AUTH

Code 401 (Class 16)

Authorization

- Basic http auth

- Authentication -- Who You Are (usually username+pw)

- Authorization -- Do you have access

- Known as "auth/auth"

Steps to create a user

1. Create a user [username, ***encrypted*** password]

   a. "hash" the password

   b. hash is a one-way algorithm (md5, bcrypt, etc)

   c. encryption you could break if know the secret

   d. We will use bcrypt. Uses blowfish cypher, which plucks parts of your password out to be used as the "secret"

2. Save hash to DB

3. Send back a JSON token (JWT)

Steps to login a user

1. Provide a username and a password (using basic http)

    a. Header: { 'authorization': 'basic', base64(user:pass) }

2. Parse the header and get the user and pass

3. Find the user in the database

4. Hash the password you were given

5. See if that hash matches what's in the database

6. Pass back a JWT

CODE

Install: express, mongoose, jsonwebtoken, bcrypt

For jsonwebtoken: use latest so that a new version breaks your code. Good idea to do this for encryption stuff so that you stay current

> "We are uncovering better ways of developing software by doing it and helping others do it. Through this work we have come to value:
>
> Individuals and interactions over processes and tools
> Working software over comprehensive documentation
> Customer collaboration over contract negotiation
> Responding to change over following a plan
>
> That is, while there is value in the items on the right, we value the items on the left more.

— *agilemanifesto.org*