pwnable.kr-balckjack-Writeup

转载

baikeng3674 于 2017-02-16 08:19:00 发布 55 收藏
原文链接：http://www.cnblogs.com/WangAoBo/p/6404135.html

MarkdownPad Document

pwnable.kr-balckjack-Writeup

该题的代码奇长无比（788行）但题挺容易，并且比较有意思

> 首先从提供的网址https://cboard.cprogramming.com/c-programming/114023-simple-blackjack-program.html查看该题用到的代码如下：

```
// Programmer: Vladislav Shulman
// Final Project
// Blackjack

// Feel free to use any and all parts of this program and claim it as your own work

//FINAL DRAFT

#include <stdlib.h>
#include <stdio.h>
#include <math.h>
#include <time.h>                //Used for srand((unsigned) time(NULL)) command
#include <process.h>             //Used for system("cls") command

#define spade 06                 //Used to print spade symbol
#define club 05                  //Used to print club symbol
#define diamond 04               //Used to print diamond symbol
#define heart 03                 //Used to print heart symbol
#define RESULTS "Blackjack.txt"  //File name is Blackjack

//Global Variables
int k;
int l;
int d;
int won;
int loss;
int cash = 500;
int bet;
int random_card;
int player_total=0;
int dealer_total;

//Function Prototypes
int clubcard();      //Displays Club Card Image
int diamondcard();   //Displays Diamond Card Image
int heartcard();     //Displays Heart Card Image
int spadecard();     //Displays Spade Card Image
int randcard();      //Generates random card
int betting();       //Asks user amount to bet
void asktitle();     //Asks user to continue
```

```
41 void rules();        //Prints "Rules of Vlad's Blackjack" menu
42 void play();         //Plays game
43 void dealer();       //Function to play for dealer AI
44 void stay();         //Function for when user selects 'Stay'
45 void cash_test();    //Test for if user has cash remaining in purse
46 void askover();      //Asks if user wants to continue playing
47 void fileresults();  //Prints results into Blackjack.txt file in program directory
48
49 //Main Function
50 int main(void)
51 {
52     int choice1;
53     printf("\n");
54     printf("\n");
55     printf("\n");
56     printf("\n              222               111                              ");
57     printf("\n            222 222            11111                               ");
58     printf("\n           222   222          11 111                              ");
59     printf("\n                222             111                                 ");
60     printf("\n               222              111                             ");
61     printf("\n");
62     printf("\n%c%c%c%c%c     %c%c            %c%c         %c%c%c%c%c    %c    %c                ",
club, club, club, club, club, spade, spade, diamond, diamond, heart, heart, heart, heart, heart, club,
club);
63     printf("\n%c    %c    %c%c           %c  %c       %c     %c   %c   %c              ", club,
club, spade, spade, diamond, diamond, heart, heart, club, club);
64     printf("\n%c    %c    %c%c          %c    %c     %c          %c  %c               ", club, club,
spade, spade, diamond, diamond, heart, club, club);
65     printf("\n%c%c%c%c%c     %c%c          %c %c%c %c     %c          %c %c              ", club,
club, club, club, club, spade, spade, diamond, diamond, diamond, diamond, heart, club, club);
66     printf("\n%c    %c    %c%c         %c %c%c%c%c %c    %c          %c%c %c             ", club,
club, spade, spade, diamond, diamond, diamond, diamond, diamond, diamond, heart, club, club, club);
67     printf("\n%c     %c   %c%c         %c      %c    %c          %c   %c               ", club,
club, spade, spade, diamond, diamond, heart, club, club);
68     printf("\n%c     %c   %c%c        %c        %c    %c     %c   %c    %c             ", club,
club, spade, spade, diamond, diamond, heart, heart, club, club);
69     printf("\n%c%c%c%c%c%c    %c%c%c%c%c%c%c   %c        %c     %c%c%c%c%c    %c     %c
", club, club, club, club, club, club, spade, spade, spade, spade, spade, spade, spade, diamond,
diamond, heart, heart, heart, heart, heart, club, club);
70     printf("\n");
71     printf("\n                        21                                    ");
72
73     printf("\n     %c%c%c%c%c%c%c%c      %c%c         %c%c%c%c%c    %c    %c               ",
diamond, diamond, diamond, diamond, diamond, diamond, diamond, diamond, heart, heart, club, club, club,
club, club, spade, spade);
74     printf("\n        %c%c        %c  %c       %c     %c   %c   %c             ", diamond, diamond,
heart, heart, club, club, spade, spade);
