1、请定义一个宏，比较两个数 a、b 的大小，不能使用大于、小于、if 语句

2、如何输出源文件的标题和目前执行行的行数

3、两个数相乘，小数点后位数没有限制，请写一个高精度算法

4、写一个病毒

5、有 A、B、C、D 四个人，要在夜里过一座桥。他们通过这座桥分别需要耗时 1、2、5、10 分钟，只有一支手电，并且同时最多只能两个人一起过桥。请问，如何安排，能够在 17 分钟内这四个人都过桥？

2005 年腾讯招聘

选择题(60)

c/c++ os linux 方面的基础知识 c 的 Sizeof 函数有好几个!

程序填空(40)

1.(20) 4 空 x5

不使用额外空间,将 A,B 两链表的元素交叉归并

2.(20) 4 空 x5

MFC 将树序列化 转存在数组或 链表中!

//

基本都是基础题目，看来腾讯不准备放弃那些有思想但是

还没有开始苦练基本功的人，只涉及到语言问题和简单的

数据结构，其他的操作系统，编译原理，离散数学，软件

工程，计算机原理，体系结构等等无一涉及，题目很多，

有 1 个选择题想不来起来是什么了，题号不与原试题相符

希望师弟师妹可以探讨探讨答案，从中学到笔试的经验

声明：以下问题仅供本校园网校内师弟师妹为了考察自己学习的参考，不要

传播

1 计算 a^b << 2 (运算符优先级问题)

2 根据先序中序求后序

3 a[3][4]哪个不能表示 a[1][1]: *(&a[0][0]) *(*(a+1)+1) *(&a[1]+1)

*(&a[0][0]+4)

4 for(int i...)
for(int j...)
printf(i,j);

printf(j)
会出现什么问题

5 for(i=0;i<10;++i,sum+=i);的运行结果

6 10 个数顺序插入查找二叉树，元素 62 的比较次数

7 10 个数放入模 10hash 链表，最大长度是多少

8 fun((exp1,exp2),(exp3,exp4,exp5))有几个实参

9 希尔 冒泡 快速 插入 哪个平均速度最快

10 二分查找是 顺序存储 链存储 按 value 有序中的哪些

11 顺序查找的平均时间

12 *p=NULL *p=new char[100] sizeof(p)各为多少

13 频繁的插入删除操作使用什么结构比较合适，链表还是数组

14 enum 的声明方式

其他 1 个选择暂时想不起来了

大题：

1 把字符串转换为小写，不成功返回 NULL,成功返回新串

```
char* toLower(char* sSrcStr)
{
char* sDest= NULL;
if( __1___)
{
int j;
sLen = strlen(sSrcStr);
sDest = new [________2_____];
```

```
if(*sDest == NULL)
return NULL;
sDest[sLen] = '\0';
while(_____3____)
sDest[sLen] = toLowerChar(sSrcStr[sLen]);
}
return sDest;
}
```

2 把字符串转换为整数 例如："-123" -> -123

```
main()
{
.....
if( *string == '-' )
n = ____1_____;
else
n = num(string);
.....
}
int num(char* string)
{
for(;!(*string==0);string++)
{
int k;
k = __2_____;
j = --sLen;
while( __3__)
k = k * 10;
num = num + k;
}
return num;
}
```

附加题：

1 linux 下调试 core 的命令，察看堆栈状态命令

2 写出 socks 套接字 服务端 客户端 通讯程序

3 填空补全程序，按照我的理解是添入：win32 调入 dll 的函数名 查找函数入口的函数名 找到函数的调用形式 把 formView 加到 singledoc 的声明 将 singledoc 加到 app 的声明

4 有关系 s(sno,sname) c(cno,cname) sc(sno,cno,grade)

1 问上课程 "db"的学生 no

2 成绩最高的学生号

3 每科大于 90 分的人数

//

试一共 60 分钟，分发试卷和收回试卷费时 5 分钟，实际考试时间 55 分钟。

选择题 36 道（都是 5 个选项的），计算题 14 道（一道题会有好几个问），题量比较大，我还有最后两个空没填写，实在是没时间了~~

题目考查的范围比较全面，但是有所侧重，例如：如果外汇相对于本国货币升值，一般来说，本国的通货膨胀率将会怎样？下面就是 5 个选项。

总体来说，试题本身难度不大，但是很费时间，阅读的速度非常重要，逻辑判断的能力要求很高，要求快速阅读、快速判断、快速计算，而且还不能粗心导致计算失误（我一般出现的情况就是计算失误~~，希望这次不会出现~~）

腾讯这次的试卷可能字体印刷的比较小了，我的视力是 5.3 的，看上去不会有任何问题，但是坐在我后面的老兄就不好了，完全是模糊的一片，不断的缩减和纸张之间的距离才能看到，可能腾讯公司在这方面的成本应该适当放宽（也许也是一种测试吧，身体素质的测试~~）

HR 说今天就会有面试通知出现，等待中……

今天下午 3 点还有一个招商银行的面试，应聘的核心业务软件开发工程师，应该没有什么问题的~~

11 月 5 日还有 KPMG 的笔试，按照我做的以前的笔试题目来说，很 Easy，全对~~但愿这次也是这样~~

如果幸运的话，如果和腾讯能够很好的契合的话，应该在一个周的时间里面就签约了，大家保佑我吧。

有朋友问我，为什么不去 Google 或者微软这样的公司，却要去腾讯？

我的回答是：我个人的能力在 Google 或者微软这样的地方是没有太大竞争优势的，而且我想做的事情并不是 Code Machine，我希望能够在我的市场洞察力下，依据市场数据做出我的策略和 idea，然后利用我的技术背景将其实现为一个原型系统，经过 Team 和部门的验证，最终与工程师们一起将其实现为公司的产品或者服务，这是一个从 idea 到 product 的过程，充满了创造的乐趣，充满了挑战，我就喜欢这样的感觉，而腾讯能够给我这样的环境，我希望我能够在腾讯 5 个多亿的用户群上为公司做出一点贡献，也是一次次自身价值的提升。

//

由于近来有些人都问我腾讯笔试和面试到底是考什么，问什么，所以就灌下这篇水文，也算是我自己复习一遍以及给有兴趣或者后来者嗤鼻一笑的机会：）

其实应聘内容也真的很难说清楚，而且我也不知道我所经历的是不是有代表性，何况我还是找工作的新手（本科也没找过工作，之前也只是应聘过华为），所以如果下文有什么疏漏之处，尽管踩我好了：）

1。笔试我想腾讯的笔试还是比较适中的，虽然广度与深度都不够，但是毕竟因为它只是笔试，只是用来筛选面试者的，而不是象学术竞赛一样一战决胜负，何况它是笔试，所以也就有笔试的局限性。（啊哦，是不是离题？）笔试主要是 C++的内容，然后还有一部分数据结构、系统平台（WIN32 和 LINUX 都有）的编程知识（线程模型、共享内存、编译或对象模型等）、JAVA（这次笔试 JAVA 有一题，是填写同步的关键字的，当然题目没有明明白白告诉你写 synchronized 这个关键字啦，否则就要被人 BS 了，哈哈。好在 JAVA 下的同步基本实现机制相当简洁，只要刚才那个关键字申明一下就可以了，学过 java 多线程模型的人都应该知道填什么，可惜我那时我也拼写错误了，漏了一个字母。。。，好象是 5 分一题的，损失不小哦）等。可以说还是比较有代表性的。

这里罗嗦几句， 有的人总是问为什么都考 C/C++，我想因为 C/C++才能比较好的表现出你的编程的水平（包括风格、惯用法、技巧性、严谨性等），就象堆积木，给你不同形状的积木越多，那你就越能堆出更多的造型。还有就是是 OOP（这里废话几句~~

