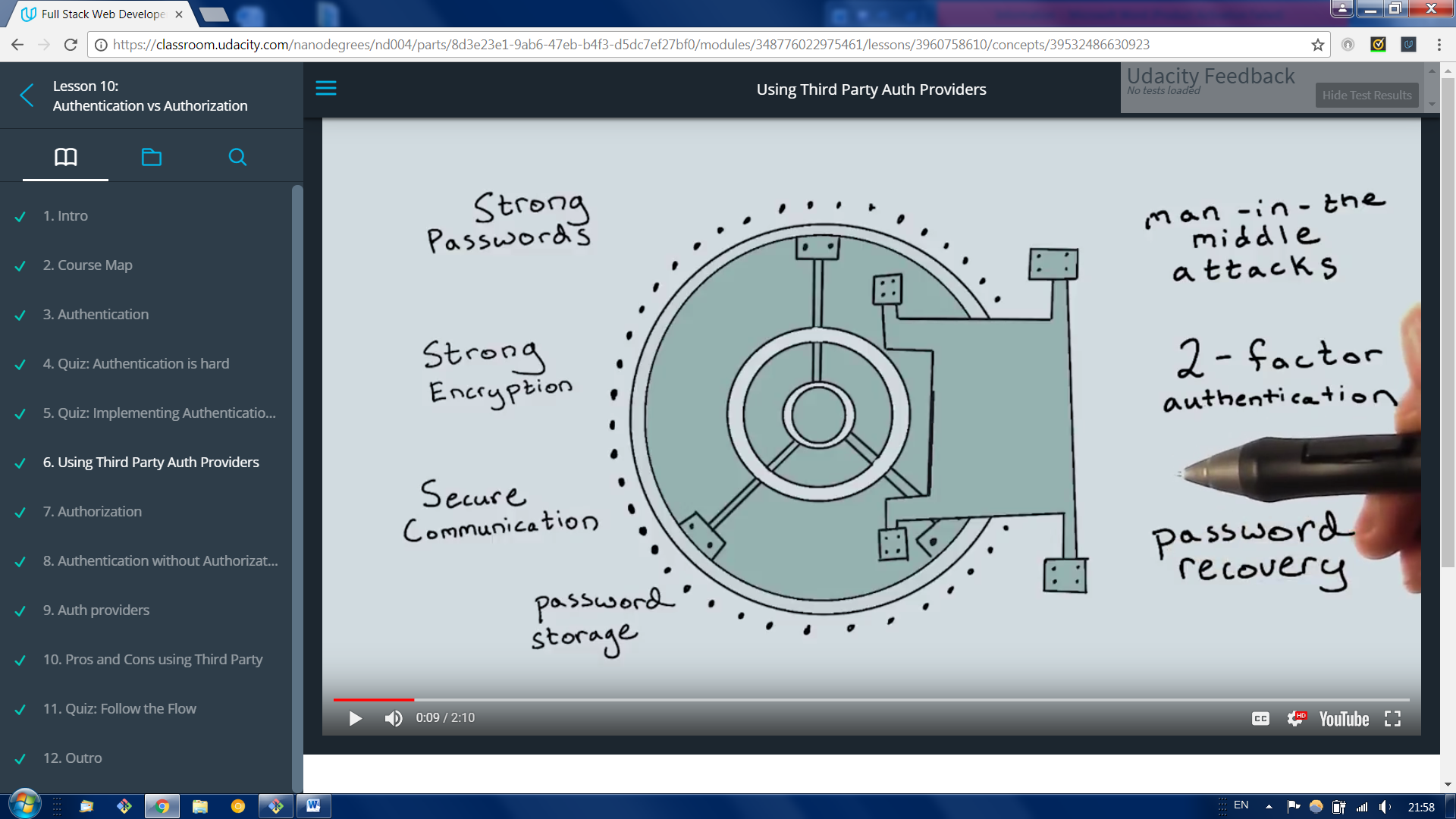
Authentication is the process of finding you are who you say you are (authenticity )



It is a lot of a security concerns , developers created free and open solution to this problems.

When authentication is successful we can move to another topic which is Authorization

Authorization checking if you have the right to access resource you need.

Auth providers

**OAuth** is an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords.[1] This mechanism is used by companies such as **Google, Facebook, Microsoft and Twitter** to permit the users to share information about their accounts with third party applications or websites.

