****1、HTTP状态码知道哪些？****

答：

　　100 Continue 继续，一般在发送post请求时，已发送了http header之后服务端将返回此信息，表示确认，之后发送具体参数信息

　　200 OK 正常返回信息

　　201 Created 请求成功并且服务器创建了新的资源

　　202 Accepted 服务器已接受请求，但尚未处理

　　301 Moved Permanently 请求的网页已永久移动到新位置。

　　302 Found 临时性重定向。

　　303 See Other 临时性重定向，且总是使用 GET 请求新的 URI。

　　304 Not Modified 自从上次请求后，请求的网页未修改过。

　　400 Bad Request 服务器无法理解请求的格式，客户端不应当尝试再次使用相同的内容发起请求。

　　401 Unauthorized 请求未授权。

　　403 Forbidden 禁止访问。

　　404 Not Found 找不到如何与 URI 相匹配的资源。

　　500 Internal Server Error 最常见的服务器端错误。

　　503 Service Unavailable 服务器端暂时无法处理请求（可能是过载或维护）。

****2、你有哪些性能优化的方法？****

答：

　　（1） 减少http请求次数：CSS Sprites, JS、CSS源码压缩、图片大小控制合适；网页Gzip，CDN托管，data缓存 ，图片服务器。

　　（2） 前端模板 JS+数据，减少由于HTML标签导致的带宽浪费，前端用变量保存AJAX请求结果，每次操作本地变量，不用请求，减少请求次数

　　（3） 用innerHTML代替DOM操作，减少DOM操作次数，优化javascript性能。

　　（4） 当需要设置的样式很多时设置className而不是直接操作style。

　　（5） 少用全局变量、缓存DOM节点查找的结果。减少IO读取操作。

　　（6） 避免使用CSS Expression（css表达式)又称Dynamic properties(动态属性)。

　　（7） 图片预加载，将样式表放在顶部，将脚本放在底部 加上时间戳。

CORS

服务器端对于CORS的支持，主要就是通过设置Access-Control-Allow-Origin来进行的。如果浏览器检测到相应的设置，就可以允许Ajax进行跨域的访问。

通过修改document.domain来跨子域

将子域和主域的document.domain设为同一个主域.前提条件：这两个域名必须属于同一个基础域名!而且所用的协议，端口都要一致，否则无法利用document.domain进行跨域

主域相同的使用document.domain

使用window.name来进行跨域

window对象有个name属性，该属性有个特征：即在一个窗口(window)的生命周期内,窗口载入的所有的页面都是共享一个window.name的，每个页面对window.name都有读写的权限，window.name是持久存在一个窗口载入过的所有页面中的

使用[HTML5](http://lib.csdn.net/base/html5" \o "HTML5知识库" \t "http://blog.csdn.net/kebi007/article/details/_blank)中新引进的window.postMessage方法来跨域传送数据

还有flash、在服务器上设置代理页面等跨域方式。个人认为window.name的方法既不复杂，也能兼容到几乎所有浏览器，这真是极好的一种跨域方法。

#### **3、XML和JSON的区别？**

(1).数据体积方面。

JSON相对于XML来讲，数据的体积小，传递的速度更快些。

(2).数据交互方面。

JSON与JavaScript的交互更加方便，更容易解析处理，更好的数据交互。

(3).数据描述方面。

JSON对数据的描述性比XML较差。

(4).传输速度方面。

JSON的速度要远远快于XML。

**4、sql注入原理**

就是通过把SQL命令插入到Web表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。

总的来说有以下几点：

1.永远不要信任用户的输入，要对用户的输入进行校验，可以通过正则表达式，或限制长度，对单引号和双"-"进行转换等。

2.永远不要使用动态拼装SQL，可以使用参数化的SQL或者直接使用存储过程进行数据查询存取。

3.永远不要使用管理员权限的数据库连接，为每个应用使用单独的权限有限的数据库连接。

4.不要把机密信息明文存放，请加密或者hash掉密码和敏感的信息。

**5、XSS原理及防范**

Xss(cross-site scripting)攻击指的是攻击者往Web页面里插入恶意 html标签或者javascript代码。比如：攻击者在论坛中放一个

看似安全的链接，骗取用户点击后，窃取cookie中的用户私密信息；或者攻击者在论坛中加一个恶意表单，

当用户提交表单的时候，却把信息传送到攻击者的服务器中，而不是用户原本以为的信任站点。

XSS防范方法

首先代码里对用户输入的地方和变量都需要仔细检查长度和对”<”,”>”,”;”,”’”等字符做过滤；其次任何内容写到页面之前都必须加以encode，避免不小心把html tag 弄出来。这一个层面做好，至少可以堵住超过一半的XSS 攻击。

