Koa实战 - 鉴权

session-cookie方式

cookie原理解析

```
// cookie.js
const http = require("http")
http
    .createServer((req, res) => {
            if(req.url === '/favicon.ico'){
          res.end('')
          return
            }
        // 观察cookie存在
        console.log('cookie:', req.headers.cookie)
        // 设置cookie
        res.setHeader('Set-Cookie', 'cookie1=abc;')
        res.end('hello cookie!!')
    })
    .listen(3000)
```

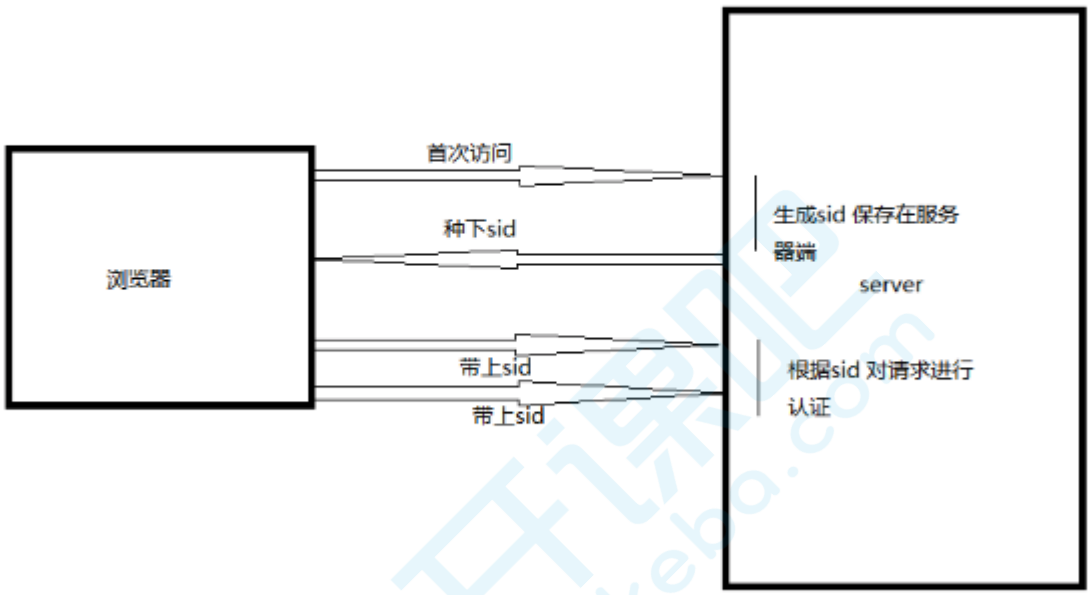
- Header Set-Cookie负责设置cookie
- 请求传递Cookie

session的原理解释

```
// cookie.js
const http = require("http")
const session = {}
http
    .createServer((req, res) => {
        // 观察cookie存在
        console.log('cookie:', req.headers.cookie)

        const sessionKey = 'sid'
        const cookie = req.headers.cookie
        if(cookie && cookie.indexOf(sessionKey) > -1 ){
            res.end('Come Back ')
            // 简略写法未必具有通用性
            const pattern = new RegExp(`${sessionKey}=([^;]+);?\s*`)
            const sid = pattern.exec(cookie)[1]
            console.log('session:',sid ,session ,session[sid])
        } else {
            const sid = (Math.random() * 99999999).toFixed()
            // 设置cookie
            res.setHeader('Set-Cookie', `${sessionKey}=${sid};`)
```

```
            session[sid] = {name : 'laowang'}
            res.end('Hello')
        }
        res.end('hello cookie!!')
    })
    .listen(3000)
```

- 原理



> 实现原理：
>
> 1. 服务器在接受客户端首次访问时在服务器端创建seesion，然后保存seesion(我们可以将seesion保存在内存中，也可以保存在redis中，推荐使用后者)，然后给这个session生成一个唯一的标识字符串,然后在响应头中种下这个唯一标识字符串。
> 2. 签名。这一步通过秘钥对sid进行签名处理，避免客户端修改sid。（非必需步骤）
> 3. 浏览器中收到请求响应的时候会解析响应头，然后将sid保存在本地cookie中，浏览器在下次http请求的请求头中会带上该域名下的cookie信息，
> 4. 服务器在接受客户端请求时会去解析请求头cookie中的sid，然后根据这个sid去找服务器端保存的该客户端的session，然后判断该请求是否合法。

