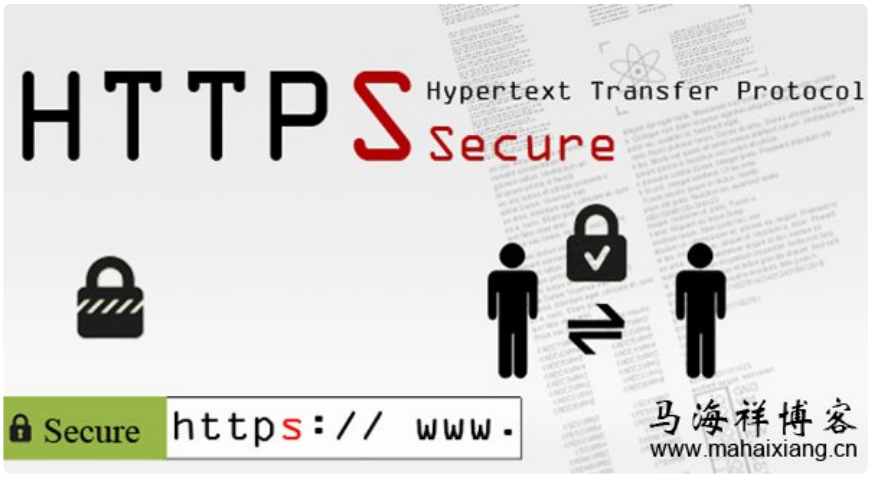
HTTP与HTTPS的区别

时间：2015-07-21 文章来源：马海祥博客 访问次数：56729 收藏到： 26

超文本传输协议HTTP协议被用于在Web浏览器和网站服务器之间传递信息，HTTP协议以明文方式发送内容，不提供任何方式的数据加密，如果攻击者截取了Web浏览器和网站服务器之间的传输报文，就可以直接读懂其中的信息，因此，HTTP协议不适合传输一些敏感信息，比如：信用卡号、密码等支付信息。



为了解决HTTP协议的这一缺陷，需要使用另一种协议：安全套接字层超文本传输协议HTTPS，为了数据传输的安全，HTTPS在HTTP的基础上加入了SSL协议，SSL依靠证书来验证服务器的身份，并为浏览器和服务器之间的通信加密。

一、HTTP和HTTPS的基本概念

HTTP：是互联网上应用最为广泛的一种网络协议，是一个客户端和服务器端请求和应答的标准（TCP），用于从WWW服务器传输超文本到本地浏览器的传输协议，它可以使浏览器更加高效，使网络传输减少。

HTTPS：是以安全为目标的HTTP通道，简单讲是HTTP的安全版，即HTTP下加入SSL层，HTTPS的安全基础是SSL，因此加密的详细内容就需要SSL。

HTTPS协议的主要作用可以分为两种：一种是建立一个信息安全通道，来保证数据传输的安全；另一种就是确认网站的真实性。

二、HTTP与HTTPS有什么区别?

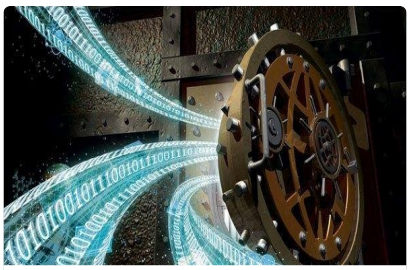
HTTP协议传输的数据都是未加密的，也就是明文的，因此使用HTTP协议传输隐私信息非常不安全，为了保证这些隐私数据能加密传输，于是网景公司设计了SSL（Secure Sockets Layer）协议用于对HTTP协议传输的数据进行加密，从而就诞生了HTTPS。

HTTPS加密、加密、及验证过程，如下图所示：

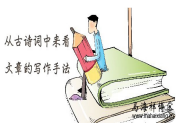
分类目录

SEO新闻	SEO思维
移动端SEO	SEO问答
医疗SEO	淘宝SEO
企业SEO	站外SEO
网站设计	交互设计
网站策划	网页制作
营销策划	营销案例
竞价技巧	数据分析
写作技巧	微信微博
自媒体	新媒体
内容营销	网站运营
O2O模式	App运营
产品运营	网赚教程
创新思维	电子商务
名人访谈	创业故事

