

Name: Gordon Foo A0199554L

Link to github repo: [https://github.com/gordonfgz/CS3219\\_OTOT\\_C.git](https://github.com/gordonfgz/CS3219_OTOT_C.git)

All credits go to: <https://www.bezkoder.com/node-js-jwt-authentication-postgresql/>

401 response on un authenticated user:

The screenshot shows a REST client interface with the following details:

- URL:** `http://localhost:8080/api/test/user`
- Method:** GET
- Headers:** 6 hidden. The visible header is `x-access-token` with a value starting with `eyJhbGciOiJIUzI1NiIsInR5cCI6Ikp...`.
- Response:** 401 Unauthorized, 8 ms, 427 B. The body is `{"message": "You are not authenticated!"}`.

200 response on authenticated user:

The screenshot shows a REST client interface with the following details:

- URL:** `http://localhost:8080/api/test/user`
- Method:** GET
- Headers:** 6 hidden. The visible header is `x-access-token` with a value starting with `eyJhbGciOiJIUzI1NiIsInR5cCI6Ikp...`.
- Response:** 200 OK, 3 ms, 382 B. The body is `User Content.`

403 response on authenticated but NOT authorised user:

GET http://localhost:8080/api/test/mod?x-access-token=eyJhbGciOiJIUzI1NiIsInR5cCI6Ikp... Send

Params Auth Headers (9) Body Pre-req. Tests Settings Cookies

Headers 8 hidden

|                                     | KEY            | VALUE                              | DES | ... | Bulk Edit | Presets     |
|-------------------------------------|----------------|------------------------------------|-----|-----|-----------|-------------|
| <input checked="" type="checkbox"/> | x-access-token | eyJhbGciOiJIUzI1NiIsInR5cCI6Ikp... |     |     |           |             |
|                                     | Key            | Value                              |     |     |           | Description |

Body 403 Forbidden 143 ms 421 B Save Response

Pretty Raw Preview Visualize JSON

```
1 {
2   "message": "Require Moderator Role!"
3 }
```

200 response on authenticated and authorised user:

GET http://localhost:8080/api/test/admin?x-access-token=eyJhbGciOiJIUzI1NiIsInR5cCI6Ikp... Send

Params Auth Headers (9) Body Pre-req. Tests Settings Cookies

Headers 8 hidden

|                                     | KEY            | VALUE                              | DES | ... | Bulk Edit | Presets     |
|-------------------------------------|----------------|------------------------------------|-----|-----|-----------|-------------|
| <input checked="" type="checkbox"/> | x-access-token | eyJhbGciOiJIUzI1NiIsInR5cCI6Ikp... |     |     |           |             |
|                                     | Key            | Value                              |     |     |           | Description |

Body 200 OK 42 ms 383 B Save Response

Pretty Raw Preview Visualize HTML

```
1 Admin Content.
```

Scalability:

More roles can be added in the initialise method:

```
function initial() {
  Role.create({
    id: 1,
    name: "user"
  });

  Role.create({
    id: 2,
    name: "moderator"
  });

  Role.create({
    id: 3,
    name: "admin"
  });
}
```

Method to check can be implemented in authJWT

```
JS authJwt.js A X JS index.js ...middleware A JS ve
middleware > JS authJwt.js > verifyToken > jwt.verify() callb

    res.status(403).send({
      message: "Require Admin Role!"
    });
    return;
  });
});
};

isModerator = (req, res, next) => {
  User.findById(req.userId).then(user => {
    user.getRoles().then(roles => {
      for (let i = 0; i < roles.length; i++) {
        if (roles[i].name === "moderator") {
          next();
          return;
        }
      }
    })
    res.status(403).send({
      message: "Require Moderator Role!"
    });
  });
});
};
```