- koa中的session使用：`npm i koa-session -S`

```
const koa = require('koa')
const app = new koa()
const session = require('koa-session')

// 签名key keys作用 用来对cookie进行签名
app.keys = ['some secret'];

// 配置项
const SESS_CONFIG = {
```

```
  key: 'kkb:sess', // cookie键名
  maxAge: 86400000, // 有效期，默认一天
  httpOnly: true, // 仅服务器修改
  signed: true, // 签名cookie
};

// 注册
app.use(session(SESS_CONFIG, app));

// 测试
app.use(ctx => {
  if (ctx.path === '/favicon.ico') return;
  // 获取
  let n = ctx.session.count || 0;
  // 设置
  ctx.session.count = ++n;
  ctx.body = '第' + n + '次访问';
});

app.listen(3000)
```

使用redis存储session

```
const redis = require('redis');

const client = redis.createClient(6379,'localhost');

client.set('hello','This is a value');

client.get('hello',function (err,v) {
    console.log("redis get ",v);
})
```

- 安装：`npm i -S koa-redis`
- 配置使用：

```
// koa-redis
const redisStore = require('koa-redis');
const redis = require('redis')
const redisClient = redis.createClient(6379, "localhost");

var wrapper = require('co-redis');
var client = wrapper(redisClient);

app.use(session({
  key:'kkb:sess',
  store: redisStore({client}) // 此处可以不必指定client
```

```
}, app));

app.use(ctx => {
  //...
  //查看redis中存储的数据
  redisClient.keys('*',(err,keys)=>{
    console.log(keys);
    keys.forEach(key=>{
      redisClient.get(key,(err,val)=>{
        console.log(val);
      })
    })
  })
});
```

- 案例：通过session实现用户鉴权
  - 登录页面，./public/login-session.html

```
<html>
  <head>
    <script src="https://cdn.jsdelivr.net/npm/vue/dist/vue.js"></script>
    <script src="https://unpkg.com/axios/dist/axios.min.js"></script>
  </head>

  <body>
    <div id="app">
      <div>
        <input v-model="username" />
        <input v-model="password" />
      </div>
      <div>
        <button @click="login">Login</button>
        <button @click="logout">Logout</button>
        <button @click="getUser">GetUser</button>
      </div>
      <div>
        <button @click="logs=[]">Clear Log</button>
      </div>
      <!-- 日志 -->
      <ul>
        <li v-for="(log,idx) in logs" :key="idx">
          {{ log }}
        </li>
      </ul>
    </div>
    <script>
      // 这行代码很关键，请求时携带cookie
      axios.defaults.withCredentials = true;
      axios.interceptors.response.use(response => {
```

```
        app.logs.push(JSON.stringify(response.data));
        return response;
      });
      var app = new Vue({
        el: "#app",
        data: {
          username: "test",
          password: "test",
          logs: []
        },
        methods: {
          login: async function() {
            await axios.post("/users/login", {
              username: this.username,
              password: this.password
            });
          },
          logout: async function() {
            await axios.post("/users/logout");
          },
          getUser: async function() {
            await axios.get("/users/getUser");
          }
        }
      });
    </script>
  </body>
</html>
```

-

> koa-bodyparser用于解析post请求体
>
> - 安装：npm i koa-bodyparser -S
> - 配置

```
// index.js
const session = require('koa-session')

// 签名key keys作用 用来对cookie进行签名
app.keys = ['some secret'];

// 配置项
const SESS_CONFIG = {
key: 'kkb:sess', // cookie键名
maxAge: 86400000, // 有效期，默认一天
httpOnly: true, // 仅服务器修改
signed: true, // 签名cookie
};

// 注册
app.use(session(SESS_CONFIG, app));
```

```
const bodyparser = require('koa-bodyparser')
app.use(bodyparser())
```

- 登录/注销接口，./routes/users.js

```
router.post("/login", async ctx => {
  // 需安装bodyparser
  const { body } = ctx.request;
  console.log("body", body);

  //登录逻辑，略

  //登录成功，设置session
  ctx.session.userinfo = body.username;
  ctx.body = {
    ok: 1,
    message: "登录成功"
  };
});
router.post("/logout", async ctx => {
  //设置session
delete ctx.session.userinfo;
  ctx.body = {
    ok: 1,
    message: "登出系统"
  };
});
router.get("/getUser", async ctx => {
    ctx.body = {
      ok: 1,
      message: "获取数据成功",
      userinfo: ctx.session.userinfo
    };
});
```