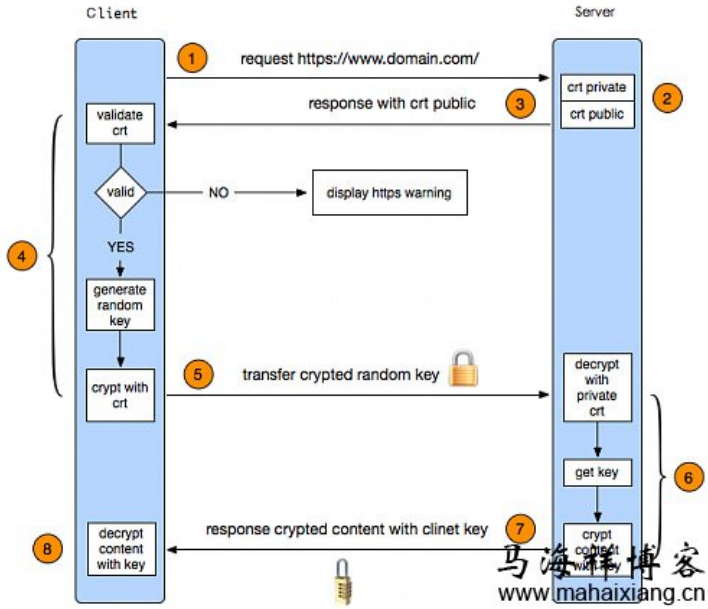
热点推荐


详解内存数据库中的索引技术


运营思维 更多>>


从古诗词中来看文章的写作手法
立即访问


一个顶尖的产品经理要具备那些能力?
立即访问



简单来说，HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议，要比http协议安全。

HTTPS和HTTP的区别主要如下：

1、https协议需要到ca申请证书，一般免费证书较少，因而需要一定费用。

2、http是超文本传输协议，信息是明文传输，https则是具有安全性的ssl加密传输协议。

3、http和https使用的是完全不同的连接方式，用的端口也不一样，前者是80，后者是443。

4、http的连接很简单，是无状态的；HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议，比http协议安全。

三、HTTPS的工作原理

我们都知道HTTPS能够加密信息，以免敏感信息被第三方获取，所以很多银行网站或电子邮箱等等安全级别较高的服务都会采用HTTPS协议。

1、客户端发起HTTPS请求

这个没什么好说的，就是用户在浏览器里输入一个https网址，然后连接到server的443端口。

2、服务端的配置

采用HTTPS协议的服务器必须要有一套数字证书，可以自己制作，也可以向组织申请，区别就是自己颁发的证书需要客户端验证通过，才可以继续访问，而使用受信任的公司申请的证书则不会弹出提示页面(startssl就是个不错的选择，有1年的免费服务)。

这套证书其实就是一对公钥和私钥，如果对公钥和私钥不太理解，可以想象成一把钥匙和一个锁头，只是全世界只有你一个人有这把钥匙，你可以把锁头给别人，别人可以用这个锁把重要的东西锁起来，然后发给你，因为只有你一个人有这把钥匙，所以只有你才能看到被这把锁锁起来的东西。

3、传送证书

这个证书其实就是公钥，只是包含了很多信息，如证书的颁发机构，过期时间等等。

4、客户端解析证书

这部分工作是有客户端的TLS来完成的，首先会验证公钥是否有效，比如颁发机构，过期时间等等，如果发现异常，则会弹出一个警告框，提示证书存在问题。

如果证书没有问题，那么就生成一个随机值，然后用证书对该随机值进行加密，就好像上面说的，把随机值用锁头锁起来，这样除非有钥匙，不然看不到被锁住的内容。

5、传送加密信息

这部分传送的是用证书加密后的随机值，目的就是让服务端得到这个随机值，以后客户端和服务端的通信就可以通过这个随机值来进行加密解密了。

6、服务段解密信息

服务端用私钥解密后，得到了客户端传过来的随机值(私钥)，然后把内容通过该值进行对称加密，所谓对称加密就是，将信息和私钥通过某种算法混合在一起，这样除非知道私钥，不然无法获取内容，而正好客户端和服务端都知道这个私钥，所以只要加密算法够彪悍，私钥够复杂，数据就够安全。