OOP 思想很重要，记得当年初次接触 C++真的是只知其所然，而不知其所以然。特别是“虚拟—virtual”这个词，可以说是最最核心的了，理解了它，你会觉得这个词实在太优美了，哈哈~~你可以这样测试你自己的 OOP 能力，针对 OOP 的三个特点用程序写出对应的例程，如果能够写得正确且健壮，那

么应该也就什么问题了）做比较大的项目现在一般都采用 OOP 来实现的了（当然对于特殊的需求、环境和人除）。VB 和 DELPHI 虽然也很流行，一方面是他们没有国际标准，其次是由于它太高级了，一些传统的编程技术被隐藏了，姑且不论 VB（6。0 以前）不支持 OOP，那就更难用它来考 OOP 了，DELPHI 支持 OOP，但是我想很多同学都只是用它进行 OBP，而不是 OOP，所以。。。

至于 JAVA，我本人也很喜欢，而且怎么说，JAVA 也很接近 C++，何况其 API 也比 C/C++ Library 更规范、全面，所以使用起来很方便。但是正如考数学分析比考高等数学往往会加深对数学的理解的道理一样，除此以外也有另一层寓意，假如你能徒手打败你的敌人，那么再给你一把利剑，我想你会在更短的时间内结束战斗，呵呵。所以考 C/C++还是比较合适的，公平是相对的。。。

2。一面面试其实也挺难说的，因为这个环节很灵活，也许在面试之前连面试官自己都不知道他自己将要问什么，呵呵。这里也只是给出一个 case（归纳法不适用，呵呵）。一面时，我只带了两页纸简历，到了面试地点，才发现很多人都是一叠资料的，有的人还不断在复习资料。。。别提当时我有多狼狈了。。。

根据外貌和谈吐可以推断出一面面试官是一个前线的技术专家。面试时首先自我介绍，我一向没刻意去背自我介绍，但是也事先想好了的。然后就是问你哪种编程技术比较拿手啊，项目经验啊，我想关键是深度一定要够，一定要体现你的参与价值和收获，不管是开发过程还是开发技术。面试时我分别从开发过程与开发技术两个方面说了两个项目，感觉面试官还是接受了

的，然后小部分技术细节，比如说在一个项目里面为了解决一个问题，你采取了什么策略，采用了什么技术，这个可千万不能说错哦，不然你就是在自打嘴巴了。。。也许我的笔试成绩还可以，所以语言层面的问题基本没有了。总结，这个面试官很实在，也相当和蔼可亲。。。

3。二面二面的面试官比一面的少，应该都是部门经理。坐这个位置的人都是技术和管理的大拿了，当然这是后来知道的啦。因此这次面试分技术和非技术两部分，不过主要还是技术的。首先还是自我介绍。。。然后面试官就开始设擂台了，问你觉得笔试试卷出得如何？我思考了 2 秒钟，说比较适中（如果我说难，那么如果是简单的话，那我就被 BS 了，实际上也不难吧，说容易吧，如果我考得不好，分数我倒是看到过，但是不知道那算高还是低，所以很容易被 BS），看面试官表情，显然我的回答应该没有 W/A 掉。

接着，他继续问到，你觉得你做错了或者没有把握的题目是哪题。我就说了两三题了，然后他奸诈的看看了我的试卷，从他的表情，我知道，嘿嘿，这个回合是我赢了。然后他就要我介绍一个有代表性的项目。显然这次跟一面要有所变化才行，毕竟是二面了。于是我挑了一个比较容易表述的，简洁清晰，又有一定技术难度的（主要是系统架构方面）展开攻防战，此情此景。。。恩，你猜对了，就象电视上看到的警察审讯嫌疑犯一样，呵呵，只是这个“警察”是面带笑容的。。。

反正，他会象导弹一样追着你来“攻击”，如果你承受不了的话就要中弹了，等到你中得多了，游戏也就 GAME OVER 了。。。我想最好还是讲得高深一。

//

网申时投的是产品类的，后来到交大听宣讲会时就又投了份搜索引擎部门的（宣讲会时拿到全场唯一的公的大得 qq 公仔，呵呵）

然后收到 2 个笔试的通知，接着到财大去笔试。以前去 google 笔试面试都是打车，最近比较穷，所以没地铁的地方就走路，真是累死！

4 号下午 3 点到财大开始技术类的笔试，笔试比较简单，就是算法、数据结构、编程、操作系统等，有一到附加题感觉说的不是很明白

晚上回来后，10 点左右就有通知了，互联网公司的效率就是快啊粗看了下，第一批进入面试的人共有 60 多，本科生不到 10 个（-_____-!）

5 号下午 3 点到兰生大酒店去面试，填表然后被面试官乘电梯从 9 楼到 8 楼（！！！）没问什么技术问题，就是介绍下自己，介绍一下获得奖，用的计算机语言

面试官 gg 说我问你什么技术问题也没什么意思，你得了这些奖说明也应该答出来说搜索引擎部门得总监他认识，会推荐（好像是）说我本科

然后说一个和面试无关得，说怎么不读研我说我生物……，他说华东理工～我还以为是挺好得，结果说不怎么样我说我们学校的生物很好得，然后他说：生物比较冷门

我郁闷，我们高考那时候生物录取分数都是最高他说可以离开了，我还意犹未尽跑到这一个多小时，聊 10 分钟就搞定了

然后又说了两句，问我非搜索引擎部门考虑嘛？深圳工作考虑嘛我说看什么部门，深圳可以考虑如此等等，总之，比较没普

这次华理又是就我一个进面试，计算机系得达人们怎么就不投简历呢？

//

首先，自我介绍．然后他就针对你的介绍提出一些问题．

然后，他就会问你对现行一些游戏的看法，建议大家最好熟悉各类网络游戏，能说出大致的缺点和优点，然后提出改进的方案，让你策划一个新的游戏．

再就是谈一下对互联网的看法．最好是沿着腾讯的发展史上说上一通．

最后就是谈一下对腾讯的看法，有什么问题要问？先夸夸腾讯，然后就提一些问题问一下，基本就是这样．

这就是上午面试的基本过程，希望对大家有所帮助．

//

1.自我介绍。我就....

2.根据做过的东西问。如游戏中的难点啊之内的。我就随便聊聊，图像显示啊。

3.倾向做前台还是后台。为什么？我说后台。再问我有什么优势？我说以前做的东西和后台差不多吧(本人以前做交换协议的)。

4.还问你有什么优点之类的？

5.后台系统的瓶颈。

感觉没有太多共同语言，他也对我不是很感兴趣。 有戏的当场就 hr 了，我直接就会了。

对我来说，能让我参加复试已经比较以外，因为和上个面试管就聊聊一会，感觉没说什么，也对我项目不敢兴趣。 上午 7 点就起来了，睡一觉起来再说。

//

两天吃了一顿饭.面了六场.三次群呕.我都坚持住了,现在还没吃饭呢.不过在第一时间给大家写写面经吧.

先说腾讯.上午去面 11 点到,被告之要推迟两小时,我晕,中午还有 EMERSON 呢.去找 HRMM,他看我一眼说:你就是 XX 啊.没关系我帮你往前安排一下,我乐,11 点半开始二面.面我的居然是个技术主管.别人都是业务主管啊.有点晕不过没紧张.面我超时了.感觉自己发挥还不错,因为他虽然一直看表但是还是对我的话很感兴趣.他是做搜索引擎的,所以问了我好多这方面的问题.一点都没准备,不过先编.BLABLABLA.他问完我我就开始给他讲我的 IDEA.

