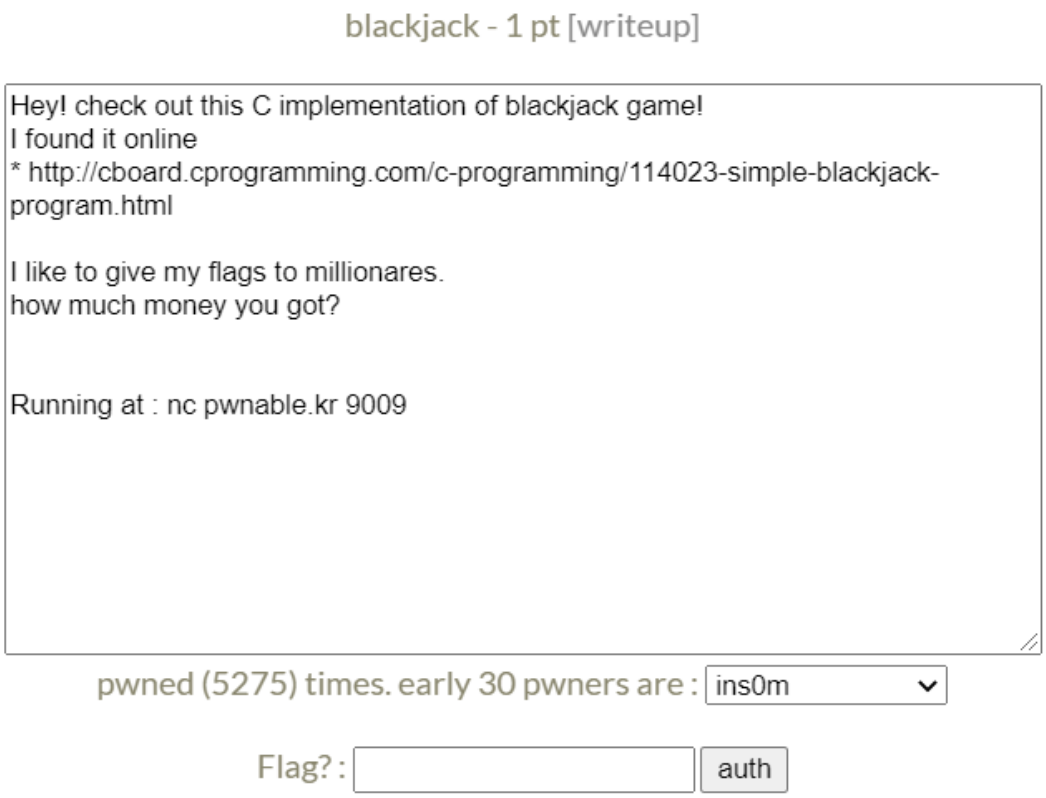
Pwnable.kr blackjack



문제에서 블랙잭 게임에 쓴 코드가 있는 주소를 알려주고 플래그를 100만장자가 되면 알려주겠다고 한다. 문제에 접속하면 즐거운 블랙잭 게임을 할 수 있는데 신들린 실력으로 100만을 모으거나 허점을 찾아야 한다.

코드를 보면 찾을 수 있을 것 같다. 100만을 모아야하니 돈과 관련된 것 혹은 게임에 관한 부분만 찾아보면 될 것이다.

```
void play() //Plays game
{

     int p=0; // holds value of player_total
     int i=1; // counter for asking user to hold or stay (aka game turns)
     char choice3;

     cash = cash;
     cash_test();
     printf("\nCash: $%d\n",cash); //Prints amount of cash user has
     randcard(); //Generates random card
     player_total = p + l; //Computes player total
     p = player_total;
     printf("\nYour Total is %d\n", p); //Prints player total
     dealer(); //Computes and prints dealer total
     betting(); //Prompts user to enter bet amount
```

여기까지 플레이에서 사전 돈이나 손패에 대한 부분이고 이 밑으로는 내 카드의 숫자가 어떻게 되는 지에 따른 게임이므로 크게 신경 쓸 필요가 없다 여기 나온 함수만 보면 될 듯 하다.