75     printf("\n        %c%c       %c    %c     %c          %c  %c              ", diamond, diamond,
heart, heart, club, spade, spade);
76     printf("\n        %c%c       %c %c%c %c     %c          %c %c             ", diamond, diamond,
heart, heart, heart, heart, club, spade, spade);
77     printf("\n        %c%c      %c %c%c%c%c %c    %c          %c%c %c             ", diamond,
diamond, heart, heart, heart, heart, heart, heart, club, spade, spade, spade);
78     printf("\n        %c%c      %c      %c    %c          %c   %c              ", diamond, diamond,
heart, heart, club, spade, spade);
79     printf("\n     %c  %c%c     %c        %c    %c     %c   %c    %c             ", diamond,
diamond, diamond, heart, heart, club, spade, spade);
80     printf("\n      %c%c%c      %c        %c     %c%c%c%c%c    %c     %c            ", diamond,
diamond, diamond, heart, heart, club, club, club, club, club, spade, spade);
```

```
81      printf("\n");
82      printf("\n         222                    111                          ");
83      printf("\n        222                     111                          ");
84      printf("\n       222                      111                          ");
85      printf("\n      222222222222222      111111111111111                      ");
86      printf("\n      2222222222222222    11111111111111111                        ");
87      printf("\n");
88      printf("\n");
89
90      asktitle();
91
92      printf("\n");
93      printf("\n");
94      system("pause");
95      return(0);
96  } //end program
97
98  void asktitle() // Function for asking player if they want to continue
99  {
100     char choice1;
101     int choice2;
102
103      printf("\n                Are You Ready?");
104      printf("\n               ----------------");
105      printf("\n                     (Y/N)\n                        ");
106      scanf("\n%c",&choice1);
107
108     while((choice1!='Y') && (choice1!='y') && (choice1!='N') && (choice1!='n')) // If invalid choice
entered
109     {
110         printf("\n");
111         printf("Incorrect Choice. Please Enter Y for Yes or N for No.\n");
112         scanf("%c",&choice1);
113     }
114
115
116     if((choice1 == 'Y') || (choice1 == 'y')) // If yes, continue. Prints menu.
117     {
118             system("cls");
119             printf("\nEnter 1 to Begin the Greatest Game Ever Played.");
120             printf("\nEnter 2 to See a Complete Listing of Rules.");
121             printf("\nEnter 3 to Exit Game. (Not Recommended)");
122             printf("\nChoice: ");
123             scanf("%d", &choice2); // Prompts user for choice
124             if((choice2<1) || (choice2>3)) // If invalid choice entered
125             {
126                 printf("\nIncorrect Choice. Please enter 1, 2 or 3\n");
127                 scanf("%d", &choice2);
128             }
129             switch(choice2) // Switch case for different choices
130             {
131                 case 1: // Case to begin game
132                    system("cls");
133
134                    play();
135
136                    break;
137
138                 case 2: // Case to see rules
139                    system("cls");
```

```
                    rules();
                    break;

                case 3: // Case to exit game
                    printf("\nYour day could have been perfect.");
                    printf("\nHave an almost perfect day!\n\n");
                    system("pause");
                    exit(0);
                    break;

                default:
                    printf("\nInvalid Input");
            } // End switch case
    } // End if loop



    else if((choice1 == 'N') || (choice1 == 'n')) // If no, exit program
    {
        printf("\nYour day could have been perfect.");
        printf("\nHave an almost perfect day!\n\n");
        system("pause");
        exit(0);
    }

    return;
} // End function

void rules() //Prints "Rules of Vlad's Blackjack" list
{
     char choice1;
     int choice2;

     printf("\n           RULES of VLAD's BLACKJACK");
     printf("\n          --------------------------");
     printf("\nI.");
     printf("\n     Thou shalt not question the odds of this game.");
     printf("\n      %c This program generates cards at random.", spade);
     printf("\n      %c If you keep losing, you are very unlucky!\n", diamond);

     printf("\nII.");
     printf("\n     Each card has a value.");
     printf("\n      %c Number cards 1 to 10 hold a value of their number.", spade);
     printf("\n      %c J, Q, and K cards hold a value of 10.", diamond);
