Securing a GraphQL API with Apollo

IMPLEMENTING HEADER AUTHENTICATION FOR APOLLO SERVER AND CLIENT

Mat Warger
SOFTWARE CONSULTANT

@mwarger mw.codes

Overview

Globomantics conference

Why add authentication?

Server-side and client-side

- JWTs
- User sign-up
- User sign-in
- Access restriction

Sound familiar?

Apollo Server and Client

These are prerequisites!

Apollo Server

GraphQL implementation based on Express server and Node.js

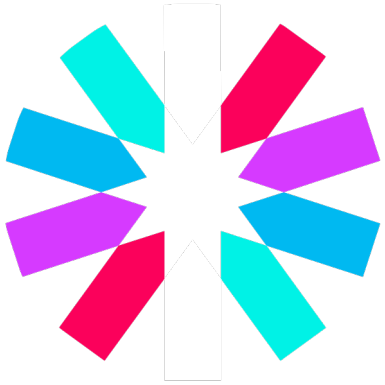
Apollo Client

React client for sending GraphQL requests, including options for caching

A Tour of Globomantics

A Tour of the Application

JSON Web Tokens (JWT)



JWTs encode information and ensure integrity

Created on the server - persisted and used on the client

- Server signs and verifies JWTs
- Client stores for future requests

Why JWTs?

- Common, easy to use, portable

Components of a JWT

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIn0.
9oDgE4J5RJ17rnI7HDS3ExuhN-sFbVTAKCsp-evkW6A

Header

Typically contains the type and algorithm used.

Payload

Contains claims. These are assertions made about the subject.

Signature

Contains the header and payload, encoded using an algorithm along with a secret.

Breaking Down a JWT

Header

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9

Payload

```
{
  "sub": "1234567890",
  "name": "John Doe"
}
```

eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIn0

Signature

```
HMACSHA256(
base64UrlEncode(header) + "."
+ base64UrlEncode(payload),
secret)
```

9oDgE4J5RJ17rnI7HDS3ExuhN-sFbVTAKCsp-evkW6A

Keep it secret! Keep it safe!

Demo

User sign-up

- Hashing and salting passwords
- Storing user data

User sign-in

- Verifying passwords
- Retrieving user data

Implementing JWTs

- Sign a payload to create a JWT
- Decode a token into a payload

Restricting access to mutations

Client-side Application

Using the Apollo Server context

Summary

Authentication accomplished!

- JWTs
- Users can sign up and sign in
- Authorization header provides authentication using token

Next: Transition to cookies