- 路由守卫中间件，./middleware/auth.js

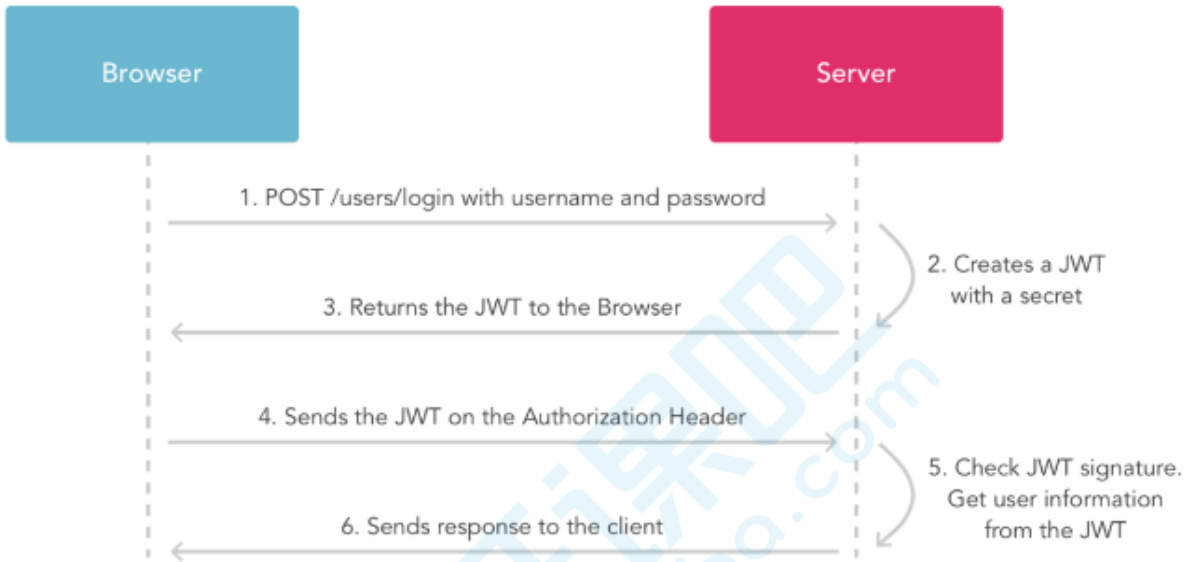
```
module.exports = async (ctx, next) => {
  if (!ctx.session.userinfo) {
    ctx.body = {
      ok: 0,
      message: "用户未登录"
    };
  } else {
    await next();
  }
};
```

- 应用守卫，./routes/users.js

```
router.get("/getUser", require("../middleware/auth"), async ctx => {...})
```

Token 验证

- 原理



- 案例：令牌认证
  - 登录页，public/login-token.html

```
<html>
  <head>
    <script src="https://cdn.jsdelivr.net/npm/vue/dist/vue.js"></script>
    <script src="https://unpkg.com/axios/dist/axios.min.js"></script>
  </head>

  <body>
    <div id="app">
      <div>
        <input v-model="username" />
        <input v-model="password" />
      </div>
      <div>
        <button v-on:click="login">Login</button>
        <button v-on:click="logout">Logout</button>
        <button v-on:click="getUser">GetUser</button>
      </div>
      <div>
        <button @click="logs=[]">Clear Log</button>
      </div>
      <!-- 日志 -->
```

```
    <ul>
      <li v-for="(log,idx) in logs" :key="idx">
        {{ log }}
      </li>
    </ul>
  </div>
  <script>
    axios.interceptors.request.use(
      config => {
        const token = window.localStorage.getItem("token");
        if (token) {
          // 判断是否存在token，如果存在的话，则每个http header都加上token
          // Bearer是JWT的认证头部信息
          config.headers.common["Authorization"] = "Bearer " + token;
        }
        return config;
      },
      err => {
        return Promise.reject(err);
      }
    );

    axios.interceptors.response.use(
      response => {
        app.logs.push(JSON.stringify(response.data));
        return response;
      },
      err => {
        app.logs.push(JSON.stringify(response.data));
        return Promise.reject(err);
      }
    );
    var app = new Vue({
      el: "#app",
      data: {
        username: "test",
        password: "test",
        logs: []
      },
      methods: {
        login: async function() {
          const res = await axios.post("/users/login-token", {
            username: this.username,
            password: this.password
          });
          localStorage.setItem("token", res.data.token);
        },
        logout: async function() {
          localStorage.removeItem("token");
        },
        getUser: async function() {
          await axios.get("/users/getUser-token");
        }
```

```
        }
      });
    </script>
  </body>
</html>
```

