百度2015安全研发笔试卷

一. 问答题

1. 请解释下常见利用内存断点调试的原理?

正确答案： 内存断点通过将目标地址所在页属性改为PAGE_NOACCESS，当你尝试执行到目标地址时就会产生异常，调试器就会中断下来或者将目标地址内存改为0xCC (INT 3)指令，当执行到该地址时候会产生一个中断，调试器就会暂停下来。

2. 对于Edit控件，你如何抓防止密码框内容被抓取?

正确答案：在处理消息事件的时候，对WM_GETTEXT和EM_GETLINE事件进行过滤

3. DNS欺骗的方式有哪些?

正确答案：hosts文件篡改， 本机DNS服务器IP地址篡改，DNS通讯包篡改。

4. 列举两种应用层中简单的跨进程DLL注入的方法。

正确答案：1、CreateRemoteThread + LoadLibraryA/W
2、SetWindowsHook/SetWindowsHookEx
3、QueueUserAPC + LoadLibraryA

5.

以下是一段汇编代码，请用C语言实现相同功能。

```
.data
SourceStringdb "Hello, World!",0
.code
start:
cld
xoreax, eax
movedi, offset SourceString
mov al, 'd'
movecx, 13
repnescas
jz wow
invokeExitProcess, 0
wow:
invokeExitProcess, 1
end start
```

正确答案：这段代码是在固定字符串里面搜索字符 ‘d’
用C语言实现

```
if (strstr (“Hello, World!”, “d”) != NULL))
    exitProcess(1);
```

```
exitProcess (0);
```

6.
假设有如下所示的一个数字金字塔，现在，要求写一个程序来查找从顶点到底部任意处结束的路径，使路径经过的数字的和最大，并输出该路径的最大和。比如以下金字塔的和最大路径的和为7+3+8+7+5=30。

7
3 2
8 1 0
2 7 4 4
4 5 2 6 5

正确答案:

```
#include <cstdio>
#include <algorithm>

int a[500500] = {0};
int dp[500500] = {0};

int main(){
    freopen("numtri.in","r",stdin);
    int row_num = 0;
    scanf("%d", &row_num);
    int elem_num = row_num * (row_num + 1) / 2; // 数字金字塔中的元素个数
    for(int i = 0;i <elem_num;i++) {
        scanf("%d",&a[i]);
    }
    for(int i=0; i<row_num; i++) {
        dp[elem_num-1-i]=a[elem_num-1-i];
    }
    int n;
    for(int i=row_num-2; i>=0; i--){
        n = i * (i + 1) / 2;
        for(int j=0; j<=i; j++) {
            dp[n+j] = a[n+j] + std::max(dp[n+j+i+1], dp[n+j+i+2]);
        }
    }

    freopen("numtri.out","w",stdout);
    printf("%d\n",dp[0]);
    return 0;
}
```

7. 假设有如下字符串： (234453)[234]{2324} 现在，要求编程分析其括号配对是否正确。请自行选择下列两种方案之一实现该程序:
方案一：不考虑括号优先级，只考虑配对正确性；方案二：考虑括号优先级，比如{1[2（3）4]5} 是正确的。但是[1{2}3]是不正确的。

正确答案：方案一：
使用栈，碰到左括号入栈，碰到右括号出栈，看最后栈是否空，是否还有未匹配完的右括号。
方案二：
思路同上，但是检查压栈时要对括号做优先级检查。

8. 百度是一个大型网站，内部含有多个产品线，比如广为人知的贴吧、知道、空间等应用。然而设计这些应用的统一登录平台却是一件非常艰巨的挑战。需要考虑到通用性和安全性。
1) 对于一个Web应用程序，主要的身份验证和凭证保持的方法主要有cookie和session两种。他们又是如何

起作用的？各有哪些优缺点？

2) 影响到cookie值作用范围的因素有哪些？请一一说明。

3) 从安全角度来考虑，一个大型网站的单点登录可能会引入哪些安全问题？如何设计安全的在线单点登录系统？

正确答案：