昨天晚上用 4 个小时写了一篇关于腾讯发展的 IDEA.能讲半个小时.不过他只让我讲了 10 分钟.没所谓,让讲就行.本来他都问完我问题了,结果最后突然又问我你编程怎么样?我狂晕.编程好我来投业务干嘛.说会 C++,问:写过什么程序/答:编过电子琴./问:具体讲讲./答:.....想不起来了.然后又问我其它技术问题,我就郁闷.面完了,他说你等等面三面,我说好。

回到大厅.XX 也过了,好啊我们是好兄弟,一起握手.等 ING.过了 15 分钟 HRMM 又说上午时间不够,所有人都改下午,我不能改啊,再上.MM 一看是我想了想说,帮我安排,于是我终于在最后一个人做了三面.不知道我那个兄弟下午面的怎样.三面面了 15 分钟,大概是对工作的看法还有薪金待遇什么的.很轻松.

然后让我等消息,就这样了.感觉自己发挥没问题,但是鉴于以前做过一件糗事,被 TENCENT 记录在案,所以要是最后被拒了也只能是那个原因了.没所谓,反正偶也没想签.

PS:大多数面业务的都是业务考官.我很巧碰到技术的.业务考官一般都问 OPEN QUESTION.比如给你 100 万怎么赚钱什么的.比较简单.没什么需要担心的.

3 面完 QQ 后打车到 EMERSON.去了发现要填表,时间好紧.匆匆填完正好进场.出来的人又是群殴.不过这次是案例分析.这个偶最喜欢也最拿手,吼吼.大概是 30 分钟做 PROJECT,10 分钟的 PREZENTATION.最后是 10 分钟的考官点评.我们抽到的项目是把一些产品卖给网通.跟运营商打交道我最在行了.所以刚开始我的思路就很明确.大家就让我做 LEADER 了.

PS:大家记住群面的时候 LEADER 是自然产生的,千万不要争,不然对大家都没好处.我们组做的项目我感觉比对手好.而且大家的 TEAMWORK 也要强于对手吧,个人感觉呵呵.偶是很重视 TEAMWORK 地.然后就完了,回来等通知,可能会有四面单挑,管他呢,反正我面完了.呵呵

写了这么多也该吃东西了,谢谢大家花时间看我写的这么多的有点罗嗦的文章.也希望北邮的同学在面试中都可以得心应手.

----------以下为一位同学的回帖----------

Re: 腾讯三面加 EMERSON 三面归来

案例分析其实重在平时的培养。

平时学的课程大家都觉得没有什么可以学习的 但是，做案例分析的时候就完全显现出来的。

首先要根据案例确定这个需要分析的重心在那里，然后根据这个重心想想平时学习中围绕这方面的问题能用到的一些东西。 用这些东西去审视一下这个案例可能出现的问题，其余的就要靠自己的见解了。

平时大家要多多注意市场状况，看看网上的一些评论，对市场的洞察力是很 重要的；比如今天的一些市场操作上的大事或者是互联网产业内的一些大事等。

大家觉得不需要学习，但是管理类和市场类还是需要很多日常的积累的，这种 洞察力不是说有就有的。

//

7 号签了腾讯～心安了不少。

回想起来，还有不少值得记下来的地方：

11 月 2 号，腾讯在华中科技大学 大学生活动中心 B 座 305 开宣讲会，18:30 开始，赶到那里的时候，18:20，上到 3 楼，My god, 走廊都挤不进去了，里面已经开讲了。正找了个阶梯从窗户外往里看，一个坐在窗户边上的 mm 往外得意的看了一眼，把窗户关上了～心里那个寒呐～～

和 mm 无奈地走出了活动中心，给队长打了个电话，队长很够哥们地蹬着破车来了，一起去了他寝室。坐着聊了片刻，到 19:30 了，想想走过去大概也开完宣讲会了。过去以后投了两份简历就回去了。

第二天，白天考完了 Tencent 地笔试，晚上又收到了 Tencent 的业务类面试通知。技术类笔试看来无望（自从到队长寝室一游之后就有了这个感觉），于是开始准备产品策划的面试。

Google 了一把“产品策划”，收获甚微，Baidu 了一把，嘿嘿，好东西出来了。花了大概半天仔细了解了一下产品策划相关的流程和要求，有把 Tencent 的发展历史和其业务认真地研究了一下，觉得对腾讯了解的差不多了。

面试的这天很快到了，之前就在 bbs 看到说去面腾讯业务类的 GG 们都是西装笔挺，到了那里一看，果然如此，技术类的和业务类的基本上是两个世界的人。看来偶在业务类的应聘者中算是够抢眼了。轮到我还有一段时间，开始和周围的人攀谈起来，大致了解了会问哪些问题，也都是之前准备过的问题，心里越来越踏实了。告诉自己，不要紧张，面试官也是人。

本来我排的时间是 14:30，叫到我的时候，已经是 16:30 了。 1507 号房间，坐下，呈上简历。

问：简单介绍一下你自己。

答：（这个问题，准备过的嘛，行云流水一番），着重介绍了一下 Ziqiang 网站的创建过程。

问：你是 leader？

答：是的。

面试官在简历上一阵狂划，似乎很在乎 leader 这个经验。

问：你对产品策划怎么看的？

答：（又是准备过的，结合 Tencent 的发展描述了一番）

问：如果我们现在有一个产品，但是它的市场反映平淡，怎么办？

答：首先是要进行市场调查，搞清楚用户对产品的看法，分析到底是产品的价格问题，还是产品的功能问题，还是说市场上有其他更好的产品。如此往复，对我们的产品进行相应的改进，循环改进。……大致如此。

问：你对 QQ 有什么意见吗？

答：有几个意见。其中一个是：腾讯目前已经有了很多很好的产品，比如 QQ 梦想地带（面试官脸上出现一阵激动），还有 QQ Mail，这都是腾讯的两个很好的栏目，但是我调查了一下我周围的朋友，知道的很少……大致如此。 ……

曰：OK，我可以告诉你，你在我这里已经 Pass 了，我会给你安排二面。

二面大约在 17:10 分开始了。

二面的面试官是个略年长的，问的问题基本相同，看样子他也是对 Ziqiang 网站那段经历最感兴趣。问的不同的问题有：

问：为什么你要加入腾讯？

答：～～mp 一番。

问：你对中国互联网的发展怎么看？

答：据第十六届 CNNIC 互联网报告，中国目前的网民总数是 1.03 亿，其中，使用 QQ 的有 8000 万人，即 80%，……又是 mp 一番，好佩服自己，居然又扯到 Tencent 上来了。 ……

二面的考官似乎很高兴。

曰：你怎么对腾讯这么了解啊？

答：首先，我接触互联网的时间很早，另外，为这次招聘，我也确实准备了很长时间。

曰：好，你到 Alex 那里做一个资格考察吧。 ……

三面在 18 层。一同上去的有 5 人，门口还站着两人，看来有的等了。

每一个出来的人，都说，他（考官）好严肃，一笑都不笑…… 我最后一个进去。考官的确很严肃，但是还称得上和蔼，只是不笑。

“还有简历吗？”

“有”，双手呈上，幸好带了两份简历过来。

“介绍一下你自己吧。”

“我叫×××，我应聘产品策划最大的优势是：我又 5 年互联网工作的经验，有丰富的策划和执行的经验～……”。

“你为什么要加入腾讯？”

mp 一番，这招真是屡试不爽啊。

“你是哪里人？“

“××××。”

“如果让你到深圳去工作，你父母会有什么意见？”

