# 设置谷歌浏览器的非安全模式

"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --user-data-dir="C:/MyChromeDevUserData" --test-type --disable-web-security

# 如果前端显示效果不对

1. 看数据chrome的network中是否加载成功
2. 对比数据是否和9000端口的一致

# Token用户登录原理

用户一旦输入用户名和密码OK以后，就派发一个Token（随机字符串）给用户，用户来访问都会携带Token

数据库存了两列

1列是token，1列就是userid

## 理解token的步骤：

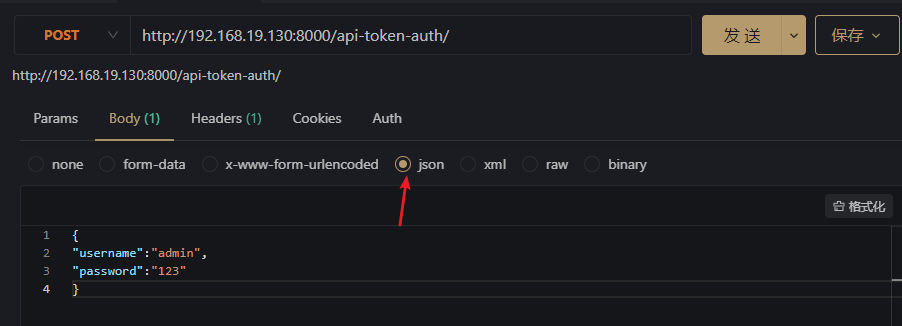
1. urls去配置连接
2. Apifox 向 <http://192.168.0.111:8000/api-token-auth/提交用户名和密码，就会得到一个token>

{

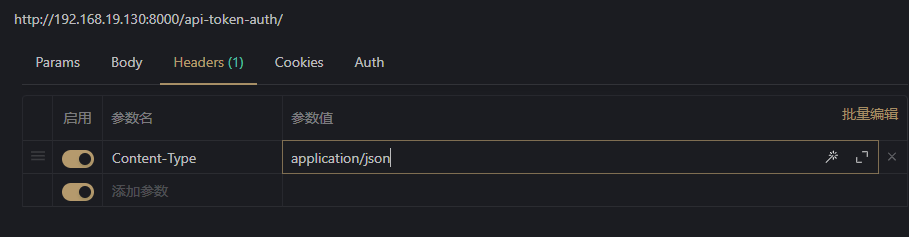
"username":"admin",

"password":"123"

}



当然不要忘记增加HTTP头部 Content-Type: application/json

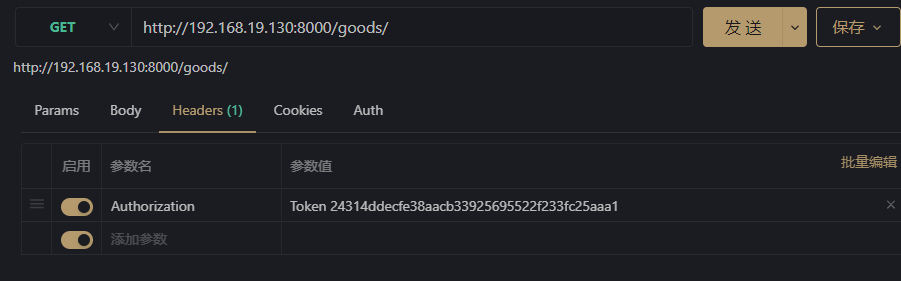


得到的token是

3a5bfe2e6daaf83c483510b50461a1808cb39dcc

3 向http://192.168.19.130:8000/goods/发送请求，头部有**Authorization，值为**

**Token xxxxxxxxxx**



## Token相对于session优势

不需要像session那样，取到session\_data，还要去解码，而是直接拿到了user\_id

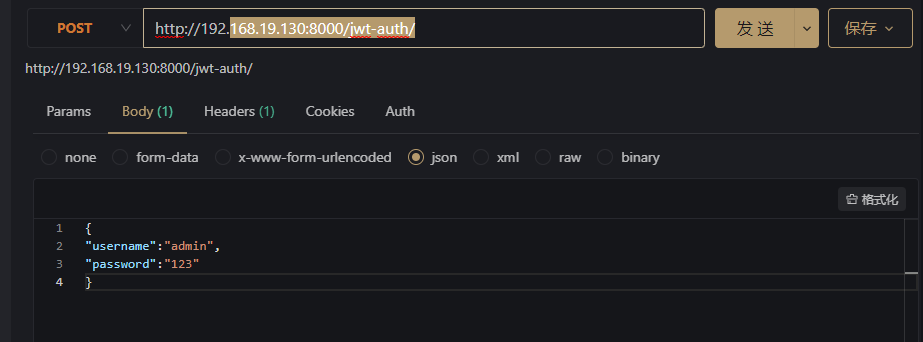
# JWT Token特点

所有的服务器有一把钥匙（解密的钥匙）

登录时，把用户的信息，通过加密算法，加密后，得到密文，这个密文就是JWT Token

## Jwt token原理理解

1、向http://192.168.19.130:8000/jwt-auth/ 发送请求



得到jwt token

{

"token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoxLCJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNjQ5MjE2ODkwLCJlbWFpbCI6IjEyM0BxcS5jb20ifQ.guIU-TJ6ECjNKUKxer6wki9mvj9Gb-duManEFwyKNbw"

}

### **Base64转换步骤:**

* **第一步，将待转换的字符串,  每三个字节分为一组，每个字节占8bit，那么共有24个二进制位。**
* **第二步，将上面的24个二进制位每6个一组，共分为4组。**
* **第三步，在每组前面添加两个0，每组由6个变为8个二进制位，总共32个二进制位，即四个字节。**
* **第四步，根据Base64编码对照表（见下图）获得对应的值。**

# 使用到的时间分为3中情况

秒数 import time time.time()

日期，日期时间 import datetime date datetime

Timedelta 时间间隔 import datetime

# 开发工作

Leetcode

# 数据分析

刷SQL题