BUG Hunting S2/L5

Manuel Di Gangi 2 febraio 2024

TRACCIA

Per agire come un Hacker bisogna capire come pensare fuori dagli schemi. L'esercizio di oggi ha lo scopo di allenare l'osservazione critica. Dato il codice in allegato, si richiede allo studente di:

- Capire cosa fa il programma senza eseguirlo.
- Individuare dal codice sorgente le casistiche non standard che il programma non gestisce (esempio, comportamenti potenziali che non sono stati contemplati).
- Individuare eventuali errori di sintassi / logici.
- Proporre una soluzione per ognuno di essi.

Funzionalità

Il programma in questione permette all'utente di effettuare: moltiplicazioni, divisioni e l'inserimento di una stinga, selezionando l'operazione mediante un menu.

Ogni operazione ha una funzione dedicata, compreso il menu.

Il codice

```
1 #include <stdio.h>
2
3 //Prototipi delle funzioni
4 void menu ();
5 void moltiplica ();
6 void dividi ();
7 void ins_string();


8 int main ()
9 {
10    char scelta = {'\0'}; //mettendo le {} lo riconosce come array
```

- Errore di sintassi: per inizializzare un char vuoto la forma corretta è `char scelta = ' ';` Utilizzando { } viene interpretato come array di char, potrebbe compilare correttamente, ma creare problemi successivamente, dal momento che non viene gestito come tale. In C \0 indica la fine di una stringa o una stringa vuota per tanto ecco il motivo per cui non inizializziamo così il char.

```
11  menu ();
12  scanf ("%d", &scelta); //sintax err. scelta è una var char quindi %c
```

- Errore di sintassi: la variabile scelta è un char per cui l'identificatore corretto da inserire nello scanf è %c → `scanf ("%c", &scelta);`

```
13  switch (scelta)
14    {
15        case 'A': // - non gestisce la casistica 'a'
16        moltiplica();
17        break;
18        case 'B':// - non gestisce la casistica 'b'
19                dividi();
21                break;
22       case 'C':// - non gestisce la casistica 'c'
23                ins_string();
24                break;
25     // - non gestisce caso default
26    }
```

- Casistica non gestita: qualora l'utente inserisca a, b, c il programma non procede con l'esecuzione. E' corretto aggiungere altri case con i caratteri minuscoli.

```
case 'A':
case 'a':
```

```
case 'B':
case 'b':
```

```
case 'C':
case 'c':
```

- Casistica non gestita: qualora l'utente inserisca un valore che non rientra nelle opzioni il programma termina. E' più indicato prevedere una situazione di default che comunica all'utente che l'input non è valido e/o gli permetta di ripetere l'inserimento.

```
default:
     printf("Scelta non valida\n");
break;
```

```
27 return 0;
28 }
29
30 void menu ()
31 {
32     printf ("Benvenuto, sono un assitente digitale, posso aiutarti a
33 sbrigare alcuni compiti\n"); //assistente manca una s
34     printf ("Come posso aiutarti?\n");
35     printf ("A >> Moltiplicare due numeri\nB >> Dividere due numeri\nC
>> Inserire una stringa\n");
36 }

37 void moltiplica ()
38 {
39     short int  a,b = 0;
40     printf ("Inserisci i due numeri da moltiplicare:");
41     scanf ("%f", &a); //non %f ma %hd
42     scanf ("%d", &b); //non %d ma %hd
```

- Errore di sintassi: le variabili 'a' e 'b' sono short int per cui l'identificatore corretto da inserire nello scanf è %hd.→ `scanf ("%hd", &a); scanf ("%hd", &b);`

```
43     short int prodotto = a * b;
44     printf ("Il prodotto tra %d e %d e': %d", a,b,prodotto); //%hd
45 }
```

- Errore di sintassi: le variabili ‘a’, ‘b’ e prodotto sono short int per cui l’identificatore corretto da inserire nello scanf è %hd.→ `printf ("Il prodotto tra %hd e %hd e': %hd", a,b,prodotto)`

```
46 void dividi ()
47 {
48         int  a,b = 0;
49         printf ("Inserisci il numeratore:");
50         scanf ("%d", &a);
51     printf ("Inserisci il denumeratore:"); //denominatore
52      scanf ("%d", &b); // != da 0
```

- Casistica non gestita: qualora l’utente inserisca 0 il programma restituirebbe un errore. E’ indicato inserire una condizione che non permetta di dividere per 0 facendo inserire all’utente un altro numero.

```
printf ("Inserisci il denumeratore:");
scanf ("%d", &b);
while(b==0)
{
    printf ("Il denominatore non può essere 0\nProva con un altro numero\n");
    scanf ("%d", &b);
}
```

```
53         int divisione = a % b; // / non %
```

- Errore di logica: l’operatore % restituisce il resto della divisione, per la divisione si utilizza l’operatore /. `int divisione = a / b;`
- Casistica non gestita: dal momento che il risultato della divisione spesso è un numero decimale, sarebbe utile utilizzare una variabile di tipo float, cambiando di conseguenza anche il relativo identificatore nell’istruzione seguente.

```
54         printf ("La divisione tra %d e %d e': %d", a,b,divisione);
55 }

56 void ins_string ()
57 {
58    char stringa[10];
59         printf ("Inserisci la stringa:");
60         scanf ("%s", &stringa);
```

- Errore di sintassi: in C le stringhe sono elaborate come array di char, di conseguenza la variabile è già un puntatore, per questo non va messa la & davanti al nome della variabile. `scanf ("%s", stringa);`
- Casistica non gestita: qualora l’utente inserisca più di 10 caratteri il programma andrebbe in stack overflow. Per agirare questo problema sarebbe ideale leggere solo i primi 9 caratteri che l’utente digita specificando %9s. `scanf ("%9s", stringa);`

```
}
```