“我很感谢我的父母，他们鼓励我从小就养成独立的性格。我所作的决定，他们一般都会支持我，因为他们相信，我的决定一定有我的理由。所以，我相信，我到深圳去工作，他们也一定会支持我。”

“如果今天晚上或者明天就要跟你签约，你同意吗？”

“我希望能尽快跟腾讯签约。”

“好的，你还有什么问题吗？”

“我们知道，在产品策划后，最重要的一个环节就是执行，只有执行到底，产品才会成功，但是这个环节也是最困难的环节。我想知道，腾讯在这个步骤上，采取了哪些有效的措施？”

“关于这个问题，因为我也不是负责这个环节的，所以我了解的也不多，如果你加入到我们公司来，我相信过几年之后，你了解的一定比我还多。”握手，告别。

“您是 Alex 吧。”

“是的。我是。”

“好的，谢谢您。”

出门。感觉很轻松，应该没多大问题了，三轮感觉都不错。看看时间，18:30。三轮一共花了 2 个小时。

7 日凌晨一点，接到 Tencent 的录取通知，好兴奋。给爸妈打了个电话，都很高兴。

7 日下午，签了。

//////////////////////////////////////

我是复读了一年才进入武大的，入学之初我就已经打定主意毕业之后就去工作，而且一定要去广东。其实我可以选择在学校里一直读下去，可是父母却会一天一天老去，而他们已经辛苦了半辈子了。早点让父母享点闲福，是我中学以来的愿望。

一开始对“工作”其实也没有什么概念，毕竟四年之后的事情太遥远。等到熟悉了校园里的生活之后，我开始思考自己以后的出路了。如果我按部就班的跟在老师后面背背书抄抄笔记写写作业考试前认真准备一下，无疑也能跻身成绩优秀学生之列，多拿些奖学金。

可是这对于找一份理想的工作来说，显然是远远不够的。对于计算机这一行来说，无论是理论知识还是编程动手能力，你都要出类拔萃到时才能脱颖而出。我正是考虑到这一点，所以在大学期间读了很多的专业书籍，课下也常常编写程序，慢慢的积累理论和实践知识。

不过总是一个人自顾自的看书编程，也不知道自己到底学得怎样。去年 10 月中旬，我看到趋势科技校园招聘的海报，心中一动，想到如果我去参加他们的笔试，不就可以检验一下暑假时学 C 的效果如何了？抱着这么简单的念头我在网上填了一个申请，没想到后来真的获得了一个笔试的机会！第一次参加企业的笔试我感到很新奇，在一大帮以求职为唯一目的的参试者中我又觉得自己有些好笑。那次笔试分为两部分，前面 45 分钟是 EQ 和 IQ 题，

后面 2 个小时是专业测试。除了 EQ 题是中文的外，其余题目全是英文的。专业测试题中有很多 C 查错题，一些计算机网络方面的题，还有两道是自编程序题，在暑假时看的《C 编程思想》正好派上了用场，所以做得蛮顺手。考完回来我记下了卷子中考到的而我又没有弄清楚的知识点，然后继续看书、上机验证。大三上很忙，很快我就忘了这回事。所以 11 月 16 号趋势科技让我去面试，我颇感意外，也犹豫了很久。在一些朋友的鼓励下，我决定去尝试一下面试的滋味。去之前看了几篇关于面试技巧的帖子，然后带着一本笔记本、几张证书的复印件就冲过去了，连简历都没有准备。因为不熟悉地方，面试那天我差点迟到，喝了杯水之后便被领到 HR 的房间了。

面试过程很简单，因为我开门见山就告诉他我是一名大三的学生，然后向他介绍说我们信息安全专业其实和他们公司的要求挺对口的。西装革履的 HR 开始时显得很惊讶（也许在疑惑自己怎么能让大三的小子混进来了呢），然后低头看我注册时的资料，然后问我专业课都学了什么，一直问了我很多密码学方面的内容。后来他问我编程学得怎样，我就把那本厚厚的笔记本拿给他看——在大一时，我花了一个暑假的时间，把那本有名的《Windows 核心编程》几乎抄了一遍——他好像蛮感兴趣，翻看了一会，问我平时是不是经常做读书笔记等等。最后他问我有什么问题可以向他提出的，我就问了一下他们公司的福利待遇怎样，还请他就怎样成为一个有用的人才给我提些建议。出来的时候看表，竟然面了近 30 分钟。后文呢？自然是没有后文啦，人家都说明了只要应届毕业生的。不过收获却不可说不大，从笔试到面试，从技术到礼仪，从谈吐到着装的细节，求职必经的一些步骤我都演练了一遍，心里也有了个底。

一晃又一年，今年的校园招聘大大提前，从 9 月份开始，我们就不断地在网上填表格注册简历。没想到第一个笔试的机会仍然是趋势科技给的，考试的内容和形式同去年一样， IQ 题部分甚至一字未改。因为有了去年的经历，所以我觉得自己应该会有一个面试的机会的。只是他们的面试通知要过两三周才发出，期间我又投了一些其他的公司，包括自己比较向往的中兴、华为、腾讯，还有威盛、网易等等。那段日子的主题几乎就是泡在网上，填表格，发简历。那时心血来潮就考了锐捷网络的笔试，接下来的电话面试被我拒掉了，我本无意去福州，也就无谓浪费彼此的时间，同时我也想好好准备第二天在华工举行的威盛电子的笔试。

在北京威盛和深圳威盛的笔试之间，我接到了趋势的面试通知。从华工赶回之后，我便着手准备去趋势的面试的材料，包括中英文简历、自荐信、他们公司的一些资料。我仍然想采取去年的策略，把自己的笔记带去以展示自己的水平和潜力。这次我穿着西装皮鞋提前到了面试的地方，却发现坐在我面前的面试官穿着牛仔衫休闲裤，斯斯文文的象刚从大学里出来的毕业生。我的第一反应是，不能再用去年的那一套了。面试的过程基本就是他问，我答，都是关于编程方面的问题，感觉上自己答得一般，唯一的亮点就是他问我编程实践中有没有碰到过什么 BUG，我问他别人的 BUG 算不算，他说“也算”，我就把自己国庆时花了蛮多时间研究过的关于 Windows 窗口重画问题的 BUG 给他讲了一遍，他听得蛮仔细的。一面出来我感觉不太顺，以为就此结束的当晚接到了二面的通知，第二天一早又赶往面试的酒店。

二面是二对一，两位面试官也很年轻，穿着休闲服，其中一位一开始就对我说“请介绍一下你毕业设计的课题”，我对他说我的毕设要下学期才进行

呢，然后他才醒悟过来我才上的大四，不是研究生。这次的面试顺畅多了，因为没有了项目经验、实习经历的囿限（我的简历对这些也只字未提），我反而可以比较自由的发挥，把话题引向对自己有利的方面。

那时我提到自己因为想学法语，所以写了个程序把一个在线法语教程上的 mp3 都下下来，没想到他们没问我那个程序的细节，反倒问我为什么要学法语，我说法国有很多有名的作家我希望有朝一日能读法文原著，他们马上问我最喜欢的法语作家是谁，我说是普鲁斯特。然后他很惊讶的说“啊！那么枯燥的东西你也能看得进去啊”，我就告诉他追忆似水年华很好看啊我还一直在看红楼梦呢。接下来的面试气氛就变得很轻松了。问的技术问题我都能在那本《Windows 核心编程》里找到答案（所幸我没有忘光），中间又穿插着一些 EQ 方面的问题，如枯燥的工作和个人兴趣怎样去取舍。面试的最后部分是英文问答，问我平时最喜欢做的事情是什么。我紧张中随口答了几样，其中有 Classic Music，他就追问我什么类型的 Classic Music，我随口答道 Liu Dehua，Mei Yanfang 等等，话一出口就意识道他们期待着的应该是莫扎特、贝多芬之类的答案，这次肯定被笑死了。果然我马上听到他们有点夸张的笑声，和一连串的“I see，I see！”了，面试到此结束，我顺利进入下一轮。