     printf("\n      %c Ace cards hold a value of 11", club);
     printf("\n     The goal of this game is to reach a card value total of 21.\n");

     printf("\nIII.");
     printf("\n     After the dealing of the first two cards, YOU must decide whether to HIT or
STAY.");
     printf("\n      %c Staying will keep you safe, hitting will add a card.", spade);
     printf("\n     Because you are competing against the dealer, you must beat his hand.");
     printf("\n     BUT BEWARE!.");
     printf("\n      %c If your total goes over 21, you will LOSE!.", diamond);
     printf("\n     But the world is not over, because you can always play again.\n");
     printf("\n%c%c%c YOUR RESULTS ARE RECORDED AND FOUND IN SAME FOLDER AS PROGRAM %c%c%c\n",
spade, heart, club, club, heart, spade);
     printf("\nWould you like to go the previous screen? (I will not take NO for an answer)");
     printf("\n                  (Y/N)\n                    ");
```

```
197      scanf("\n%c",&choice1);
198
199      while((choice1!='Y') && (choice1!='y') && (choice1!='N') && (choice1!='n')) // If invalid
choice entered
200     {
201         printf("\n");
202         printf("Incorrect Choice. Please Enter Y for Yes or N for No.\n");
203         scanf("%c",&choice1);
204     }
205
206
207     if((choice1 == 'Y') || (choice1 == 'y')) // If yes, continue. Prints menu.
208     {
209             system("cls");
210             asktitle();
211     } // End if loop
212
213
214
215     else if((choice1 == 'N') || (choice1 == 'n')) // If no, convinces user to enter yes
216     {
217         system("cls");
218         printf("\n                I told you so.\n");
219         asktitle();
220     }
221
222     return;
223 } // End function
224
225 int clubcard() //Displays Club Card Image
226 {
227
228
229     srand((unsigned) time(NULL)); //Generates random seed for rand() function
230     k=rand()%13+1;
231
232     if(k<=9) //If random number is 9 or less, print card with that number
233     {
234     //Club Card
235     printf("-------\n");
236     printf("|%c    |\n", club);
237     printf("|  %d  |\n", k);
238     printf("|    %c|\n", club);
239     printf("-------\n");
240     }
241
242
243     if(k==10) //If random number is 10, print card with J (Jack) on face
244     {
245     //Club Card
246     printf("-------\n");
247     printf("|%c    |\n", club);
248     printf("|  J  |\n");
249     printf("|    %c|\n", club);
250     printf("-------\n");
251     }
252
253
254     if(k==11) //If random number is 11, print card with A (Ace) on face
255     {
```

```
    {
    //Club Card
    printf("-------\n");
    printf("|%c    |\n", club);
    printf("|  A  |\n");
    printf("|    %c|\n", club);
    printf("-------\n");
    if(player_total<=10) //If random number is Ace, change value to 11 or 1 depending on dealer
total
         {
             k=11;
         }

         else
         {

             k=1;
         }
    }


    if(k==12) //If random number is 12, print card with Q (Queen) on face
    {
    //Club Card
    printf("-------\n");
    printf("|%c    |\n", club);
    printf("|  Q  |\n");
    printf("|    %c|\n", club);
    printf("-------\n");
    k=10; //Set card value to 10
    }


    if(k==13) //If random number is 13, print card with K (King) on face
    {
    //Club Card
    printf("-------\n");
    printf("|%c    |\n", club);
    printf("|  K  |\n");
    printf("|    %c|\n", club);
    printf("-------\n");
    k=10; //Set card value to 10
    }
    return k;
}// End function

int diamondcard() //Displays Diamond Card Image
{


    srand((unsigned) time(NULL)); //Generates random seed for rand() function
    k=rand()%13+1;

    if(k<=9) //If random number is 9 or less, print card with that number
    {
    //Diamond Card
    printf("-------\n");
    printf("|%c    |\n", diamond);
    printf("|  %d  |\n", k);
    printf("|    %c|\n", diamond);
```

```
314     printf("-------\n");
315     }
316 
317     if(k==10) //If random number is 10, print card with J (Jack) on face
318     {
319     //Diamond Card
320     printf("-------\n");
321     printf("|%c    |\n", diamond);
322     printf("|  J  |\n");
323     printf("|    %c|\n", diamond);
324     printf("-------\n");
325     }
326 
327     if(k==11) //If random number is 11, print card with A (Ace) on face
328     {
329     //Diamond Card
330     printf("-------\n");
331     printf("|%c    |\n", diamond);
332     printf("|  A  |\n");
333     printf("|    %c|\n", diamond);
334     printf("-------\n");
