# 智邮普创 SEC - 2023 第一次面试题目

**ATTENTION**

- 需要编写代码的题目请在面试前思考并准备，优先使用C语言编写；
- 需要携带电脑到面试现场，请提前配置环境。在Linux环境下运行的题目需要提前装好虚拟机（软件&镜像）；
- 客观题题目难度与顺序无关，难度组成：五道基础题、两道中等题，另有一道Linux指令分析题、一道IDA程序分析题和三道编程题。

## 0x00 | Introducing Yourself

介绍你自己，可以自行选择简历的形式。

**提示**

- 内容包括但不限于需要包含姓名、班级、学号、个人经历、个人技能、自我介绍；
- 简历可以打印，方便查看[Optional]；
- 如使用*Markdown* 撰写可加分[Optional]。

## 0x01 | 分析此函数并解释原因

```
// 代码片段
int func1()
{
    int a =10;
    int* b = &a;
    while (*b)
    {
        switch ((a++) *2)
        {
        case 1:
            printf("This");
        default:
            printf("");
        case '_':
            printf("\x12");
                break;
        case 3:
            printf("is");
```

```
        case 2:
            printf("a");
            break;
        case 40:
            printf("zypc2023");
            break;
        case 42:
            printf("interview");
            printf("\n");
            return 0;
        case 100:
            printf("question");
        }
    }

}

```

## 0x02 | 分析以下程序的输出并说明原因

```c
#include <stdio.h>
int main(){
    unsigned int a,c;
    a = 9876543210;
    c = 9 * a;
    printf("%u",c);
}
```

## 0x03 | 分析以下程序

```c
#include <stdio.h>
int main() {
    int x = 5;
    int y = 10;
    int z = 15;
    int result = (x++ > 5) || (--y == 9) && (z += 5);
    printf("%d %d %d %d\n", x, y, z, result);
    return 0;
}
```

## 0x04 | 分析以下代码的输出并说明原因

```c
#include <stdio.h>
#include <string.h>
int main(){
    char str[] = "abc\000def\n";
    int str_len ,str_size;
    str_len = strlen(str);
    str_size = sizeof(str);
    printf("%d,%d",str_len,str_size);
    return 0;
}
```

## 0x05 | 说出以下程序的输出

```c
//代码片段
main(){
    int a=65;
    char c='A';
    printf("%x,%d",a,c);
}
```

## 0x06 | 分析以下代码的输出并说明原因

```c
#include<stdio.h>
int main(){
    char w;
    int x,result;
    float y;
    double z;
    result = sizeof(w*x+z-y);
    printf("%d",result);
    return 0;
}
```

## 0x07 | 分析以下程序

分析以下程序，给出正确的输出结果。

```c
#include <stdio.h>

void swapChars(char *a, char *b) {
    char temp = *a;
    *a = *b;
    *b = temp;
}

void modifyString(char *str) {
    char *ptr1 = str + 1;
    char *ptr2 = str + 3;
    char *ptr3 = str + 4;
    swapChars(ptr1, ptr2);
    swapChars(ptr2, ptr3);
}

int main() {
    char str[10] = "abcdefgh";
    char *ptr = str;

    for (int i = 0; i < 4; i++) {
        modifyString(ptr);
        ptr++;
    }
    printf("%s\n", str);
    return 0;
}
```

## 0x08 | Linux命令分析

Linux是计算机领域常见的操作系统门类，分析以下Linux命令行操作：

```
curl -LO https://xupt.edu.cn/ZYPC_php_program.zip && unzip ZYPC_php_program.zip -d /tmp/zypc && rm ZYPC_php_program.zip && find /tmp/zypc -type f -exec chmod 644 {} \; && sed -i 's/flag{/zypc_flag{/g' /tmp/zypc/src/*.php && mv /tmp/zypc/src/* /www && git add . && tar -czvf new_archive.tar.gz /www 2>&1 | tee bash_log.txt | grep "docker" > result.txt && vim result.txt
```

**提示**

这道题禁用了代码高亮，你可以尝试将命令拆解，再逐一分析。

**三点思考** `Optional`

1. `sed` 中的替换字符串为什么使用 `/` 作为分隔符？能否使用其他字符分隔？
2. 在文件权限修改的部分，为什么需要 `find` 配合使用来更改权限？能否直接使用 `chmod` 修改整一个目录的权限？
3. 这段命令的用途可能是什么？

