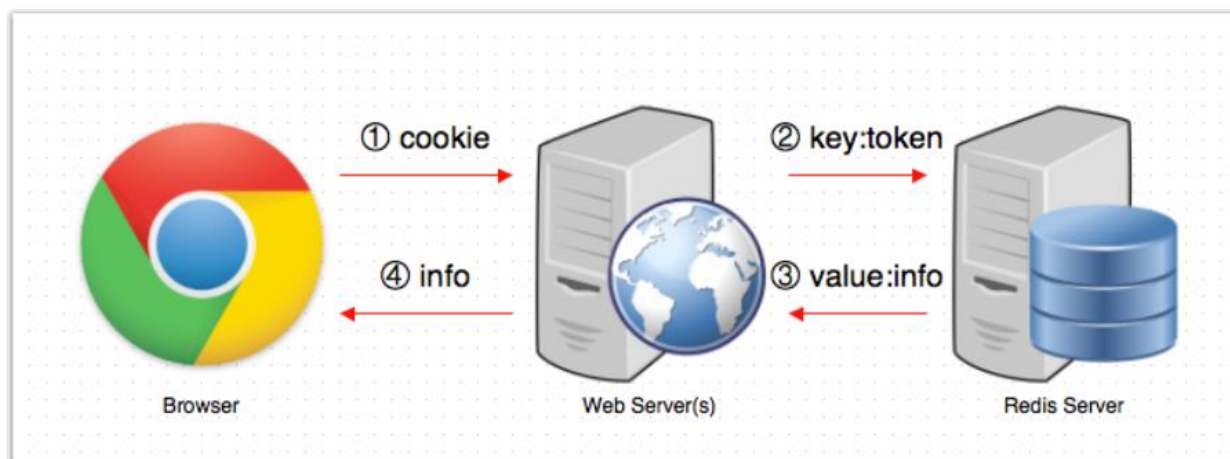


## 登录流程

- 1、用户从浏览器中将登录信息传到Web Server 中处理
- 2、Web Server 首先进行用户信息验证，当验证通过的时候，根据用户的客户端信息（IP、浏览器信息等）进行散列，形成一个token将会是Redis中的Key，同时将经常需要获取的内容（用户ID、姓名等）组装成Value，根据需要可以是json格式或者HashTable，然后设定一个expiretime保存进Redis
- 3、将生成的token保存在用户的浏览器cookie中



## 验证流程

- 1、用户访问需要进行验证登录的内容时。客户端会将cookie传到Web Server 中
- 2、Web Server从cookie中获取到token的值，判断token是否存在于Redis 中

**3、若存在则将Redis中保存的信息返回到Web Server中进行处理，判断此次获取是否合法：**

**\*\* 客户端的信息是否和生成token时的一致（IP、浏览器信息）**

**\*\* Value中保存的内容是否和当前操作匹配（用户ID是否和当前处理的ID，或者如果                      将IP等信息放到内容中也可以将上一条的验证在这里处理）**

**4、所有验证通过则将正常的结果返回给用户，有需要的话还可以在这个过程中重置或延长原来Redis key的生存时间**