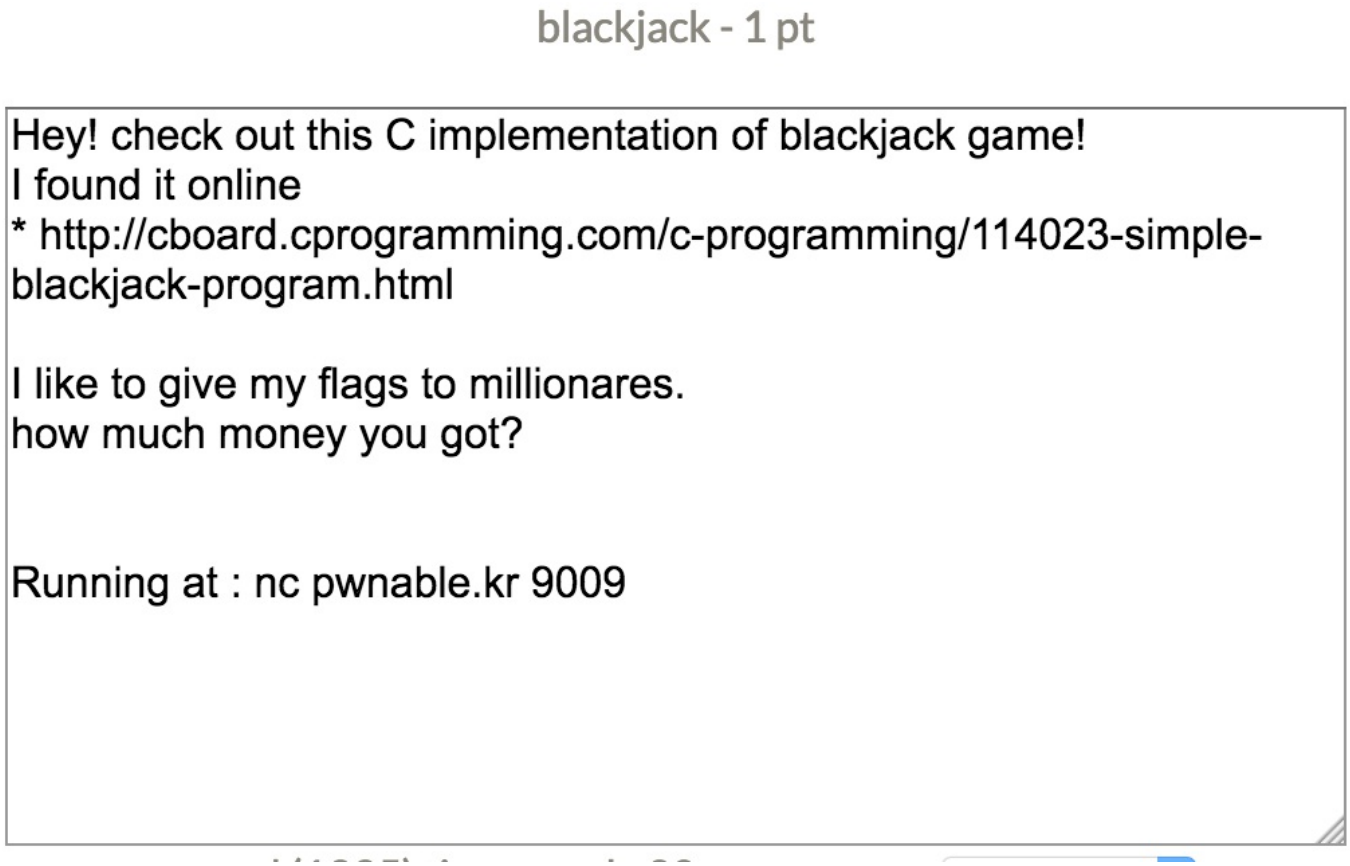
2017.7.25.

