Cookie：位于用户的计算机上，用来维护用户计算机中的信息，直到用户删除。比如我们在网页上登录某个软件时输入用户名及密码时如果保存为cookie，则每次我们访问的时候就不需要登录网站了。我们可以在浏览器上保存任何文本，而且我们还可以随时随地的去阻止它或者删除。我们同样也可以禁用或者编辑cookie，但是有一点需要注意不要使用cookie来存储一些隐私数据，以防隐私泄露

session：称为会话信息，位于web服务器上，主要负责访问者与网站之间的交互，当访问浏览器请求http地址时，将传递到web服务器上并与访问信息进行匹配， 当关闭网站时就表示会话已经结束，网站无法访问该信息了，所以它无法保存永久数据，我们无法访问以及禁用网站。

session与cookie的区别

1. Cookie以文本文件格式存储在浏览器中，而session存储在服务端
2. cookie的存储限制了数据量，只允许4KB，而session是无限量的
3. 设置cookie时间可以使cookie过期。但是使用session-destory（），我们将会销毁会话。
4. Cookie存储在客户端阅读器中，对客户端可见,客户端上的某些程序可能会窥探、副本以更正cookie的内容。session存储在服务器上，对客户端是透明的。不存在敏感信息泄露的风险
5. 想要网站会永久记录用户的登录信息，使用cookies将是一个不错的选择。只需将cookie的到期时间属性设置为一个非常大的数字。由于Session依赖于名为JSESSIONID的cookie，并且Cookie JSESSIONID的到期时间默认为-1，因此只需关闭阅读器就会使Session无效，Session将无法永久完成信息。无法使用URL地址重写，如果设置Session的超时时间太长，服务器将累积的Sessions越多，导致内存溢出的可能性就越大。

Session部署

1，使用数据库来存储session

2，使用cookie来存储session

3，使用redis来存储session

4，使用tomcat的session复制

5，使用mamcached来存储session