第三面是小组讨论的形式，我们组 6 个人有 5 个都是硕士，我一个小本在里面显得非常的弱小。另一方面我也不擅长在公众面前表达自己，所以这一面表现平平。讨论结束面试官让每一个人都用三句话概括一下自己左手边的同学的缺点，轮到我时我却想不出一言来，干站着，窘迫极了。三面完之后，仍然是让我们回去等消息。不过我是再也等不到任何消息啦。

趋势三面之后第二天（11 月 3 日）是腾讯的笔试，也是热闹非常。

笔试题分两部分，前面是技术测试题，25 道必答的选择题，考的基本上是 C 语言和数据结构，还有两道选答题，是数据库和网络方面的，都很简单。

后面部分是开放性问题，问你最难忘的事情是什么啊，在大学里参加过什么社会活动呀，你觉得自己做得最失败的事情是什么呀，诸如此类的，我都认真答了。

晚上 9 点多的时候我收到了腾讯初试的短信，非常的感慨，心想他们的效率可真高！不过等我登陆他们的招聘公告页，一看技术类的初试名单，就倒吸了一口冷气，那上面足足有 150 个名字！怎样在这些精英们的重围中杀出来呢？能通过笔试的筛选已经表明大家的技术基础俱不赖了，面试能不能胜出就看谁能从面试官那里拿到更多的加分了。因此我想无论是开头的自我介绍还是各种材料，都应该比别人特别才好。自我介绍原本很平淡，但因为历史上所谓的“鬼门关”就在我们家乡，我每年都要“从鬼门关上走几遭”，这就显得有点意思了。简历只是稍稍改了一下求职目标，至于没有项目经验和实习经历的问题，我可以参考趋势面试时的做法，把自己平时编程实践时作的笔记带去，这应该比简历上那些短短几十字的模式化的描述更有说服力。

面试前应该多了解一下你应聘的公司，所以我把他们招聘页面上的关于腾讯发展历程、公司理念的部分 Copy 过来，准备打印后带去的。

面试的最后面试官通常都会留点时间回答你的问题的，问什么问题看来也得好好研究一下。一时也没有什么好点子，就随意的在 QQ.COM 上面逛，逛到 QQMail 之后，看到有个“ QQ 邮箱论坛”，灵光一闪，去里面借用一下广大 QQ 用户的意见不是很好的主意么？进去之后一个题为“建议 QQ 和邮箱的

密码分开设置”的帖子吸引了我，让我想起前段时间做的用 Sniffer 监听免费邮箱密码的实验，心想如果 QQMail 登陆也是用 POST 方式的话，也必定存在被监听的危险。

转回来一看，果然用的是未加密的 POST 方式。这也使我怀疑起平时使用的 QQ 秀、QQ 家园等服务来，他们的登陆是不是也存在同样的问题呢？搬出做实验用的 Ethere al 来一试，全都不出所料。这时我有点兴奋起来了，一不做二不休，把 QQ.COM 上所有需要登陆的服务都试了一遍，然后把它们的 URL 和结果记录下来，好家伙，足足有 24 项服务都是使用未加密的 POST 方式提交登陆信息的，而几乎所有的服务都是和 QQ 号关联的，这样 QQ.COM 的弱安全性就使我们 QQ 的整体安全性大打折扣，试问谁愿意为没有足够安全保障的服务长期付费呢？我就把这些 URL 列出来和前面的公司信息一起打了出来，面试前事先翻到安全问题那一页。这样材料基本上就全了。

//

我是过年后从腾讯离职的，个人原因（继续念书去了），凭心而论，腾讯在国内的 IT 企业不管是待遇还是企业文化还是算不错的，上面说的有真有假，也有一些兄弟开玩笑的。

我说说我知道的情况吧。

1：应届生薪水开的差不多 7W/年，硕 10W/年，即便差也差的不多，但招的人还是有一定要求，不是那么好混进去的。

2：腾讯的福利是互联网企业里算是很好的，只和网易，新浪,搜狐,TOM，盛大相比，和 IBM，微软，华为比，个人感觉行业差距较大，没有可比性，另外个人也不了解。

3：应届生面试通过，在入职前的确会发 50 个连号的 QQ 号，那是用来赠送给班级的同学的，听 HR 的人说还是很受欢迎的，你想毕业后天隔一方，都用连号的 QQ，在一个群里还是挺有意思的。

4：内部员工可以每月 5 折限量购买 100 个 Q 币，不过我都没买过，一般找业务线的同事要二十个充充会员什么的。

5：腾讯在深圳市内有几条班车线，有公司专用电梯，自己用大楼已经动工，据说 08 年投入使用。35 层，据内部传说不出租，全部自用，个人表示怀疑能用的完么？？

5：腾讯是没有住房公积金的，保险一般按最低交。季度，年终，双薪，项目奖金都有的。除非你所在部门很烂，项目连续失败，每月工资收入能拿到税后 5 千，年入 10 万基本没有问题。

6：挖人很厉害，不管从营运到产品到研发，很多牛人都是用很高的价钱挖过来的。也推荐内部举荐形式，有专项伯乐奖金。大家都很乐意推荐朋友来面试，如通过，部门经理级 10000，teamleader 级 5000,普通员工级 500.

7:公司管理还算很人性化，多少天病假不扣工资啊，内部活动也挺多的，上 QQ 当然可以，呵，，，不过你上 MSN 也没人会过问。你基本不犯大错不会裁人。不过现在人多了，有未位淘汰制了。

8：公司对外形象还是比较注意，出差普通员工住宿一级城市 550，其他 450,出租车全报，补助是另算（我的级别是 80 块，不高）。不过基本不用花钱，补助算是买烟钱了。。吃饭睡觉都在酒店里搞定好了。有业务线同事常

出差以前都是去机场买票，现在卡的紧些了，都要通过行政从统一票务公司拿票了。

9：最后说一点，腾讯是一家互联网公司，研发能在公司受很重视，很大原因还是几个大老板都是技术出身，你去看看其他互联网公司的研发人员就知道腾讯还算是比上不足，比下有余了。当然很多牛人有机会去 IBM，去微软自有长远的发展，腾讯才 8 年历史，

要走的路还很长。虽然我已离职，还是希望她能一路走好，他的优秀的企业文化和公司氛围希望可以坚持。虽然现在发展过快，管理/执行都出现了一些问题，相信可以慢慢解决。

每次在天涯上看到很多网友说 QQ 这也要收费，那也要收费。但我只想说，腾讯是一家商业公司，他只能保证基本的功能免费，如果所有的业务全免费，腾讯也就倒了。也就没有 QQ 了。

MSN 后面有微软，ICQ 后面有 AOL，QQ 后面什么都没有，正是如此 QQ 才是全球范围能唯一能养活自己的 IM 通信厂商。有人说腾讯是一家没有技术含量的公司，中国的互联网应用技术中能在国际上叫的上号的，也只有 IM 这一项了。从软件质量，功能应用，我也有和 MSN，GTALK，YAHOO MSG 的即通人员有过行业交流，在他们眼里 QQ 仍是现在做的最为优秀的 IM 软件。记得一次我用一个刚带截屏功能的测试版给 YAHOO MSG 一个瑞典哥们做 QQ 截屏演示的时候，他说：中国人太厉害了，太有想象力了。

