android:usesCleartextTraffic=”false”
默认为 true，该属性用于应用的 NetworkSecurityPolicy，并且声明是否允许未加密的网络流量。当 usesCleartextTraffic 被设置为 false，应用程序会在使用 HTTP 而不是 HTTPS 时崩溃。你可以在 John Kozyrakis 的博客文章中阅读更多关于 Android M 加密连接的相关内容。

该属性 Api 级别 26，默认 true，允许使用不加密传输。
但 API 28，默认 false

Android 致力于保证其用户、设备和数据的安全。我们保证数据安全的一种方式是通过保护所有进入或离开使用 TLS 技术的 Android 设备数据。正如我们在 Android P 开发人员预览版中所宣布的那样，我们通过默认阻止 Android P 应用使用未加密连接通信来进一步提升安全性。

这是我们多年来为保护 Android 用户所做的各种更改。为了防止意外的未加密连接，我们在 Android Marshmallow(安卓 6.0)中引入了 **android:usesCleartextTraffic** 这样一个 manifest 属性。在 Android Nougat(安卓 7.0)中，我们通过创建网络安全配置(Network Security Config)功能扩展了该属性，该功能允许应用程序警告开发者在没有加密的情况下发送网络流量。在 Android Nougat(安卓 7.0)和 Oreo(安卓 8.0)中，我们仍然允许明文连接。

允许明文通信连接到特定的域

如果你需要允许连接到特定域或一组域，可以使用以下配置示例：

```
<network-security-config>
    <domain-config cleartextTrafficPermitted="true">
        <domain includeSubdomains="true">insecure.example.com</domain>
        <domain
includeSubdomains="true">insecure.cdn.example.com</domain>
    </domain-config></network-security-config>
```

允许连接到任意不安全的域

如果你的应用支持通过不安全连接的 URL 打开任意内容，则应该禁用链接到自己服务器的明文连接，但同时支持与其他任意主机的明文连接。请记住，对于通过不安全连接收到的数据应该保持谨慎，因为它可能在传输过程中被篡改。

```
<network-security-config>
    <domain-config cleartextTrafficPermitted="false">
        <domain includeSubdomains="true">example.com</domain>
```

```
        <domain includeSubdomains="true">cdn.example2.com</domain>
    </domain-config>
    <base-config cleartextTrafficPermitted="true"
/></network-security-config>
```