



## §. 关于动态内存申请后越界访问的深度讨论

★ 如何判断动态申请越界（C方式，**注意源程序后缀为.c**）

```
#define _CRT_SECURE_NO_WARNINGS
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
```

```
int main()
{
```

```
    char *p;
    p = (char *)malloc(10 * sizeof(char));
    if (p == NULL)
        return -1;
    strcpy(p, "123456789");
```

```
① p[10] = 'a';    //此句越界
   p[14] = 'A';    //此句越界
   p[15] = 'B';    //此句越界
```

```
② p[10] = '\xfd'; //此句越界
   printf("addr:%p\n", p);
```

```
   for (int i = -4; i < 16; i++) //注意，只有0-9是合理范围，其余都是越界读
       printf("%p:%02x\n", (p+i), p[i]);
```

```
③ free(p);
```

```
   return 0;
```

```
}
```

在VS2022的x86/Debug模式下运行：

- 1、①②③全部注释，观察运行结果
- 2、①放开，②③注释，观察运行结果
- 3、①③放开，②注释，观察运行结果
- 4、①②③全部放开，观察运行结果

结论：VS的Debug模式是如何判断  
动态申请内存访问越界的？

再观察下面四种环境下的运行结果：

VS2022 x86/Release

Dev 32bit-Debug

Dev 32bit-Release

Linux

每种讨论的结果可截图+文字说明，  
如果几种环境的结果一致，用一个  
环境的截图+文字说明即可（可加页）



### 1、①②③全部注释

```
Microsoft Visual Studio 调试控制台
addr:014A6390
014A638C:fffffffd
014A638D:fffffffd
014A638E:fffffffd
014A638F:fffffffd
014A6390:31
014A6391:32
014A6392:33
014A6393:34
014A6394:35
014A6395:36
014A6396:37
014A6397:38
014A6398:39
014A6399:00
014A639A:fffffffd
014A639B:fffffffd
014A639C:fffffffd
014A639D:fffffffd
014A639E:41
014A639F:42

D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c.exe (进程 22580) 已退出，代码为 0。
按任意键关闭此窗口。...
```

### 2、①放开，②③注释

```
Microsoft Visual Studio 调试控制台
addr:0108A658
0108A654:fffffffd
0108A655:fffffffd
0108A656:fffffffd
0108A657:fffffffd
0108A658:31
0108A659:32
0108A65A:33
0108A65B:34
0108A65C:35
0108A65D:36
0108A65E:37
0108A65F:38
0108A660:39
0108A661:00
0108A662:61
0108A663:fffffffd
0108A664:fffffffd
0108A665:fffffffd
0108A666:41
0108A667:42

D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c.exe (进程 24360) 已退出，代码为 0。
按任意键关闭此窗口。...
```

### 3、①③放开，②注释

```
D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c.exe
addr:00FDA658
00FDA654:fffffffd
00FDA655:fffffffd
00FDA656:fffffffd
00FDA657:fffffffd
00FDA658:31
00FDA659:32
00FDA65A:33
00FDA65B:34
00FDA65C:35
00FDA65D:36
00FDA65E:37
00FDA65F:38
00FDA660:39
00FDA661:00
00FDA662:61
00FDA663:fffffffd
00FDA664:fffffffd
00FDA665:fffffffd
00FDA666:41
00FDA667:42

Microsoft Visual C++ Runtime Library
Debug Error
Program: D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c.exe
HEAP CORRUPTION DETECTED: after Normal block (#73) at 0x00FDA655:
CRT detected that the application wrote to memory after end of heap
buffer.
(Press Retry to debug the application)
中止(A) 重试(R) 忽略(I)
```

### 4、①②③全部放开

```
Microsoft Visual Studio 调试控制台
addr:0164A658
0164A654:fffffffd
0164A655:fffffffd
0164A656:fffffffd
0164A657:fffffffd
0164A658:31
0164A659:32
0164A65A:33
0164A65B:34
0164A65C:35
0164A65D:36
0164A65E:37
0164A65F:38
0164A660:39
0164A661:00
0164A662:fffffffd
0164A663:fffffffd
0164A664:fffffffd
0164A665:fffffffd
0164A666:41
0164A667:42

D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c.exe (进程 15680) 已退出，代码为 0。
按任意键关闭此窗口。...
```

## VS2022的x86/Debug

结论：VS的Debug模式通过释放内存(free)时与申请的内存最后紧连的一块未申请内存是否有改变来进行判定内存访问越界



1、①②③全部注释

```
Microsoft Visual Studio 调试控制台

addr:00767D98
00767D94:40
00767D95:07
00767D96:00
00767D97:ffffff8e
00767D98:31
00767D99:32
00767D9A:33
00767D9B:34
00767D9C:35
00767D9D:36
00767D9E:37
00767D9F:38
00767DA0:39
00767DA1:00
00767DA2:00
00767DA3:00
00767DA4:70
00767DA5:63
00767DA6:41
00767DA7:42

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c.exe (进程 21984) 已退出, 代码为 0。
按任意键关闭此窗口。...
```

2、①放开，②③注释

```
Microsoft Visual Studio 调试控制台

addr:008CA548
008CA544:ffffffc1
008CA545:23
008CA546:00
008CA547:0e
008CA548:31
008CA549:32
008CA54A:33
008CA54B:34
008CA54C:35
008CA54D:36
008CA54E:37
008CA54F:38
008CA550:39
008CA551:00
008CA552:61
008CA553:00
008CA554:00
008CA555:00
008CA556:41
008CA557:42

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c.exe (进程 28112) 已退出, 代码为 0。
按任意键关闭此窗口。...
```

3、①③放开，②注释

```
Microsoft Visual Studio 调试控制台

addr:00E6A548
00E6A544:ffffffe4
00E6A545:ffffff94
00E6A546:00
00E6A547:0e
00E6A548:31
00E6A549:32
00E6A54A:33
00E6A54B:34
00E6A54C:35
00E6A54D:36
00E6A54E:37
00E6A54F:38
00E6A550:39
00E6A551:00
00E6A552:61
00E6A553:00
00E6A554:00
00E6A555:00
00E6A556:41
00E6A557:42

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c.exe (进程 7232) 已退出, 代码为 0。
按任意键关闭此窗口。...
```

4、①②③全部放开

```
Microsoft Visual Studio 调试控制台

addr:0126A548
0126A544:ffffff9f
0126A545:63
0126A546:00
0126A547:0e
0126A548:31
0126A549:32
0126A54A:33
0126A54B:34
0126A54C:35
0126A54D:36
0126A54E:37
0126A54F:38
0126A550:39
0126A551:00
0126A552:fffffffd
0126A553:00
0126A554:00
0126A555:00
0126A556:41
0126A557:42

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c.exe (进程 22568) 已退出, 代码为 0。
按任意键关闭此窗口。...
```



1、①②③全部注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr: 00C20D90
00C20D8C: ffffffff8f
00C20D8D: 00
00C20D8E: 00
00C20D8F: 0e
00C20D90: 31
00C20D91: 32
00C20D92: 33
00C20D93: 34
00C20D94: 35
00C20D95: 36
00C20D96: 37
00C20D97: 38
00C20D98: 39
00C20D99: 00
00C20D9A: 44
00C20D9B: 61
00C20D9C: 74
00C20D9D: 61
00C20D9E: 41
00C20D9F: 42

Process exited after 0.06508 seconds with return value 0
请按任意键继续. . .
```

2、①放开，②③注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr: 00CC0D90
00CC0D8C: ffffffff94
00CC0D8D: 22
00CC0D8E: 00
00CC0D8F: 0e
00CC0D90: 31
00CC0D91: 32
00CC0D92: 33
00CC0D93: 34
00CC0D94: 35
00CC0D95: 36
00CC0D96: 37
00CC0D97: 38
00CC0D98: 39
00CC0D99: 00
00CC0D9A: 61
00CC0D9B: 61
00CC0D9C: 74
00CC0D9D: 61
00CC0D9E: 41
00CC0D9F: 42

Process exited after 0.0584 seconds with return value 0
请按任意键继续. . .
```

3、①③放开，②注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr: 00C90D90
00C90D8C: 05
00C90D8D: ffffffffbd
00C90D8E: 00
00C90D8F: 0e
00C90D90: 31
00C90D91: 32
00C90D92: 33
00C90D93: 34
00C90D94: 35
00C90D95: 36
00C90D96: 37
00C90D97: 38
00C90D98: 39
00C90D99: 00
00C90D9A: 61
00C90D9B: 61
00C90D9C: 74
00C90D9D: 61
00C90D9E: 41
00C90D9F: 42

Process exited after 0.05321 seconds with return value 0
请按任意键继续. . .
```

4、①②③全部放开

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr: 00BC0D90
00BC0D8C: 49
00BC0D8D: 75
00BC0D8E: 00
00BC0D8F: 0e
00BC0D90: 31
00BC0D91: 32
00BC0D92: 33
00BC0D93: 34
00BC0D94: 35
00BC0D95: 36
00BC0D96: 37
00BC0D97: 38
00BC0D98: 39
00BC0D99: 00
00BC0D9A: ffffffffdd
00BC0D9B: 61
00BC0D9C: 74
00BC0D9D: 61
00BC0D9E: 41
00BC0D9F: 42

Process exited after 0.05577 seconds with return value 0
请按任意键继续. . .
```



1、①②③全部注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:00860D90
00860D8C:fffffe9
00860D8D:fffffd8
00860D8E:00
00860D8F:0e
00860D90:31
00860D91:32
00860D92:33
00860D93:34
00860D94:35
00860D95:36
00860D96:37
00860D97:38
00860D98:39
00860D99:00
00860D9A:44
00860D9B:61
00860D9C:74
00860D9D:61
00860D9E:41
00860D9F:42

Process exited after 0.06195 seconds with return value 0
请按任意键继续. . .
```

2、①放开，②③注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:00C00D90
00C00D8C:ffffff87
00C00D8D:31
00C00D8E:00
00C00D8F:0e
00C00D90:31
00C00D91:32
00C00D92:33
00C00D93:34
00C00D94:35
00C00D95:36
00C00D96:37
00C00D97:38
00C00D98:39
00C00D99:00
00C00D9A:61
00C00D9B:61
00C00D9C:74
00C00D9D:61
00C00D9E:41
00C00D9F:42

Process exited after 0.06628 seconds with return value 0
请按任意键继续. . .
```

3、①③放开，②注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:00DB0D90
00DB0D8C:33
00DB0D8D:14
00DB0D8E:00
00DB0D8F:0e
00DB0D90:31
00DB0D91:32
00DB0D92:33
00DB0D93:34
00DB0D94:35
00DB0D95:36
00DB0D96:37
00DB0D97:38
00DB0D98:39
00DB0D99:00
00DB0D9A:61
00DB0D9B:61
00DB0D9C:74
00DB0D9D:61
00DB0D9E:41
00DB0D9F:42

Process exited after 0.05765 seconds with return value 0
请按任意键继续. . .
```

4、①②③全部放开

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:00B50D90
00B50D8C:fffffffd
00B50D8D:31
00B50D8E:00
00B50D8F:0e
00B50D90:31
00B50D91:32
00B50D92:33
00B50D93:34
00B50D94:35
00B50D95:36
00B50D96:37
00B50D97:38
00B50D98:39
00B50D99:00
00B50D9A:fffffffd
00B50D9B:61
00B50D9C:74
00B50D9D:61
00B50D9E:41
00B50D9F:42

Process exited after 0.06348 seconds with return value 0
请按任意键继续. . .
```