7、传输加密后的信息

这部分信息是服务段用私钥加密后的信息，可以在客户端被还原。

8、客户端解密信息

客户端用之前生成的私钥解密服务段传过来的信息，于是获取了解密后的内容，整个过程第三方即使监听到了数据，也束手无策。

四、搜索引擎对HTTPS的态度

百度推出了全站HTTPS加密搜索服务，以此解决“第三方”对用户隐私的嗅探和劫持，其实，早在2010年5月份，谷歌便开始提供HTTPS加密搜索服务，在HTTPS网页的抓取问题上，百度在2014年9月份的一份公告中表示“百度不会主动抓取HTTPS网页”，谷歌在算法更新中则表示“同等条件下，使用HTTPS加密技术的站点在搜索排名上更具优势”。

那么，在这种大环境下，站长是否该采用“具有风险”的HTTPS协议呢？HTTPS对搜索引擎的SEO影响又如何呢？

1、谷歌的态度

谷歌在HTTPS站点的收录问题上与对HTTP站点态度并无什么不同之处，甚至把“是否使用安全加密”（HTTPS）作为搜索排名算法中的一个参考因素，采用HTTPS加密技术的网站能得到更多的展示机会，排名相对同类网站的HTTP站点也更有优势。

而且谷歌曾明确表示“希望所有的站长都能将使用HTTPS协议，而非HTTP”更是表明了其对达到“HTTPS everywhere”这一目标的决心。

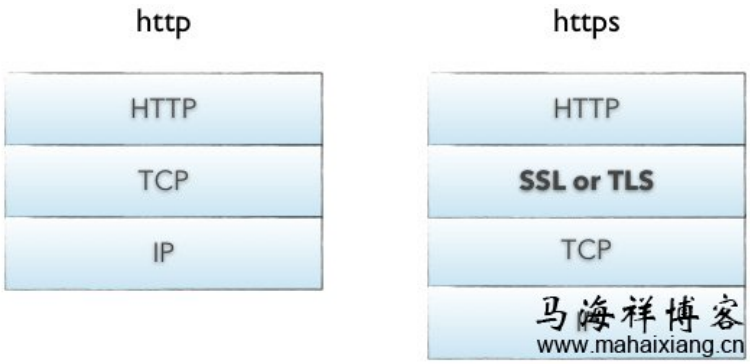
2、百度的态度

虽然百度曾表示“不会主动抓取https网页”，但对于“很多https网页无法被收录”也是“耿耿于怀”，去年9月份，百度曾就“https站点如何建设才能对百度友好”问题发布了一篇文章，给出了“提高https站点的百度友好度”的四项建议及具体操作。

此外，近日的“百度全站HTTPS加密搜索”事件也再次彰显了百度对HTTPS加密的重视，可见，百度并不“反感”HTTPS站点，所以“不主动抓取”应该也只是暂时的吧！

五、HTTPS要比HTTP多用多少服务器资源?