335     if(player_total<=10) //If random number is Ace, change value to 11 or 1 depending on dealer
total
336         {
337             k=11;
338         }
339 
340         else
341         {
342             k=1;
343         }
344     }
345 
346     if(k==12) //If random number is 12, print card with Q (Queen) on face
347     {
348     //Diamond Card
349     printf("-------\n");
350     printf("|%c    |\n", diamond);
351     printf("|  Q  |\n");
352     printf("|    %c|\n", diamond);
353     printf("-------\n");
354     k=10; //Set card value to 10
355     }
356 
357     if(k==13) //If random number is 13, print card with K (King) on face
358     {
359     //Diamond Card
360     printf("-------\n");
361     printf("|%c    |\n", diamond);
362     printf("|  K  |\n");
363     printf("|    %c|\n", diamond);
364     printf("-------\n");
365     k=10; //Set card value to 10
366     }
367     return k;
368 }// End function
369 
370 int heartcard() //Displays Heart Card Image
371 {
372 
```

```
372
373
374     srand((unsigned) time(NULL)); //Generates random seed for rand() function
375     k=rand()%13+1;
376
377     if(k<=9) //If random number is 9 or less, print card with that number
378     {
379     //Heart Card
380     printf("-------\n");
381     printf("|%c    |\n", heart);
382     printf("|  %d  |\n", k);
383     printf("|    %c|\n", heart);
384     printf("-------\n");
385     }
386
387     if(k==10) //If random number is 10, print card with J (Jack) on face
388     {
389     //Heart Card
390     printf("-------\n");
391     printf("|%c    |\n", heart);
392     printf("|  J  |\n");
393     printf("|    %c|\n", heart);
394     printf("-------\n");
395     }
396
397     if(k==11) //If random number is 11, print card with A (Ace) on face
398     {
399     //Heart Card
400     printf("-------\n");
401     printf("|%c    |\n", heart);
402     printf("|  A  |\n");
403     printf("|    %c|\n", heart);
404     printf("-------\n");
405     if(player_total<=10) //If random number is Ace, change value to 11 or 1 depending on dealer
total
406          {
407              k=11;
408          }
409
410          else
411          {
412              k=1;
413          }
414     }
415
416     if(k==12) //If random number is 12, print card with Q (Queen) on face
417     {
418     //Heart Card
419     printf("-------\n");
420     printf("|%c    |\n", heart);
421     printf("|  Q  |\n");
422     printf("|    %c|\n", heart);
423     printf("-------\n");
424     k=10; //Set card value to 10
425     }
426
427     if(k==13) //If random number is 13, print card with K (King) on face
428     {
429     //Heart Card
430     printf("-------\n");
```

```
431     printf("|%c    |\n", heart);
432     printf("|  K  |\n");
433     printf("|    %c|\n", heart);
434     printf("-------\n");
435     k=10; //Set card value to 10
436     }
437     return k;
438 } // End Function
439
440 int spadecard() //Displays Spade Card Image
441 {
442
443
444     srand((unsigned) time(NULL)); //Generates random seed for rand() function
445     k=rand()%13+1;
446
447     if(k<=9) //If random number is 9 or less, print card with that number
448     {
449     //Spade Card
450     printf("-------\n");
451     printf("|%c    |\n", spade);
452     printf("|  %d  |\n", k);
453     printf("|    %c|\n", spade);
454     printf("-------\n");
455     }
456
457     if(k==10) //If random number is 10, print card with J (Jack) on face
458     {
459     //Spade Card
460     printf("-------\n");
461     printf("|%c    |\n", spade);
462     printf("|  J  |\n");
463     printf("|    %c|\n", spade);
464     printf("-------\n");
465     }
466
467     if(k==11) //If random number is 11, print card with A (Ace) on face
468     {
469     //Spade Card
470     printf("-------\n");
471     printf("|%c    |\n", spade);
472     printf("|  A  |\n");
473     printf("|    %c|\n", spade);
474     printf("-------\n");
475     if(player_total<=10) //If random number is Ace, change value to 11 or 1 depending on dealer
total
476         {
477             k=11;
478         }
479
480         else
481         {
482             k=1;
483         }
484     }
485
486     if(k==12) //If random number is 12, print card with Q (Queen) on face
487     {
488     //Spade Card
489     printf("-------\n");
```

```
    printf("-------\n");
    printf("|%c    |\n", spade);
    printf("|  Q  |\n");
    printf("|    %c|\n", spade);
    printf("-------\n");
    k=10; //Set card value to 10
    }

    if(k==13) //If random number is 13, print card with K (King) on face
    {
    //Spade Card
    printf("-------\n");
