haoqicat 16/12/5 下午3:37



Mongoose 连接两座 孤岛之间的桥梁

第二章:后端实现用户 认证接口

> 借助 Mongoose 保存 用户信息到 MongoDB 数据库

# JWT 知识科普

后面代码中咱们的 token-based 认证过程是通过 JWT 标准来完成的。

### 什么是 JSON Web Tokens?

JWT 是 JSON Web Token 的简写,它定义了一种在客户端和服务器端安全传输数据的规范。通过 JSON格式 来传递信息。

#### JWT 的基本组成

由一个点隔开的三段乱码

aaaaaaaaa.bbbbbbbbbbbccccccccc

haoqicat 16/12/5 下午3:37

第一段是 header ,第二段是 payload (主体信息),第三段是 signature (数字签名)。

那么这三段分别都是是如何得到的呢?参考这里。

其中我要强调一下的是最后一段,也就是数字签名这一段,运算过程如下:

```
var encodedString = base64UrlEncode(header) +
HMACSHA256(encodedString, 'secret');
```

注意,签名是由服务器完成的, secret 是服务器上存储的密钥,信息签名后整个 token 会发送给浏览器,每次浏览器 发送请求中都包含 secret 所以可以跟服务器达成互信,完成认证过程。

#### 谁在用 JWT?

- https://auth0.com/
- o google
- facebook
- o github

总之, JWT 技术已经非常主流了。

#### 参考资料

- https://scotch.io/tutorials/the-anatomy-of-ajson-web-token
- https://auth0.com/blog/json-web-token-signing-

haoqicat 16/12/5 下午3:37

## algorithms-overview/

欢迎添加 Peter 的微信: happypeter1983

冀ICP备15007992号-3