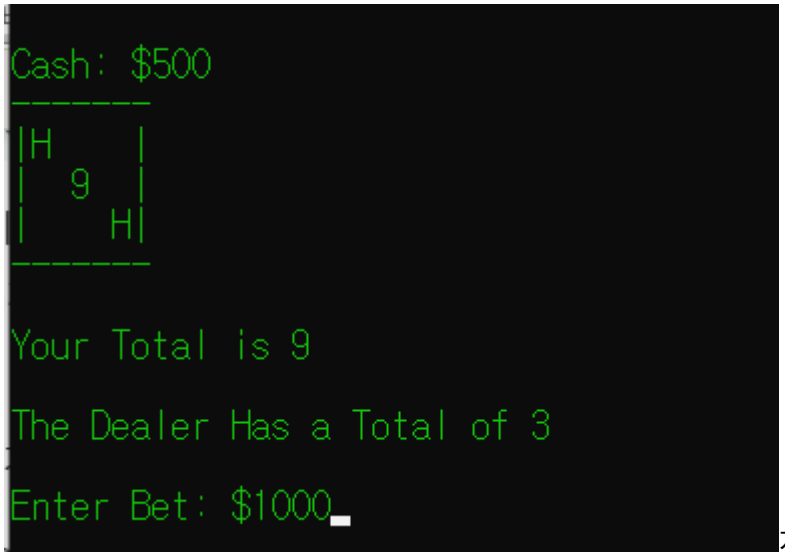
Cash_test(), randcard(), dealer(), betting() 함수 중 우리가 공략할 부분이 있을 것이다.

Cash_test()는 그저 플레이가 가능한 지 확인하는 함수이고 randcard()와 dealer() 함수에서 카드를 배분할 때 srand()함수를 사용하므로 완전 랜덤이라 공략이 안 된다.

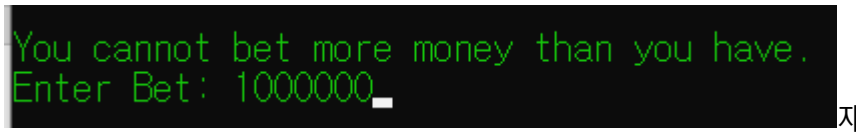
```
int betting() //Asks user amount to bet
{
 printf("\n\nEnter Bet: $");
 scanf("%d", &bet);

 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;
} // End Function
```

Betting()을 보면 처음에 베팅할 때 가진 돈보다 큰 경우 재입력을 받고 재입력 값에 대한 검증없이 바로 리턴한다. 이 부분을 공략하면 될 듯 하다.

처음에 가진 돈보다 많이 입력하고 재입력할 때 100만을 입력 후 이기면 될 것이다.

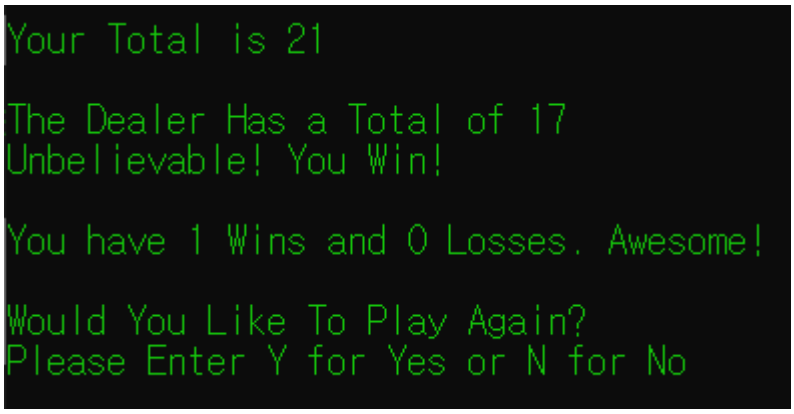


처음 500달러 소유, 1000입력

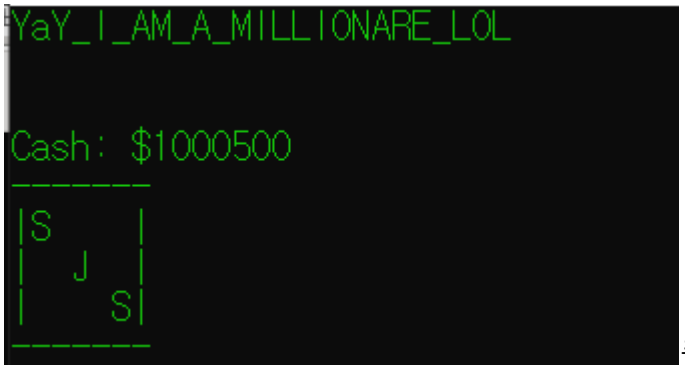


재입력에서 100만 입력

이후 이길 때 까지 반복



깔끔한 승리 이후 Y입력



플래그가 출력됩니다.