Sungkyu Cho - sungkyu1.cho@gmail.com

PWNABLE KR - TODDLER - blackjack - 1pt

보통은 flag를 읽도록 시스템 구성을 우회하는 문제를 봐왔는데, 이번에는 그냥 nc로 서버에 접속해보라고하는 게 전부였음



분명히 1pt이기 때문에 쉬운 문제일 거 같긴한데 ~~나한테는 어려워도~~ 사실 처음에 어떻게 접근해야 하나 많이 난감했음. ~~늘 그랬나..~~

0.우선은 소스코드 살펴보기

nc 로 접속해봤자 줄창 게임만 하게되고, 처음 홈페이지에서 제시하는 링크로 접속해서 살펴보기로 함.

블랙잭 소스코드 링크

- 소스코드는 그냥 모듈화해서 그럭저럭 잘 읽히는 편이고, 게임을 한번 해보면 대충 무슨 코드인지 더 잘 알겠는데.
- 일단은 기존처럼 flag를 읽는 것이라 생각하고, `nc` 명령어를 살펴봄

  netcat 사용법 링크

- `-o` 옵션으로 주고받는 패킷도 살펴보고 ~~혹시 숨겨진 게 있을까~~ `-l` 로 리버스 쉘을 걸어야 하나 ~~될 리가 없잖아~~ 이것 저것 해봤지만 실패

- 입력값도 잘 처리하는 거 같아서, 버퍼가 넘칠 부분이 잘 보이지를 않았는데..

```
YaY_I_AM_A_MILLIONARE_LOL


Cash: $1783794164
-------
|C    |
|  J  |
|    C|
-------

Your Total is 10

The Dealer Has a Total of 6

Enter Bet: $
```

```
} // End Function

void cash_test() //Test for if user has cash remaining in p
urse
{
     if (cash <= 0) //Once user has zero remaining cash, ga
me ends and prompts user to play again
     {
        printf("You Are Bankrupt. Game Over");
        cash = 500;
        askover();
     }
} // End Function

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 p
layer has
 {
        printf("\nYou cannot bet more money than you have."
);
        printf("\nEnter Bet: ");
        scanf("%d", &bet);
        return bet;
 }
 else return bet;
} // End Function
```

- 갑자기 성공하고 말았다 - _ -;;

1.Check it up

문제는 `betting()` 함수였는데. 대충봐도 뭔가 이상하다.금액이 잔금이랑 맞지 않으면 체크하는 것까지는 좋은데, 대충봐도 **계속 체크해야 하는 루틴이 없이** 그냥 한번 `cash`와 비교하고 넘어가고는 값을 return 해버리고 있다.

```
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
```

- 실제로 `bet` 변수는 전역변수로 선언이 되어 있으며, 배팅 금액을 입력받은 후 -> 가진 금액보다 작으면 다시 입력받고 -> 그리고 끝남.

- 재입력값을 다시는 체크하는 루틴이 어디에도 없음

- 마지막으로, 그 재입력값 `bet`이 승리했을 때는 기존의 자금 `cash`와 더해져서 `cash = cash + bet`이지만, 지면 `cash = cash - bet`이기 때문에. 이겨야 한다. **(이점을 이용하면, bet을 음수로 하면 져도 된다)**

