面试官：说说 Cookie 和 Token 的区别?

写在前面

说到 cookie、token 应该没有人不知道的吧，而如果说让大家说出 cookie、token 到底是什么关系，大家能说出来吗，往往这种看似简单的东西，一到关键的场面，就很容易让我们陷入尴尬，明明知道是什么，却解释不清楚，被 Pass 后一脸冤枉，因此，本篇我们就来稍微回顾下 cookie 相关的基础知识，给自己充充电吧！！！！

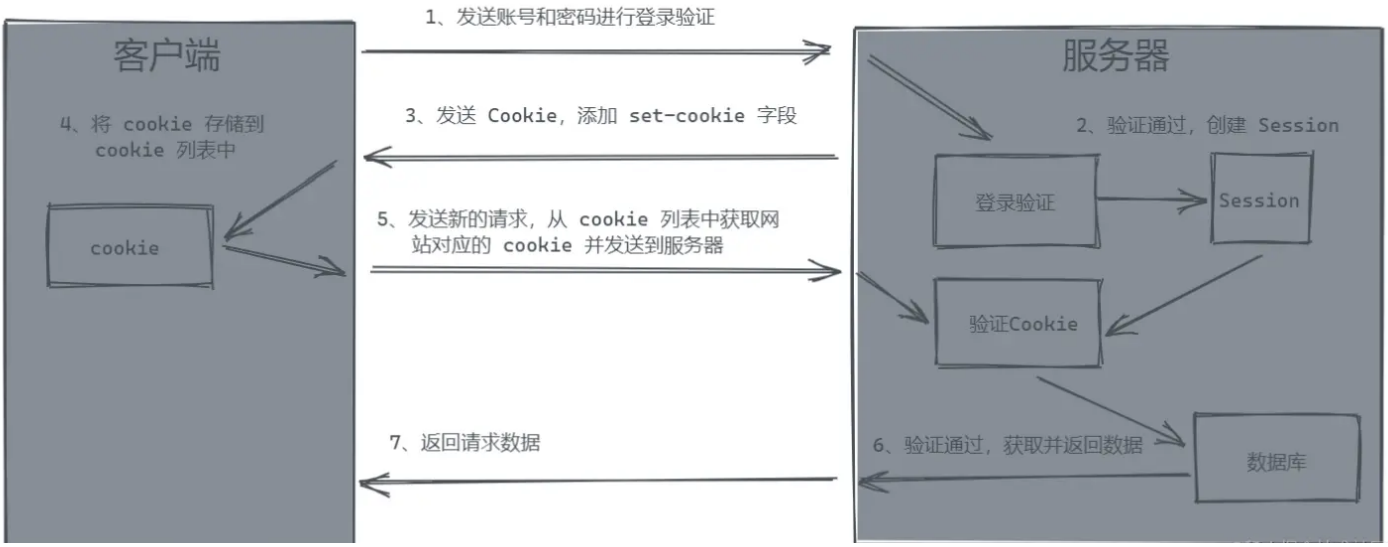
Cookie

Cookie，有时也用其复数形式 Cookies。类型为小型文本文件，是某些网站为了辨别用户身份，进行Session跟踪而储存在用户本地终端上的数据（通常经过加密），由用户客户端计算机暂时或永久保存的信息。 看完“百度百科”的概念解释，依然是流于文字，我们来从原理方面解释下。

为什么要有 Cookie 呢?

我们都知道一般接口但是通过 HTTP 协议来进行数据交换的，而 HTTP 协议的特点是，无状态，工作前通过三次握手建立连接，工作完成后立刻通过四次挥手断开连接，每次连接都是独立存在的，没有任何状态将请求串联成一个整体，因此每次都需要重新验证是身份，即耗费了性能，也给黑客的攻击留下隐患。

那么 Cookie 的作用是什么呢，它的出现，就是来弥补 HTTP 无状态的问题的，Cookie 可以作为一个状态保存的状态机，用来保存用户的相关登录状态，当第一次验证通过后，服务器可以通过 set-cookie 令客户端将自己的 cookie 保存起来，当下一次再发送请求的时候，直接带上 cookie 即可，而服务器检测到客户端发送的 cookie 与其保存的 cookie 值保持一致时，则直接信任该连接，不再进行验证操作。大致的过程如下图



Token

Token, 令牌，代表执行某些操作的权利的对象，看了概念的我白了一眼，还是好好介绍一下吧。
Token，简单来说，就是类似 cookie 的一种验证信息，客户端通过登录验证后，服务器会返回给客户端一个加密的 token，然后当客户端再次向服务器发起连接时，带上token，服务器直接对token进行校验即可完成权限校验。

有了 Cookie 为什么还需要 Token?

Cookie 作为 HTTP 规范，其出现历史久远，因此存在一些历史遗留问题，比如跨域限制等，并且 Cookie 作为 HTTP 规范中的内容，其存在默认存储以及默认发送的行为，存在一定的安全性问题。相较于 Cookie，token 需要自己存储，自己进行发送，不存在跨域限制，因此 Token 更加的灵活，没有 Cookie 那么多的“历史包袱”束缚，在安全性上也能够做更多的优化。

Token 传递过程

Token 的传递过程和 Cookie 差不多，依然是通过验证后返回，然后存储到客户端，当下一次再次发起请求时，携带该验证信息进行快速验证。如下图

Token 有什么 优势?

从上面对于 Token 和 Cookie 的分析，我们知道了 Cookie 由于存储的内存空间只有 4kb，因此存储的主要是一个用户 id，其他的用户信息都存储在服务器的 Session 中，而 Token 没有内存限制，用户信息可以存储 Token 中，返回给用户自行存储，因此可以看出，采用 Cookie 的话，由于所有用户都需要在服务器的 Session 中存储相对应的用户信息，所以如果用户量非常大，这对于服务器来说，将是非常大的性能压力，而Token 将用户信息返回给客户端各自存储，也就完全避开这个问题了。

总结

虽然 Token 作为更加现代的存储方式被广泛采用，但是 Cookie 仍然是非常重要的验证方式，因此，我们不仅需要掌握 Token 的验证方式，也需要掌握 Cookie ，通过对比两种方式，了解其差异和优缺点，我们才能够更好地理解客户端验证的方式，也能够为我们学习和分析相关安全问题提供很好的底层原理支撑！