# http特点

• web应用是基于HTTP协议的,而HTTP协议恰恰是一种无状态协议



### cookie

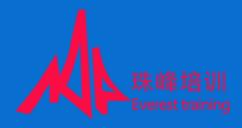
cookie是网站为了辩别用户身份,进行会话跟踪而存储在客户上的数据

• 通过响应头向客户端设置cookie

Set-Cookie: name=zfpx

• 读取客户端过来的cookie

Cookie: key1=value1; key2=value2



#### 设置cookie

#### res.cookie(name, value, [, options]);

参数	chrome对应属性	类型	说明
domain	Domain	String	域名,默认是当前域名
path	Path	String	域名,默认是/
expires	Expires	Date	过期时间,如果没以有指定或为0表示当前会话有效
maxAge	Max-Age	Number	有效时间(单位是毫秒)
httpOnly	НТТР	Boolean	不能通过浏览器javascript访问
secure	Secure	String	只通过https协议访问
signed	无	String	是否对cookie进行加密

# cookie使用注意事项

- 可能被客户端篡改,使用前验证合法性
- 不要存储 敏感数据 , 比如用户密码 , 账户余额
- 使用 httpOnly 保证安全
- 尽量减少 cookie 的 **体积**
- 设置正确的 domain 和 path , 减少数据传输



#### session

- 会话跟踪,数据存放在服务器端
- 需要借助 cookie 存储一个 会话ID, 服务器可以根据 会话ID 来查询出 详细的 session 数据



## session步骤

- 生成全局 唯一标识符 (sessionid)
- 开辟 数据存储 空间
- 将session的全局唯一标示符 发送给客户端



# cookie VS session

- 应用场景
- 安全性
- 性能
- 时效性
- 存储



