User Authentication and Application Security

Node.js Accelerator – Jan’23

Agenda

1. Authentication Types
2. Session Vs Tokens
3. JWT
4. Bcrypt
5. Auth0

Toptal®

Node.js Accelerator

Jan 2023

Authentication Types

Common Authentication types:

- Password based authentication
- Two-factor/multi factor authentication
- Biometric authentication
- Single sign-on (SSO)
- Token-based authentication
- Certificate-based authentication

Session Vs Tokens

Features	Session	Token
Authentication details	Server side	With the user
Authentication method	Generally the cookie	Its own Token
How to validate a request	Server memory/database	Token decrypt + validating signature
Scalability	Limited scalability due server memory	High scalability due serverless token
Where is suitable	Server side rendered pages in the same domain (like Next.js applications with next-auth)	Mobile apps, single page applications and machine to machine apps

JWT

JSON Web Token (JWT) is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object.

- Good usage for Authorization and Information Exchange
- In HTTP requests set in the Authorization header starting with **Bearer** + JWT_TOKEN

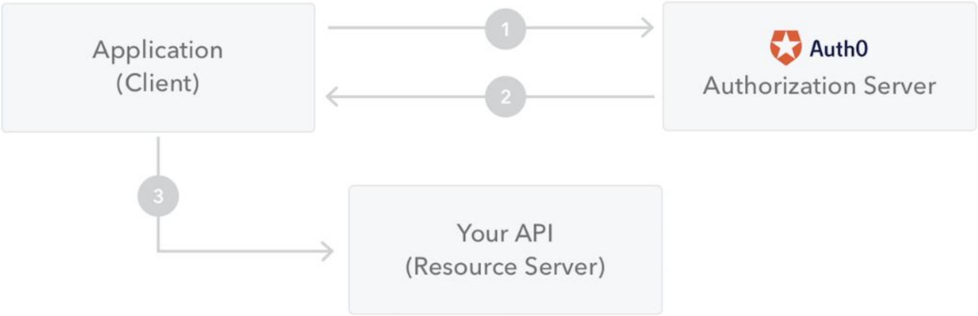


Image from jwt.io

Bcrypt

In some scenarios that you are in a need to store user sensitive information like passwords due not using a third party such as Auth0, Cognito or others then you might be safely hashing the required information.

A good way to do so is using Bcrypt

Hashing:

```
bcrypt.hash(myPlaintextPassword,
saltRounds, function(err, hash) {
    // Store hash in your password DB.
  });
```

Comparing:

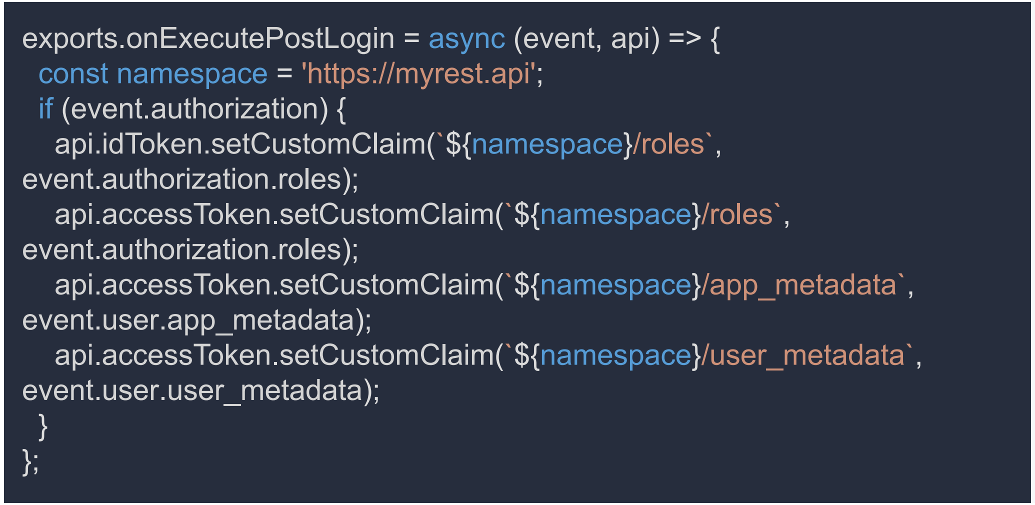
```
bcrypt.compare(myPlaintextPassword,
hash, function(err, result) {
    // result == true
  });
```

More on Bcrypt here

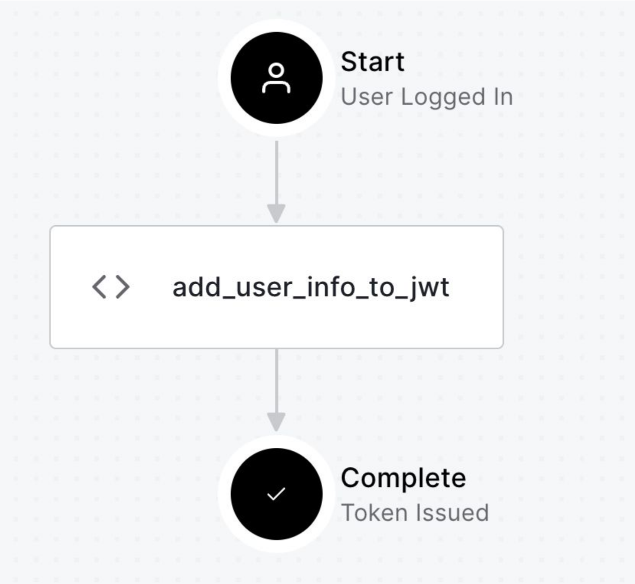
Auth0

Let’s see Auth0 in action within our scaffolded office hour project

Sometimes we want to add more information in our JWT. An example how actions can help for this:



```
exports.onExecutePostLogin = async (event, api) => {
  const namespace = 'https://myrest.api';
  if (event.authorization) {
    api.idToken.setCustomClaim(`${namespace}/roles`,
event.authorization.roles);
    api.accessToken.setCustomClaim(`${namespace}/roles`,
event.authorization.roles);
    api.accessToken.setCustomClaim(`${namespace}/app_metadata`,
event.user.app_metadata);
    api.accessToken.setCustomClaim(`${namespace}/user_metadata`,
event.user.user_metadata);
  }
};
```



Toptal®

ACTION ITEMS

Week 4

Action Items

Udemy Path

1. We strongly recommend you to explore below module through Udemy this week and learn about Node.js essentials

Module	Topic	Description	Udemy Link	

Toptal®