Authentication

Questions

- How should I store user passwords?
- What's a hash?
- How do I make sure a database field is never NULL?
- How do I create a password hash?
- How do I compare a plaintext password to a saved hash?

How should I store user passwords?

- Use `bcrypt` to create hashes.
- Store the hashes in the database.

NEVER STORE THEM AS PLAIN TEXT!

What's a hash?

- it's basically a string, fed into a crypto function
- guaranteed to be unique based on the contents of the string
- cannot be reversed

How do I know if they typed their password correctly?

- The `bcrypt` module can `.compare` a plaintext password to a previously hashed password.

How do I make sure a database field is never NULL?

```
create table users (
  id serial primary key,
  name text,
  username varchar(200) not null,
  password varchar(300) not null,
);
```

How do I create a password hash?

```
const bcrypt = require('bcrypt');
const saltRounds = 10;
const salt = bcrypt.genSaltSync(saltRounds);
const hash = bcrypt.hashSync(password, salt);
```

How do I compare a plaintext password to a saved hash?

```
const didMatch = bcrypt.compareSync(aPassword, theUser.pwhash);
if (didMatch) {
    res.redirect('/welcome');
} else {
    res.redirect('/login');
}
```

This example is an excerpt from an express.js app