<https://en.wikipedia.org/wiki/OAuth>

**Pros and Cons**

**Pros**

* Outsorce auth handling to Oauth providers
* Easier to register users ( the don’t have to fiil another form and store password to this application)

**Neutral**

* Users need to have a 3rd party account

**Con’s**

* User don’t rus you app/site with the data provided by third part Oauth provider (ex fecebook)
  + = keep aouth scope minimal and use only what is necessary for your app
* Limited/restricted internet access ( local authentication might be better in this case)
* Security provided by auth is good but you might need stronger yet

Creating google Sign in

Flow in web security refers to the way the information flows between client servers and Oauth providers.

Oauth2

1.Client side Auth Flow

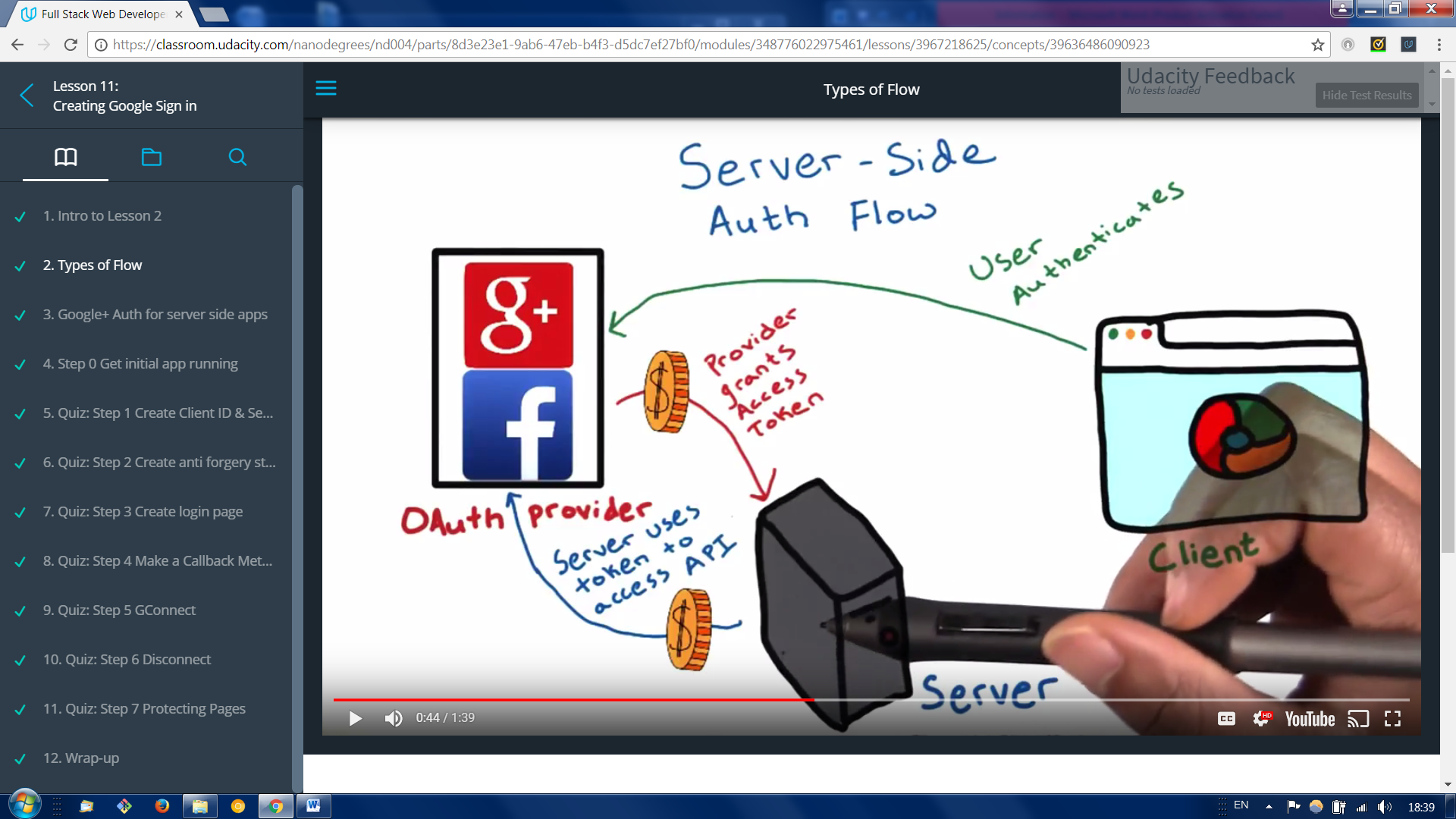
All the code is initiated from user browser side through java script this is useful for single page browser based web applications.