HTTPS其实就是建构在SSL/TLS之上的 HTTP协议，所以，要比较HTTPS比HTTP多用多少服务器资源，马海祥认为主要看SSL/TLS本身消耗多少服务器资源。



HTTP使用TCP三次握手建立连接，客户端和服务器需要交换3个包（具体可查看马海祥博客《HTTP服务的七层架构技术解析及运用》的相关介绍）；HTTPS除了TCP的三个包，还要加上ssl握手需要的9个包，所以一共是12个包。

HTTP建立连接，按照下面链接中针对Computer Science House的测试，是114毫秒；HTTPS建立连接，耗费436毫秒，ssl部分花费322毫秒，包括网络延时和ssl本身加解密的开销（服务器根据客户端的信息确定是否需要生成新的主密钥；服务器回复该主密钥，并返回给客户端一个用主密钥认证的信息；服务器向客户端请求数字签名和公开密钥）。

当SSL连接建立后，之后的加密方式就变成了3DES等对于CPU负荷较轻的对称加密方式，相对前面SSL建立连接时的非对称加密方式，对称加密方式对CPU的负荷基本可以忽略不记，所以问题就来了，如果频繁的重建ssl的session，对于服务器性能的影响将会是致命的，尽管打开HTTPS保活可以缓解单个连接的性能问题，但是对于并发访问用户数极多的大型网站，基于负荷分担的独立的SSL termination proxy就显得必不可少了，Web服务放在SSL termination proxy之后，SSL termination proxy既可以是基于硬件的，譬如F5；也可以是基于软件的，譬如维基百科用到的就是Nginx。

那采用HTTPS后，到底会多用多少服务器资源，2010年1月Gmail切换到完全使用HTTPS， 前端处理SSL机器的CPU负荷增加不超过1%，每个连接的内存消耗少于20KB，网络流量增加少于2%，由于Gmail应该是使用N台服务器分布式处理，所以CPU负荷的数据并不具有太多的参考意义，每个连接内存消耗和网络流量数据有参考意义，这篇文章中还列出了单核每秒大概处理1500次握手（针对1024-bit 的 RSA），这个数据很有参考意义。

Heartbleed这个被称作史上最大的网络安全漏洞，想必很多人都有所耳闻，Heartbleed之所以能够出现，其实和我们这个问题关系还不小，前面我们谈到了频繁重建SSL/TLS的session对于服务器影响是致命的，所以，聪明的RFC在2012年提出了RFC6520 TLS的心跳扩展，这个协议本身是简单和完美的，通过在客户端和服务器之间来回发送心跳的请求和应答，保活TLS session，减少重建TLS的session的性能开销，令

人遗憾的是，openssl在实现这个心跳扩展时，犯了一个低级的错误，没有对收到的心跳请求进行长度检查，直接根据心跳请求长度拷贝数据区，导致简单的心跳应答中可能包含了服务器端的核心数据区内容，用户名，密码，信用卡信息，甚至服务器的私有密钥都有可能泄露。

六、HTTPS的优点

正是由于HTTPS非常的安全，攻击者无法从中找到下手的地方，从站长的角度来说，HTTPS的优点有以下2点：

1、SEO方面

谷歌曾在2014年8月份调整搜索引擎算法，并称“比起同等HTTP网站，采用HTTPS加密的网站在搜索结果中的排名将会更高”。

2、安全性

尽管HTTPS并非绝对安全，掌握根证书的机构、掌握加密算法的组织同样可以进行中间人形式的攻击，但HTTPS仍是现行架构下最安全的解决方案，主要有以下几个好处：

（1）、使用HTTPS协议可认证用户和服务器，确保数据发送到正确的客户机和服务器；

（2）、HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议，要比http协议安全，可防止数据在传输过程中不被窃取、改变，确保数据的完整性。

（3）、HTTPS是现行架构下最安全的解决方案，虽然不是绝对安全，但它大幅增加了中间人攻击的成本。

七、HTTPS的缺点

虽然说HTTPS有很大的优势，但其相对来说，还是有些不足之处的，具体来说，有以下2点：

1、SEO方面

据ACM CoNEXT数据显示，使用HTTPS协议会使页面的加载时间延长近50%，增加10%到20%的耗电，此外，HTTPS协议还会影响缓存，增加数据开销和功耗，甚至已有安全措施也会受到影响也会因此而受到影响。

