**Jingle项目接口签名**

**防止接口参数被篡改、防止接口被刷、验签**

**加密方式：Hmac-sha256（密钥，加密数据）**

**签名头：**

**x-appId-header 账户**

**x-sign-header 签名(接口加密后)**

**x-nonce-header 随机数**

**x-request-time-header 请求时间**

**x-skip-header 跳过校验**

**说明：**

**x-appId-header 账户**

**这个账号，为每个客户下发一套账号和密码，这个账号用于后端获取密码，用密码对接口参数进行加密，然后与前端传过来的加密参数进行校验**

**x-sign-header 签名**

**这个sign，当前请求求接口的参数与密码使用sha256进行加密后的64位字符串**

**x-nonce-header 随机数**

**这个随机数，随机数在有限时间内，只能请求一次，随机数定为10位长度，有效时间为600秒**

**x-request-time-header 请求时间**

**这个请求时间，指的是发起请求到后端接受请求之间的时间段，是否超过指定时间，**

**默认有效时间为300秒，时间格式20190731145710，14位长度**

**例子：**

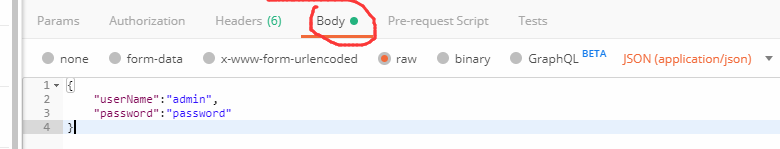
**Body：请求是Json方式**

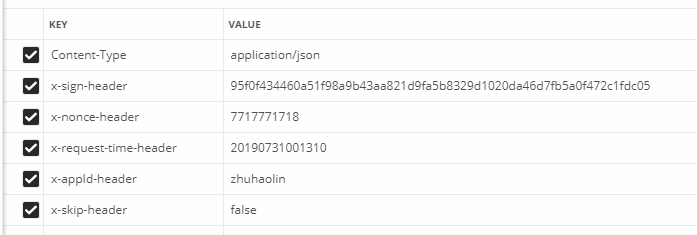
**密码：dabai@2019**

**数据：Json字符串**

**排序：不需要，加密的Json格式和传到后端的Json格式要一致(包括顺序)**

**例如：**





**Params：请求是param参数方式**

<http://ip:port/web/users>?id=abcd&name=zhuhaolin

**密码：dabai@2019**

**数据：**

**单个参数：id=abcd、name=zhuhaolin**

**多个参数：id=abcd、name=zhu,hao,lin**

**排序：对key进行排序(按字符串正序)**

**对key的值进行排序(按字符串正序)**

**例如：**

**单参数：**

**加密格式：name=zhuhaolinid=abcd**

**多参数：**

**加密格式：name=hao,lin,zhuid=abcd**

**Path：请求是路径参数方式**

<http://ip:port/web/users/efgh/abcd>

**密码：dabai@2019**

**数据：**

**efgh**

**abcd**

**排序：按字符串正序**

**例如：**

**加密格式：abcd,efgh**

**Body、params、path共存：**

**Body：**

**{"userName":"admin","password":"password"}**

**Params：**

**var3=2,3,a,朱**

**var4=4,5**

**Path：**

**1,2**

**无缝拼接：**

**{"userName":"admin","password":"password"} var3=2,3,a,朱var4=4,51,2**