    printf("|%c    |\n", spade);
    printf("|  K  |\n");
    printf("|    %c|\n", spade);
    printf("-------\n");
    k=10; //Set card value to 10
    }
    return k;
} // End Function

int randcard() //Generates random card
{


     srand((unsigned) time(NULL)); //Generates random seed for rand() function
     random_card = rand()%4+1;

     if(random_card==1)
     {
         clubcard();
         l=k;
     }

     if(random_card==2)
     {
         diamondcard();
         l=k;
     }

     if(random_card==3)
     {
         heartcard();
         l=k;
     }

     if(random_card==4)
     {
         spadecard();
         l=k;
     }
     return l;
} // End Function

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;
```

```
549
550     cash = cash;
551     cash_test();
552     printf("\nCash: $%d\n",cash); //Prints amount of cash user has
553     randcard(); //Generates random card
554     player_total = p + l; //Computes player total
555     p = player_total;
556     printf("\nYour Total is %d\n", p); //Prints player total
557     dealer(); //Computes and prints dealer total
558     betting(); //Prints user to enter bet amount
559
560     while(i<=21) //While loop used to keep asking user to hit or stay at most twenty-one times
561                  //  because there is a chance user can generate twenty-one consecutive 1's
562     {
563         if(p==21) //If user total is 21, win
564         {
565             printf("\nUnbelievable! You Win!\n");
566             won = won+1;
567             cash = cash+bet;
568             printf("\nYou have %d Wins and %d Losses. Awesome!\n", won, loss);
569             dealer_total=0;
570             askover();
571         }
572
573         if(p>21) //If player total is over 21, loss
574         {
575             printf("\nWoah Buddy, You Went WAY over.\n");
576             loss = loss+1;
577             cash = cash - bet;
578             printf("\nYou have %d Wins and %d Losses. Awesome!\n", won, loss);
579             dealer_total=0;
580             askover();
581         }
582
583         if(p<=21) //If player total is less than 21, ask to hit or stay
584         {
585             printf("\n\nWould You Like to Hit or Stay?");
586
587             scanf("%c", &choice3);
588             while((choice3!='H') && (choice3!='h') && (choice3!='S') && (choice3!='s')) // If
invalid choice entered
589             {
590                 printf("\n");
591                 printf("Please Enter H to Hit or S to Stay.\n");
592                 scanf("%c",&choice3);
593             }
594
595
596             if((choice3=='H') || (choice3=='h')) // If Hit, continues
597             {
598                 randcard();
599                 player_total = p + l;
600                 p = player_total;
601                 printf("\nYour Total is %d\n", p);
602                 dealer();
603                  if(dealer_total==21) //Is dealer total is 21, loss
604                  {
605                      printf("\nDealer Has the Better Hand. You Lose.\n");
606                      loss = loss+1;
607                      cash = cash - bet;
```

```
                    cash = cash - bet;
                    printf("\nYou have %d Wins and %d Losses. Awesome!\n", won, loss);
                    dealer_total=0;
                    askover();
                }

                if(dealer_total>21) //If dealer total is over 21, win
                {
                    printf("\nDealer Has Went Over!. 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((choice3=='S') || (choice3=='s')) // If Stay, does not continue
            {
               printf("\nYou Have Chosen to Stay at %d. Wise Decision!\n", player_total);
               stay();
            }
         }
            i++; //While player total and dealer total are less than 21, re-do while loop
    } // End While Loop
} // End Function

void dealer() //Function to play for dealer AI
{
    int z;

    if(dealer_total<17)
    {
     srand((unsigned) time(NULL) + 1); //Generates random seed for rand() function
     z=rand()%13+1;
     if(z<=10) //If random number generated is 10 or less, keep that value
     {
        d=z;

     }

     if(z>11) //If random number generated is more than 11, change value to 10
     {
        d=10;
     }

     if(z==11) //If random number is 11(Ace), change value to 11 or 1 depending on dealer total
     {
        if(dealer_total<=10)
        {
            d=11;
        }

        else
        {
            d=1;
        }
     }
    dealer_total = dealer_total + d;
    }