而且HTTPS协议的加密范围也比较有限，在黑客攻击、拒绝服务攻击、服务器劫持等方面几乎起不到什么作用。

最关键的，SSL证书的信用链体系并不安全，特别是在某些国家可以控制CA根证书的情况下，中间人攻击一样可行。

2、经济方面

（1）、SSL证书需要钱，功能越强大的证书费用越高，个人网站、小网站没有必要一般不会用。

（2）、SSL证书通常需要绑定IP，不能在同一IP上绑定多个域名，IPv4资源不可能支撑这个消耗（SSL有扩展可以部分解决这个问题，但是比较麻烦，而且要求浏览器、操作系统支持，Windows XP就不支持这个扩展，考虑到XP的装机量，这个特性几乎没用）。

（3）、HTTPS连接缓存不如HTTP高效，大流量网站如非必要也不会采用，流量成本太高。

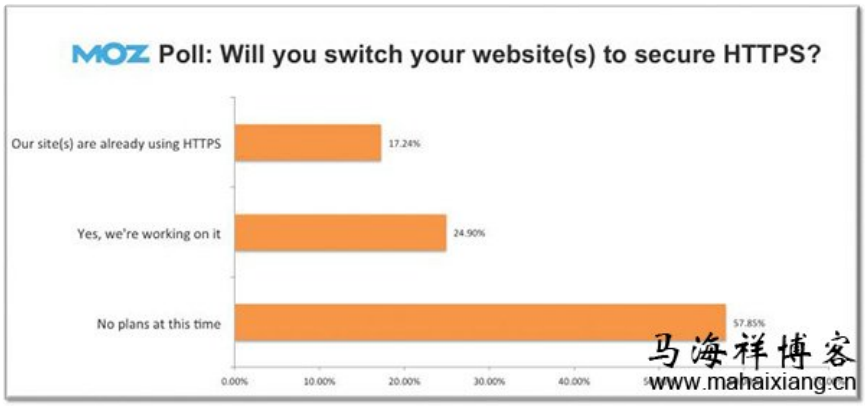
（4）、HTTPS连接服务器端资源占用高很多，支持访客稍多的网站需要投入更大的成本，如果全部采用HTTPS，基于大部分计算资源闲置的假设的VPS的平均成本会上去。

（5）、HTTPS协议握手阶段比较费时，对网站的相应速度有负面影响，如非必要，没有理由牺牲用户体验。

八、网站是否需要采用HTTPS加密?

虽然谷歌和百度都对HTTPS“另眼相看”，但这并不意味着站长们都应该把网站协议转换成HTTPS的！

早在去年9月份，Moz就针对“采用HTTPS协议”展开了一项调查，结果如下图：



注：调查开展时间在谷歌宣布“使用HTTPS协议的网站可以获得更好的排名”后

如上图所示，在此项调查中，17.24%的站长表示其网站已采用HTTPS协议；24.9%的站长表示正在搭建中；57.85%的站长表示目前仍无此项计划，从这些数据可以看出，当时大部分的站长还是没有选择使用HTTPS协议，那么，站长们到底该不该选择有利有弊的HTTPS协议呢?

从这些数据可以看出，当时大部分的站长还是没有选择使用HTTPS协议，那么站长们到底该不该选择有利有弊的HTTPS协议呢?

首先说说谷歌方面，虽然谷歌不断强调“使用HTTPS加密技术的网站能获得更好的排名”，但也不能排除这是“别有用心”之举。

国外分析师就曾针对这一问题表示：谷歌之所以做出这一举动（更新算法，将是否采用HTTPS加密技术作为搜索引擎排名的的一个参考因素）也许并非是为了提高用户的搜索体验和互联网安全问题，只是为了挽回在“棱镜门”丑闻中的“损失”，这是一个典型的打着“牺牲小我”旗号的利我之举，高举“安全影响排名”旗帜、高呼“HTTPS everywhere”口号，然后不费吹灰之力让广大站长们心甘情愿的投入HTTPS协议阵营。

