今日内容：精通Postman接口测试之接口鉴权，接口Mock，接口加解密以及接口签名Sign

@auth：码尚学院_百里老师

@Email：2971330037@qq.com

一、接口鉴权（鉴定是否有访问接口的权限）

(1) cookie，session，token鉴权。

cookie鉴权：

cookie它是服务器产生的，保存在浏览器，主要是因为http协议无连接，无状态。（超市：没有会员卡，cookie：会员卡）

cookie通过键值对的方式来保存记录。原理：第1次访问服务器的时候，那么服务器就会产生cookie并且在响应头的set-cookie里面发送给浏览器，浏览器保存，在第2-N次请求时会带上cookie信息。

cookie一般包括信息：name，value，domain,path，expries，size。

回话级cookie和持久化cookie。

缓存并不等于cookie。

session鉴权：

session它是服务器产生的，保存在服务器的内存。它可以通过cookie来传参sessionid。原理：当你登录的时候，那么服务器会生成session，它通过cookie把sessionid传给客户端，然后在后面所有的请求里面都会自动的带上sessionid。然后和服务器的内存中的ssioniid对比以判断是否是同一个客户端。保存在服务器的内存里面的ssession的失效时间为30分钟。

在apache-tomcat-8.5.43\conf\web.xml文件里面的session-timeout可以修改默认的失效的时间。

sessionid可以隐藏域，也可以url或者是cookie传递。

token鉴权：

token是服务器的产生的，保存在服务器的文件或数据库（硬盘），一般情况下接口测试通过一个专门的获取token的 接口或者是登录接口来获取token.,获取后每次请求其他接口都必须带上token鉴权。

面试题：cookie,session,token的相同点和不同点？

相同点：

都是在服务器产生的，都是用于鉴权。只是保存在不同的地方。

不同点：

cookie保存在客户端，所以不安全，一般情况下用cookie保存一些非重要的数据，而通过session去保存一些重要的数据，session是保存在服务器的内存当中，而token是独立的鉴权，它和sesion和cookie无关。

(2)Postman的鉴权方式。

bearer token鉴权：就是发送一个鉴权码（令牌）。

basic Auth鉴权：通过用户名和密码实现鉴权。

二、接口Mock Sersver

mock测试就是测试过程中，对于一些不容易创建或者是不容易获取的比较复杂的对象，用一个模拟的对象去代替。

mock一把是为了解决单元之间的耦合依赖关系。（桩服务）

比如：工作中前后端分离，前端已经开发好了，但是后端的接口没有开发好。

项目之间的对接。（开发电子商务，支付宝支付。）

三、接口的加解密

接口加密：接口测试当中把传输的数据加密成密文（0101011101100）再传输。
接口解密：获取密文后把密文还原成原始数据。

1.目前市面上的加密方式
对称式加密（私钥加密）：DES，AES，Base64
非对称式加密（双钥加密）：RSA（公钥《公开》和私钥《保密》）
只加密不解密：MD5，SHA1，SHA3.....（就是这两种）

http://www.bejson.com

Postman实现解密接口（可遇不可求，除非自定义。）

四、接口签名sign（接口鉴权的一种）

BATJ，金融项目，银行项目等。

1.什么是接口签名？
接口签名就是使用appid,appsecret,nonce(流水号),timestamp，以及其它的各种参数按照一定的规则（ASCII排序）组成用来识别你的账号有没有访问api接口的权限的字符串，组成之后再进行加密，这个经过加密之后的字符串就是sign签名。
appid和appsec在线下针对不同的接口调用方提供的。
流水号nonce，订单号一般是一串10位以上的随机一组数字或者随机的一组字符串。数字+字符串（guid）。
timestamp时间戳，一般10分钟之内有效。

2、为什么要做接口签名？（大大提高接口的安全性）
(1)防止接口鉴权码泄漏，接口被伪装攻击，（签名，只需要提供签名不需要鉴权码）
(2) 防止接口数据被篡改，（原理：签名针对的是所有的请求数据，只要有一个数字别改动了，那么sign就变了。就会请求失败。）
(3)防止接口被重复提交，nonce是唯一的。并且只有10分钟之内有效。

3、接口签名的规则有很多，每个公司都不一样，但是大同小异（90%以上相似）。举例：
(1)获取到所有的参数包括params和body，把所有的参数的key按照ascii码升序排列。
{a:2,c:1,b:3}改成{a:2,b:3,c:1,}
(2)把参数按照key=value的方式组合，多个参数用&分开。
a=2&b=3&c=1
(3)用申请到的appid和appsecret拼接到参数的最前面
appid=123&appsecret=456&a=2&b=3&c=1
(4)把订单号和时间戳拼接到参数的最后面
appid=123&appsecret=456&a=2&b=3&c=1&nonce=12121313&timestamp=235235235
(5)把上述字符串通过MD5加密。加密之后大写。形成sign
sign=WEO987979798DDFGF767FDG
(6)然后把sign放到url或者请求头（一般用这种）或请求体里面发送给服务器做鉴权。

```
//接口签名
//1.获取到asppid和appsecret
var appid = "test";
var appsecret = "123";
console.log(appid);
console.log(appsecret);
```

```
//2.获得nonce流水号
var nonce = getnonce(1000000000,9999999999);
console.log(nonce);
//3.获得时间戳
var timestamp = new Date().getTime();
console.log("timestamp="+timestamp)
//4.获取到params里面的参数
var params_args = pm.request.url.query.members;
console.log("params_args="+params_args);
//5.获取到body里面的参数(JSON.parse加载成对象，JSON.stringify加载成字符串)
var body_args =  request.data;
console.log("body_args="+JSON.stringify(body_args));
//6.把params和body的参数组合成一个变量
for(var i=0;i<params_args.length;i++){
    body_args[params_args[i].key] = params_args[i].value;
}
console.log("body_args2="+JSON.stringify(body_args));
//7.把组合的数据按照key升序
body_args = objectsort(body_args)
console.log("body_args3="+JSON.stringify(body_args));
//8.把字典格式的参数转换成key=value&key=value的格式
var new_string = "";
for(var key in body_args){
    new_string += key + "=" + body_args[key] + "&";
}
console.log("new_string="+JSON.stringify(new_string));
//9.在字符串的前面加上aooid和appsecret，在字符串的后面加nonce,timestamp.
new_string = "appid="+appid+"&"+"appsecret="+appsecret+"&"+new_string+"nonce="+nonce+"&"+"timestamp="+timestamp;
console.log(new_string);
//10.对上述字符做MD5加密后并大写形成sign签名，然后把sign保存为全局变量
var sign =  CryptoJS.MD5(new_string).toString().toUpperCase();
console.log("sign="+sign);
pm.globals.set("sign",sign);
//------------------------------------------------------
//获得任意长度的随机数字
function getnonce(min,max){
    return Math.floor(Math.random() * (max - min + 1)) + min;
}
//把对象的key升序排序函数（此方法固定）
function objectsort(obj){
    var new_key = Object.keys(obj).sort();
    console.log(new_key);
    var arr = {};
    for(var i=0;i<new_key.length;i++){
        arr[new_key[i]] = obj[new_key[i]];
    }
    return arr;
}
```

四、作业

1.理解各种不同的接口鉴权方式以及了解他们的用法。

2.调通Postman加密接口。

3.调通接口签名sign。

最后：麻烦在VIP课程下面给百里一个好评！非常感谢！