```

```
667       printf("\nThe Dealer Has a Total of %d", dealer_total); //Prints dealer total
668
669 } // End Function
670
671 void stay() //Function for when user selects 'Stay'
672 {
673       dealer(); //If stay selected, dealer continues going
674       if(dealer_total>=17)
675       {
676        if(player_total>=dealer_total) //If player's total is more than dealer's total, win
677        {
678           printf("\nUnbelievable! You Win!\n");
679           won = won+1;
680           cash = cash+bet;
681           printf("\nYou have %d Wins and %d Losses. Awesome!\n", won, loss);
682           dealer_total=0;
683           askover();
684        }
685        if(player_total<dealer_total) //If player's total is less than dealer's total, loss
686        {
687           printf("\nDealer Has the Better Hand. You Lose.\n");
688           loss = loss+1;
689           cash = cash - bet;
690           printf("\nYou have %d Wins and %d Losses. Awesome!\n", won, loss);
691           dealer_total=0;
692           askover();
693        }
694        if(dealer_total>21) //If dealer's total is more than 21, win
695        {
696           printf("\nUnbelievable! You Win!\n");
697           won = won+1;
698           cash = cash+bet;
699           printf("\nYou have %d Wins and %d Losses. Awesome!\n", won, loss);
700           dealer_total=0;
701           askover();
702        }
703       }
704       else
705       {
706           stay();
707       }
708
709 } // End Function
710
711 void cash_test() //Test for if user has cash remaining in purse
712 {
713       if (cash <= 0) //Once user has zero remaining cash, game ends and prompts user to play again
714       {
715          printf("You Are Bankrupt. Game Over");
716          cash = 500;
717          askover();
718       }
719 } // End Function
720
721 int betting() //Asks user amount to bet
722 {
723  printf("\n\nEnter Bet: $");
724  scanf("%d", &bet);
725
```

```
 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

void askover() // Function for asking player if they want to play again
{
    char choice1;

     printf("\nWould You Like To Play Again?");
     printf("\nPlease Enter Y for Yes or N for No\n");
     scanf("\n%c",&choice1);

    while((choice1!='Y') && (choice1!='y') && (choice1!='N') && (choice1!='n')) // If invalid choice
entered
    {
        printf("\n");
        printf("Incorrect Choice. Please Enter Y for Yes or N for No.\n");
        scanf("%c",&choice1);
    }


    if((choice1 == 'Y') || (choice1 == 'y')) // If yes, continue.
    {
            system("cls");
            play();
    }

    else if((choice1 == 'N') || (choice1 == 'n')) // If no, exit program
    {
        fileresults();
        printf("\nBYE!!!!\n\n");
        system("pause");
        exit(0);
    }
    return;
} // End function

void fileresults() //Prints results into Blackjack.txt file in program directory
{
    FILE *fpresults; //File pointer is fpresults
    fpresults = fopen(RESULTS, "w"); //Creates file and writes into it
    if(fpresults == NULL) // what to do if file missing from directory
    {
               printf("\nError: File Missing\n");
               system("pause");
               exit(1);
    }
    else
    {
     fprintf(fpresults,"\n\t RESULTS");
     fprintf(fpresults,"\n\t---------\n");
     fprintf(fpresults,"\nYou Have Won %d Times\n", won);
     fprintf(fpresults,"\nYou Have Lost %d Times\n", loss);
     fprintf(fpresults,"\nKeep Playing and Set an All-Time Record!");
```

```
785     }
786      fclose(fpresults);
787      return;
788 } // End Function
```