然后是百度方面，虽然百度宣布全站进入HTTPS加密搜索时代，但至今仍“不会主动抓取HTTPS页面”，也从未就“未来是否会调整算法”问题表过态，如果站长在采用HTTPS协议后仍需制作个“http可访问版”、或是通过301重定向“自动跳入https版本”，那么，采用HTTPS协议的代价就不再只是多花money的问题了。

在思考“到底该不该采用HTTPS协议”这个问题时，多考虑考虑怎样做对你的用户更友好吧（具体可查看马海祥博客《从SEO的角度来分析网站是否该采用HTTPS协议》的相关介绍）！

如果你的网站属于电子商务、金融、社交网络等领域的话，那最好是采用HTTPS协议；如果是博客站点、宣传类网站、分类信息网站、或者是新闻网站之类的话，大可不必跟风而行，毕竟HTTPS协议不仅耗钱，浪费精力，而且暂时也不利于网站的SEO工作。详情可查看：我到底该不该用“影响搜索排名”的HTTPS?

九、站长如何搭建HTTPS站点?

说到HTTPS站点的搭建，就不得不提到SSL协议，SSL是Netscape公司率先采用的网络安全协议，它是在传输通信协议（TCP/IP）上实现的一种安全协议，采用公开密钥技术，SSL广泛支持各种类型的网络，同时提供三种基本的安全服务，它们都使用公开密钥技术。

1、SSL的作用

（1）、认证用户和服务器，确保数据发送到正确的客户机和服务器；

（2）、加密数据以防止数据中途被窃取；

（3）、维护数据的完整性，确保数据在传输过程中不被改变。

而SSL证书指的是在SSL通信中验证通信双方身份的数字文件，一般分为服务器证书和客户端证书，我们通常说的SSL证书主要指服务器证书，SSL证书由受信任的数字证书颁发机构CA（如VeriSign，GlobalSign，WoSign等），在验证服务器身份后颁发，具有服务器身份验证和数据传输加密功能，分为扩展验证型(EV)SSL证书、组织验证型(OV)SSL证书、和域名验证型（DV）SSL证书。

2、SSL证书申请的3个主要步骤

对于SSL证书的申请，主要有以下3个步骤：

（1）、制作CSR文件

所谓CSR就是由申请人制作的Certificate Secure Request证书请求文件，制作过程中，系统会产生2个密钥，一个是公钥就是这个CSR文件；另外一个是私钥，存放在服务器上。

要制作CSR文件，申请人可以参考WEB SERVER的文档，一般APACHE等，使用OPENSSL命令行来生成KEY+CSR2个文件，Tomcat，JBoss，Resin等使用KEYTOOL来生成JKS和CSR文件，IIS通过向导建立一个挂起的请求和一个CSR文件。

（2）、CA认证

将CSR提交给CA，CA一般有2种认证方式：

①、域名认证：一般通过对管理员邮箱认证的方式，这种方式认证速度快，但是签发的证书中没有企业的名称。

②、企业文档认证：需要提供企业的营业执照，一般需要3-5个工作日。

也有需要同时认证以上2种方式的证书，叫EV证书，这种证书可以使IE7以上的浏览器地址栏变成绿色，所以认证也最严格。

（3）、证书的安装

在收到CA的证书后，可以将证书部署上服务器，一般APACHE文件直接将KEY+CER复制到文件上，然后修改HTTPD.CONF文件；TOMCAT等，需要将CA签发的证书CER文

件导入JKS文件后，复制上服务器，然后修改SERVER.XML；IIS需要处理挂起的请求，将CER文件导入。

十、免费证书推荐

使用SSL证书不仅能让信息的安全性更有保障，还可以提高用户对于网站的信任度，但鉴于对建站成本的考虑，很多站长对其望而却步，在网络上免费始终是一个永远不过时的市场，主机空间有免费的，而SSL证书自然也有免费的，此前，便有消息称，Mozilla、思科、Akamai、IdenTrust、EFF、以及密歇根大学的研究人员将开启Let's Encrypt CA项目，计划从今夏开始，为网站提供免费SSL证书以及证书管理服务（注：如需更高级的复杂证书，则需付费），同时，还降低了证书安装的复杂程度，安装时间仅需20-30秒。

