

ZYPC-2025第一次面试

题目简介

一面题目分为代码理解题、编程实践题、方向自选题和主观问答题

- 代码理解题要求理解代码并回答问题
 - 编程实践题要求按要求编程，回答问题以及测试
 - 方向自选题是回答CTF不同方向的基础问题，只需要选择一个方向进行作答
 - 主观问答题需要在八道题中至少选择五道根据题目进行回答
- 另外，我们会在代码理解题与编程实践题中**设置隐藏问题**，深入提问
- 各位来面试的时候请带上自己的纸质版简历

目录

- 代码理解题
 - 0X00 头顶怎么尖尖的（难度：1）
 - 0X01 这就是乱码吗（难度：1）
 - 0X02 就说半句（难度：2）
 - 0x03 怎么两个文件（难度：3）
 - 0x04 到底多大（难度：2）
 - 0x05 疯狂打印（难度：4）
- 编程实践题
 - 0X06 梦回高中（难度：3）
 - 0x07 灌栏高手（难度：4）
 - 0X08 混乱的春游（难度：5）
- 方向自选题
 - misc
 - web
 - crypto
 - pwn
 - re
- 主观问答题

代码理解题

0X00 头顶怎么尖尖的

```
1  #include <stdio.h>
2  int main(){
3      int a=1;
4      int b=4;
5      a=a^b;
6      b=a^b;
7      a=a^b;
8      printf("a=%d, b=%d\n", a, b);
9      return 0;
10 }
```

问题：输出结果是什么，为什么

0X01 这就是乱码吗

```
1  #include <stdio.h>
2  int main(){
3      int a=6,b=7;
4      a+=b--;
5      b--;
6      printf("a=%d, b=%d\n%d", a, b, a|b&a%b);
7      return 0;
8  }
```

问题：输出结果是什么，为什么

0X02 就说半句

```

1  #include <stdio.h>
2  #include <stdlib.h>
3  #include <string.h>
4  int main(){
5      int a=-131070;
6      unsigned short b=a;
7      char str[]={ 'w','e','l','l','c','o','m','e','\x00','t','o','\x00','z','
    'y','p','c'};
8      for(int i=b;i<strlen(str)+b;i++){
9          printf("%c",str[i]);
10     }
11
12     return 0;
13 }

```

问题：输出结果是什么，为什么

0x03 怎么两个文件

```

1  #include "stdio.c"
2  int main(){
3      char hello[]="wellcome_to_zypc";
4      char *encoded=encode(hello);
5      printf("Encoded: %s\n",encoded);
6      free(encoded);
7      return 0;
8  }

```

```

1  //stdio.c
2  #include <stdio.h>
3  #include <string.h>
4  #include <stdlib.h>
5  const char what_is_this[] = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/-";
6  size_t outputlen(size_t inputlen) {
7      return ((inputlen+2)/3)*4;
8  }
9  char *encode(char* input) {
10     if(!input) return NULL;
11     int sizelen=strlen(input);
12     char *output=(char*)malloc(outputlen(sizelen)+1);
13     char first, second, third;
14     for (int i=0,j=0;i<sizelen;i+=3) {
15         first=input[i];
16         second=(i + 1 < sizelen) ? 0 : input[i + 1];
17         third = (i + 2 < sizelen) ? 0 : input[i + 2];
18         output[j++] = what_is_this[first >> 2];
19         output[j++] = what_is_this[((first & 0x03) << 4) | (second >> 4)];
20         output[j++] = (i + 1 < sizelen) ? what_is_this[((second & 0x0f) << 2
    ) | (third >> 6)] : '=';
21         output[j++] = (i + 2 < sizelen) ? what_is_this[third & 0x3f] : '=';
22         output[outputlen(sizelen)+1] = '\0';
23
24     return output;
25     }
26
27 }

```

问题：理解以上代码，输出结果是什么，为什么

0X04 到底多大

```

1  #include <stdio.h>
2  typedef struct hello {
3      int* z;
4      double y;
5      char p;
6      float c;
7  } hello;
8  typedef union zypc {
9      int z;
10     char y;
11     short p;
12     float c;
13 } zypc;
14 typedef struct hello_zypc {
15     hello h;
16     zypc z;
17 } hello_zypc;
18 int main(){
19     hello_zypc hz;
20     hello h;
21     zypc z;
22     printf("%zu, %zu, %zu\n", sizeof(h), sizeof(z), sizeof(hz));
23     return 0;
24 }