首先，避免直接在cookie 中泄露用户隐私，例如email、密码等等。

其次，通过使cookie 和系统ip 绑定来降低cookie 泄露后的危险。这样攻击者得到的cookie 没有实际价值，不可能拿来重放。

如果网站不需要再浏览器端对cookie 进行操作，可以在Set-Cookie 末尾加上HttpOnly 来防止javascript 代码直接获取cookie 。

尽量采用POST 而非GET 提交表单

**6、XSS与CSRF有什么区别吗？**

XSS是获取信息，不需要提前知道其他用户页面的代码和数据包。CSRF是代替用户完成指定的动作，需要知道其他用户页面的代码和数据包。

要完成一次CSRF攻击，受害者必须依次完成两个步骤：

登录受信任网站A，并在本地生成Cookie。

在不登出A的情况下，访问危险网站B。

CSRF的防御

服务端的CSRF方式方法很多样，但总的思想都是一致的，就是在客户端页面增加伪随机数。

通过验证码的方法

#### **7、Web Worker 和webSocket**

worker主线程:

1.通过 worker = new Worker( url ) 加载一个JS文件来创建一个worker，同时返回一个worker实例。

2.通过worker.postMessage( data ) 方法来向worker发送数据。

3.绑定worker.onmessage方法来接收worker发送过来的数据。

4.可以使用 worker.terminate() 来终止一个worker的执行。

WebSocket是Web应用程序的传输协议，它提供了双向的，按序到达的数据流。他是一个[Html5](http://lib.csdn.net/base/html5" \o "HTML5知识库" \t "http://blog.csdn.net/kebi007/article/details/_blank)协议，WebSocket的连接是持久的，他通过在客户端和服务器之间保持双工连接，服务器的更新可以被及时推送给客户端，而不需要客户端以一定时间间隔去轮询。

#### HTTP和HTTPS

HTTP协议通常承载于TCP协议之上，在HTTP和TCP之间添加一个安全协议层（SSL或TSL），这个时候，就成了我们常说的HTTPS。

默认HTTP的端口号为80，HTTPS的端口号为443。

#### 为什么HTTPS安全

因为网络请求需要中间有很多的服务器路由器的转发。中间的节点都可能篡改信息，而如果使用HTTPS，密钥在你和终点站才有。https之所以比http安全，是因为他利用ssl/tls协议传输。它包含证书，卸载，流量转发，负载均衡，页面适配，浏览器适配，refer传递等。保障了传输过程的安全性

#### **8、什么是Etag？**

当发送一个服务器请求时，浏览器首先会进行缓存过期判断。浏览器根据缓存过期时间判断缓存文件是否过期。

情景一：若没有过期，则不向服务器发送请求，直接使用缓存中的结果，此时我们在浏览器控制台中可以看到 200 OK(from cache) ，此时的情况就是完全使用缓存，浏览器和服务器没有任何交互的。

情景二：若已过期，则向服务器发送请求，此时请求中会带上①中设置的文件修改时间，和Etag

然后，进行资源更新判断。服务器根据浏览器传过来的文件修改时间，判断自浏览器上一次请求之后，文件是不是没有被修改过；根据Etag，判断文件内容自上一次请求之后，有没有发生变化

情形一：若两种判断的结论都是文件没有被修改过，则服务器就不给浏览器发index.html的内容了，直接告诉它，文件没有被修改过，你用你那边的缓存吧—— 304 Not Modified，此时浏览器就会从本地缓存中获取index.html的内容。此时的情况叫协议缓存，浏览器和服务器之间有一次请求交互。

情形二：若修改时间和文件内容判断有任意一个没有通过，则服务器会受理此次请求，之后的操作同①

① 只有get请求会被缓存，post请求不会

#### Expires和Cache-Control

Expires要求客户端和服务端的时钟严格同步。HTTP1.1引入Cache-Control来克服Expires头的限制。如果max-age和Expires同时出现，则max-age有更高的优先级。

Cache-Control: no-cache, private, max-age=0

ETag: abcde

Expires: Thu, 15 Apr 2014 20:00:00 GMT

Pragma: private

Last-Modified: $now // RFC1123 format

#### **9、ETag应用:**

Etag由服务器端生成，客户端通过If-Match或者说If-None-Match这个条件判断请求来验证资源是否修改。常见的是使用If-None-Match。请求一个文件的流程可能如下：

====第一次请求===

1.客户端发起 HTTP GET 请求一个文件；

2.服务器处理请求，返回文件内容和一堆Header，当然包括Etag(例如"2e681a-6-5d044840")(假设服务器支持Etag生成和已经开启了Etag).状态码200

====第二次请求===

客户端发起 HTTP GET 请求一个文件，注意这个时候客户端同时发送一个If-None-Match头，这个头的内容就是第一次请求时服务器返回的Etag：2e681a-6-5d0448402.服务器判断发送过来的Etag和计算出来的Etag匹配，因此If-None-Match为False，不返回200，返回304，客户端继续使用本地缓存；流程很简单，问题是，如果服务器又设置了Cache-Control:max-age和Expires呢，怎么办

答案是同时使用，也就是说在完全匹配If-Modified-Since和If-None-Match即检查完修改时间和Etag之后，

服务器才能返回304.(不要陷入到底使用谁的问题怪圈)

为什么使用Etag请求头?