而需要复杂证书的往往是大中型网站，诸如个人博客之类的小型站点完全可以先尝试免费SSL证书，如果想要购买低价SSL证书可查看站长之家之前发布的文章：如何购买廉价SSL证书？。

下面马海祥博客再为大家介绍几款免费SSL证书，比如：CloudFlare SSL、StartSSL、Wosign沃通SSL、NameCheap等。

1、CloudFlare SSL

CloudFlare是美国一家提供CDN服务的网站，在世界各地都有自己的CDN服务器节点，国内外很多大型公司或者网站都在使用CloudFlare的CDN服务，当然国内站长最常用的就是CloudFlare的免费CDN，加速也很好，CloudFlare提供的免费SSL证书是UniversalSSL，即通用SSL，用户无需向证书发放机构申请和配置证书就可以使用的SSL证书，CloudFlare向所有用户(包括免费用户)提供SSL加密功能，web界面5分钟内就设置好证书，24小时内完成自动部署，为网站的流量提供基于椭圆曲线数字签名算法（ECDSA）的TLS加密服务。

2、StartSSL

StartSSL是StartCom公司旗下的SSL证书，提供免费SSL证书服务，且StartSSL被包括Chrome、Firefox、IE在内的主流浏览器支持，几乎所有的主流浏览器都可以正常识别StartSSL，任何个人都可以从StartSSL中申请到免费一年的SSL证书。

3、Wosign沃通SSL

Wosign沃通是国内一家提供SSL证书服务的网站，其免费的SSL证书申请比较简单，在线开通，一个SSL证书只能对应一个域名，支持证书状态在线查询协议(OCSP)。

4、NameCheap

NameCheap是一家领先的ICANN认可的域名注册和网站托管公司，成立于2000年，该公司提供免费DNS解析，网址转发（可隐藏原URL，支持301重定向）等服务，此外，NameCheap还提供了一年的SSL证书免费服务。

马海祥博客点评：

从商业机构到政府部门再到个人家庭，越来越多的用户使用网络来处理事务，交流信息和进行交易活动，这些都不可避免地涉及到网络安全问题，尤其是认证和加密问题，特别是在网上进行购物交易活动中，必须保证交易双方能够互相确认身份，安全地传输敏感信息，事后不能否认交易行为，同时还要防止他人截获篡改宝贵信息或假冒交易方。

那么，我们该如何提高站点信息的安全性呢？目前最简单的解决方案就是利用SSL安全技术来实现WEB的安全访问。

相关标签搜索： https http

上一篇：如何收集和存储服务器运营的数据
下一篇：今日头条的个性化推荐算法

相关文章推荐：

您可能还会对以下这些文章感兴趣！

计算机的开机启动原理

计算机从打开电源到开始操作，整个启动可以说是一个非常复杂的过程。总体来说，计算机的整个启动过程分成四个阶段：第一阶段：BIOS；第二阶段：主引导记录；第三阶段：硬盘启动；第四阶段：操作系统；直至执行/bin/login程序，跳出登录界面，等待用户输入用户名和密码。……【查看全文】

阅读：3039 关键词： 计算机 计算机启动 计算机原理 开机启动原理 日期：2014-01-16

详解内存数据库中的索引技术

传统的数据库管理系统把所有数据都放在磁盘上进行管理，所以称作磁盘数据库（DRDB:Disk-Resident Database），磁盘数据库需要频繁地访问磁盘来进行数据的操作，磁盘的读写速度远远小于CPU处理数据的速度，所以磁盘数据库的瓶颈出现在磁盘读写上，基于此，内存数据库的概……【查看全文】

阅读：3257 关键词： 内存数据库 索引技术 数据库 日期：2015-01-09

HTTP、SSL/TLS和HTTPS协议的区别与联系

HTTPS是为了安全性而设置的，要验证很多的信息，相对应http请求的速度肯定有点慢，如果使用HTTPS的话很麻烦的，无意给服务器和客户端增加了很大的压力，所以平时最好不要使用HTTPS，如果牵扯到个人隐私或者是其他的什么重要信息就一定要这么做了，很多的时候你感觉有点问题，……【查看全文】