### 1、①②③全部注释

```
[u2152041@oop ~]$ ./test
addr:0x60eeb0
0x60eeac:00
0x60eead:00
0x60eeae:00
0x60eeaf:00
0x60eeb0:31
0x60eeb1:32
0x60eeb2:33
0x60eeb3:34
0x60eeb4:35
0x60eeb5:36
0x60eeb6:37
0x60eeb7:38
0x60eeb8:39
0x60eeb9:00
0x60eeba:00
0x60eebb:00
0x60eebc:00
0x60eebd:00
0x60eebe:41
0x60eebf:42
```

### 2、①放开，②③注释

```
[u2152041@oop ~]$ ./test
addr:0x8f8eb0
0x8f8eac:00
0x8f8ead:00
0x8f8eae:00
0x8f8eaf:00
0x8f8eb0:31
0x8f8eb1:32
0x8f8eb2:33
0x8f8eb3:34
0x8f8eb4:35
0x8f8eb5:36
0x8f8eb6:37
0x8f8eb7:38
0x8f8eb8:39
0x8f8eb9:00
0x8f8eba:61
0x8f8ebb:00
0x8f8ebc:00
0x8f8ebd:00
0x8f8ebe:41
0x8f8ebf:42
```

### 3、①③放开，②注释

```
[u2152041@oop ~]$ ./test
addr:0x2165eb0
0x2165eac:00
0x2165ead:00
0x2165eae:00
0x2165eaf:00
0x2165eb0:31
0x2165eb1:32
0x2165eb2:33
0x2165eb3:34
0x2165eb4:35
0x2165eb5:36
0x2165eb6:37
0x2165eb7:38
0x2165eb8:39
0x2165eb9:00
0x2165eba:61
0x2165ebb:00
0x2165ebc:00
0x2165ebd:00
0x2165ebe:41
0x2165ebf:42
```

### 4、①②③全部放开

```
[u2152041@oop ~]$ ./test
addr:0x1f5eeb0
0x1f5eeac:00
0x1f5eead:00
0x1f5eeae:00
0x1f5eeaf:00
0x1f5eeb0:31
0x1f5eeb1:32
0x1f5eeb2:33
0x1f5eeb3:34
0x1f5eeb4:35
0x1f5eeb5:36
0x1f5eeb6:37
0x1f5eeb7:38
0x1f5eeb8:39
0x1f5eeb9:00
0x1f5eeba:ffffffffd
0x1f5eebb:00
0x1f5eebc:00
0x1f5eebd:00
0x1f5eebe:41
0x1f5eebf:42
```



## §. 关于动态内存申请后越界访问的深度讨论

★ 如何判断动态申请越界 (C++方式, 注意源程序后缀为.cpp)

```
#define _CRT_SECURE_NO_WARNINGS
#include <iostream>
#include <cstring>
using namespace std;
```

```
int main()
{
```

```
    char *p;
    p = new(nothrow) char[10];
    if (p == NULL)
        return -1;
    strcpy(p, "123456789");
```

```
① p[10] = 'a';    //此句越界
   p[14] = 'A';    //此句越界
   p[15] = 'B';    //此句越界
```

```
② p[10] = '\xfd'; //此句越界
```

```
    cout << "addr:" << hex << (void *) (p) << endl;
    for (int i = -4; i < 16; i++) //注意, 只有0-9是合理范围, 其余都是越界读
        cout << hex << (void *) (p + i) << ":" << int(p[i]) << endl;
```

```
③ delete[] p;
```

```
    return 0;
```

```
}
```

在VS2022的x86/Debug模式下运行:

- 1、①②③全部注释, 观察运行结果
- 2、①放开, ②③注释, 观察运行结果
- 3、①③放开, ②注释, 观察运行结果
- 4、①②③全部放开, 观察运行结果

结论: VS的Debug模式是如何判断  
动态申请内存访问越界的?

再观察下面四种环境下的运行结果:

VS2022 x86/Release

Dev 32bit-Debug

Dev 32bit-Release

Linux

每种讨论的结果可截图+文字说明,  
如果几种环境的结果一致, 用一个  
环境的截图+文字说明即可(可加页)



1、①②③全部注释

```
Microsoft Visual Studio 调试控制台
addr:00C78048
00C78044:ffffffffd
00C78045:ffffffffd
00C78046:ffffffffd
00C78047:ffffffffd
00C78048:31
00C78049:32
00C7804A:33
00C7804B:34
00C7804C:35
00C7804D:36
00C7804E:37
00C7804F:38
00C78050:39
00C78051:0
00C78052:ffffffffd
00C78053:ffffffffd
00C78054:ffffffffd
00C78055:ffffffffd
00C78056:41
00C78057:42

D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c++.exe (进程 20468) 已退出, 代码为 0。
按任意键关闭此窗口。 . . .
```

3、①③放开，②注释

```
D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c++.exe
addr:00F2F050
00F2F04C:ffffffffd
00F2F04D:ffffffffd
00F2F04E:ffffffffd
00F2F04F:ffffffffd
00F2F050:31
00F2F051:32
00F2F052:33
00F2F053:34
00F2F054:35
00F2F055:36
00F2F056:37
00F2F057:38
00F2F058:39
00F2F059:0
00F2F05A:61
00F2F05B:ffffffffd
00F2F05C:ffffffffd
00F2F05D:ffffffffd
00F2F05E:41
00F2F05F:42

Microsoft Visual C++ Runtime Library

Debug Error!

Program: D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c++.exe

HEAP CORRUPTION DETECTED: after Normal block (#150) at
0x00F2F050.
CRT detected that the application wrote to memory after end of heap
buffer.

(Press Retry to debug the application)

中止(A) 重试(R) 忽略(I)
```

2、①放开，②③注释

```
Microsoft Visual Studio 调试控制台
addr:00C0F098
00C0F094:ffffffffd
00C0F095:ffffffffd
00C0F096:ffffffffd
00C0F097:ffffffffd
00C0F098:31
00C0F099:32
00C0F09A:33
00C0F09B:34
00C0F09C:35
00C0F09D:36
00C0F09E:37
00C0F09F:38
00C0F0A0:39
00C0F0A1:0
00C0F0A2:61
00C0F0A3:ffffffffd
00C0F0A4:ffffffffd
00C0F0A5:ffffffffd
00C0F0A6:41
00C0F0A7:42

D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c++.exe (进程 2620) 已退出, 代码为 0。
按任意键关闭此窗口。 . . .
```

4、①②③全部放开

```
Microsoft Visual Studio 调试控制台
addr:00B6F540
00B6F53C:ffffffffd
00B6F53D:ffffffffd
00B6F53E:ffffffffd
00B6F53F:ffffffffd
00B6F540:31
00B6F541:32
00B6F542:33
00B6F543:34
00B6F544:35
00B6F545:36
00B6F546:37
00B6F547:38
00B6F548:39
00B6F549:0
00B6F54A:ffffffffd
00B6F54B:ffffffffd
00B6F54C:ffffffffd
00B6F54D:ffffffffd
00B6F54E:41
00B6F54F:42

D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c++.exe (进程 26276) 已退出, 代码为 0。
按任意键关闭此窗口。 . . .
```

结论：VS的Debug模式通过释放内存(delete)时与申请的内存最后紧连的一块未申请内存是  
否有改变来进行判定内存访问越界 VS2022的x86/Debug





### 1、①②③全部注释

```
Microsoft Visual Studio 调试控制台
addr:014B9A48
014B9A44:0
014B9A45:0
014B9A46:0
014B9A47:ffffff8e
014B9A48:31
014B9A49:32
014B9A4A:33
014B9A4B:34
014B9A4C:35
014B9A4D:36
014B9A4E:37
014B9A4F:38
014B9A50:39
014B9A51:0
014B9A52:0
014B9A53:0
014B9A54:0
014B9A55:0
014B9A56:41
014B9A57:42

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c++.exe (进程 28048) 已退出，代码为 0。
按任意键关闭此窗口。 . .
```

### 2、①放开，②③注释

```
Microsoft Visual Studio 调试控制台
addr:00C40D70
00C40D6C:49
00C40D6D:0
00C40D6E:0
00C40D6F:ffffff8e
00C40D70:31
00C40D71:32
00C40D72:33
00C40D73:34
00C40D74:35
00C40D75:36
00C40D76:37
00C40D77:38
00C40D78:39
00C40D79:0
00C40D7A:61
00C40D7B:0
00C40D7C:46
00C40D7D:0
00C40D7E:41
00C40D7F:42

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c++.exe (进程 13372) 已退出，代码为 0。
按任意键关闭此窗口。 . .
```

### 3、①③放开，②注释

```
Microsoft Visual Studio 调试控制台
addr:0127C780
0127C77C:43
0127C77D:2
0127C77E:0
0127C77F:ffffff8e
0127C780:31
0127C781:32
0127C782:33
0127C783:34
0127C784:35
0127C785:36
0127C786:37
0127C787:38
0127C788:39
0127C789:0
0127C78A:61
0127C78B:0
0127C78C:57
0127C78D:0
0127C78E:41
0127C78F:42

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c++.exe (进程 19952) 已退出，代码为 0。
按任意键关闭此窗口。 . .
```

### 4、①②③全部放开

```
Microsoft Visual Studio 调试控制台
addr:0124E8B8
0124E8B4:0
0124E8B5:5
0124E8B6:0
0124E8B7:ffffff8e
0124E8B8:31
0124E8B9:32
0124E8BA:33
0124E8BB:34
0124E8BC:35
0124E8BD:36
0124E8BE:37
0124E8BF:38
0124E8C0:39
0124E8C1:0
0124E8C2:fffffffd
0124E8C3:0
0124E8C4:0
0124E8C5:0
0124E8C6:41
0124E8C7:42

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c++.exe (进程 27708) 已退出，代码为 0。
按任意键关闭此窗口。 . .
```

1、①②③全部注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0xd90dd0
0xd90dce:7f
0xd90dcd:ffffffd6
0xd90dce:0
0xd90dcf:e
0xd90dd0:31
0xd90dd1:32
0xd90dd2:33
0xd90dd3:34
0xd90dd4:35
0xd90dd5:36
0xd90dd6:37
0xd90dd7:38
0xd90dd8:39
0xd90dd9:0
0xd90dda:0
0xd90ddb:0
0xd90ddc:0
0xd90ddd:0
0xd90dde:41
0xd90ddf:42

Process exited after 0.1292 seconds with return value 0
请按任意键继续. . .
```

2、①放开，②③注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0x930dd0
0x930dce:6b
0x930dcd:74
0x930dce:0
0x930dcf:e
0x930dd0:31
0x930dd1:32
0x930dd2:33
0x930dd3:34
0x930dd4:35
0x930dd5:36
0x930dd6:37
0x930dd7:38
0x930dd8:39
0x930dd9:0
0x930dda:61
0x930ddb:0
0x930ddc:0
0x930ddd:0
0x930dde:41
0x930ddf:42

Process exited after 0.1234 seconds with return value 0
请按任意键继续. . .
```

3、①③放开，②注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0xcb0dd0
0xcb0dce:6b
0xcb0dcd:ffffffc2
0xcb0dce:0
0xcb0dcf:e
0xcb0dd0:31
0xcb0dd1:32
0xcb0dd2:33
0xcb0dd3:34
0xcb0dd4:35
0xcb0dd5:36
0xcb0dd6:37
0xcb0dd7:38
0xcb0dd8:39
0xcb0dd9:0
0xcb0dda:61
0xcb0ddb:0
0xcb0ddc:0
0xcb0ddd:0
0xcb0dde:41
0xcb0ddf:42