- 登录接口
  - 安装依赖：`npm i jsonwebtoken koa-jwt -S`
  - 接口编写，routes/users.js

```
const jwt = require("jsonwebtoken");
const jwtAuth = require("koa-jwt");
const secret = "it's a secret";

router.post("/login-token", async ctx => {
  const { body } = ctx.request;
  //登录逻辑，略
  //设置session
  const userinfo = body.username;
  ctx.body = {
    message: "登录成功",
    user: userinfo,
    // 生成 token 返回给客户端
    token: jwt.sign(
      {
        data: userinfo,
        // 设置 token 过期时间，一小时后，秒为单位
        exp: Math.floor(Date.now() / 1000) + 60 * 60
      },
      secret
    )
  };
});

router.get(
  "/getUser-token",
  jwtAuth({
    secret
  }),
  async ctx => {
    // 验证通过，state.user
    console.log(ctx.state.user);

    //获取session
    ctx.body = {
      message: "获取数据成功",
      userinfo: ctx.state.user.data
    };
  }
);
```

JWT(JSON WEB TOKEN)原理解析

1. Bearer Token包含三个组成部分：令牌头、payload、哈希

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkYXRhIjp7InVzZXJuYW1lIjoiYWJjIiwicGFzc3dvcmQiOiIxMTExMTEifSwiZXhwIjoxNTU3MTU1NzMwLCJpYXQiOjE1NTcxNTIxMzB9.pjGaxzX2srG_MEZizzmFEy7JM3t8tjkiu3yULgzFwUk

1. 签名：默认使用base64对payload编码，使用hs256算法对令牌头、payload和密钥进行签名生成哈希
2. 验证：默认使用hs256算法对hs256算法对令牌中数据签名并将结果和令牌中哈希比对

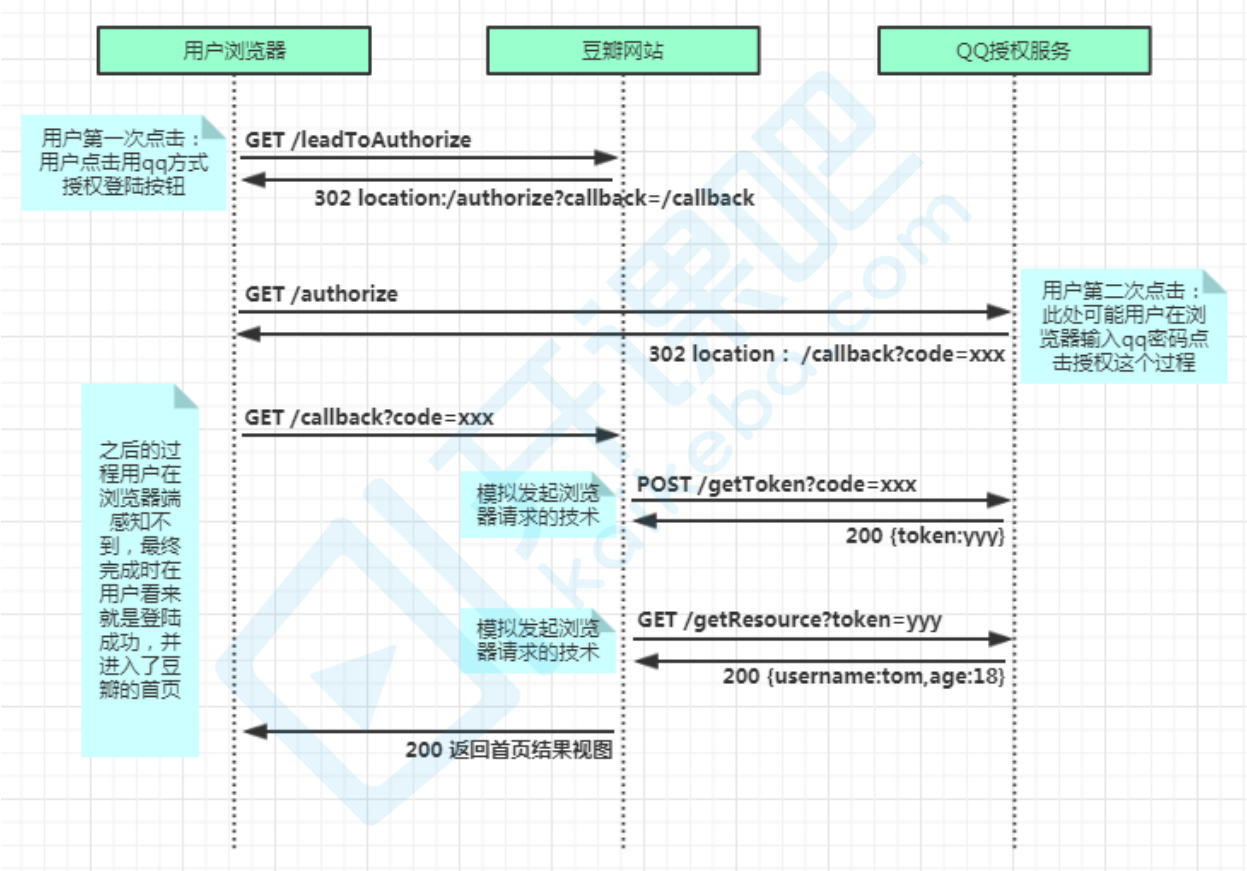
```
// jsonwebtoken.js

const jsonwebtoken = require('jsonwebtoken')
const secret = '12345678'
const opt = {
  secret: 'jwt_secret',
  key: 'user'
}
const user = {
  username: 'abc',
  password: '111111'
}

const token = jsonwebtoken.sign({
  data: user,
  // 设置 token 过期时间
  exp: Math.floor(Date.now() / 1000) + (60 * 60),
}, secret)

console.log('生成token:' + token)
// 生成
token:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkYXRhIjp7InVzZXJuYW1lIjoiYWJjIiwicGFzc3dvcmQiOiIxMTExMTEifSwiZXhwIjoxNTQ2OTQyMzk1LCJpYXQiOjE1NDY5Mzg3OTV9.VPBCQgLB7XPBq3RdHK9WQMkPp3dw65JzEKm_LZZjP9Y
console.log('解码:', jsonwebtoken.verify(token, secret, opt))
// 解码: { data: { username: 'abc', password: '111111' },
//  exp: 1546942395,
//  iat: 1546938795 }
```