阅读：14035 关键词： http ssl https https协议 日期：2016-05-13

今日头条的个性化推荐算法

互联网给用户带来了大量的信息，满足了用户在信息时代对信息的需求，但也使得用户在面对大量信息时无法从中获得对自己真正有用的那部分信息，对信息的使用效率反而降低了，而通常解决这个问题最常规的办法是推荐系统。推荐系统能有效帮助用户快速发现感兴趣和高质量的信……【查看全文】

阅读：12908 关键词： 今日头条 日期：2016-01-20

详解大型网站系统的特点和架构演化发展历程

大型网站的挑战主要来自庞大的用户，高并发的访问和海量数据，任何简单的业务一旦需要处理数以P计的数据和面对数以亿计的用户，问题就会变得棘手，大型网站架构主要就是解决这类问题。大型网站不是从无到有一步就搭建好一个大型网站，而是能够伴随小型网站业务的渐进发……【查看全文】

阅读：853 关键词： 大型网站 网站架构 网站系统 日期：2017-03-02

基于贝叶斯推断应用原理的过滤垃圾邮件研究

随着电子邮件的应用与普及，垃圾邮件的泛滥也越来越多地受到人们的关注。而目前正确识别垃圾邮件的技术难度非常大。传统的垃圾邮件过滤方法，主要有关键词法和校验码法等。前者的过滤依据是特定的词语；后者则是计算邮件文本的校验码，再与已知的垃圾邮件进行对比。它们……【查看全文】

阅读：855 关键词： 贝叶斯推断 贝叶斯应用 贝叶斯原理 过滤垃圾邮件 垃圾邮件 日期：

HTTPS建设使用的方案教程解析

百度已对部分地区开放HTTPS加密搜索服务，随后，百度实行全站化HTTPS安全加密服务，百度HTTPS安全加密已覆盖主流浏览器，旨在用户打造了一个更隐私化的互联网空间、加速了国内互联网的HTTPS化。同时也希望更多网站加入到HTTPS的队伍中来，为网络安……【查看全文】

阅读：42 关键词： seo https 日期：2018-02-01

如何开启苹果系统的两步验证机制，避免iCloud帐号遭到攻击

首先，你需要登录至苹果的网页版Apple ID管理系统，你需要点击“管理你的Apple ID”，随后输入帐号密码信息。在登录之后，你需要从左侧导航栏中选择“密码和安全”选项，在这里，你将需要验证安全问题，随后下拉至“两步验证”区域，点击蓝色的“开始”链接并阅读其中的……【查看全文】

阅读：1407 关键词： 苹果系统 验证机制 icloud攻击 icloud帐号 icloud 日期：2014-09-

关于大型网站架构的负载均衡技术详解

负载均衡是将负载（工作任务，访问请求）进行平衡、分摊到多个操作单元（服务器，组件）上进行执行，是解决高性能，单点故障（高可用），扩展性（水平伸缩）的终极解决方案。面对大量用户访问、高并发请求，海量数据，可以使用高性能的服务器、大型数据库，存储设备，高性能W……【查看全文】

阅读：809 关键词： 大型网站 网站架构 负载均衡 日期：2016-08-05

HTTP服务的七层架构技术解析及运用

一般来说，计算机领域的体系结构普遍采用了分层的方式，从最底层的硬件往高层依次有：操作系统->驱动程序->运行库->系统程序->应用程序等等。从网络分层模型OSI来讲，由上至下为：应用层->表示层->会话层->传输层->网络层->数据链路层->物理层。当然实际应用的TCP/IP协……【查看全文】

阅读：4386 关键词： 七层架构解析 七层架构运用 七层架构技术 http服务 日期：2014-09-

↓ 点击查看更多 ↓

网站导航

关注微信公众号