Process exited after 0.1161 seconds with return value 0
请按任意键继续. . .
```

4、①②③全部放开

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0x9c0dd0
0x9c0dce:2
0x9c0dcd:8
0x9c0dce:0
0x9c0dcf:e
0x9c0dd0:31
0x9c0dd1:32
0x9c0dd2:33
0x9c0dd3:34
0x9c0dd4:35
0x9c0dd5:36
0x9c0dd6:37
0x9c0dd7:38
0x9c0dd8:39
0x9c0dd9:0
0x9c0dda:ffffffd
0x9c0ddb:0
0x9c0ddc:0
0x9c0ddd:0
0x9c0dde:41
0x9c0ddf:42

Process exited after 0.1189 seconds with return value 0
请按任意键继续. . .
```

1、①②③全部注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0xc90dd0
0xc90dcc:ffffff9c
0xc90dcd:49
0xc90dce:0
0xc90dcf:e
0xc90dd0:31
0xc90dd1:32
0xc90dd2:33
0xc90dd3:34
0xc90dd4:35
0xc90dd5:36
0xc90dd6:37
0xc90dd7:38
0xc90dd8:39
0xc90dd9:0
0xc90dda:0
0xc90ddb:0
0xc90ddc:0
0xc90ddd:0
0xc90dde:41
0xc90ddf:42

Process exited after 0.1195 seconds with return value 0
请按任意键继续. . .
```

2、①放开，②③注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0x9a0dd0
0x9a0dcc:ffffff93
0x9a0dcd:ffffffcf
0x9a0dce:0
0x9a0dcf:e
0x9a0dd0:31
0x9a0dd1:32
0x9a0dd2:33
0x9a0dd3:34
0x9a0dd4:35
0x9a0dd5:36
0x9a0dd6:37
0x9a0dd7:38
0x9a0dd8:39
0x9a0dd9:0
0x9a0dda:61
0x9a0ddb:0
0x9a0ddc:0
0x9a0ddd:0
0x9a0dde:41
0x9a0ddf:42

Process exited after 0.141 seconds with return value 0
请按任意键继续. . .
```

3、①③放开，②注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0xcf0dd0
0xcf0dcc:ffffffe3
0xcf0dcd:78
0xcf0dce:0
0xcf0dcf:e
0xcf0dd0:31
0xcf0dd1:32
0xcf0dd2:33
0xcf0dd3:34
0xcf0dd4:35
0xcf0dd5:36
0xcf0dd6:37
0xcf0dd7:38
0xcf0dd8:39
0xcf0dd9:0
0xcf0dda:61
0xcf0ddb:0
0xcf0ddc:0
0xcf0ddd:0
0xcf0dde:41
0xcf0ddf:42

Process exited after 0.1215 seconds with return value 0
请按任意键继续. . .
```

4、①②③全部放开

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0xd50dd0
0xd50dcc:ffffff89
0xd50dcd:ffffffc1
0xd50dce:0
0xd50dcf:e
0xd50dd0:31
0xd50dd1:32
0xd50dd2:33
0xd50dd3:34
0xd50dd4:35
0xd50dd5:36
0xd50dd6:37
0xd50dd7:38
0xd50dd8:39
0xd50dd9:0
0xd50dda:fffffffd
0xd50ddb:0
0xd50ddc:0
0xd50ddd:0
0xd50dde:41
0xd50ddf:42

Process exited after 0.1185 seconds with return value 0
请按任意键继续. . .
```



# 1、①②③全部注释

```
[u2152041@oop ~]$ ./test
addr:0xc69eb0
0xc69eac:0
0xc69ead:0
0xc69eae:0
0xc69eaf:0
0xc69eb0:31
0xc69eb1:32
0xc69eb2:33
0xc69eb3:34
0xc69eb4:35
0xc69eb5:36
0xc69eb6:37
0xc69eb7:38
0xc69eb8:39
0xc69eb9:0
0xc69eba:61
0xc69ebb:0
0xc69ebc:0
0xc69ebd:0
0xc69ebe:0
0xc69ebf:42
```

# 2、①放开，②③注释

```
[u2152041@oop ~]$ ./test
addr:0x11f9eb0
0x11f9eac:0
0x11f9ead:0
0x11f9eae:0
0x11f9eaf:0
0x11f9eb0:31
0x11f9eb1:32
0x11f9eb2:33
0x11f9eb3:34
0x11f9eb4:35
0x11f9eb5:36
0x11f9eb6:37
0x11f9eb7:38
0x11f9eb8:39
0x11f9eb9:0
0x11f9eba:61
0x11f9ebb:0
0x11f9ebc:0
0x11f9ebd:0
0x11f9ebe:41
0x11f9ebf:42
```

# 3、①③放开，②注释

```
[u2152041@oop ~]$ ./test
addr:0x16f5eb0
0x16f5eac:0
0x16f5ead:0
0x16f5eae:0
0x16f5eaf:0
0x16f5eb0:31
0x16f5eb1:32
0x16f5eb2:33
0x16f5eb3:34
0x16f5eb4:35
0x16f5eb5:36
0x16f5eb6:37
0x16f5eb7:38
0x16f5eb8:39
0x16f5eb9:0
0x16f5eba:61
0x16f5ebb:0
0x16f5ebc:0
0x16f5ebd:0
0x16f5ebe:41
0x16f5ebf:42
```

# 4、①②③全部放开

```
[u2152041@oop ~]$ ./test
addr:0x1ff5eb0
0x1ff5eac:0
0x1ff5ead:0
0x1ff5eae:0
0x1ff5eaf:0
0x1ff5eb0:31
0x1ff5eb1:32
0x1ff5eb2:33
0x1ff5eb3:34
0x1ff5eb4:35
0x1ff5eb5:36
0x1ff5eb6:37
0x1ff5eb7:38
0x1ff5eb8:39
0x1ff5eb9:0
0x1ff5eba:ffffffffd
0x1ff5ebb:0
0x1ff5ebc:0
0x1ff5ebd:0
0x1ff5ebe:41
0x1ff5ebf:42
```



## §. 关于动态内存申请后越界访问的深度讨论

★ 如何判断普通数组的越界访问 (C++方式, 注意源程序后缀为. cpp)

```
/* 2152041 王浩 计科 */
#define _CRT_SECURE_NO_WARNINGS
#include <iostream>
#include <cstring>
using namespace std;

int main()
{
    char p[10];
    strcpy(p, "123456789");
    ① p[10] = 'a';    //此句越界
    p[14] = 'A';    //此句越界
    p[15] = 'B';    //此句越界
    ② p[10] = '\xfd'; //此句越界
    cout << "addr:" << hex << (void *) (p) << endl;
    for (int i = -4; i < 16; i++) //注意, 只有0-9是合理范围, 其余都是越界读
        cout << hex << (void *) (p + i) << ":" << int(p[i]) << endl;

    return 0;
}
```

数组为char a[10]形式

在理解P. 1/P. 2的情况下, 自行构造相似的程序, 来观察数组越界后的内存表现, 并验证与动态申请是否相似

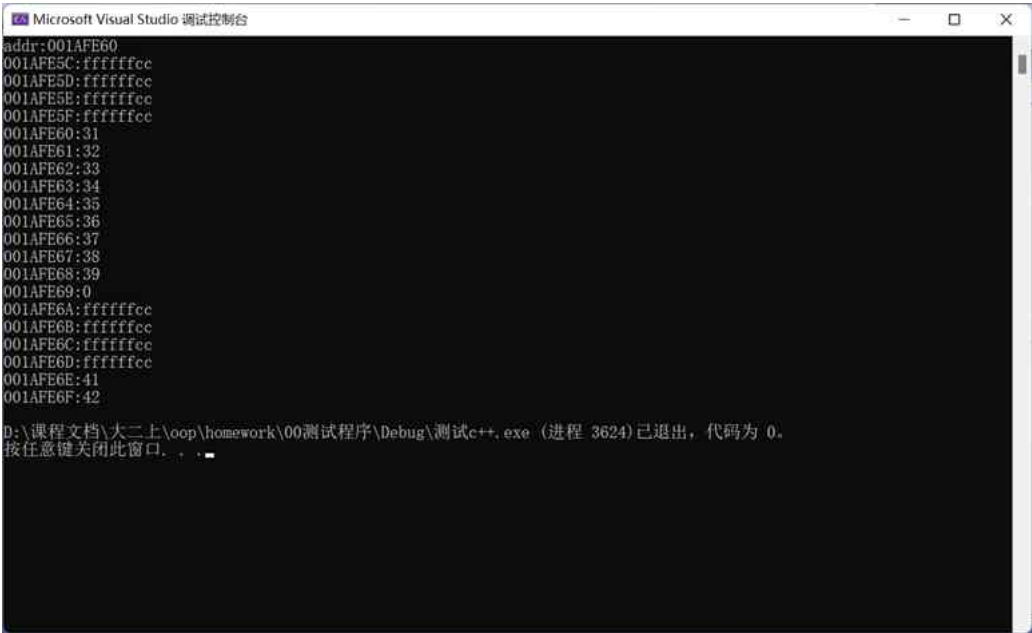
要求:

- 1、数组用 char a[10]; 形式
- 2、数组用 int a[10]; 形式
- 3、测试程序在下面五种环境下运行  
VS2022 x86/Debug  
VS2022 x86Release  
Dev 32bit-Debug  
Dev 32bit-Release  
Linux
- 4、每种讨论的结果可截图+文字说明, 如果几种环境的结果一致, 用一个环境的截图+文字说明即可(可加页)