> **参考文档:**
>
> jsonwebtoken、koa-jwt
>
> 阮一峰 JWT解释

> http://www.ruanyifeng.com/blog/2018/07/json_web_token-tutorial.html

OAuth(开放授权)

- 概述：三方登入主要基于OAuth 2.0。OAuth协议为用户资源的授权提供了一个安全的、开放而又简易的标准。与以往的授权方式不同之处是OAUTH的授权不会使第三方触及到用户的帐号信息（如用户名与密码），即第三方无需使用用户的用户名与密码就可以申请获得该用户资源的授权，因此OAUTH是安全的。
- OAuth登录流程



- 案例：OAuth登录
  - 登录页面 index.html

```
<html>
<head>
  <script src="https://cdn.jsdelivr.net/npm/vue/dist/vue.js"></script>
  <script src="https://unpkg.com/axios/dist/axios.min.js"></script>
</head>
<body>
  <div id="app">
      <a href='/github/login'>login with github</a>
  </div>
</body>
</html>
```

- 登录接口 index.js

```
const Koa = require('koa')
const router = require('koa-router')()
const static = require('koa-static')
const app = new Koa();
const axios = require('axios')
const querystring = require('querystring')

app.use(static(__dirname + '/'));
const config = {
    client_id: '73a4f730f2e8cf7d5fcf',
    client_secret: '74bde1aec977bd93ac4eb8f7ab63352dbe03ce48'
}

router.get('/github/login', async (ctx) => {
    var dataStr = (new Date()).valueOf();
    //重定向到认证接口,并配置参数
    var path = "https://github.com/login/oauth/authorize";
    path += '?client_id=' + config.client_id;

    //转发到授权服务器
    ctx.redirect(path);
})
router.get('/github/callback', async (ctx) => {
    console.log('callback..')
    const code = ctx.query.code;
    const params = {
        client_id: config.client_id,
        client_secret: config.client_secret,
        code: code
    }
    let res = await axios.post('https://github.com/login/oauth/access_token',
params)
    const access_token = querystring.parse(res.data).access_token
    res = await axios.get('https://api.github.com/user?access_token=' +
access_token)
    console.log('userAccess:', res.data)
    ctx.body = `
```

```
        <h1>Hello ${res.data.login}</h1>
        <img src="${res.data.avatar_url}" alt=""/>
    `


})

app.use(router.routes()); /*启动路由*/
app.use(router.allowedMethods());
app.listen(3000);
```

开课吧kaikeba.com