It is quick and easy but lot of trust is on browser or mobile device

2. Mobile authentications

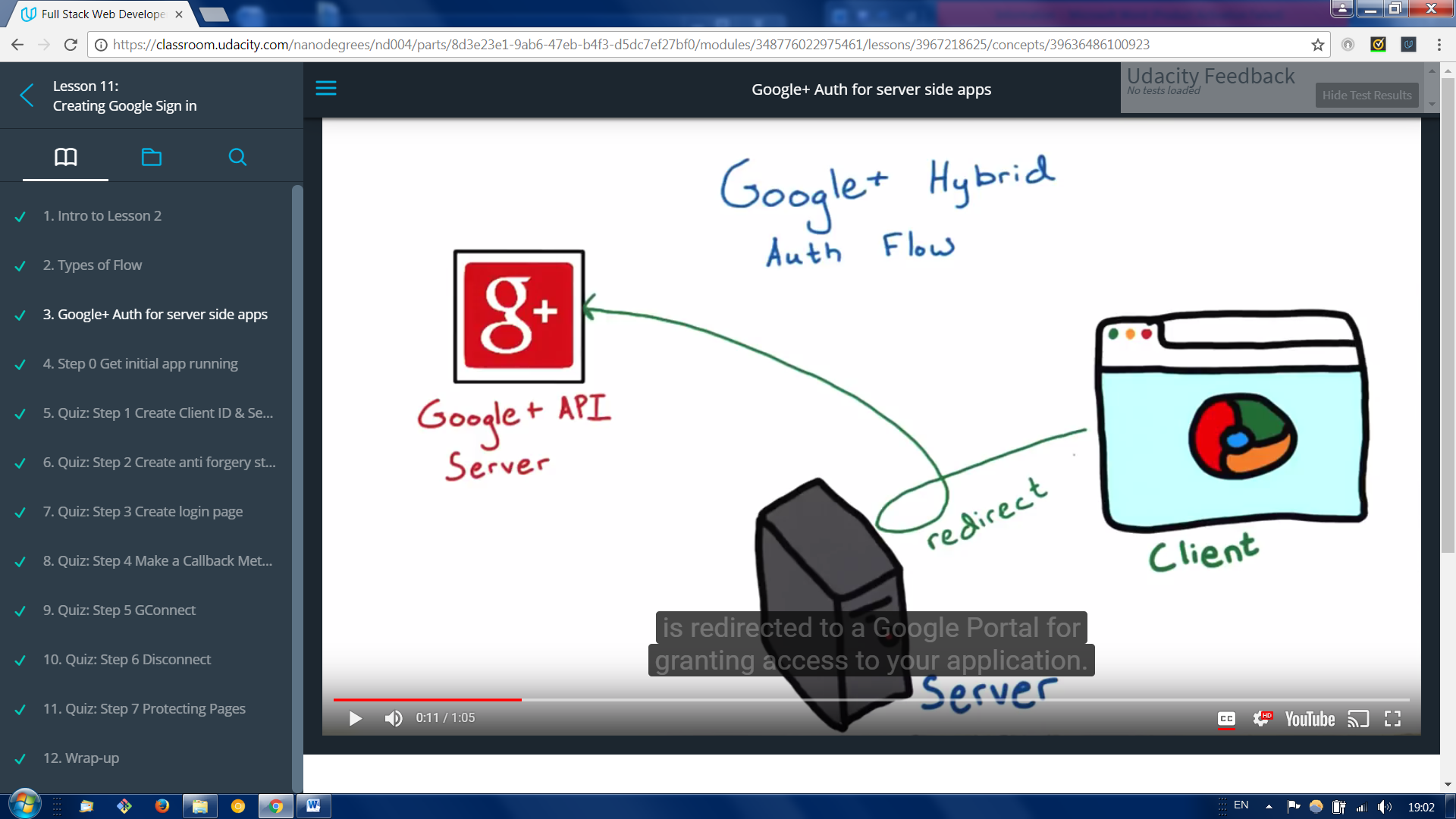
Mobile application can obtain authentication

