**一、原理区别**

HTTP定义了与服务器交互的不同方法，其中最基本的四种：GET，POST，PUT，DELETE，HEAD，其中GET和HEAD被称为安全方法，因为使用GET和HEAD的HTTP请求不会产生什么动作。不会产生动作意味着GET和HEAD的HTTP请求不会在服务器上产生任何结果。但是安全方法并不是什么动作都不产生，这里的安全方法仅仅指不会修改信息。

根据HTTP规范，POST可能会修改服务器上的资源的请求。比如CSDN的博客，用户提交一篇文章或者一个读者提交评论是通过POST请求来实现的，因为再提交文章或者评论提交后资源（即某个页面）不同了，或者说资源被修改了，这些便是“不安全方法”。

**二、实现方式的区别**

GET请求，请求的数据会附加在URL之后，以?分割URL和传输数据，多个参数用&连接。

POST请求会把请求的数据放置在HTTP请求包的包体中

**三、传输数据长度**

在HTTP规范中，没有对URL的长度和传输的数据大小进行限制。但是在实际开发过程中，对于GET，特定的浏览器和服务器对URL的长度有限制。因此，在使用GET请求时，传输数据会受到URL长度的限制。

对于POST，由于不是URL传值，理论上是不会受限制的，但是实际上各个服务器会规定对POST提交数据大小进行限制，Apache、IIS都有各自的配置。

**四、安全性**

POST的安全性比GET的高