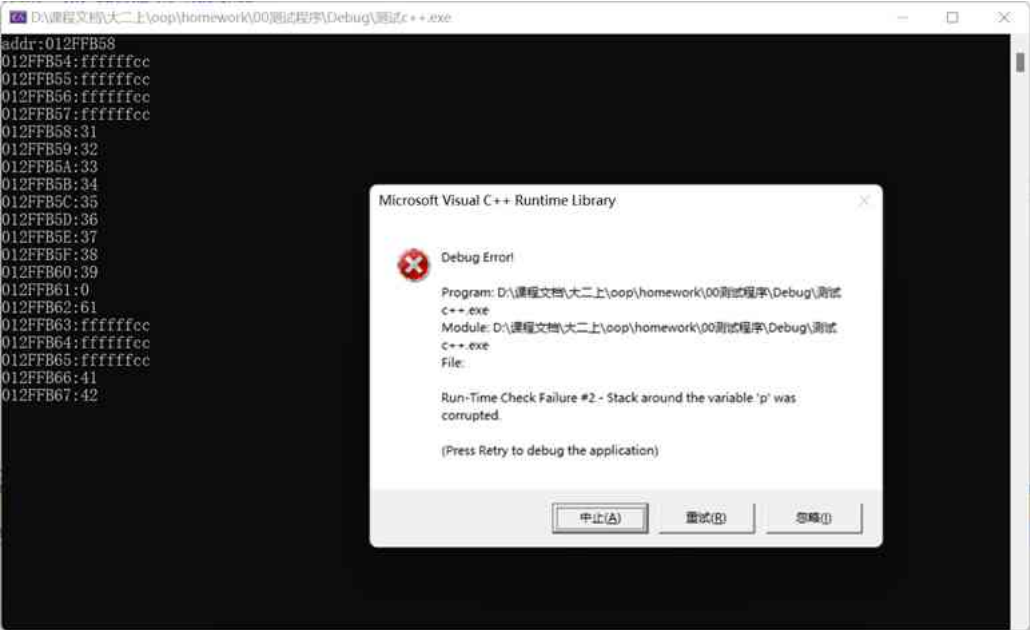




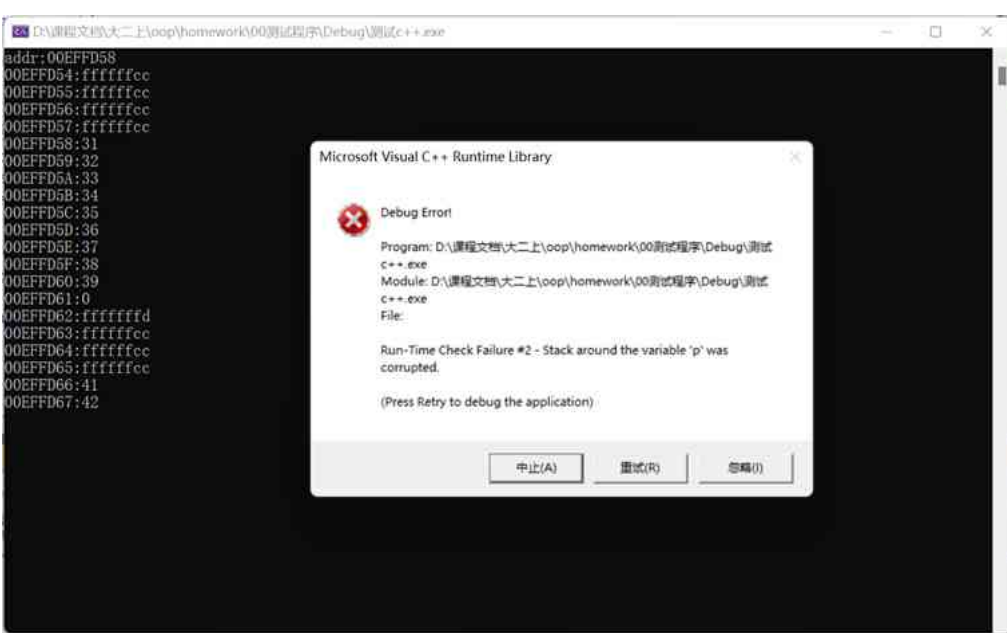
1、①②全部注释



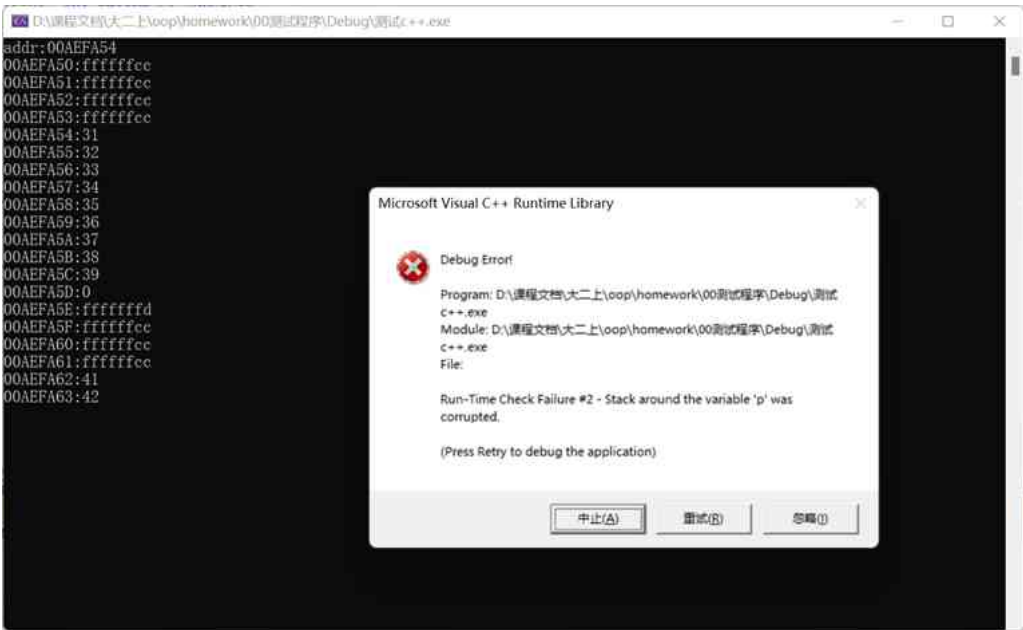
2、①放开, ②注释



3、②放开, ①注释



4、①②全部放开





## 1、①②全部注释

```
Microsoft Visual Studio 调试控制台

addr:00F8FA64
00F8FA60:48
00F8FA61:ffffff86
00F8FA62:26
00F8FA63:1
00F8FA64:31
00F8FA65:32
00F8FA66:33
00F8FA67:34
00F8FA68:35
00F8FA69:36
00F8FA6A:37
00F8FA6B:38
00F8FA6C:39
00F8FA6D:0
00F8FA6E:0
00F8FA6F:0
00F8FA70:52
00F8FA71:2c
00F8FA72:41
00F8FA73:75

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c++.exe (进程 17984) 已退出, 代码为 0。
按任意键关闭此窗口。 . . .
```

## 3、②放开, ①注释

```
Microsoft Visual Studio 调试控制台

addr:0115F92C
0115F928:20
0115F929:ffffffaa
0115F92A:32
0115F92B:1
0115F92C:31
0115F92D:32
0115F92E:33
0115F92F:34
0115F930:35
0115F931:36
0115F932:37
0115F933:38
0115F934:39
0115F935:0
0115F936:fffffffd
0115F937:0
0115F938:52
0115F939:2c
0115F93A:41
0115F93B:75

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c++.exe (进程 25140) 已退出, 代码为 0。
按任意键关闭此窗口。 . . .
```

## 2、①放开, ②注释

```
Microsoft Visual Studio 调试控制台

addr:00BBF9F4
00BBF9F0:60
00BBF9F1:ffffffac
00BBF9F2:15
00BBF9F3:1
00BBF9F4:31
00BBF9F5:32
00BBF9F6:33
00BBF9F7:34
00BBF9F8:35
00BBF9F9:36
00BBF9FA:37
00BBF9FB:38
00BBF9FC:39
00BBF9FD:0
00BBF9FE:61
00BBF9FF:0
00BBFA00:52
00BBFA01:2c
00BBFA02:41
00BBFA03:75

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c++.exe (进程 4540) 已退出, 代码为 0。
按任意键关闭此窗口。 . . .
```

## 4、①②全部放开

```
Microsoft Visual Studio 调试控制台

addr:00FAFF04
00FAFF00:ffffffd8
00FAFF01:ffffffad
00FAFF02:1b
00FAFF03:1
00FAFF04:31
00FAFF05:32
00FAFF06:33
00FAFF07:34
00FAFF08:35
00FAFF09:36
00FAFF0A:37
00FAFF0B:38
00FAFF0C:39
00FAFF0D:0
00FAFF0E:fffffffd
00FAFF0F:75
00FAFF10:64
00FAFF11:16
00FAFF12:ffffffea
00FAFF13:0

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c++.exe (进程 25356) 已退出, 代码为 0。
按任意键关闭此窗口。 . . .
```

1、①②全部注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0x78feb2
0x78feae:0
0x78feaf:0
0x78feb0:34
0x78feb1:0
0x78feb2:31
0x78feb3:32
0x78feb4:33
0x78feb5:34
0x78feb6:35
0x78feb7:36
0x78feb8:37
0x78feb9:38
0x78feba:39
0x78febb:0
0x78febc:a
0x78febd:0
0x78febe:0
0x78febf:0
0x78fec0:41
0x78fec1:42

Process exited after 0.121 seconds with return value 0
请按任意键继续. . .
```

2、①放开，②注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0x78feb2
0x78feae:0
0x78feaf:0
0x78feb0:34
0x78feb1:0
0x78feb2:31
0x78feb3:32
0x78feb4:33
0x78feb5:34
0x78feb6:35
0x78feb7:36
0x78feb8:37
0x78feb9:38
0x78feba:39
0x78febb:0
0x78febc:a
0x78febd:0
0x78febe:0
0x78febf:0
0x78fec0:41
0x78fec1:42

Process exited after 0.1068 seconds with return value 0
请按任意键继续. . .
```

3、②放开，①注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0x78feb2
0x78feae:0
0x78feaf:0
0x78feb0:34
0x78feb1:0
0x78feb2:31
0x78feb3:32
0x78feb4:33
0x78feb5:34
0x78feb6:35
0x78feb7:36
0x78feb8:37
0x78feb9:38
0x78feba:39
0x78febb:0
0x78febc:a
0x78febd:0
0x78febe:0
0x78febf:0
0x78fec0:41
0x78fec1:42

Process exited after 0.1055 seconds with return value 0
请按任意键继续. . .
```

4、①②全部放开

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0x78feb2
0x78feae:0
0x78feaf:0
0x78feb0:34
0x78feb1:0
0x78feb2:31
0x78feb3:32
0x78feb4:33
0x78feb5:34
0x78feb6:35
0x78feb7:36
0x78feb8:37
0x78feb9:38
0x78feba:39
0x78febb:0
0x78febc:a
0x78febd:0
0x78febe:0
0x78febf:0
0x78fec0:41
0x78fec1:42

Process exited after 0.1396 seconds with return value 0
请按任意键继续. . .
```

1、①②全部注释

```
DA\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0x77feb2
0x77feae:0
0x77feaf:0
0x77feb0:34
0x77feb1:0
0x77feb2:31
0x77feb3:32
0x77feb4:33
0x77feb5:34
0x77feb6:35
0x77feb7:36
0x77feb8:37
0x77feb9:38
0x77feba:39
0x77febb:0
0x77febc:a
0x77febd:0
0x77febe:0
0x77febf:0
0x77fec0:41
0x77fec1:42

Process exited after 0.09971 seconds with return value 0
请按任意键继续. . .
```

2、①放开，②注释

```
DA\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0x77feb2
0x77feae:0
0x77feaf:0
0x77feb0:34
0x77feb1:0
0x77feb2:31
0x77feb3:32
0x77feb4:33
0x77feb5:34
0x77feb6:35
0x77feb7:36
0x77feb8:37
0x77feb9:38
0x77feba:39
0x77febb:0
0x77febc:a
0x77febd:0
0x77febe:0
0x77febf:0
0x77fec0:41
0x77fec1:42

Process exited after 0.1127 seconds with return value 0
请按任意键继续. . .
```

3、②放开，①注释

```
DA\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0x77feb2
0x77feae:0
0x77feaf:0
0x77feb0:34
0x77feb1:0
0x77feb2:31
0x77feb3:32
0x77feb4:33
0x77feb5:34
0x77feb6:35
0x77feb7:36
0x77feb8:37
0x77feb9:38
0x77feba:39
0x77febb:0
0x77febc:a
0x77febd:0
0x77febe:0
0x77febf:0
0x77fec0:41
0x77fec1:42

Process exited after 0.1041 seconds with return value 0
请按任意键继续. . .
```

4、①②全部放开

```
DA\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0x77feb2
0x77feae:0
0x77feaf:0
0x77feb0:34
0x77feb1:0
0x77feb2:31
0x77feb3:32
0x77feb4:33
0x77feb5:34
0x77feb6:35
0x77feb7:36
0x77feb8:37
0x77feb9:38
0x77feba:39
0x77febb:0
0x77febc:a
0x77febd:0
0x77febe:0
0x77febf:0
0x77fec0:41
0x77fec1:42

Process exited after 0.1081 seconds with return value 0
请按任意键继续. . .
```





## 1、①②全部注释

```
[u2152041@oop ~]$ ./test
addr:0x7ffc0bc38612
0x7ffc0bc3860e:0
0x7ffc0bc3860f:0
0x7ffc0bc38610:0
0x7ffc0bc38611:0
0x7ffc0bc38612:31
0x7ffc0bc38613:32
0x7ffc0bc38614:33
0x7ffc0bc38615:34
0x7ffc0bc38616:35
0x7ffc0bc38617:36
0x7ffc0bc38618:37
0x7ffc0bc38619:38
0x7ffc0bc3861a:39
0x7ffc0bc3861b:0
0x7ffc0bc3861c:a
0x7ffc0bc3861d:0
0x7ffc0bc3861e:0
0x7ffc0bc3861f:0
0x7ffc0bc38620:41
0x7ffc0bc38621:42
```

