公告详情

课堂作业发布

发布于2024-12-16 16:37

课堂作业 1-1

要求：

1、请大家思考，希望通过本门课程学到的东西，同时通过手电脑，查阅资料，给出自己的理解，并写下来提交。

2、通过手机、电脑，查阅资料，请各位同学给出 linux el件的格式说明,并和 PE 列表做一个对比，简要说明两者的差

3、通过手机或者电脑，请大家简答 android 和 ios App 格式是什么样的?

课堂作业 2-1

1、请同学们详细给出如下函数调用过程中栈的数据变化：

```
int funcb(int a, int b)
{...
}
int funca()
{...
    funcb(4,2);
...
}
```

2、下列哪些措施不是有效的缓冲区溢出的防护措施？

A.使用标准的 C 语言字符串库进行操作；　B.严格验证输入字符串长度；

C.过滤不合规则的字符；　　D.使用第三方安全的字符串库操作。

3、字符串"hello!"的长度为（ ）字节，存储该字符串需要（ ）字节。

A. 6、6；　B. 6、7；　C. 7、6；　D. 7、7

4、通过手机等工具查阅，重新整理并描绘出 utf-8 的编码规则；给出下面编码的 names 字符串的长度。

```
char names[]
= "\xE7\xBD\x91\xE5\xAE\x89\x31\x31\x38\x30\x36\xE7\x8F\xAD\x00"
```

请大家把把整理好的答案写到【数学】作业纸上。请务必写上学号，班级和姓名。

课堂作业 3-1

1、根据课堂的内容，详细描述 C++虚函数的实现，画出 C++虚函数在内存中的布和实现示意图，并简单叙述一个利用虚表对虚函数开展攻击的过程。

2、通过手机、电脑，查阅资料，结合课堂的讲课内容，请各位同学画出 Linux 内存堆中空闲列表的结构，不限于 dlmalloc，并且使用文字辅助说明，并写到业纸上。

上课后 15 分钟以内提交，请务必写上学号，班级和姓名，并以数学作业纸提交

课堂作业 4-1

通过 dlmalloc(书上的版本) unlink 技术，构造代码实现攻击者提供 4 字节
写入到同样是攻击者指定的 4 字节地址。给出程序代码，并辅助详细的运
说明。

请学委把作业收上来！务必使用数学作业纸，写上姓名，班级号和学号，
面不够，尽量写在背面，不用两张纸。

课堂作业 4-2

1. 回顾 Linux 的相关技术，根据以下代码回答问题：

```
1. static char *GOT_LOCATION = (char *)0x0804c98c;
2. static char shellcode[] =
3.   "\xeb\x0cjump12chars_"  3.   /* jump */
4.   "\x90\x90\x90\x90\x90\x90\x90\x90"
5.
6. int main(void){
7.   int size = sizeof(shellcode);
8.   void *shellcode_location;
9.   void *first, *second, *third, *fourth;
10.   void *fifth, *sixth, *seventh;
11.   shellcode_location = (void *)malloc(size);
12.   strcpy(shellcode_location, shellcode);
13.   first = (void *)malloc(256);
14.   second = (void *)malloc(256);
15.   third = (void *)malloc(256);
16.   fourth = (void *)malloc(256);
17.   free(first);
18.   free(third);
19.   fifth = (void *)malloc(128);
20.   free(first);
21.   sixth = (void *)malloc(256);
22.   *((void **)(sixth+0))=(void *)(GOT_LOCATION-12);
23.   *((void **)(sixth+4))=(void *)shellcode_location;
24.   seventh = (void *)malloc(256);
25.   strcpy(fifth, "something");
26.   return 0;
27. }
```

1) 当 first 块在初次释放时，会被放入_____

2) 为 second 和 fourth 块分配空间是为_____

3) first 所指向的内存块被分配给了_____块和_____块，程序行至第_____行时，程序的控制权被转移到 shellcode 中

课堂作业 5-1

1、请仔细分析如下代码：

```
01. int main(int argc, char *argv[]) {
02.     unsigned short int total;
03.     total = strlen(argv[1])+strlen(argv[2])+1;
04.     char *buff = (char *)malloc(total);
05.     strcpy(buff, argv[1]);
06.     strcat(buff, argv[2]);
07. }
```

通过查阅资料，互相讨论，把该代码可能的问题列举出来，针对每一个问题并进行简单的说明。

2、代码如下图所示，在计算前会把比 int 小的整型提升为 int，则会发生整截断的有：

```
char cresult1, cresult2, c1, c2, c3;
c1 = 100;
c2 = 90;
c3 = -120;
cresult1 = c1 + c2 ;
cresult2 = c1 + c2 + c3;
```

A. cresult1, cresult2　　B. cresult1　　C. cresult2　　D. 无

3、以下关于范围检查的说法中错误的是：

A. 所有外部输入的数据都要进行上下界检查

B. 任何能够限制过大或过小输入的措施，都有助于防止溢出和其他类型范错误

C. 如果适当地运用类型范围检查，就够消除所有的整型漏洞

D. 同时使用隐式和显式检查过于累赘，不推荐使用

课堂作业 5-2

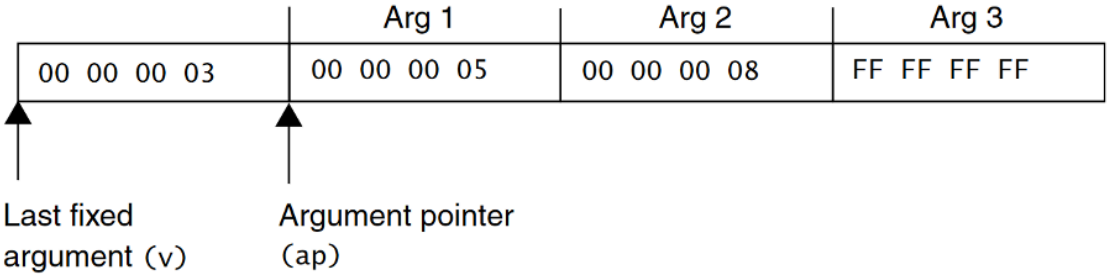
对于乘法的后验检测，对于 16 位带符号整数，进行简化对溢出的检测：将
和 RHS 两个操作数都转型成 32 位值，并将乘积结果存储到 32 位的目的域中.
果结果积右移 16 位和右移 15 位所得结果不一致，则说明发生了溢出。请问这
为什么呢？举例子说明。

课堂作业 6-1

1.根据以下代码回答问题：

```
1  int average(int first, ...) {
2      int count = 0, sum = 0, i = first;
3      va_list marker;
4      va_start(marker, first);
5      while (i != -1) {
6          sum += i;
7          count++;
8          i = va_arg(marker, int);
9      }
10     va_end(marker);
11     return(sum ? (sum / count) : 0);
12 }
```

调用 average(3,5,8,-1)时，参数被安排在栈上的示例图：



在用 va_start()初始化字符指针后，字符指针指向(　　)，当 va_sta
返回时， va_list 将指向(　　)

A. 最后一个定参的地址　　B. 最后一个可选参数的地址

C. 最后一个定参之后的参数　　D. 第一个可选参数的地址

请用 15 分钟时间来完成，并写到作业纸上。请务必写上学号，班级和姓名
完后请学委把作业收上来！

课堂作业 6-2

1.速查阅相关资料，请大家整理 printf 的安全问题，并详细解释通过 printf 如做到查看某个具体位置的内存的内容。

请用 10 分钟时间来完成，并写到作业纸上。请务必写上学号，班级和姓名。完后请学委把作业收上来！