腾讯做即通研发的兄弟们是给我们中国人争了光这是没说的。天涯上 MSN 和 QQ 对比也是比较多的，其实本质就是任何一个厂商都不能把所有的

市场份额站完，市场的细分就导致总有各自的优势。离职的时候老大问了我一句话“念完书如果没有打算自己创业，还会回腾讯么？我回答是：你把位子让给我，我就回来，哈！！

腾讯在业内是一家很低调的公司，可能和几位老大的个性有关，大家也很难看到媒体上腾讯的宣传。其实上面一些内容都是有违公司规定的，即便我已离职，这个马甲，也只用一次。只是把原来好多想说的话一气说完而已。

//

武大的信息安全专业，到今年已经毕业三届了，不过好像没听说有几个毕业生真正在做安全相关的技术工作的，我那届有两三个在金山做杀毒的。在腾讯的安全部门，就我一个是武大的；还有一个信安的师弟在 QQ 医生那个项目组，也算是安全相关吧，不过这个组并不归属于我们部门。

在腾讯，安全工作主要是在三个层次上进行的：（1）传统的主机与网络层安全，主要包括网络入侵检测、主机完整性审计、防 DDOS 攻击、网络及主机防火墙等等；（2）稍往上的是软件与应用安全，包括客户端软件漏洞挖掘、Web 应用漏洞挖掘、通用 Fuzzy 平台等等；最上面一层的是业务安全，也就是跟“人”（而不是底层技术）相关的了，比如说盗号行为分析、密码保护系统等等。　　应用安全大体可以分两端：（1） QQ 客户端以及附属组件等客户端软件的安全，其中最大的一个安全胁便是溢出攻击了。06 年底到今年，对于控件溢出漏洞的关注是最突出的，不独腾讯，包括微软、雅虎、阿里巴巴、迅雷等等，都爆出过漏洞的报告。（2）以 WEB 应用为主体的服务器端的安全，目前主要是寻找 CGI 程序中存在的漏洞，报告并要求业务部门去修改。国外的 Web 安全研究早在 98 年就很热了，专业做 web 安全的，有

不少业绩能达数千万美元的公司。国内就不一样了，因为真正研究这个技术的人少，虽然问题一直存在，却因为黑客的关注并不是很多（而且几乎都是在很浅的层次上的），威胁也就变得不那么紧急了。

说实话，我们读书时教的那点信息安全知识，对于日新日异的互联网来说，显得有点学究和过时，用上的机会不多。特别是应用安全方面，业界还没有形成系统的知识和理论体系，可以参考的，是一篇又一篇散落在互联网中的文档。我们是边学习边研究，然后又快速地为眼下的问题找到一个合适的解决方案。这时候，一个老练的程序员是我们最期盼的了，因为一定方案定下来就得着手开发相应的系统，没有一定的编程功底，是没法胜任的。奇怪很，社会上那么多程序员，我们招了一年多，却没有招到几个合适的后台开发。所以我们小组几个开发不得不一直都很忙，有时一个人同时承担两三个项目的开发工作。

参考：http://bbs.whu.edu.cn/bbscon.php?board=C.S&id=1103428705

在 12 月 26 日凌晨，有人利用了百度空间的模板漏洞，专门制作了一个能够自我复制和传播的空间蠕虫，在短短的时间内，就有数千用户的空间受到了感染。百度官方的公告（可以在这里看到：http://hi.baidu.com/%B0%D9%B6%C8%BF%D5%BC%E4/blog/item/0e3433fa69eeb61aa8d3110f.html）说，这个蠕虫含有恶意代码，并传播垃圾消息，百度已经紧急对此漏洞进行了处理，云云。

对于一个互联网公司来说，这个是典型的安全事件。百度的安民公告写得很专业；不过在温情脉脉的公告背后，我想一定是公关部门、安全部门、

开发部门等多个部门的联动，紧张对应对这个可能给他们带来大麻烦的事件。在腾讯，我们有时候也会面对这样的安全事件。

百度空间所谓的模板漏洞，用专业的术语来说，叫做“跨站脚本注入漏洞”。简单地说，就是用户输入的内容里面包含了网页脚本代码（这对于任何应用来说都不应该允许的，因为它会使得这个网页的行为失去控制，所以必须要执行过滤才能保存到服务器上），而百度的过滤算法出现了漏洞，被别人绕过去了。蠕虫的作者据说是一个叫“剑心”的人，我想他大概是和我们同龄，甚至更小，放这个蠕虫出来，有点“好玩”的意味（参考他的博客 http://www.loveshell.net/blog/blogview.asp?logID=283）。

其实网络上很多基于 Web 的应用都存在这种漏洞----他们的开发也不是不知道----实在是太普遍了，出现蠕虫只是迟早的事情。也许很多人会奇怪，既然他们知道有问题，为什么不一下子都改掉呢？这里面也许有很多原因；但是我想很重要的一个是：因为它们从来没有出过大事情遭受到大麻烦，所以他们就拖着不动它。以我的经验为例：我们在工作中发现不少可能导致服务器被黑掉的 WEB 漏洞，报告给负责开发的人之后，他们也许会马上修改，也许会跟你扯一下皮（怎么也不相信自己的程序有问题），也许会有这样那样的理由推诿--总的来说，修改程序会增加额外的工作量，但既然这个程序在上面跑了数月甚至数年也没有发生什么事，可见改不改迟点改与早点改并没有太大的关系，我们眼下还有更多重要的事情要忙呢。往往是，安全人员的殷勤并没有受到多大的重视。但是一旦外界爆出了一点什么事情，那就不同了。比如说，有一个 CGI 程序没有过滤一些敏感的关键词，你输入什么就显

示什么，就技术的角度来说是没有任何的安全威胁的。但经过媒体一曝光，就变成了一个紧急而且重要的事情，开发得赶紧修改程序，即使停掉业务也在所不惜，公关部得随时准备应对，上头也会很关注，闹不好一干人士还可能被罚钱。从这里也可以看出，对于所谓的用户价值，一个公司所真正关注的，和他们所声称的，实际上有着微妙的差别的。有时候我们在做推动工作的时候，就不得不借助一两次这样的事件，趁着“上头非常关注”的东风，把安全策略和政策推到其它部门去。

在腾讯在安全有一个非常大的优势，那就是它拥有一个巨大而复杂的网络（数万台的服务器，上百 G 的流量带宽），各种各样的安全威胁它都遭遇过，这对于每一个做技术的员工来说，都是一个难得的研究与学习的条件。不过仅有技术并不能解决问题，要把企业的安全做好，还得有政策以及领导的支持。对于每年为公司带来数亿实实在在的收入的业务部门来说，安全部门的“贡献”实在不值一提。也无怪乎我们一直都是支持与服务的角色，做什么事情都好像在求着他们。

参考：http://bbs.whu.edu.cn/bbscon.php?board=C.S&id=1103428801

公司的班车还得等到 9 点 15 才有，索性多写一篇吧----写了一天的代码，实在有点闷了。　　在我刚加入腾讯的安全部门时，这个部门的力量还是挺少的，而事情则是非常的多，所以很多人都忙得不可开交。虽然一个混乱的环境对员工的长期发展来说是不利的，但是因为事事都是刚开端，我们也就有机会成为某种技术的开创者或者某种制度的制定者，这对我们的成长却又是难得的机会。

