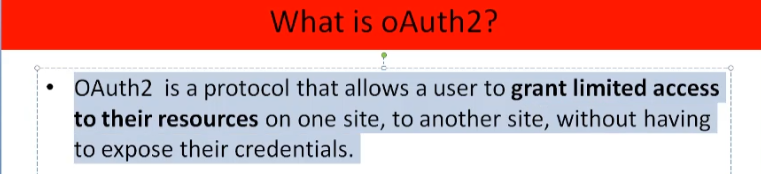
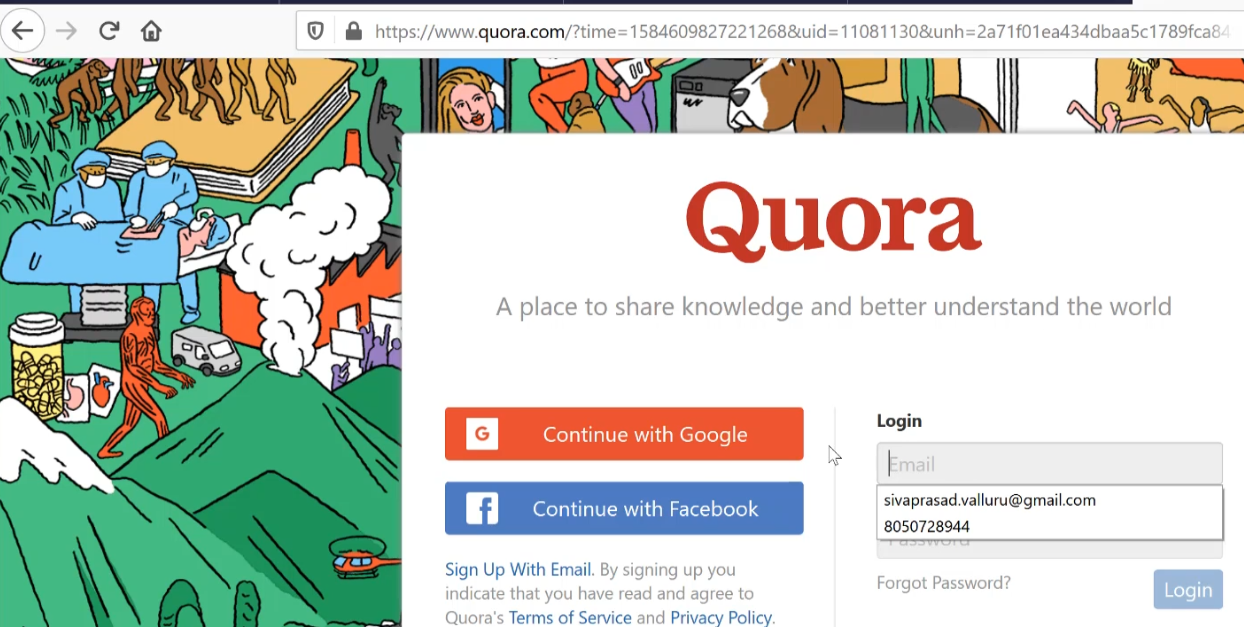
