Currently on: Module 3

You can limit what pieces of information a token can access (ex/ only have access to a user’s twitter profile, or only the user’s tweets)

Can also revoke access to tokens

---

**Passport setup basics**

npm install –save express-session

\*\*\*\*\*

app.js

\*\*\*\*\*

var session = require(‘express-session’);

app.use(session({secret: ‘anything’}));

app.use(passport.initialize());

app.use(passport.session());

passport.serializeUser(function(user,done){

done(null, user.id);

});

passport.deserializeUser(function(userID, done){

user.findbyid(userID);

done(null, user);

}));

---

On npmjs.com, search for the passport package you want to use

Have to go on console.developers.google.com to create a project

Then go to APIs & auth -> Credentials -> Create new Client ID

Select Web application as the Application type

Take great care in setting up your “Authorized redirect URIs”

Ex/ <http://localhost:3000/auth/google>

At this point you should have your Client ID, Client secret and Redirect URIs

Go back to APIs and click on the APIs you want to enable (author enables Google+ API and Contacts API)

Contacts API gives you access to the user’s email address