在一开始，我被安排做 web 漏洞的查找，头说我至少要手工测试过 1 万个页面之后，才有可能对漏洞查找有深刻的了解。但实际上不需要这么多的实践，我就掌握了基本的门路（嗯，实际上这些技巧并不复杂，甚至在彭国军老师的网络安全实验课上就有，只是我那时也没有太留心:P ），发现了不少问题。在接二连三地发了 N 个漏洞报告之后，头说，看来我们问题还是挺严重的，你组织一次培训吧，给开发讲讲这个 web 安全编程。

我那时是不太情愿的，因为我是个非常害怕在公众前面讲话的人，只要站在讲台上就会紧张、脸红、说不出话来。但是既然是工作要求，我也就不得不硬着头皮来了。我花了两个多星期来准备 PPT（第一次发现会熟练地用 PowerPoint 实在也是一个非常必要的技能），把网上找到的材料，加上自己总结的案例，将近有 70 页。我把什么都放到 PPT 上了，因为我怕自己紧张全都忘记了。

培训的报名工作是 team leader 组织的。到了培训的那天（我记得是去年的 10 月 30 日，那入职刚四个月），他告诉我报名的人有 90 多。等到去了培训教室，我才发现整个教室都坐满了人，还有人站着的。想着里面有同时进来的同事，也有很多可能是做了很多年的开发，我，一个编写的代码加起来没超过 3 千行的乳臭未干的小孩，却来给他们讲怎样编写安全的程序，实在是可笑。一开始我非常紧张，说话结结巴巴，身体都是抖的，只是照着投影念。但不久到了熟悉的内容之后，我慢慢地忘记了紧张，稍为自在点了。那次没想到一下子讲了 2 个半小时，出来后快虚脱了。后来听到一个同事说，讲得还不错，收获很大；那场面太壮观了，她来公司后还没有见过那么大规模人数的培训。我想自己的技术实在是比较肤浅的，但对于不同部门的人来

说，我这点肤浅的知识就是我异于他们的优势了（在分工越来越细的今天，专业的差别可能就会形成这种“隔行如隔山”的效果）。这时候的培训，并不是展现个人的高超技术，而更重要的是，普及某种知识和技能而已。

后来这种安全培训成为了一种每月例行的工作。虽然每个月都讲相同的内容想起来就觉得是一件很乏味的事情，但每次的听众都不同，而你也可以在讲的过程中不断地进步，比如说，深化内容，讲得更有趣更生动。照组内另一位同事所说，要达到这样的一种境界：一份只有寥寥数字的提纲的 PPT，能讲到可长即长，可短即短，随手拈来，那才是水平。

参考：http://bbs.whu.edu.cn/bbscon.php?board=C.S&id=1103428806

在第一篇文章里，芒果说到应用安全的两大块内容：客户端的安全和 Web 服务的安全。就技术方面，从本质上来说，我们当下所做的事情，其实是一种特殊形式的软件测试而已。也许大家还记得软件工程书上说的什么白盒啊黑盒啊，什么测试用例啊，这些概念也能在安全测试中用到。相对于一般的功能测试与性能测试，安全测试有一个专门的称谓：渗透测试，听起来就像我们正在一个看不见的战场上向敌方阵地渗透进去一样，无形中就增添了一份神秘感。

不过说到底，渗透测试还是某种形式的测试而已。一般的测试是看软件或系统是否实现了既定的功能，它运行起来是否与预期的一致，它跑得够不够快。在具体做的时候，一般都有专业的软件来做这些事情：输入一些数据，看输出来是否是正常行为所预期的数据。渗透测试呢，却是看你的软件或系

统在完成正常的功能之外，还能不能做一些理应不被允许的事情。具体做的时候，也是输入一些数据，但看输出来是否是异常行为所预期的数据。

举个例子来说，QQ 的自定义表情包功能，普通的测试会准备一堆这些表情包，打开自定义表情的菜单，调出一个对话框，然后选择一个表情包，按下导入按钮，再在聊天窗口中使用刚才导入的表情包中的一个表情。在这个过程中，测试员只需验证表情包是否导入成功、导入进去的表情包内容与源包是否一致，最后能否在聊天中正常使用。而渗透测试呢，基本上也是这样的过程，但是关注点有些差异。在这个例子里，我们关心这个操作的发起权是否完全掌握在正常用户手里（例如：是否可以通过网页调用的方式发起这个操作，就像弹出一个“与我交谈”的临时对话框一样）；在与操作系统交互时，是否能够逾越既定的限制（比如说，释放这个表情包的时候，它能不能够跳出用户所指定的保存目录）；在解析非正常的数据文件时，程序会不会崩溃；诸如此类。测试的时候呢，也是有一定的方法依循的，比如说路径操作，一般就是在路径名中加入..\(或者是../)；文件解析呢，就是拿一些非正常的文件让它去读取----在这里，非正常的意思是很直观的，就是除了正常格式以外的所有文件，比如说新建一个 txt，在里面胡乱输入一段文字，保存后把后缀名改为.eip，就形成了一个“非正常的”表情包文件。

一般来说，软件或者应用的正常行为都是一个很小的集合，我们通过有限的用例就能够遍历所有的可能性从而验证它是否实现了预期的功能。这样很容易就能想到，软件的非正常行为则可能是一个巨大的充满了未知数的集合，要进行测试则是非常困难的：首先，我们要测试和验证什么，这是不甚明确的；其次，即使是验证一个可能的问题，需要的测试用例可能是数量巨

大的。想一下表情包的例子：一个测试员要证明它能正常解析，他只需准备数百个不同大小不同内容的正常表情包，全部跑一遍，如果每一个都正确导入了，他就可以声明这个功能是正常的，它通过了测试。 相反，一个安全测试员如果要想验证，在非正常的文件格式下，这个程序会崩溃，那么他就得准备几乎是天文数字的表情包，用一台专门的机器连续跑上几天几夜（是的，我们客户端测试小组就是这样做的），看它会不会死掉。想想看，即使只用 4 个字节，就能构造出 43 亿个不同内容的文件，要想找出那些会使程序死掉的文件格式，无异于海里寻针。一般在实际操作的时候，也只是选取一些特定的排列格式（比如说全 0 或者全是 0xff 或者 0 与 0xff 相间）。

这样的测试我们有时候也叫做 Fuzz。文件格式的 Fuzz 只是一个方面，网络协议的 Fuzz 是另一个方面，简单地说就是动态改变一个数据包的内容，看接收方的程序会不会死掉或者崩溃。可以想象，这并不比文件格式 Fuzz 好做多少。在业界，关于 Fuzz 已经有不少参考资料，也有各种各样的 Fuzz 工具，我们的工作，也就是参考这些已有的资料，以及各样的工具平台，然后自己摸索来发现问题的，负责这一块的，也都是 06、07 年毕业的学生。由此可见，做安全研究，其实也没有太大的门槛的。只不过在学校里太闭塞，又没有好的指引，所以觉得渺茫而已。大家有兴趣的，可以下载这些工具来试着玩玩----找个流行的 IM 工具（不独是 QQ，MSN 啊，Yahoo 通啊），没事的时候就让 Fuzz 工具来跑跑，兴许能发现一两个 0day（所谓的 0day 就是外界没有公开的漏洞），然后用来做一些有趣的事情，比如说，给一个看着不爽的家伙发一个消息，他的 IM 就立马崩溃……