View Code

虽然代码足足有近800行，但根据代码的流程逐渐分析，还是能分析出以下信息：

1. 游戏规则

    1. 玩家在每轮游戏开始之前设置赌资；
    2. 玩家的任务是通过hit（继续加扑克牌）或者stay（等待）使自己的点数之和等于21；
    3. 卡片1~10的点数即为相对应的数字，卡片J，Q，K的点数为10，卡片A的点数为11；
    4. 当自己的点数大于了21，或者自己的点数小于了庄家的点数，玩家输；则要从赌本中减去赌资；
    5. 当玩家的点数之和等于21时，玩家胜；玩家就从庄家处赚取同赌资金额的金钱；

2. 当玩家的赌本大于**1000000**时，胜利，即可拿到**flag**；

由以上分析，首先先到了三种方法作弊（或者相信自己的人品无穷大，可以通过自己的努力能成为百万富翁）：

1. 直接修改赌本为 ≥ 1000000；
2. 通过修改， 使自己每局都能获胜，那么需要。
3. 在每局结束时动手脚，增加赌本

分析代码，前两种想法没有找到相应的漏洞，
第三种方法，分析**betting函数**:

```
1 int betting() //Asks user amount to bet
2 {
3  printf("\n\nEnter Bet: $");
4  scanf("%d", &bet);
5 
6  if (bet > cash) //If player tries to bet more money than player has
7  {
8         printf("\nYou cannot bet more money than you have.");
9         printf("\nEnter Bet: ");
10        scanf("%d", &bet);
11        return bet;
12 }
13 else return bet;
14 } // End Function
```

- 可以看出函数对输入的赌资只做了是否小于赌本的判断，那么我们就可以输入一个负的大小合适的赌本（大小合适指不会数据溢出），如**-1000000**；
- 那么，如果我们输掉了那一局，我们的赌本就要减负的1000000，就是加正的1000000，就可以拿到flag；

经过几次探索，拿到flag如下：

则flag即为***YaY_I_AM_A_MILLIONARE_LOL***
2017-2-16 8:16;47

转载于:https://www.cnblogs.com/WangAoBo/p/6404135.html