## 2、①放开，②注释

```
[u2152041@oop ~]$ ./test
addr:0x7ffef727dff2
0x7ffef727dfee:0
0x7ffef727dfe0:0
0x7ffef727dff0:0
0x7ffef727dff1:0
0x7ffef727dff2:31
0x7ffef727dff3:32
0x7ffef727dff4:33
0x7ffef727dff5:34
0x7ffef727dff6:35
0x7ffef727dff7:36
0x7ffef727dff8:37
0x7ffef727dff9:38
0x7ffef727dffA:39
0x7ffef727dffB:0
0x7ffef727dffC:a
0x7ffef727dffD:0
0x7ffef727dffE:0
0x7ffef727dffF:0
0x7ffef727e000:41
0x7ffef727e001:42
```

## 3、② 放开，①注释

```
[u2152041@oop ~]$ ./test
addr:0x7fffd6cf5c62
0x7fffd6cf5c5e:0
0x7fffd6cf5c5f:0
0x7fffd6cf5c60:0
0x7fffd6cf5c61:0
0x7fffd6cf5c62:31
0x7fffd6cf5c63:32
0x7fffd6cf5c64:33
0x7fffd6cf5c65:34
0x7fffd6cf5c66:35
0x7fffd6cf5c67:36
0x7fffd6cf5c68:37
0x7fffd6cf5c69:38
0x7fffd6cf5c6a:39
0x7fffd6cf5c6b:0
0x7fffd6cf5c6c:a
0x7fffd6cf5c6d:0
0x7fffd6cf5c6e:0
0x7fffd6cf5c6f:0
0x7fffd6cf5c70:41
0x7fffd6cf5c71:42
```

## 4、①②全部放开

```
[u2152041@oop ~]$ ./test
addr:0x7ffe0a8e1642
0x7ffe0a8e163e:0
0x7ffe0a8e163f:0
0x7ffe0a8e1640:0
0x7ffe0a8e1641:0
0x7ffe0a8e1642:31
0x7ffe0a8e1643:32
0x7ffe0a8e1644:33
0x7ffe0a8e1645:34
0x7ffe0a8e1646:35
0x7ffe0a8e1647:36
0x7ffe0a8e1648:37
0x7ffe0a8e1649:38
0x7ffe0a8e164a:39
0x7ffe0a8e164b:0
0x7ffe0a8e164c:a
0x7ffe0a8e164d:0
0x7ffe0a8e164e:0
0x7ffe0a8e164f:0
0x7ffe0a8e1650:41
0x7ffe0a8e1651:42
```





## §. 关于动态内存申请后越界访问的深度讨论

★ 如何判断普通数组的越界访问 (C++方式, 注意源程序后缀为 .cpp)

```
/* 2152041 王浩 计科 */
#define _CRT_SECURE_NO_WARNINGS
#include <iostream>
#include <cstring>
using namespace std;

int main()
{
    int p[10] = { 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 };
    ① p[10] = 10;    //此句越界
    p[14] = 14;    //此句越界
    p[15] = 15;    //此句越界
    ② p[10] = (int)' \xfd'; //此句越界
    cout << "addr:" << hex << (void *) (p) << endl;
    for (int i = -4; i < 16; i++) //注意, 只有0-9是合理范围, 其余都是越界读
        cout << hex << (void *) (p + i) << ":" << int(p[i]) << endl;

    return 0;
}
```

数组为int a[10]形式

在理解P. 1/P. 2的情况下, 自行构造相似的程序, 来观察数组越界后的内存表现, 并验证与动态申请是否相似

要求:

- 1、数组用 char a[10]; 形式
- 2、数组用 int a[10]; 形式
- 3、测试程序在下面五种环境下运行  
VS2022 x86/Debug  
VS2022 x86Release  
Dev 32bit-Debug  
Dev 32bit-Release  
Linux
- 4、每种讨论的结果可截图+文字说明, 如果几种环境的结果一致, 用一个环境的截图+文字说明即可(可加页)



## 1、①②全部注释

```
Microsoft Visual Studio 调试控制台

addr: 00DFFB70
00DFFB60: cccccccc
00DFFB64: ffffffff
00DFFB68: cccccccc
00DFFB6C: cccccccc
00DFFB70: 0
00DFFB74: 1
00DFFB78: 2
00DFFB7C: 3
00DFFB80: 4
00DFFB84: 5
00DFFB88: 6
00DFFB8C: 7
00DFFB90: 8
00DFFB94: 9
00DFFB98: cccccccc
00DFFB9C: 7113e645
00DFFBA0: dffbc0
00DFFBA4: f530d3
00DFFBA8: e
00DFFBAC: f

D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c++.exe (进程 2752) 已退出, 代码为 0。
按任意键关闭此窗口。 . . .
```

## 3、②放开, ①注释

```
D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c++.exe

addr: 00AFFDB0
00AFFDA0: cccccccc
00AFFDA4: ffffffff
00AFFDA8: cccccccc
00AFFDAC: cccccccc
00AFFDB0: 0
00AFFDB4: 1
00AFFDB8: 2
00AFFDBC: 3
00AFFDC0: 4
00AFFDC4: 5
00AFFDC8: 6
00AFFDCC: 7
00AFFDD0: 8
00AFFDD4: 9
00AFFDD8: ffffffff
00AFFDDC: d0045d18
00AFFDE0: affe00
00AFFDE4: 1e30d3
00AFFDE8: e
00AFFDEC: f
```

Microsoft Visual C++ Runtime Library.

Debug Error

Program: D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c++.exe  
Module: D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c++.exe  
File:

Run-Time Check Failure #2 - Stack around the variable 'p' was corrupted.

(Press Retry to debug the application)

中止(A) 重试(R) 忽略(I)

## 2、①放开, ②注释

```
D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c++.exe

addr: 0098F9DC
0098F9CC: cccccccc
0098F9D0: ffffffff
0098F9D4: cccccccc
0098F9D8: cccccccc
0098F9DC: 0
0098F9E0: 1
0098F9E4: 2
0098F9E8: 3
0098F9EC: 4
0098F9F0: 5
0098F9F4: 6
0098F9F8: 7
0098F9FC: 8
0098FA00: 9
0098FA04: a
0098FA08: 6e5f277
0098FA0C: 98fa2c
0098FA10: 730d3
0098FA14: e
0098FA18: f
```

Microsoft Visual C++ Runtime Library.

Debug Error

Program: D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c++.exe  
Module: D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c++.exe  
File:

Run-Time Check Failure #2 - Stack around the variable 'p' was corrupted.

(Press Retry to debug the application)

## 4、①②全部放开

```
D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c++.exe

addr: 006FFE48
006FFE38: cccccccc
006FFE3C: ffffffff
006FFE40: cccccccc
006FFE44: cccccccc
006FFE48: 0
006FFE4C: 1
006FFE50: 2
006FFE54: 3
006FFE58: 4
006FFE5C: 5
006FFE60: 6
006FFE64: 7
006FFE68: 8
006FFE6C: 9
006FFE70: ffffffff
006FFE74: 8b70169c
006FFE78: 6ffe98
006FFE7C: 1630d3
006FFE80: e
006FFE84: f
```

Microsoft Visual C++ Runtime Library.

Debug Error

Program: D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c++.exe  
Module: D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c++.exe  
File:

Run-Time Check Failure #2 - Stack around the variable 'p' was corrupted.

(Press Retry to debug the application)



1、①②全部注释

```
Microsoft Visual Studio 调试控制台
addr:003CFD24
003CFD14:431400
003CFD18:8cde68
003CFD1C:8c0c68
003CFD20:75408ca0
003CFD24:0
003CFD28:1
003CFD2C:2
003CFD30:3
003CFD34:4
003CFD38:5
003CFD3C:6
003CFD40:7
003CFD44:8
003CFD48:9
003CFD4C:43e0940
003CFD50:431684
003CFD54:3cfd9c
003CFD58:4315fc
003CFD5C:1
003CFD60:8c0c68

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c++.exe (进程 14280)已退出, 代码为 0。
按任意键关闭此窗口。 . .
```

3、②放开，①注释

```
Microsoft Visual Studio 调试控制台
addr:00CFF988
00CFF978:e10a0
00CFF97C:e1400
00CFF980:f5de98
00CFF984:f5ac60
00CFF988:0
00CFF98C:1
00CFF990:2
00CFF994:3
00CFF998:4
00CFF99C:5
00CFF9A0:6
00CFF9A4:7
00CFF9A8:8
00CFF9AC:9
00CFF9B0:ffffffffd
00CFF9B4:7f13e0c0
00CFF9B8:e1684
00CFF9BC:ffa04
00CFF9C0:e15fc
00CFF9C4:1

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c++.exe (进程 29892)已退出, 代码为 0。
按任意键关闭此窗口。 . .
```

2、①放开，②注释

```
Microsoft Visual Studio 调试控制台
addr:0042FB50
0042FB40:5410a0
0042FB44:541400
0042FB48:b4e0a0
0042FB4C:b40b70
0042FB50:0
0042FB54:1
0042FB58:2
0042FB5C:3
0042FB60:4
0042FB64:5
0042FB68:6
0042FB6C:7
0042FB70:8
0042FB74:9
0042FB78:a
0042FB7C:ef702f0e
0042FB80:42fbc8
0042FB84:5415fc
0042FB88:1
0042FB8C:b40b70

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c++.exe (进程 17468)已退出, 代码为 0。
按任意键关闭此窗口。 . .
```

4、①②全部放开

```
Microsoft Visual Studio 调试控制台
addr:012FF8C0
012FF8B0:2f10a0
012FF8B4:2f1400
012FF8B8:14bde88
012FF8BC:14b0c80
012FF8C0:0
012FF8C4:1
012FF8C8:2
012FF8CC:3
012FF8D0:4
012FF8D4:5
012FF8D8:6
012FF8DC:7
012FF8E0:8
012FF8E4:9
012FF8E8:ffffffffd
012FF8EC:4d70c003
012FF8F0:2f1684
012FF8F4:12ff93c
012FF8F8:2f15fc
012FF8FC:1

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c++.exe (进程 19928)已退出, 代码为 0。
按任意键关闭此窗口。 . .
```

1、①②全部注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0x78fe94
0x78fe84:4cf007
0x78fe88:78ffcc
0x78fe8c:76f7dcd0
0x78fe90:30e99cd8
0x78fe94:0
0x78fe98:1
0x78fe9c:2
0x78fea0:3
0x78fea4:4
0x78fea8:5
0x78feac:6
0x78feb0:7
0x78feb4:8
0x78feb8:9
0x78febcb:a
0x78fec0:40bc30
0x78fec4:78fee0
0x78fec8:78ff68
0x78fecc:e
0x78fed0:f

Process exited after 0.132 seconds with return value 0
请按任意键继续. . .
```

3、②放开，①注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0x78fe94
0x78fe84:4cf007
0x78fe88:78ffcc
0x78fe8c:76f7dcd0
0x78fe90:48d951a7
0x78fe94:0
0x78fe98:1
0x78fe9c:2
0x78fea0:3
0x78fea4:4
0x78fea8:5
0x78feac:6
0x78feb0:7
0x78feb4:8
0x78feb8:9
0x78febcb:a
0x78fec0:40bc30
0x78fec4:78fee0
0x78fec8:78ff68
0x78fecc:e
0x78fed0:f

Process exited after 0.1059 seconds with return value 0
请按任意键继续. . .
```

