



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？
2. 对于Edit控件，你如何防止密码框内容被抓取？
3. DNS欺骗的方式有哪些？
4. 列举两种应用层中简单的跨进程DLL注入的方法。
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

repnscas

jz wow

invokeExitProcess, 0

wow:

invokeExitProcess, 1

end start
```



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

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。

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？



技术QQ群：157594705



微信：www_nowcoder_com



微博：<http://www.weibo.com/nowcoder>

登录牛客网，参与以上题目讨论，查看更多笔试面试题