# 0x09 | linux可执行文件逆向分析

分析以下文件，以Linux系统运行，交互使其输出 `Right!` 。

文件链接：https://pan.baidu.com/s/1aRANSfqqK66vcJmXx5ZuBg?pwd=zypc。

**提示**

- 由于条件限制，文件名经过修改，你需要还原一下；
- 你可能需要了解**Linux文件后缀名。**

# 0x0A | 编程题

三道编程题中 `Check A` 和 `Check B` 为必做， `Check C` 为选做。

## Check A | 字数统计

编写一个程序，实现一个子函数用来计算输入的字符串中的单词个数。单词之间由一个或多个空格分隔，不考虑标点符号。

### 要求

在主函数里输入一个字符串，然后调用子函数计算并输出该字符串中的单词个数。

## Check B | Fibonacci Sequence

请编写一个**递归函数**，计算斐波那契数列的第N项（N>0）。尽可能使函数高效。仅需要编写核心代码部分。

### 需要完善的代码

```c
#include <stdio.h>

unsigned long long fibonacci(int n) {
    //
    // 在这里编写函数
    //
}

int main() {
    int n = 50;
    unsigned long long result = fibonacci(n);
    printf("Fibonacci(%d) = %llu\n", n, result);
    return 0;
}
```

## Check C | 对话问答 Optional

### 要求

假如你是一位客服，要求对客户的提问进行回答。在用户的两次提问间隔中，允许有一次或多次回答，但每一次提问后至少要有一个回答才可以解除客户的疑问。

### Input

- 每个测试点第一行为测试的次数，也就是一共有多少组对话；
- 第二行是该组对话的问答次数总和；
- 第三行则是具体的对话，`A` 代表 *Answer*，即回答，`Q` 代表 *Question*，即提问。
- 我们确保第一个字母永远是 `Q` 。

### Output

对于每组对话，判断其是否符合要求，符合则输出 `Yes` ，反之则输出 `No` 。

### Sample

| Input 输入 | Output 输出 |
| --- | --- |
| 5<br>4<br>QQAA<br>4<br>QQAQ<br>3<br>QAA<br>1<br>Q<br>14<br>QAQQAQAAQQQAAA | <br><br><br>Yes<br>No<br>Yes<br>No<br>Yes |

**Sample 解释:**

- 第一组对话，有两个问题，两个回答，**问题数等于回答数**，所以输出 `Yes` ；
- 第二组对话，有三个问题，一个回答，**问题数大于回答数**，所以输出 `No` ；
- 第三组对话，有一个问题，两个回答，**问题数小于回答数**，所以输出 `Yes` ；
- 第四组对话，**只有问题没有回答**，所以输出 `No` ；
- 第五组对话，**每一个Q都有一个A去解决**，所以输出 `Yes` 。

# 0x0B | 主观部分

### 在以下题目中选择五道进行作答。

1. 浅谈你对网络安全的理解；
2. 谈谈你对CTF竞赛和渗透测试的理解；
3. 你学习过什么编程语言？浅谈一下你对它的认知和它的优缺点；
4. 什么是解释性语言，什么是编译性语言，浅谈他们的区别；
5. 谈谈你了解的web安全漏洞或二进制安全漏洞，并解释它们的原理；
6. 什么是白盒测试，什么是灰盒测试，什么是黑盒测试？浅谈它们的区别；
7. 假如你需要爆破一个八位的纯数字PIN码，服务器每秒可尝试十次，PIN码12h内有效，讲讲你的PIN码获取思路；
8. CTF竞赛中常见的类型有很多，例如pwn、web、crypto等，请选择其中一种类型，简要介绍其基本原理和你是如何解决相关题目的；
9. 请解释什么是漏洞利用 *Exploit* ？讨论漏洞利用在黑客攻击中的作用，并探讨预防漏洞利用的方法；
10. 网络安全是一个不断演进的领域，新的威胁和安全技术层出不穷。请谈谈你是如何保持对网络安全知识的更新和学习的。