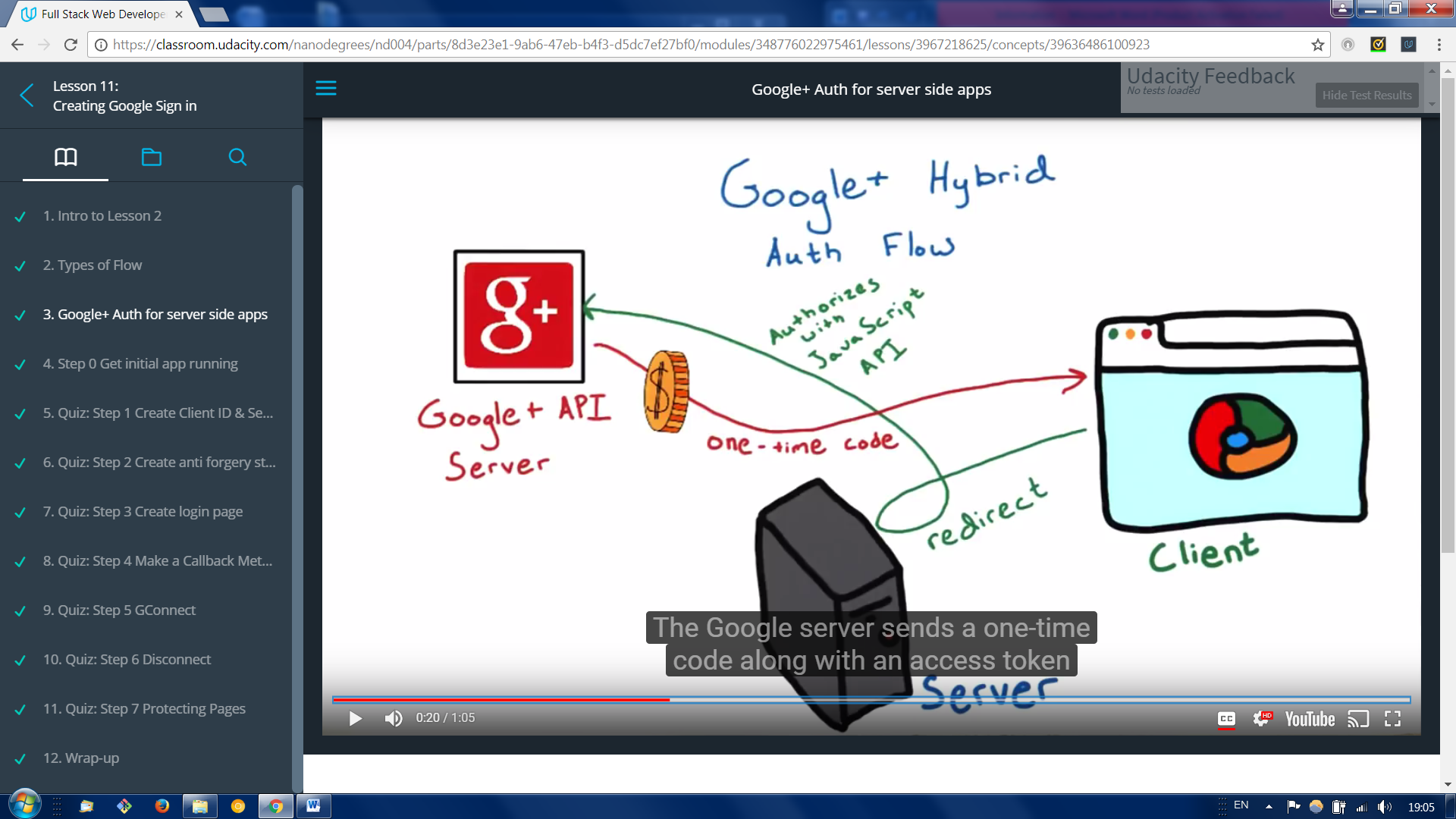
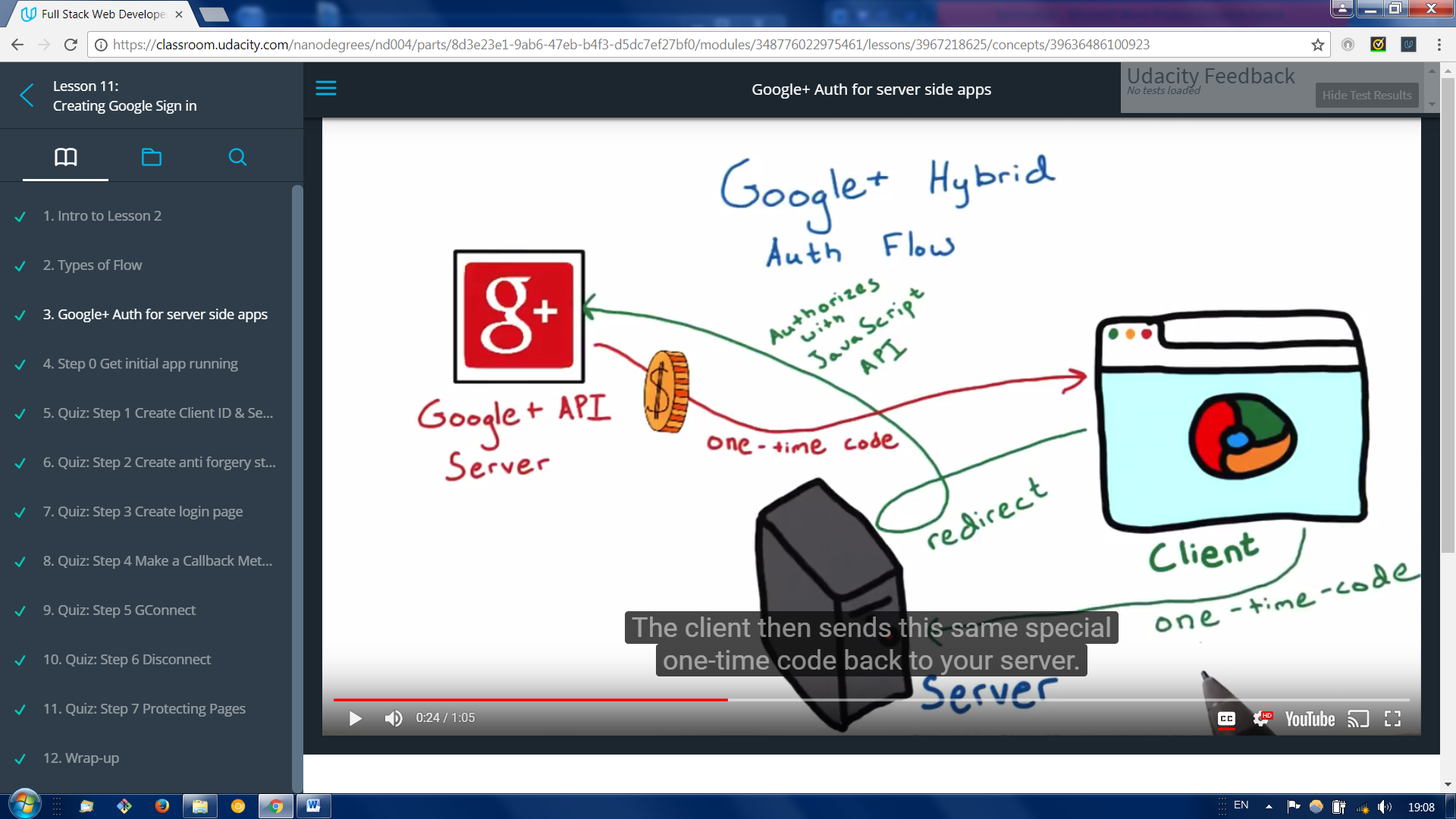
3. Server-side Auth Flow gives more power to the server based application, server now responsible for secure session checking and secure storage of this access tokens