2、①放开，②注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0x78fe94
0x78fe84:4cf007
0x78fe88:78ffcc
0x78fe8c:76f7dcd0
0x78fe90:9203a2ee
0x78fe94:0
0x78fe98:1
0x78fe9c:2
0x78fea0:3
0x78fea4:4
0x78fea8:5
0x78feac:6
0x78feb0:7
0x78feb4:8
0x78feb8:9
0x78febcb:a
0x78fec0:40bc30
0x78fec4:78fee0
0x78fec8:78ff68
0x78fecc:e
0x78fed0:f

Process exited after 0.1067 seconds with return value 0
请按任意键继续. . .
```

4、①②全部放开

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0x78fe94
0x78fe84:4cf007
0x78fe88:78ffcc
0x78fe8c:76f7dcd0
0x78fe90:40cb06f2
0x78fe94:0
0x78fe98:1
0x78fe9c:2
0x78fea0:3
0x78fea4:4
0x78fea8:5
0x78feac:6
0x78feb0:7
0x78feb4:8
0x78feb8:9
0x78febcb:a
0x78fec0:40bc40
0x78fec4:78fee0
0x78fec8:78ff68
0x78fecc:e
0x78fed0:f

Process exited after 0.1186 seconds with return value 0
请按任意键继续. . .
```

1、①②全部注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0x77fe94
0x77fe84:4cf007
0x77fe88:77ffcc
0x77fe8c:76f7dcd0
0x77fe90:6982ee46
0x77fe94:0
0x77fe98:1
0x77fe9c:2
0x77fea0:3
0x77fea4:4
0x77fea8:5
0x77feac:6
0x77feb0:7
0x77feb4:8
0x77feb8:9
0x77febca:a
0x77fec0:40bc30
0x77fec4:77fee0
0x77fec8:77ff68
0x77fecc:e
0x77fed0:f

Process exited after 0.1338 seconds with return value 0
请按任意键继续. . .
```

2、①放开，②注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0x77fe94
0x77fe84:4cf007
0x77fe88:77ffcc
0x77fe8c:76f7dcd0
0x77fe90:c830d342
0x77fe94:0
0x77fe98:1
0x77fe9c:2
0x77fea0:3
0x77fea4:4
0x77fea8:5
0x77feac:6
0x77feb0:7
0x77feb4:8
0x77feb8:9
0x77febca:a
0x77fec0:40bc30
0x77fec4:77fee0
0x77fec8:77ff68
0x77fecc:e
0x77fed0:f

Process exited after 0.153 seconds with return value 0
-
```

3、②放开，①注释

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0x77fe94
0x77fe84:4cf007
0x77fe88:77ffcc
0x77fe8c:76f7dcd0
0x77fe90:658229fa
0x77fe94:0
0x77fe98:1
0x77fe9c:2
0x77fea0:3
0x77fea4:4
0x77fea8:5
0x77feac:6
0x77feb0:7
0x77feb4:8
0x77feb8:9
0x77febca:a
0x77fec0:40bc30
0x77fec4:77fee0
0x77fec8:77ff68
0x77fecc:e
0x77fed0:f

Process exited after 0.2105 seconds with return value 0
请按任意键继续. . .
```

4、①②全部放开

```
D:\课程文档\大二上\oop\homework\00测试程序\test.exe
addr:0x77fe94
0x77fe84:4cf007
0x77fe88:77ffcc
0x77fe8c:76f7dcd0
0x77fe90:be29c5d2
0x77fe94:0
0x77fe98:1
0x77fe9c:2
0x77fea0:3
0x77fea4:4
0x77fea8:5
0x77feac:6
0x77feb0:7
0x77feb4:8
0x77feb8:9
0x77febca:a
0x77fec0:40bc40
0x77fec4:77fee0
0x77fec8:77ff68
0x77fecc:e
0x77fed0:f

Process exited after 0.1041 seconds with return value 0
请按任意键继续. . .
```





## 1、①②全部注释

```
[u2152041@oop ~]$ ./test
addr:0x7ffcfa9c9500
0x7ffcfa9c94f0:fa9c9668
0x7ffcfa9c94f4:7ffc
0x7ffcfa9c94f8:401284
0x7ffcfa9c94fc:0
0x7ffcfa9c9500:0
0x7ffcfa9c9504:1
0x7ffcfa9c9508:2
0x7ffcfa9c950c:3
0x7ffcfa9c9510:4
0x7ffcfa9c9514:5
0x7ffcfa9c9518:6
0x7ffcfa9c951c:7
0x7ffcfa9c9520:8
0x7ffcfa9c9524:9
0x7ffcfa9c9528:0
0x7ffcfa9c952c:b
0x7ffcfa9c9530:1
0x7ffcfa9c9534:0
0x7ffcfa9c9538:e
0x7ffcfa9c953c:f
段错误 (核心已转储)
```

## 2、①放开，②注释

```
[u2152041@oop ~]$ ./test
addr:0x7ffc67d75a90
0x7ffc67d75a80:67d75bf8
0x7ffc67d75a84:7ffc
0x7ffc67d75a88:40128b
0x7ffc67d75a8c:0
0x7ffc67d75a90:0
0x7ffc67d75a94:1
0x7ffc67d75a98:2
0x7ffc67d75a9c:3
0x7ffc67d75aa0:4
0x7ffc67d75aa4:5
0x7ffc67d75aa8:6
0x7ffc67d75aac:7
0x7ffc67d75ab0:8
0x7ffc67d75ab4:9
0x7ffc67d75ab8:a
0x7ffc67d75abc:b
0x7ffc67d75ac0:1
0x7ffc67d75ac4:0
0x7ffc67d75ac8:e
0x7ffc67d75acc:f
段错误 (核心已转储)
```

## 3、②放开，①注释

```
[u2152041@oop ~]$ ./test
addr:0x7ffd4fb1ee80
0x7ffd4fb1ee70:4fb1efe8
0x7ffd4fb1ee74:7ffd
0x7ffd4fb1ee78:40128b
0x7ffd4fb1ee7c:0
0x7ffd4fb1ee80:0
0x7ffd4fb1ee84:1
0x7ffd4fb1ee88:2
0x7ffd4fb1ee8c:3
0x7ffd4fb1ee90:4
0x7ffd4fb1ee94:5
0x7ffd4fb1ee98:6
0x7ffd4fb1ee9c:7
0x7ffd4fb1eea0:8
0x7ffd4fb1eea4:9
0x7ffd4fb1eea8:ffffffffd
0x7ffd4fb1eeac:b
0x7ffd4fb1eeb0:1
0x7ffd4fb1eeb4:0
0x7ffd4fb1eeb8:e
0x7ffd4fb1eebc:f
段错误 (核心已转储)
```

## 4、①②全部放开

```
[u2152041@oop ~]$ ./test
addr:0x7ffd32b3a690
0x7ffd32b3a680:32b3a7f8
0x7ffd32b3a684:7ffd
0x7ffd32b3a688:401292
0x7ffd32b3a68c:0
0x7ffd32b3a690:0
0x7ffd32b3a694:1
0x7ffd32b3a698:2
0x7ffd32b3a69c:3
0x7ffd32b3a6a0:4
0x7ffd32b3a6a4:5
0x7ffd32b3a6a8:6
0x7ffd32b3a6ac:7
0x7ffd32b3a6b0:8
0x7ffd32b3a6b4:9
0x7ffd32b3a6b8:ffffffffd
0x7ffd32b3a6bc:b
0x7ffd32b3a6c0:1
0x7ffd32b3a6c4:0
0x7ffd32b3a6c8:e
0x7ffd32b3a6cc:f
段错误 (核心已转储)
```



## §. 关于动态内存申请后越界访问的深度讨论

★ 如何判断普通数组的越界访问（C方式，**注意源程序后缀为.c**）

```
/* 2152041 王浩 计科 */
#define _CRT_SECURE_NO_WARNINGS
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int main()
{
    char p[10];

    strcpy(p, "123456789");
    // p[10] = 'a';    //此句越界
    p[14] = 'A';    //此句越界
    p[15] = 'B';    //此句越界
    // p[10] = '\xfd'; //此句越界
    printf("addr:%p\n", p);
    for (int i = -4; i < 16; i++) //注意，只有0-9是合理范围，其余都是越界读
        printf("%p:%02x\n", (p + i), p[i]);

    return 0;
}
```

数组为char a[10]形式

在理解P. 1/P. 2的情况下，自行构造相似的程序，来观察数组越界后的内存表现，并验证与动态申请是否相似

要求：

- 1、数组用 char a[10]; 形式
- 2、数组用 int a[10]; 形式
- 3、测试程序在下面五种环境下运行  
VS2022 x86/Debug  
VS2022 x86Release  
Dev 32bit-Debug  
Dev 32bit-Release  
Linux
- 4、每种讨论的结果可截图+文字说明，如果几种环境的结果一致，用一个环境的截图+文字说明即可（可加页）



## 1、①②全部注释

```
Microsoft Visual Studio 调试控制台

addr: 004FF838
004FF834: ffffffff
004FF835: ffffffff
004FF836: ffffffff
004FF837: ffffffff
004FF838: 31
004FF839: 32
004FF83A: 33
004FF83B: 34
004FF83C: 35
004FF83D: 36
004FF83E: 37
004FF83F: 38
004FF840: 39
004FF841: 00
004FF842: ffffffff
004FF843: ffffffff
004FF844: ffffffff
004FF845: ffffffff
004FF846: 41
004FF847: 42

D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c.exe (进程 6296) 已退出。 代码为 0。
按任意键关闭此窗口。 . . .
```

## 2、①放开，②注释

```
D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c.exe

addr: 010FF778
010FF774: ffffffff
010FF775: ffffffff
010FF776: ffffffff
010FF777: ffffffff
010FF778: 31
010FF779: 32
010FF77A: 33
010FF77B: 34
010FF77C: 35
010FF77D: 36
010FF77E: 37
010FF77F: 38
010FF780: 39
010FF781: 00
010FF782: 61
010FF783: ffffffff
010FF784: ffffffff
010FF785: ffffffff
010FF786: 41
010FF787: 42

Microsoft Visual C++ Runtime Library.

Debug Error!

Program: D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c.exe
Module: D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c.exe
File:

Run-Time Check Failure #2 - Stack around the variable 'p' was corrupted.

(Press Retry to debug the application)
```

## 3、②放开，①注释

```
D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c.exe

addr: 006FF998
006FF994: ffffffff
006FF995: ffffffff
006FF996: ffffffff
006FF997: ffffffff
006FF998: 31
006FF999: 32
006FF99A: 33
006FF99B: 34
006FF99C: 35
006FF99D: 36
006FF99E: 37
006FF99F: 38
006FF9A0: 39
006FF9A1: 00
006FF9A2: ffffffff
006FF9A3: ffffffff
006FF9A4: ffffffff
006FF9A5: ffffffff
006FF9A6: 41
006FF9A7: 42

Microsoft Visual C++ Runtime Library

Debug Error!

Program: D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c.exe
Module: D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c.exe
File:

Run-Time Check Failure #2 - Stack around the variable 'p' was corrupted.

(Press Retry to debug the application)
```

## 4、①②全部放开

```
D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c.exe

addr: 004FF75C
004FF758: ffffffff
004FF759: ffffffff
004FF75A: ffffffff
004FF75B: ffffffff
004FF75C: 31
004FF75D: 32
004FF75E: 33
004FF75F: 34
004FF760: 35
004FF761: 36
004FF762: 37
004FF763: 38
004FF764: 39
004FF765: 00
004FF766: ffffffff
004FF767: ffffffff
004FF768: ffffffff
004FF769: ffffffff
004FF76A: 41
004FF76B: 42

Microsoft Visual C++ Runtime Library

Debug Error!