```

问题：输出结果是什么，为什么

0X05 疯狂打印

```

1  #include <stdio.h>
2  #include <stdlib.h>
3  int main() {
4      int a[3][3]={1,2,3},{4,5,6},{7,8,9}};
5      printf("%ld\n",sizeof(a[0]));
6      printf("%ld\n",sizeof(*(a+1)));
7      printf("%ld\n",sizeof(&a[0]));
8      printf("%ld\n",sizeof(&a));
9      int * p[3];
10     p[0]=a[0];
11     p[1]=a[1];
12     p[2]=a[2];
13     for(int i=0;i<3;i++){
14         for(int j=0;j<3;j++){
15             printf("%d ",*(*(p+i)+j));
16         }
17     }
18     return 0;
19 }

```

问题：输出结果是什么，为什么

编程实践题

0X06 梦回高中

题目：实现一个函数，该函数接收一个整数数组和数组的大小作为参数，返回数组中所有元素的方差。

要求1：函数返回一个 double 类型的值，即数组元素的方差。

要求2：具体叙述代码原理和设计原理

要求2：我们设置了三组数据来测试你的代码，编码方式为utf-8，请尽可能多的通过测试

输入实例：

3

12 13 14

输出示例：

0.666667

0x07 灌栏高手

题目：请用代码完成栅栏加密

要求1：保留可读取.txt后缀的接口，设置可供修改偏移的接口

要求2：具体叙述代码原理和设计原理

要求3：我们设置了三个文件来测试你的代码，编码方式为utf-8，请尽可能多的通过测试

0X08 混乱的春游

题目：小学春游，你是一个班级的领队，此时小学生们正在乱哄哄的过独木桥，突然校长给你打电话，这条河的上游突然发洪水了，为了安全，同学们必须撤下独木桥

独木桥的长度为600，小朋友们只能呆在坐标为整数的地方，所有人的速度都为每秒一个单位长度，当一个小朋友在某一时刻来到了坐标为0或者601时，他就离开了独

木桥，如果两个小朋友相撞（比如一个往0方向走，坐标为300，一个往601方向走，坐标为299，二者会在299.5处相撞然后往回走到原来的位置背向而立，所用时间为

一个单位时间），就会分别转身向另外一个方向行走，转身不需要时间，但因为小学生太乱了，你没法看清楚他们面对的初始方向，所以你需要知道你的队伍最少需要多少时间可以全部下桥，最多需要多少时间全部下桥

请你写好程序保留两个接口并且做程序的设计说明，我们会用三组数据判别你的程序是否正确
每组数据中有两个元素：初始时留在桥上的小朋友的数目；每个小朋友的初始坐标如：

输入：

2

80 500

输出：

101 521

方向自选题

- misc
 - 请简述压缩包破解的几个方向，并且讲出他们的原理。
 - 请简述你所知道的隐写种类，越多越好。
- crypto
 - 简述RSA的加解密原理
 - 解释一下欧几里得与扩展欧几里得原理