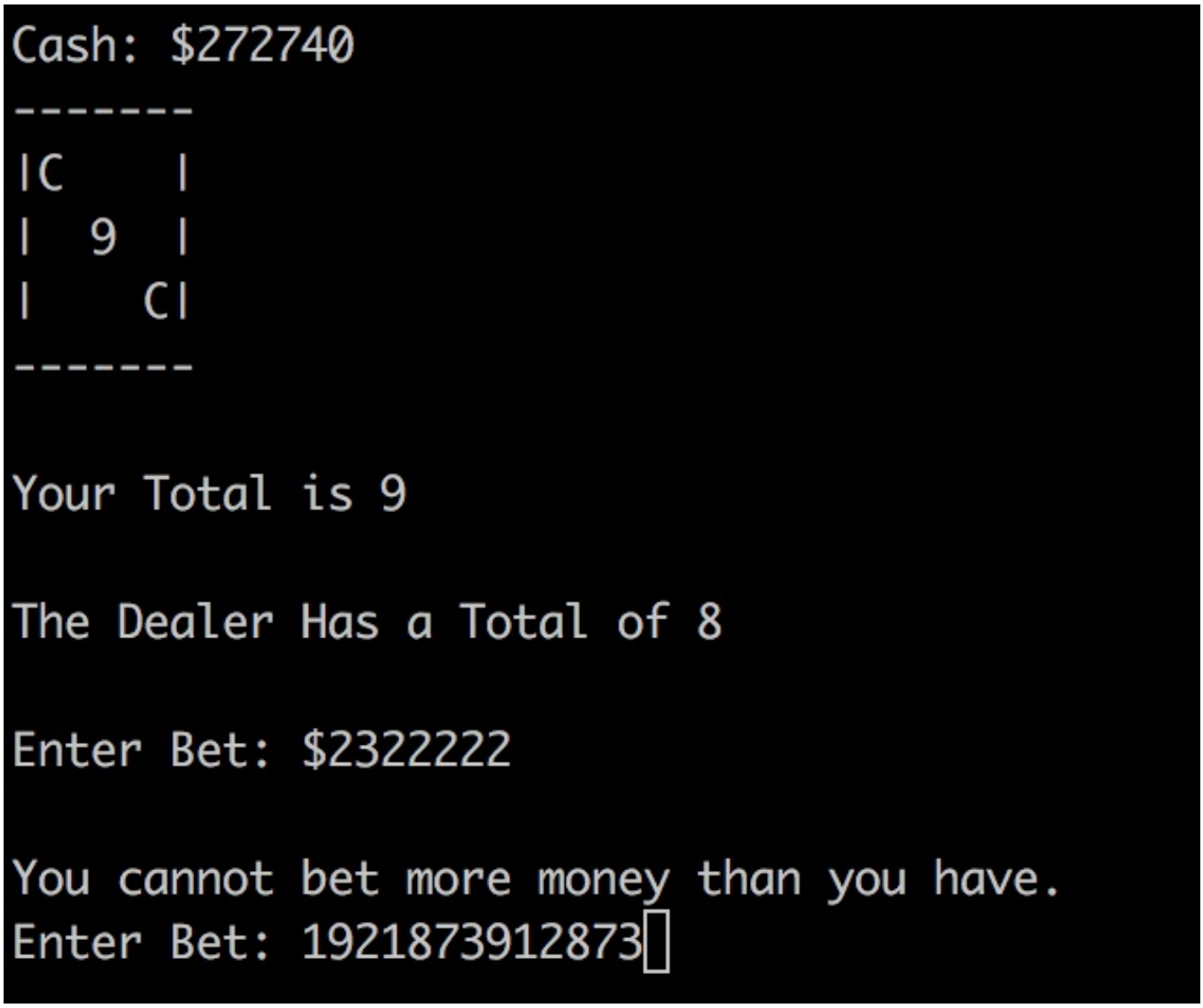
```
if (bet > cash) //If player tries to bet more money than player has search hit BOTTOM, con

  if((choice1 == 'Y') || (choice1 == 'y')) // If yes, continue. Prints menu.
  h
You Win!\n");
            won = won+1;
            cash = cash+bet;
            printf("\nYou have %d Wins and %d Losses. Awesome!\n", won, loss);
            dealer_total=0;
            askover();
        }

        if(p>21) //If player total is over 21, loss
        {
            printf("\nWoah Buddy, You Went WAY over.\n");
            loss = loss+1;
            cash = cash - bet;
            printf("\nYou have %d Wins and %d Losses. Awesome!\n", won, loss);
            dealer_total=0;
            askover();
        }
```

