# 笔记

Cookie：

存在浏览器端的；

安全性较低；

大小是有限制的；

实现会话控制；

班主任 巡查—》验证的过程—》服务器端验证；

**Session**；

存在服务器上：每一个客户端都会有一个自己的session记录；

安全性较高：因为是存在存在服务器上的，客户无法操作；

大小没有限制：；

实现会话控制、权限控制；

**Session依赖于COOKIE：如果有session的存在，必然有一个cookie和session有关系，cookie里面存的值，是当前客户端对应的session记录的唯一主键id；**

Cookie[‘conn.sid’] = ‘asdasdfaf7845a1fssdfsdfklml&\*)(JLJKKKhjasdasd’;



当用户再次发起请求的时候，请求头里面会跟上这个cookie信息；

服务器端收到这个cookie信息之后，根据该值，找到对应的session记录；

Cookie和session在当前域名下的每个页面都可以访问；

我们做 管理系统：

登录银行账号---》转账—》记录转账地址

直接访问 转账地址 进行 转账---》是要禁止的；

**验证 session 信息—》如果没有对应的session信息—》禁止操作—》引导用户登录—》返回登录页面**；

管理系统—》增删查改—》必须登录—》验证session信息；

是不是可以做项目了？

CAI

验证码：

1. 随机生成一个字符串：Math.random()---》存到SESSION里面；
2. 显示到图片:生成图片；
3. 用户输入的验证码和图片上的验证码进行对比；

密码：明文密码 加密密码

拖库：数据库被攻击了

Md5：很多时候我们称为加密，实际是一种算法，hash算法，不可破解；

长度都是32位；