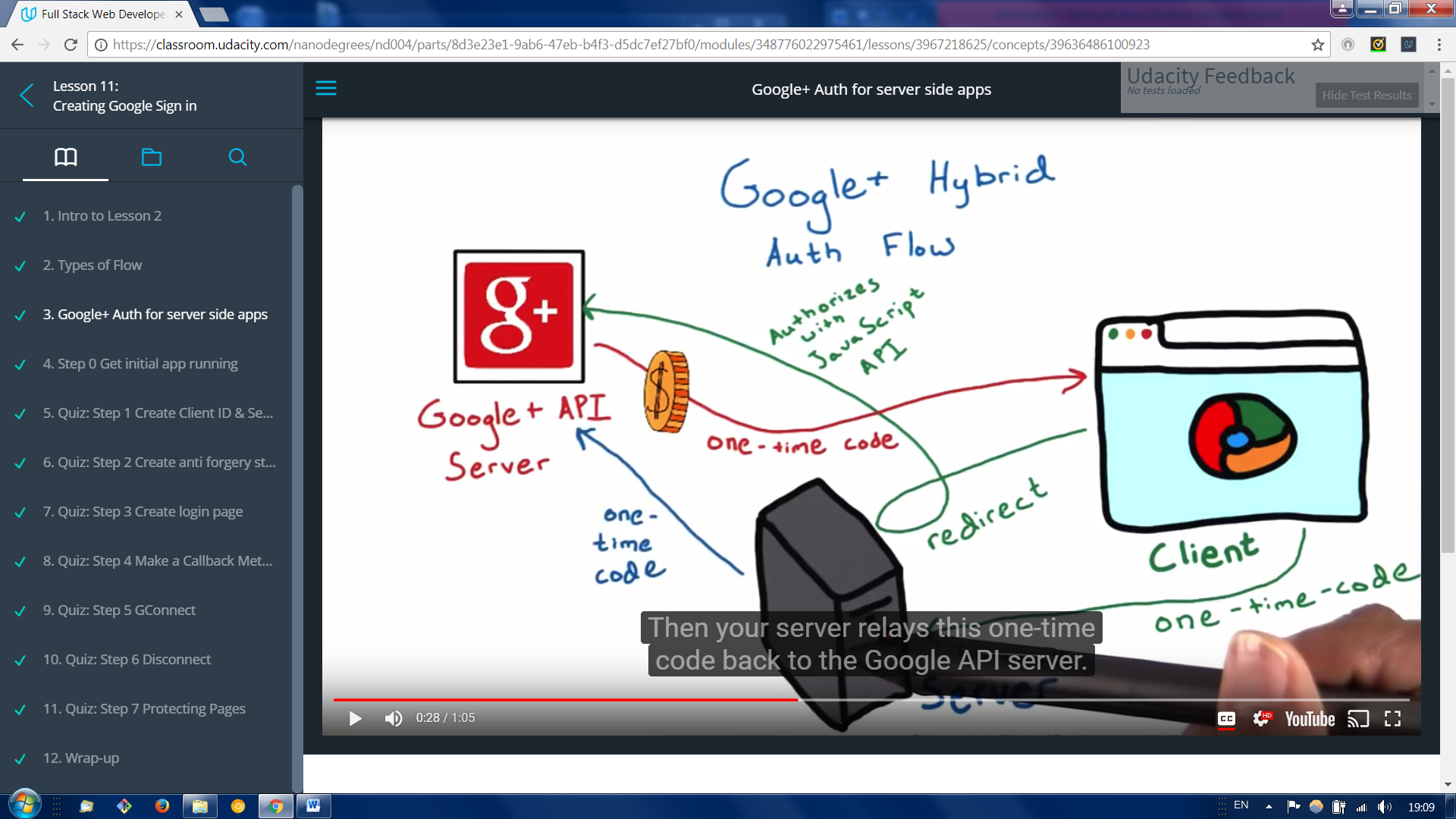
Server flow allows the server to obtain the access token to allow the server to make API requests on behalf of the user. The user has the option to set a time out or revoke access to these tokens at any time.

