**第一题**

ilist = (int \*) malloc(size2);//这里只分配了size2个字节，而不是size2\*4个字节

scanf("%s", str); /\* user inputs a string \*/这里没有指定输入字符串的长度，也会产生越界

scanf("%d", ilist + i); /\* user inputs an integer \*/这样是不可以的因为list只分配了size2个字节，而一个整数占四个字节，所以list输入不到最后就会越界，并且产生的是堆上的越界，非常危险

}

并且程序结束后没有释放内存

}

**第二题**

/\* return 1 if str is "1", 0 otherwise \*/  
int checkIf1(char \*str) {

char \*newstr = malloc(strlen(str) + 1);//这里没有将malloc返回的指针转换为char

strcpy(newstr, str); /\* set newstr to str \*/

if (strcmp(newstr, "1") == 0) { /\* newstr is "1" \*/

return 1;//这里没有释放内存

}

free(newstr);释放内存时候没有将newstr指向NULL

return 0;

}  
  
void main() {

char \*strArr[4] = {"1", "2", "3", "4"};

int i;

for(i = 0; i < 4; i++) {

printf("%d\n", checkIf1(strArr[i]));

}

**第三题**

struct data {

char \*str1, \*str2;

};   
  
/\* returns two strings concatenated if they are not the same, NULL otherwise \*/  
char \*mergeSingleIfDifferent(char \*s1, char \*s2) {

char \*str = (char \*) malloc(strlen(s1) + strlen(s2) + 1);  
if (strcmp(s1, s2) == 0) { /\* strings are equal \*/

str = NULL;//这里没有释放str的内存

}  
else {

strcpy(str, s1);

strcat(str, s2);

}

return str;

}  
  
/\* copies merged strings (or NULL) into array of strings passed in (results) \*/  
void mergeArrayIfDifferent(char \*results[], char \*strA1[], char \*strA2[], int size) {

int i;  
  
for(i = 0; i < size; i++) {

results[i] = mergeSingleIfDifferent(strA1[i], strA2[i]);

}

}

void printAndFree(int c, char \*str) {

if (str != NULL) {

printf("%d: %s\n", c, str);  
free(str);

}

}  
  
void main() {

char \*strArr1[8] = {"1", "2", "3", "4", "5", "6", "7", "8"};  
char \*strArr2[8] = {"a", "2", "c", "4", "e", "6", "g", "8"};  
char \*results[8];  
int i;  
  
mergeArrayIfDifferent(results, strArr1, strArr2, 8);  
for(i = 0; i < 8; i++) {//

printAndFree(i, results);//这里应该是results[i]不然会出现free没有分配过的指针

}

}