2. Exploit

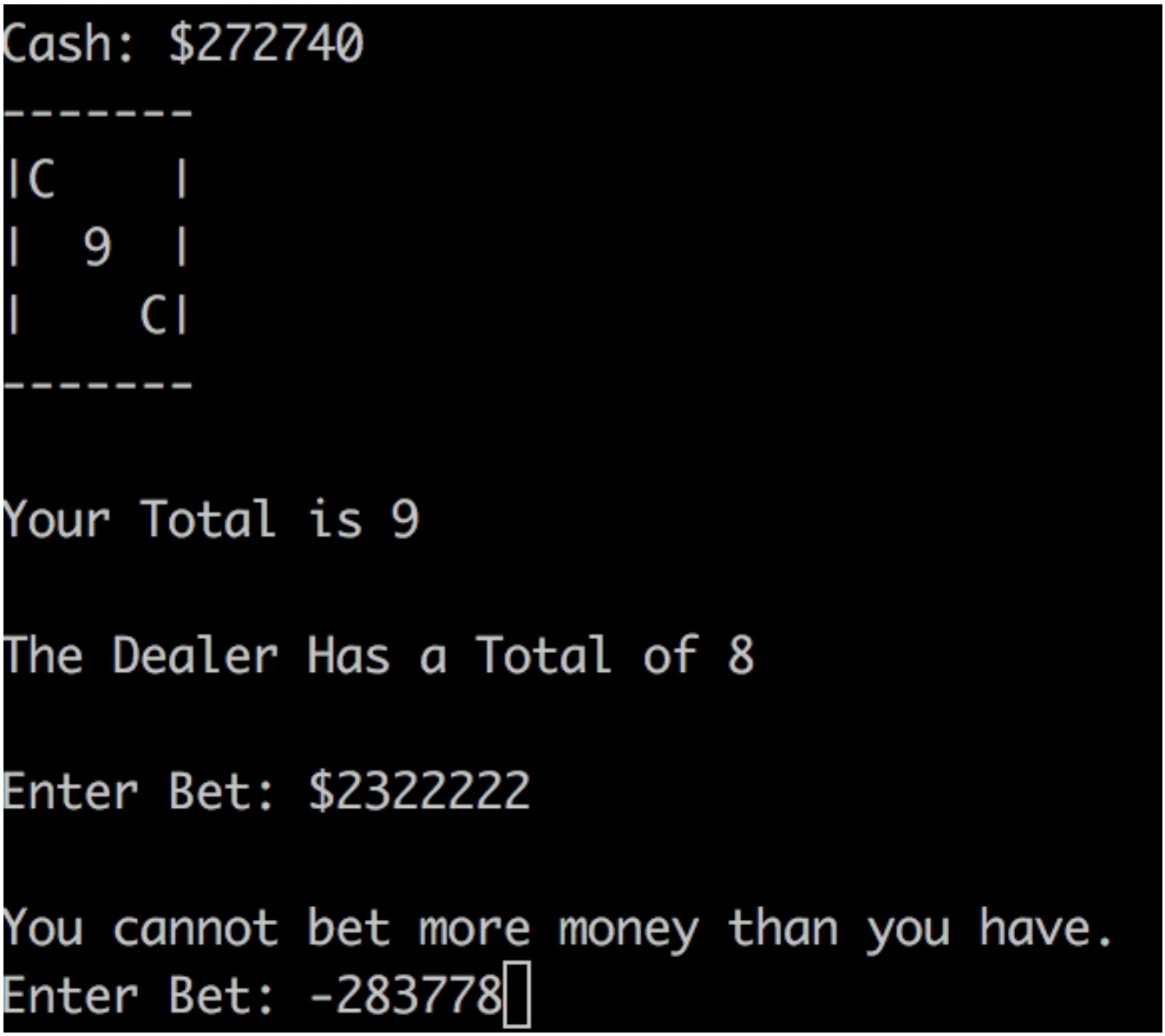
- 걍 두 번째 입력받을 때 굉장히 큰 수를 집어넣으면 끝
- 이러고 이기거나


Cash: $272740

|C |
| 9 |
| C|

Your Total is 9
The Dealer Has a Total of 8
Enter Bet: $2322222
You cannot bet more money than you have.
Enter Bet: 1921873912873

- 이러고 지거나


Cash: $272740

|C |
| 9 |
| C|

Your Total is 9
The Dealer Has a Total of 8
Enter Bet: $2322222
You cannot bet more money than you have.
Enter Bet: -283778