Google Auth use hybridized flow for loggins that requires authentication to happen on the client , but allows the server to make API calls on behalf of the client.

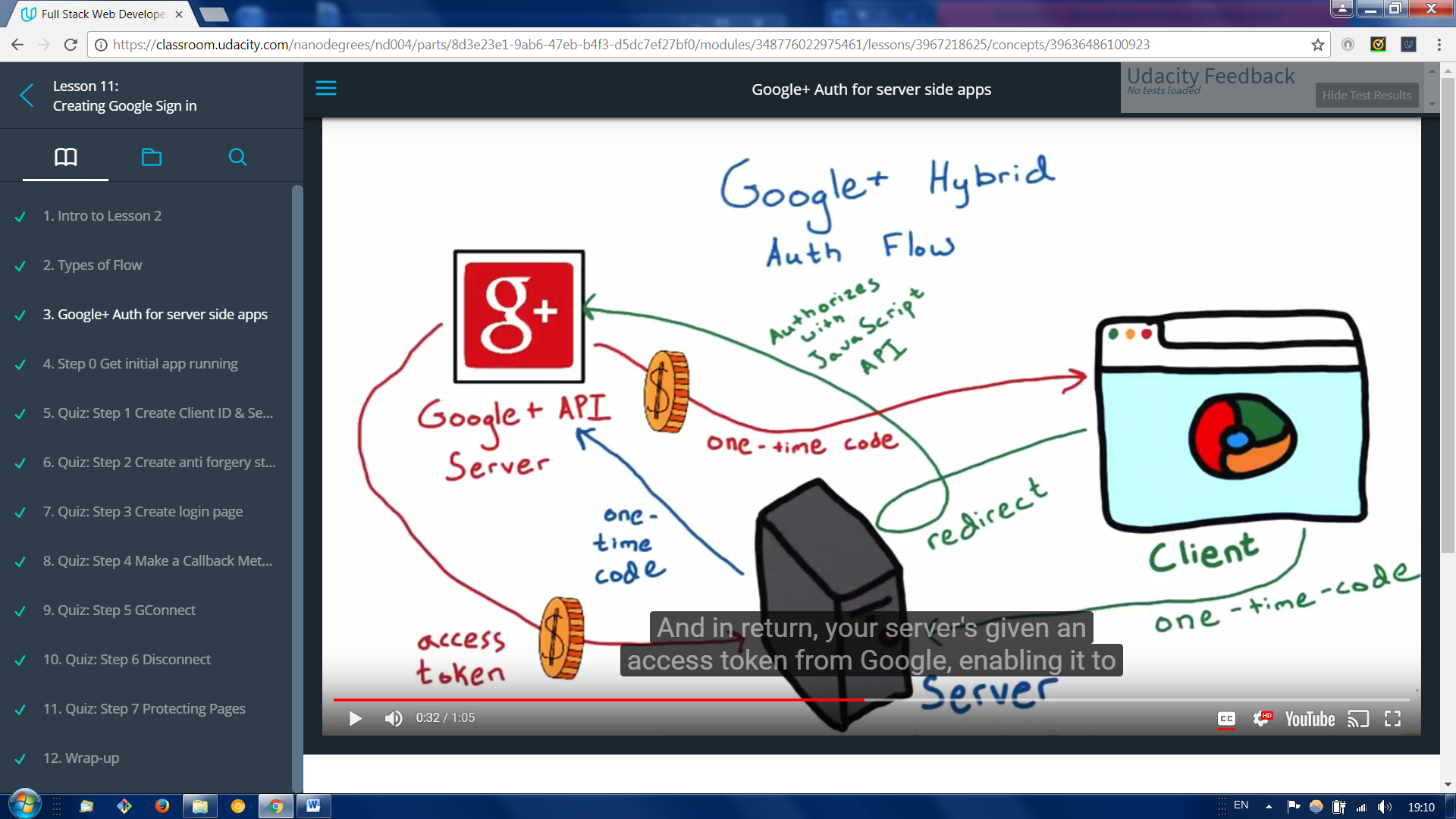


1. A user opts to log in with the Google account . and is redirected to google portal for granting access to your application. The user authorizes your app on the client side using the javaScript API client.
2.  The Google server sends a one- time code along with an access token back to the client.
3. 