Program: D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c.exe
Module: D:\课程文档\大二上\oop\homework\00测试程序\Debug\测试c.exe
File:

Run-Time Check Failure #2 - Stack around the variable 'p' was corrupted.

(Press Retry to debug the application)
```



1、①②全部注释

```
Microsoft Visual Studio 调试控制台
addr:00DCFE68
00DCFE64:ffffff98
00DCFE65:ffffffab
00DCFE66:28
00DCFE67:01
00DCFE68:31
00DCFE69:32
00DCFE6A:33
00DCFE6B:34
00DCFE6C:35
00DCFE6D:36
00DCFE6E:37
00DCFE6F:38
00DCFE70:39
00DCFE71:00
00DCFE72:41
00DCFE73:75
00DCFE74:03
00DCFE75:13
00DCFE76:63
00DCFE77:00

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c.exe (进程 25716) 已退出, 代码为 0。
按任意键关闭此窗口。 . . .
```

2、①放开，②注释

```
Microsoft Visual Studio 调试控制台
addr:005EFE88
005EFE84:ffffff98
005EFE85:ffffffab
005EFE86:ffffffb9
005EFE87:00
005EFE88:31
005EFE89:32
005EFE8A:33
005EFE8B:34
005EFE8C:35
005EFE8D:36
005EFE8E:37
005EFE8F:38
005EFE90:39
005EFE91:00
005EFE92:61
005EFE93:75
005EFE94:05
005EFE95:13
005EFE96:fffffec
005EFE97:00

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c.exe (进程 20952) 已退出, 代码为 0。
按任意键关闭此窗口。 . . .
```

3、②放开，①注释

```
Microsoft Visual Studio 调试控制台
addr:0075FC4C
0075FC48:ffffff98
0075FC49:ffffffab
0075FC4A:ffffff8a
0075FC4B:00
0075FC4C:31
0075FC4D:32
0075FC4E:33
0075FC4F:34
0075FC50:35
0075FC51:36
0075FC52:37
0075FC53:38
0075FC54:39
0075FC55:00
0075FC56:fffffffd
0075FC57:75
0075FC58:05
0075FC59:13
0075FC5A:23
0075FC5B:00

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c.exe (进程 17076) 已退出, 代码为 0。
按任意键关闭此窗口。 . . .
```

4、①②全部放开

```
Microsoft Visual Studio 调试控制台
addr:007BFF18
007BFF14:ffffff98
007BFF15:ffffffab
007BFF16:fffffac
007BFF17:00
007BFF18:31
007BFF19:32
007BFF1A:33
007BFF1B:34
007BFF1C:35
007BFF1D:36
007BFF1E:37
007BFF1F:38
007BFF20:39
007BFF21:00
007BFF22:fffffffd
007BFF23:75
007BFF24:05
007BFF25:13
007BFF26:6b
007BFF27:00

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c.exe (进程 6296) 已退出, 代码为 0。
按任意键关闭此窗口。 . . .
```

VS2022 x86/Release      Dev 32bit-Debug

Dev 32bit-Release





1、①②全部注释

```
addr:0x7fffd5f57c42
0x7fffd5f57c3e:00
0x7fffd5f57c3f:00
0x7fffd5f57c40:0d
0x7fffd5f57c41:00
0x7fffd5f57c42:31
0x7fffd5f57c43:32
0x7fffd5f57c44:33
0x7fffd5f57c45:34
0x7fffd5f57c46:35
0x7fffd5f57c47:36
0x7fffd5f57c48:37
0x7fffd5f57c49:38
0x7fffd5f57c4a:39
0x7fffd5f57c4b:00
0x7fffd5f57c4c:0a
0x7fffd5f57c4d:00
0x7fffd5f57c4e:00
0x7fffd5f57c4f:00
0x7fffd5f57c50:41
0x7fffd5f57c51:42
```

2、①放开，②注释

```
addr:0x7ffc85d8a0e2
0x7ffc85d8a0de:00
0x7ffc85d8a0df:00
0x7ffc85d8a0e0:0d
0x7ffc85d8a0e1:00
0x7ffc85d8a0e2:31
0x7ffc85d8a0e3:32
0x7ffc85d8a0e4:33
0x7ffc85d8a0e5:34
0x7ffc85d8a0e6:35
0x7ffc85d8a0e7:36
0x7ffc85d8a0e8:37
0x7ffc85d8a0e9:38
0x7ffc85d8a0ea:39
0x7ffc85d8a0eb:00
0x7ffc85d8a0ec:0a
0x7ffc85d8a0ed:00
0x7ffc85d8a0ee:00
0x7ffc85d8a0ef:00
0x7ffc85d8a0f0:41
0x7ffc85d8a0f1:42
```

3、② 放开，①注释

```
addr:0x7ffffc049662
0x7ffffc04965e:00
0x7ffffc04965f:00
0x7ffffc049660:0d
0x7ffffc049661:00
0x7ffffc049662:31
0x7ffffc049663:32
0x7ffffc049664:33
0x7ffffc049665:34
0x7ffffc049666:35
0x7ffffc049667:36
0x7ffffc049668:37
0x7ffffc049669:38
0x7ffffc04966a:39
0x7ffffc04966b:00
0x7ffffc04966c:0a
0x7ffffc04966d:00
0x7ffffc04966e:00
0x7ffffc04966f:00
0x7ffffc049670:41
0x7ffffc049671:42
```

4、①②全部放开

```
addr:0x7ffd7c77ad22
0x7ffd7c77ad1e:00
0x7ffd7c77ad1f:00
0x7ffd7c77ad20:0d
0x7ffd7c77ad21:00
0x7ffd7c77ad22:31
0x7ffd7c77ad23:32
0x7ffd7c77ad24:33
0x7ffd7c77ad25:34
0x7ffd7c77ad26:35
0x7ffd7c77ad27:36
0x7ffd7c77ad28:37
0x7ffd7c77ad29:38
0x7ffd7c77ad2a:39
0x7ffd7c77ad2b:00
0x7ffd7c77ad2c:0a
0x7ffd7c77ad2d:00
0x7ffd7c77ad2e:00
0x7ffd7c77ad2f:00
0x7ffd7c77ad30:41
0x7ffd7c77ad31:42
```





## §. 关于动态内存申请后越界访问的深度讨论

★ 如何判断普通数组的越界访问（C方式，**注意源程序后缀为.c**）

```
/* 2152041 王浩 计科 */
#define _CRT_SECURE_NO_WARNINGS
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int main()
{
    char p[10];

    strcpy(p, "123456789");
    // p[10] = 'a';    //此句越界
    p[14] = 'A';    //此句越界
    p[15] = 'B';    //此句越界
    // p[10] = '\xfd'; //此句越界
    printf("addr:%p\n", p);
    for (int i = -4; i < 16; i++) //注意，只有0-9是合理范围，其余都是越界读
        printf("%p:%02x\n", (p + i), p[i]);

