1. 跨站脚本攻击 xss Cross Site Scripting和 跨站请求伪造（csrf Cross-site request forgery）

xss:反射型（非持久型） 存储型 （持久型） dom型

攻击:

url的写入js代码 然后在脚本中提取url的js代码并执行；

富文本xss攻击

防御：

过滤 转义 编码

csrf

防御：

浏览器cookies设置samesites设置为strict

服务端同源检测

1. http缓存实践



1. 非对称加密和对称加密
2. https工作原理
3. promise实现原理
4. 5.lazyman 异步任务调度器 深拷贝（循环引用）
5. reduce参数 callback initialValue

其中callback参数：

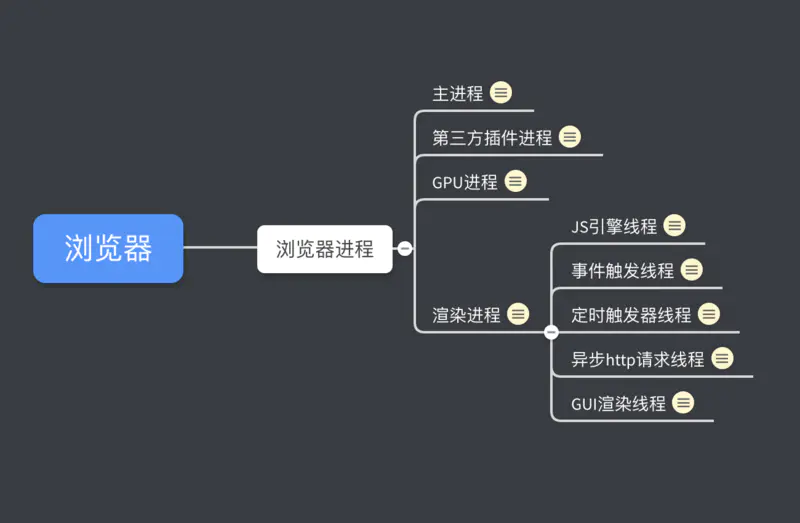
accumulator 累计器

currentValue 当前值

currentIndex 当前索引

array 数组

1. 浏览器垃圾回收机制 标记清楚 引用计数（循环引用 需要手动切除）
2. 浏览器**四大进程 五大线程**



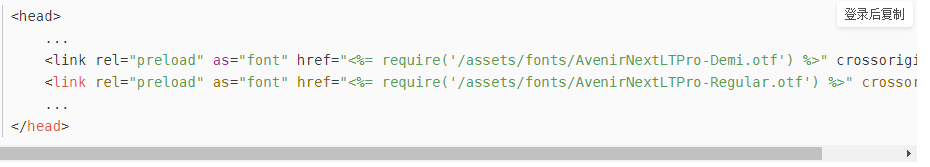
prefetch通常翻译为预提取，preload则翻译为预加载。



dns prefetch



图片prefetch



字体preload 提前加载

dva 流程

1.view dispatch action

2.effect接收action，call一个异步请求 并且put reducer

3.reducer接收state并且更新state

4.view更新

Subscriptio 订阅数据源