Etag 主要为了解决 Last-Modified 无法解决的一些问题。

#### **10、栈和队列的区别?**

栈的插入和删除操作都是在一端进行的，而队列的操作却是在两端进行的。

队列先进先出，栈先进后出。

栈只允许在表尾一端进行插入和删除，而队列只允许在表尾一端进行插入，在表头一端进行删除

#### **11、栈和堆的区别？**

栈区（stack）— 由编译器自动分配释放 ，存放函数的参数值，局部变量的值等。

堆区（heap） — 一般由程序员分配释放， 若程序员不释放，程序结束时可能由OS回收。

堆（数据结构）：堆可以被看成是一棵树，如：堆排序；

栈（数据结构）：一种先进后出的数据结构。

#### **12、关于Http 2.0 你知道多少？**

HTTP/2引入了“服务端推（server push）”的概念，它允许服务端在客户端需要数据之前就主动地将数据发送到客户端缓存中，从而提高性能。

HTTP/2提供更多的加密支持

HTTP/2使用多路技术，允许多个消息在一个连接上同时交差。

它增加了头压缩（header compression），因此即使非常小的请求，其请求和响应的header都只会占用很小比例的带宽。

#### **13、WEB应用从服务器主动推送Data到客户端有那些方式？**

Javascript数据推送

Commet：基于HTTP长连接的服务器推送技术

基于WebSocket的推送方案

SSE（Server-Send Event）：服务器推送数据新方式

#### **15、说说你对AMD和Commonjs的理解**

CommonJS是服务器端模块的规范，[Node.js](http://lib.csdn.net/base/nodejs" \o "Node.js知识库" \t "http://blog.csdn.net/kebi007/article/details/_blank)采用了这个规范。CommonJS规范加载模块是同步的，也就是说，只有加载完成，才能执行后面的操作。AMD规范则是非同步加载模块，允许指定回调函数。

AMD推荐的风格通过返回一个对象做为模块对象，CommonJS的风格通过对module.exports或exports的属性赋值来达到暴露模块对象的目的。

#### document.write()的用法

document.write()方法可以用在两个方面：页面载入过程中用实时脚本创建页面内容，以及用延时脚本创建本窗口或新窗口的内容。

document.write只能重绘整个页面。innerHTML可以重绘页面的一部分

#### **16、说说mongoDB和MySQL的区别**

[MySQL](http://lib.csdn.net/base/mysql" \o "MySQL知识库" \t "http://blog.csdn.net/kebi007/article/details/_blank)是传统的关系型[数据库](http://lib.csdn.net/base/mysql" \o "MySQL知识库" \t "http://blog.csdn.net/kebi007/article/details/_blank)，[MongoDB](http://lib.csdn.net/base/mongodb" \o "MongoDB知识库" \t "http://blog.csdn.net/kebi007/article/details/_blank)则是非关系型数据库

mongodb以BSON结构（二进制）进行存储，对海量数据存储有着很明显的优势。

对比传统关系型数据库,NoSQL有着非常显著的性能和扩展性优势，与关系型数据库相比，MongoDB的优点有：   
①弱一致性（最终一致），更能保证用户的访问速度：   
②文档结构的存储方式，能够更便捷的获取数据。

#### **17、讲讲304缓存的原理**

服务器首先产生ETag，服务器可在稍后使用它来判断页面是否已经被修改。本质上，客户端通过将该记号传回服务器要求服务器验证其（客户端）缓存。

304是HTTP状态码，服务器用来标识这个文件没修改，不返回内容，浏览器在接收到个状态码后，会使用浏览器已缓存的文件

客户端请求一个页面（A）。 服务器返回页面A，并在给A加上一个ETag。 客户端展现该页面，并将页面连同ETag一起缓存。 客户再次请求页面A，并将上次请求时服务器返回的ETag一起传递给服务器。 服务器检查该ETag，并判断出该页面自上次客户端请求之后还未被修改，直接返回响应304（未修改——Not Modified）和一个空的响应体。

1. **是否了解公钥加密和私钥加密。**

一般情况下是指私钥用于对数据进行签名，公钥用于对签名进行验证;

HTTP网站在浏览器端用公钥加密敏感数据，然后在服务器端再用私钥解密。