参考：http://bbs.whu.edu.cn/bbscon.php?board=C.S&id=1103428856

嗯，趁着兴头再写一篇吧，反正明天是放假，一年里有两三个晚上睡得晚一点也不算太过份~~

上一篇讲到在客户端安全方面，我们可以做些什么事情，又是怎么做的。这一篇就讲一下另一块，在 web 安全这方面，我们在做的，又是什么样的事情，使用的是什么样的技术。　　让我先把时间回退到大学时代：那时候听到很多故事，什么中美黑客大战啦，大陆与台湾的黑客大战啦，白宫的官方网站被黑啦，谁家的小孩因为入侵什么重要的系统被抓啦，诸如此类的非常多，那时觉得很神奇，也对信息安全这个专业充满幻想，以为学到最后，我们也能如传说中的黑客那样，在网络上自由自在地游弋。不过幻想始终是幻想，直到毕业了我也不知道在实际中我怎样才能“黑”掉一台服务器。虽然幻想没有实现，不过我也知道不要把传说太当真。不过在大三的时候，发生了一件让我难以接受的事情：同班同学告诉我，我们学院网站的数据库被别的学校的一个学生用什么方法下载了！这个消息让我非常沮丧：一是我们计算机学院的网站（很多人都会有一种看法，即某个机构的网站在一定程度上代表这个机构的计算水平）竟然这样不堪一击；二是我们一直引以为傲的信息安全，所教导的学生，却无法做到一件一个不太入流的大学里的一个普通学生所能做到的事情，这很让我对自己所受的教育产生怀疑。

直到参加工作一段时间之后，当初的怀疑与沮丧才消除：从根本上来说，怎样攻占站点其实只是一种实际的技术而已，这种技术和学习某一门编程语言一样，是可以通过自学与实践很快就掌握的，会与不会只是一个谁先学谁后学的问题。但更重要的，却是解决问题的思维方式与方法论，而这则会决定一个人以后能在多大的天地做出贡献。

有点罗嗦了，呵呵。把主题集中回 web 安全这里：web 安全往具体里说也包括很多，渗透测试是其中很重要的一个方面。我在腾讯一年半的时间里，做的都是这个事情。从本质上来说，web 渗透测试就是一种黑盒测试，但比起客户端软件来说，做起来就容易很多。这是由 web 应用的特点所决定的：传统上，每一个 web 程序都是一个功能单一、体积小巧的独立程序，输入有限，输出有限，能访问的资源也有限。这样无论是普通的功能与性能测试，还是安全渗透测试，都比较容易进行。

总的来说，web 渗透测试就是给目标程序提交各种“变态”的参数，看这个程序能不能访问到正常情况下不允许访问的数据、文件，是否输出了一些不太安全的内容到返回页面上。所需的全部家当呢，就是一个浏览器了，可能还得加上一个可以查看 HTTP 请求的工具。

比如说，我们查看山水的一篇帖子，是在浏览器地址栏里面输入这样形式的地址来进行的：

http://bbs.whu.edu.cn/bbsrecon.php?id=2525

在这里，bbsrecon.php 就是一个 web 程序，id 就是这个程序的输入参数，2525 就是一个具体的输入数据实例。我们可以猜测，这个 web 程序以这个 id 为索引，去后台数据库里查找一条匹配的记录，然后把内容复制到一个网页框架里，再返回来给我们的浏览器；也有可能，论坛的帖子是以文件形式存放的，这个 web 程序用这个 id 形成一个具体的文件名，然后

首先，这个程序是一个黑盒子，我是不知道它里面的具体实现的。但是我可以通过一些固定的模式来测试去得到足够的信息来猜测它是怎么做的。这样的模式是通用而且非常简单的：我在看到“?id=2525”这样形式的链接地

址时，就会习惯地在参数后面多加一个引号（或者是双引号），再按下回车让浏览器发送这样的一个请求：

http://bbs.whu.edu.cn/bbsrecon.php?id=2525'　　为什么是单双引号呢？因为这个符号可以构成一个很奇妙的测试用例：（1）原本是一串数字的2525，现在因为末尾的引号而变成了一个不合法的数字，程序怎样处理一个原本期望是数字串但实际却含有非数字字符的输入呢？（2）对于使用数据来做存储的应用来说，它极有可能利用输入参数来构造一个 SQL 语句传给后台数据库，才能最终完成的请求，我们可以猜想这个语句具有这样的形式：select * from article where aid=2525 。而我们额外添加的引号有可能原封不动地添加到这个 SQL 语句的末尾----而这如果传到 DB 中去的话，势必会引起一个语法错误，这时的 web 程序，又是怎么应对呢？（3）如果使用文件来做存储，它可能会把 id=2525 映射成一个实际的路径：/data/bbs/article_2525.html，类似这样的形式，那么多余的一个引号如果也原样传进来，最后构成的一个路径十有八九是不存在的文件路径，读取文件失败，程序又会怎样响应呢？

在考虑不周的程序中，非正常的输入会导致程序运行失败（通常返回一个“内部服务器错误”的页面），有些程序员会把错误信息打印出来，比如说类型不对啊，SQL 语句非法啊，读取什么文件失败啊----在这一步，程序已经开口告诉我们很多信息了。在网上有非常多的站点都存在这样的问题的，不信你可以试试（只需简单地在地址栏的参数后面加一个引号）。

也有可能程序对错误进行了处理，在操作失败的时候输出一个提示信息（比如说，对不起，系统繁忙之类的），从而掩盖了底层的出错信息。但是

如果程序没有对输入进行过滤的话，我们还是有办法知道的：因为一个失败的操作所得到的结果和一个成功的操作所得到的结果是不一样的，这种不一样必然又会反映到最终返回的页面上。我们要做的，就是用其它的的例子继续测试，直到我们能够确认它有问题或者没有问题为止，而这些用例的数量是很有限的，可以在数分钟内就能测试完毕。

比如说，对于文件类型的存储，要确认是否有问题的话，就在参数后面有序地添加../序列（我们知道这会返回到上一层的目录），并指向一个可能的文件（比如 windows 的 c:/boot.ini，linux 的/etc/passwd），一直到 5~6 层（再高也不太可能了），如果有漏洞的话，它就会在某一层成功，打开你所指定的文件，并把这个文件的内容读取出来返回到你的浏览器上。这就是文件型漏洞的测试方法。而对于 SQL 型呢，你就在脑海中想着一个正常的 SQL 语句，后面跟着你输入的参数，你怎样在这个 SQL 语句中“插入”其它的语句来控制它呢？用“ and 1=1 ”和“ and 1=2 ”来对比一下如何？熟悉 SQL 的同学会明白，and 1=1 是一个为真的条件，附加在原 SQL 语句后对查询结果无影响，但 and 1=2 是一个为假的条件，附在原 SQL 语句后却会使得整个查询返回一个空集。DB 有没有数据给 web 程序，是可以在浏览器上一目了然地看到的，所以我们就能知道我们能否通过 URL 参数来控制后台 DB。这种漏洞就是 SQL 注入漏洞，网上很多入侵的案例，都是通过这种漏洞来进行的。大家想验证一下的，也可以在 google 中找些来试下（比如说：在 google 中查找 inurl:id inurl:php 就可以找到不少 xxx.php?id=yyy 形式的链接）。这种漏洞还是非常普遍的。

至于另外一种比较典型的漏洞跨站脚本漏洞，就是在参数后面加入一段 HTML 的代码，比如说这样的形式 id=2525<script>alert('xss')</script>，看最后返回来的页面中有没有包含你输入的这段 HTML 代码，如果有的话，就是有跨站漏洞了。对于论坛、发帖等形式的也一样，在输入中包含 HTML 代码，保存，如果最后这段代码能够原封不动地显示出来，那就是有这个问题了（也就意味着，你也可以制造一只类似于百度蠕虫一样的跨站蠕虫了）。

嗯，基本上，web 测试的原理就这样，不过要做到纯熟，还是需要很多的练习，并且要多看一些有深度的文档，这样才有进步。