    return 0;
}
```

数组为int a[10]形式

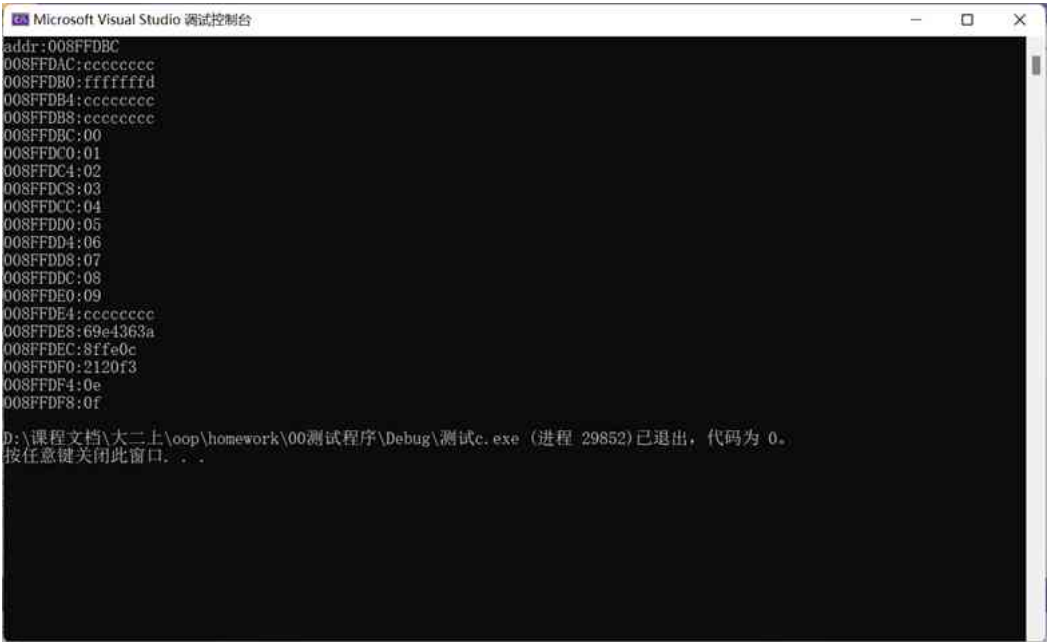
在理解P. 1/P. 2的情况下，自行构造相似的程序，来观察数组越界后的内存表现，并验证与动态申请是否相似

要求：

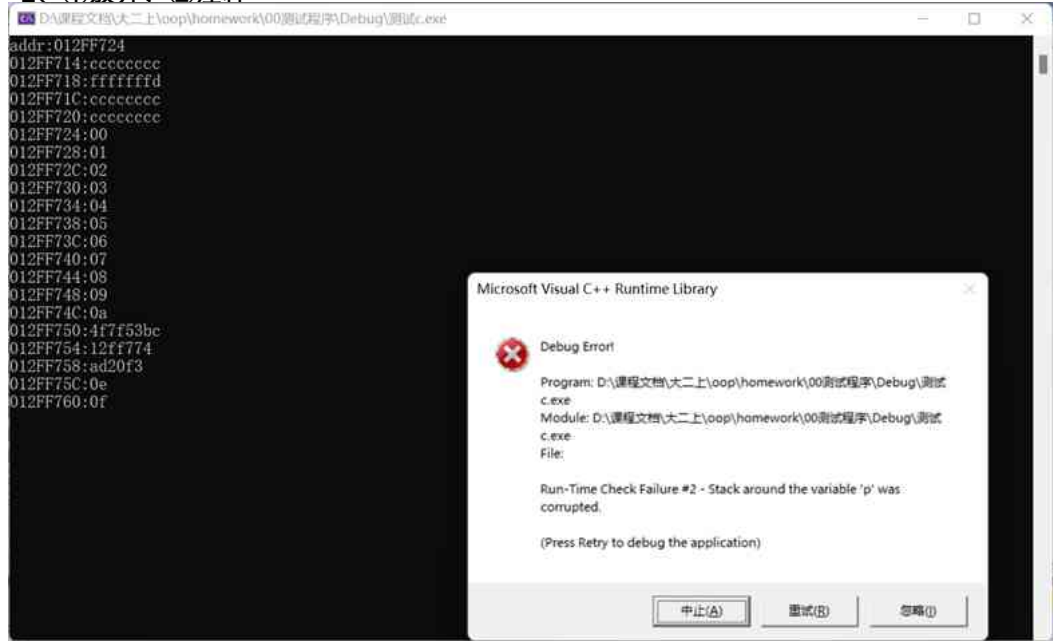
- 1、数组用 char a[10]; 形式
- 2、数组用 int a[10]; 形式
- 3、测试程序在下面五种环境下运行  
VS2022 x86/Debug  
VS2022 x86Release  
Dev 32bit-Debug  
Dev 32bit-Release  
Linux
- 4、每种讨论的结果可截图+文字说明，如果几种环境的结果一致，用一个环境的截图+文字说明即可(可加页)



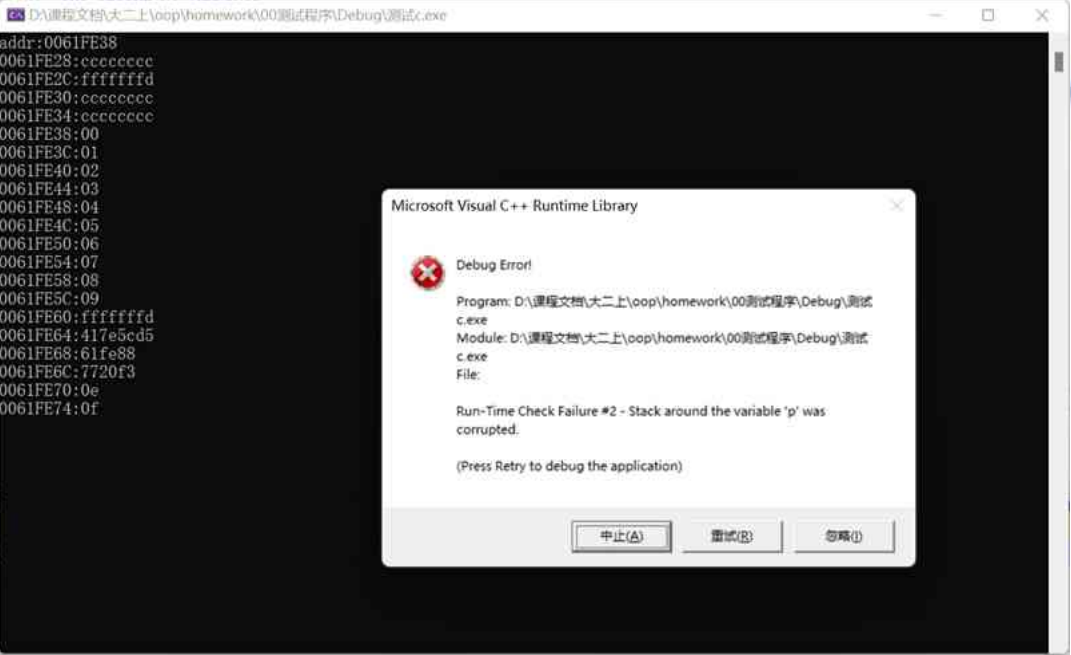
### 1、①②全部注释



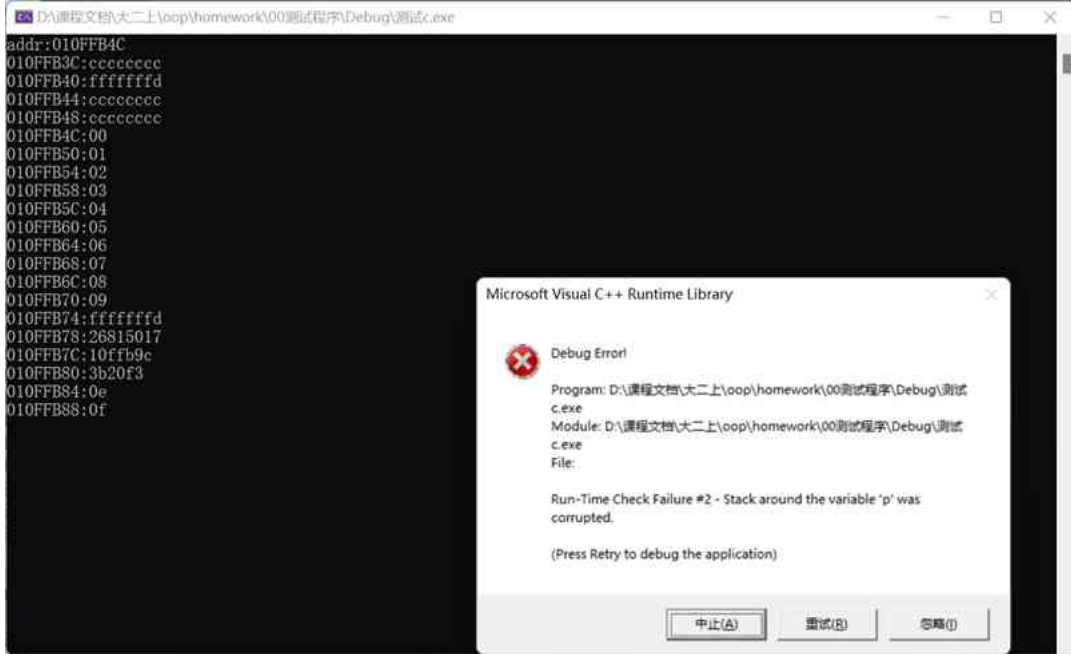
### 2、①放开，②注释



### 3、②放开，①注释



### 4、①②全部放开





1、①②全部注释

```
Microsoft Visual Studio 调试控制台
addr:001BF8F8
001BF8E8:d82108
001BF8EC:d82108
001BF8F0:6ade20
001BF8F4:6aabc0
001BF8F8:00
001BF8FC:01
001BF900:02
001BF904:03
001BF908:04
001BF90C:05
001BF910:06
001BF914:07
001BF918:08
001BF91C:09
001BF920:54d5f723
001BF924:1bfc6c
001BF928:d81289
001BF92C:01
001BF930:6aabc0
001BF934:6ade20

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c.exe (进程 27584) 已退出, 代码为 0。
按任意键关闭此窗口。 . . .
```

3、②放开，①注释

```
Microsoft Visual Studio 调试控制台
addr:0094FCA0
0094FC90:842108
0094FC94:842108
0094FC98:e2de50
0094FC9C:c2ab40
0094FCA0:00
0094FCA4:01
0094FCA8:02
0094FCAC:03
0094FCB0:04
0094FCB4:05
0094FCB8:06
0094FCBC:07
0094FCC0:08
0094FCC4:09
0094FCC8:ffffffffd
0094FCCC:4ab52fff
0094FCD0:94fd18
0094FCD4:841297
0094FCD8:01
0094FCDc:c2ab40

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c.exe (进程 28984) 已退出, 代码为 0。
按任意键关闭此窗口。 . . .
```

2、①放开，②注释

```
Microsoft Visual Studio 调试控制台
addr:0116FAC0
0116FAB0:ab2108
0116FAB4:ab2108
0116FAB8:143de18
0116FABC:143aaa0
0116FAC0:00
0116FAC4:01
0116FAC8:02
0116FACC:03
0116FAD0:04
0116FAD4:05
0116FAD8:06
0116FADC:07
0116FAE0:08
0116FAE4:09
0116FAE8:0a
0116FAEC:450ca16
0116FAF0:116fb38
0116FAF4:ab1297
0116FAF8:01
0116FAFC:143aaa0

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c.exe (进程 3184) 已退出, 代码为 0。
按任意键关闭此窗口。 . . .
```

4、①②全部放开

```
Microsoft Visual Studio 调试控制台
addr:0077FA2C
0077FA1C:672108
0077FA20:672108
0077FA24:bbdde0
0077FA28:bba658
0077FA2C:00
0077FA30:01
0077FA34:02
0077FA38:03
0077FA3C:04
0077FA40:05
0077FA44:06
0077FA48:07
0077FA4C:08
0077FA50:09
0077FA54:ffffffffd
0077FA58:3a775d10
0077FA5C:77faa4
0077FA60:671297
0077FA64:01
0077FA68:bba658

D:\课程文档\大二上\oop\homework\00测试程序\Release\测试c.exe (进程 3792) 已退出, 代码为 0。
按任意键关闭此窗口。 . . .
```



## 1、①②全部注释

```
addr:0x7ffc31bb22f0
0x7ffc31bb22e0:00
0x7ffc31bb22e4:00
0x7ffc31bb22e8:4011d3
0x7ffc31bb22ec:00
0x7ffc31bb22f0:00
0x7ffc31bb22f4:01
0x7ffc31bb22f8:02
0x7ffc31bb22fc:03
0x7ffc31bb2300:04
0x7ffc31bb2304:05
0x7ffc31bb2308:06
0x7ffc31bb230c:07
0x7ffc31bb2310:08
0x7ffc31bb2314:09
0x7ffc31bb2318:01
0x7ffc31bb231c:0b
0x7ffc31bb2320:01
0x7ffc31bb2324:00
0x7ffc31bb2328:0e
0x7ffc31bb232c:0f
段错误 (核心已转储)
```

## 2、①放开，②注释

```
addr:0x7ffcff515c00
0x7ffcff515bf0:00
0x7ffcff515bf4:00
0x7ffcff515bf8:4011da
0x7ffcff515bfc:00
0x7ffcff515c00:00
0x7ffcff515c04:01
0x7ffcff515c08:02
0x7ffcff515c0c:03
0x7ffcff515c10:04
0x7ffcff515c14:05
0x7ffcff515c18:06
0x7ffcff515c1c:07
0x7ffcff515c20:08
0x7ffcff515c24:09
0x7ffcff515c28:0a
0x7ffcff515c2c:0b
0x7ffcff515c30:01
0x7ffcff515c34:00
0x7ffcff515c38:0e
0x7ffcff515c3c:0f
段错误 (核心已转储)
```

## 3、②放开，①注释

```
addr:0x7ffd2a7652d0
0x7ffd2a7652c0:00
0x7ffd2a7652c4:00
0x7ffd2a7652c8:4011da
0x7ffd2a7652cc:00
0x7ffd2a7652d0:00
0x7ffd2a7652d4:01
0x7ffd2a7652d8:02
0x7ffd2a7652dc:03
0x7ffd2a7652e0:04
0x7ffd2a7652e4:05
0x7ffd2a7652e8:06
0x7ffd2a7652ec:07
0x7ffd2a7652f0:08
0x7ffd2a7652f4:09
0x7ffd2a7652f8:ffffffffd
0x7ffd2a7652fc:0b
0x7ffd2a765300:01
0x7ffd2a765304:00
0x7ffd2a765308:0e
0x7ffd2a76530c:0f
段错误 (核心已转储)
```

## 4、①②全部放开

```
addr:0x7fffa620d9f0
0x7fffa620d9e0:00
0x7fffa620d9e4:00
0x7fffa620d9e8:4011e1
0x7fffa620d9ec:00
0x7fffa620d9f0:00
0x7fffa620d9f4:01
0x7fffa620d9f8:02
0x7fffa620d9fc:03
0x7fffa620da00:04
0x7fffa620da04:05
0x7fffa620da08:06
0x7fffa620da0c:07
0x7fffa620da10:08
0x7fffa620da14:09
0x7fffa620da18:ffffffffd
0x7fffa620da1c:0b
0x7fffa620da20:01
0x7fffa620da24:00
0x7fffa620da28:0e
0x7fffa620da2c:0f
段错误 (核心已转储)
```





## §. 关于动态内存申请后越界访问的深度讨论

★ 最后一页：仔细总结本作业（多种形式的测试程序/多个编译器环境/不同结论），谈谈你对内存越界访问的整体理解  
包括但不限于操作系统/编译器如何防范越界、你应该养成怎样的使用习惯来尽量防范越界

内存访问时，操作系统和编译器不可能时刻监控着每块内存的变化，所以会通过相邻内存是否改变来进行简化编译过程。操作系统会监控数组和相应的动态申请的内存变化，而编译器则会监控数组的索引是否越界来判断是否越界访问。

为了防范越界，首先应该对申请的内存大小有着良好的认知，知道边界的位置，其次要在对相应的内存进行改变时进行测试，防止未知情况下的越界访问。