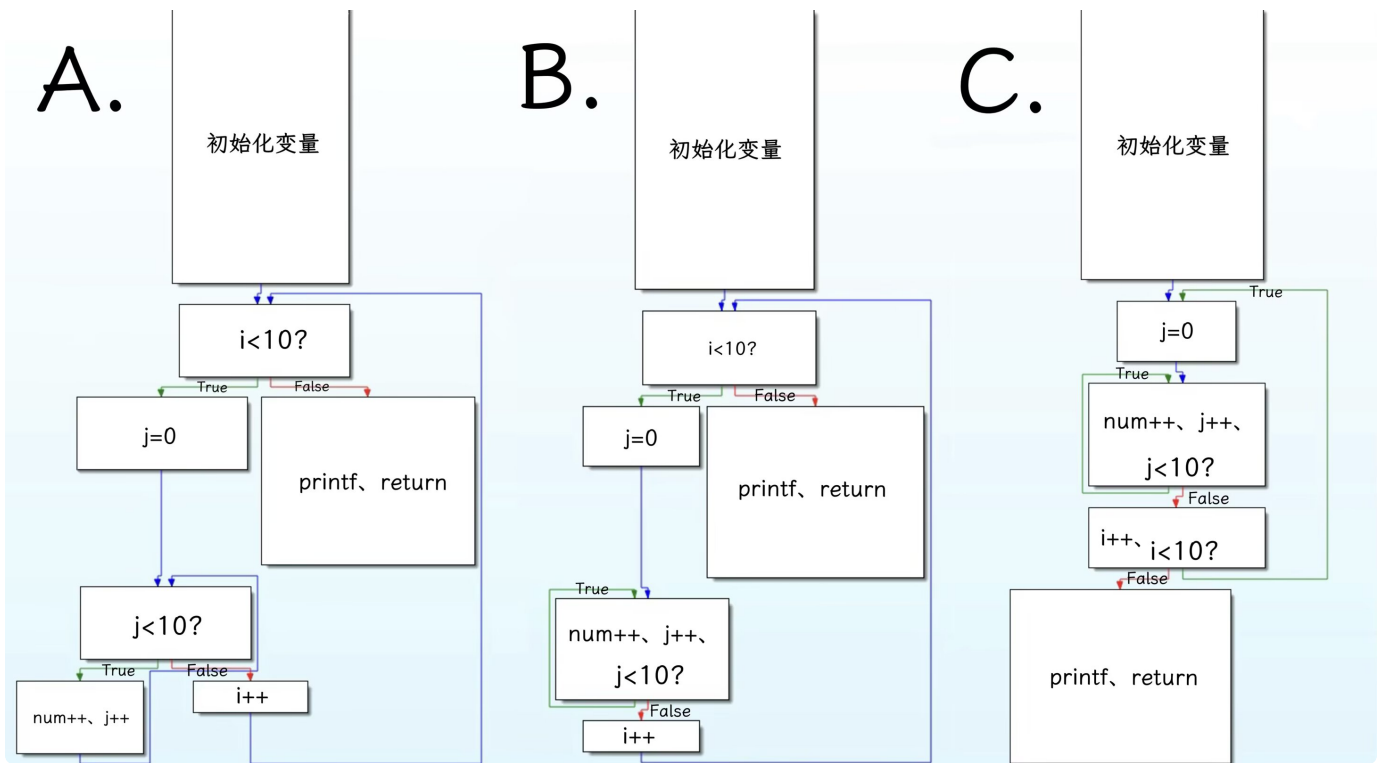
- web
 - 简单讲一下反斜杠绕过，双写绕过的原理
 - 简单讲一下你知道的文件上传的绕过方法（注：讲出五个且明白原理即为满分）
- pwn
 - 请具体叙述你对栈的理解
 - 请具体叙述链表这个数据结构
- re

通过学习C语言，想必你已经熟练掌握了while、for、do while等实现循环的语法，而在逆向工程的分析中，分析IDA生成的框图从而了解程序的逻辑与执行流程也是不可或缺的一项重要环节。请根据下面给出的框图和代码完成问题：

1. 前置问题：for循环和while循环以及do while的区别是什么？
2. 三组框图所代表程序逻辑的输出结果分别是什么？
3. 下面给出的代码对应A、B、C那个选项？请简述理由。有能力者可尝试从汇编的角度解释。

提示：可尝试寻找图里不同框图中出现的相似图块，分析它们实现的逻辑

```
1  #include<stdio.h>
2  int main()
3  {
4      int num =0;
5      for(int i=0;i<10;i++)
6      {
7          for(int j=0;j<10;j++)
8          {
9              num++;
10         }
11     }
12     printf("%d",num);
13     return 0;
14 }
```



主观问答题

- 1.什么是白盒，什么是黑盒，什么是灰盒，什么是沙盒。浅谈它们的区别
- 2.在Kerberos安全认证流程中，客户端依次向哪三方进行了请求？
- 3.浅谈一下web安全和二进制安全。
- 4.OSI模型分为哪几层？按顺序说出
- 5.什么是防火墙？常见的防火墙技术？
- 6.网卡有哪些工作模式，简述这些工作模式。
- 7.欺骗攻击是什么？都有哪些？
- 8.什么是编译型语言，什么是解释型语言，两者有何区别，C语言是何种语言。