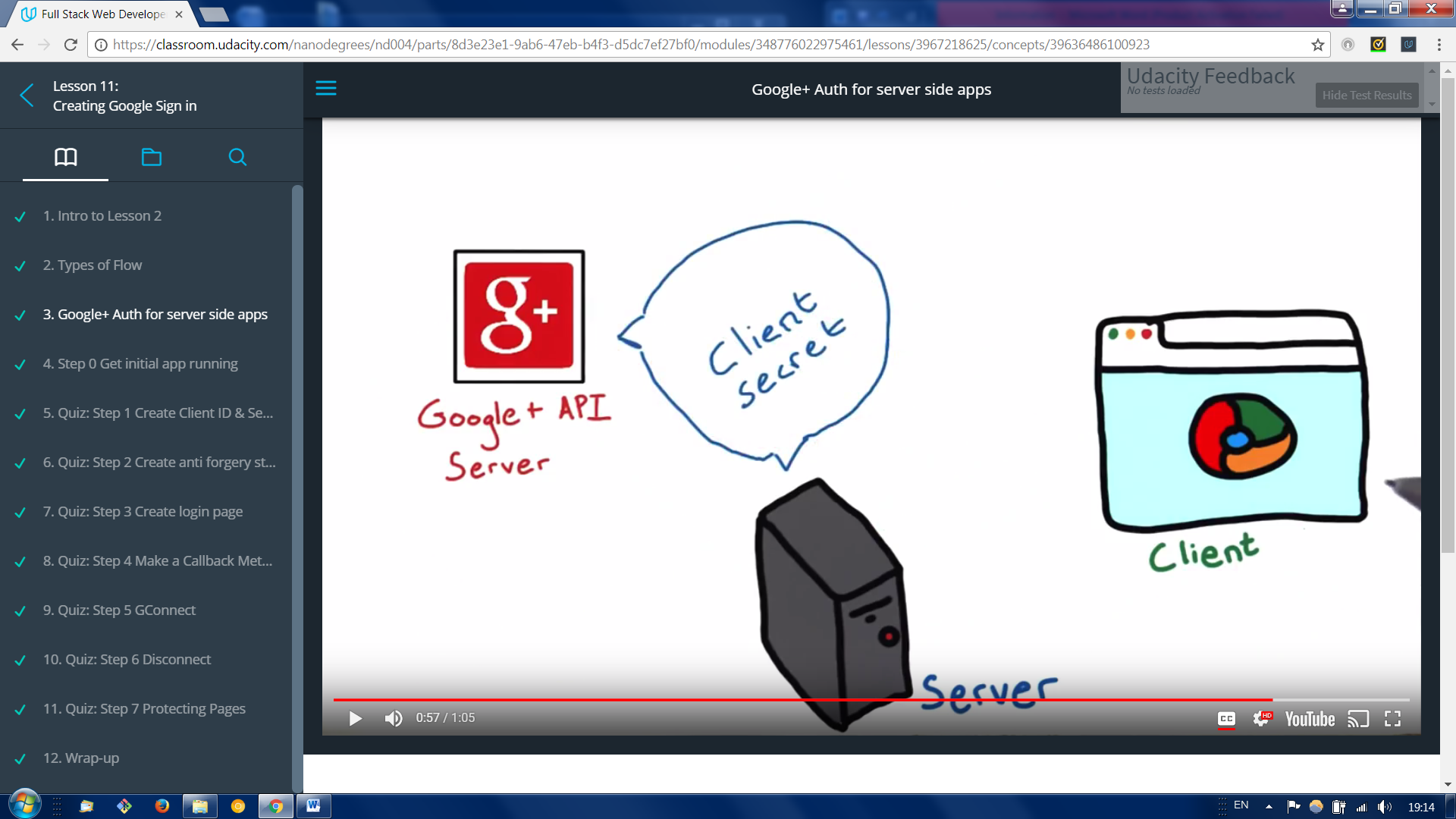
The client then sends this same special one-time code back to your server.

1. 

Then your server relays this one-time code back to Google API server

1. 
2. And in return , your server’s given an access token from Google, enabling it to make its own API calls, which can be done even when the user is offline.

This one-time code flow has a security advantage over a pure server side flow This is because, with one-time codes, Google provides tokens directly to your server, without any intermediaries. Even if one time code is discovered, it is extremely hard to use without your application’s client secret.



A client secret is a special code Google issues to verify your application.

2 Creating Login through Google API

Step 1

Create Client ID & Secret

<https://console.developers.google.com>

create new project , and select credential where you need to create new client ID , web application should be selected or specified as interface changed through this course.

We have to go through consent screen where we specify our email and product name .

Now in authorized javascript origins we have to specify our url address ( <http://localhost:5000> this is needed for our local version to work)

Now we have project called RestaurantMenu App with

client id: **652245020503-o4lvag05eho5uunqjocf7htpqbo3qahp.apps.googleusercontent.com**

Client secret : **N27nsg\_5btm4serq84TIlS49**

Step 2

Create anti forgery state token. We nee to be sure that it’s actually the user who came up with that request and it isn’t someone tricking them into sending it.

Anti forgery tokens protect the security of your users by preventing anti-forgery request attacks.

First step is to create a unique session token that your client side code returns alongside the Google generated authorization code. You will verify this unique session token with your server when a request is made to verify that the user is making the request and not a malicious script.