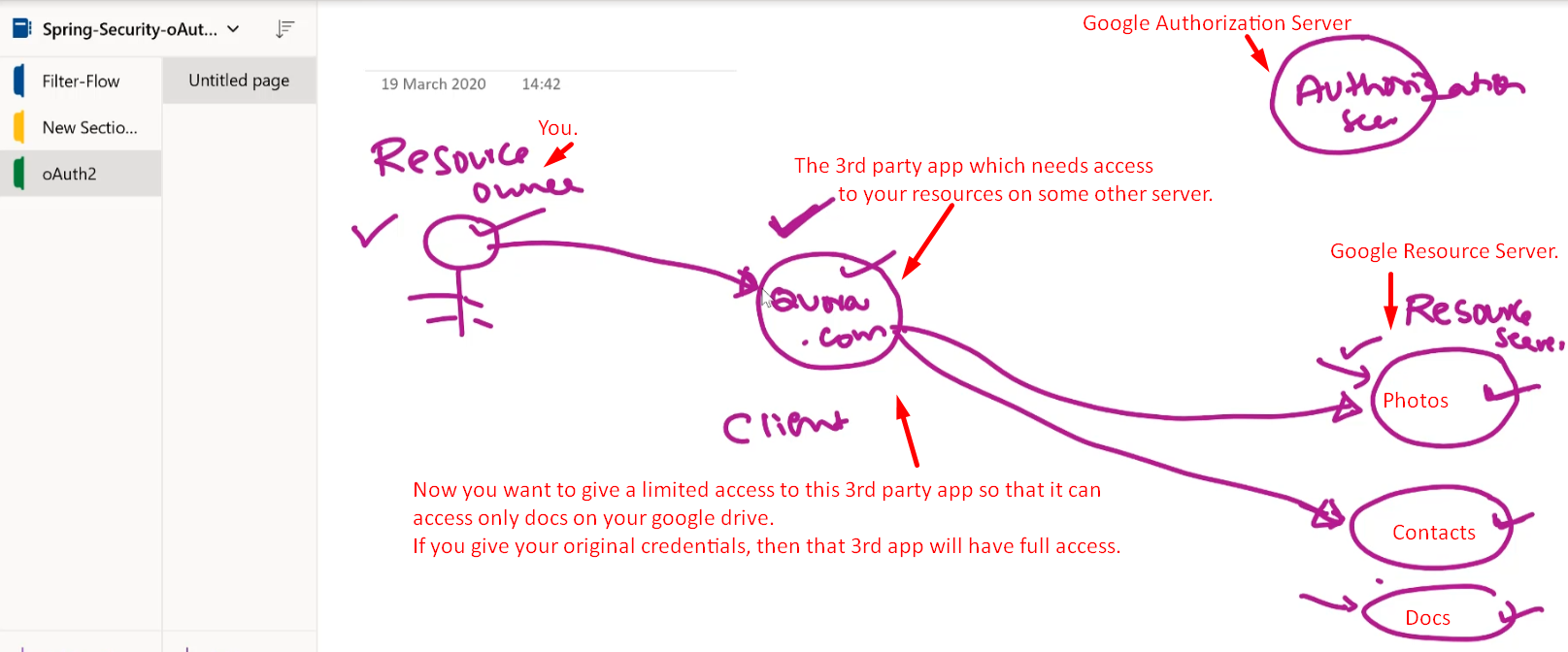
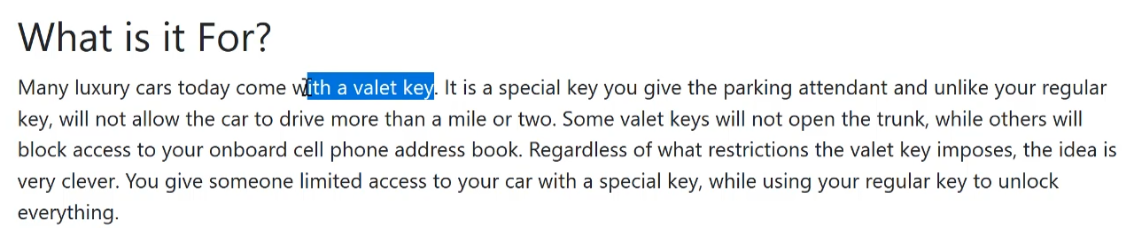
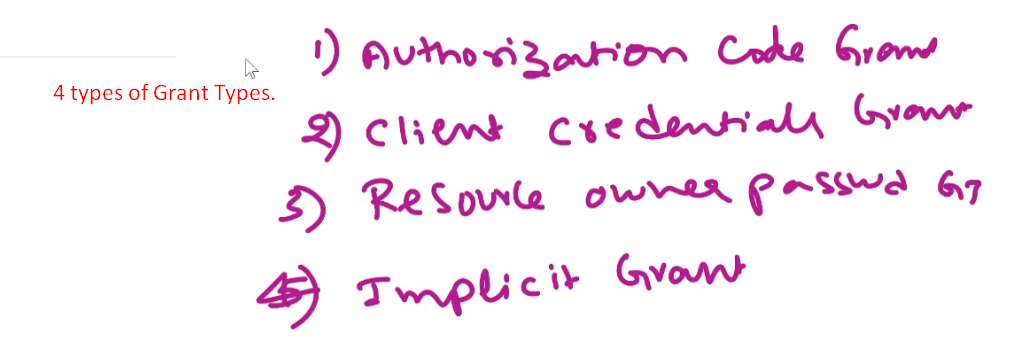
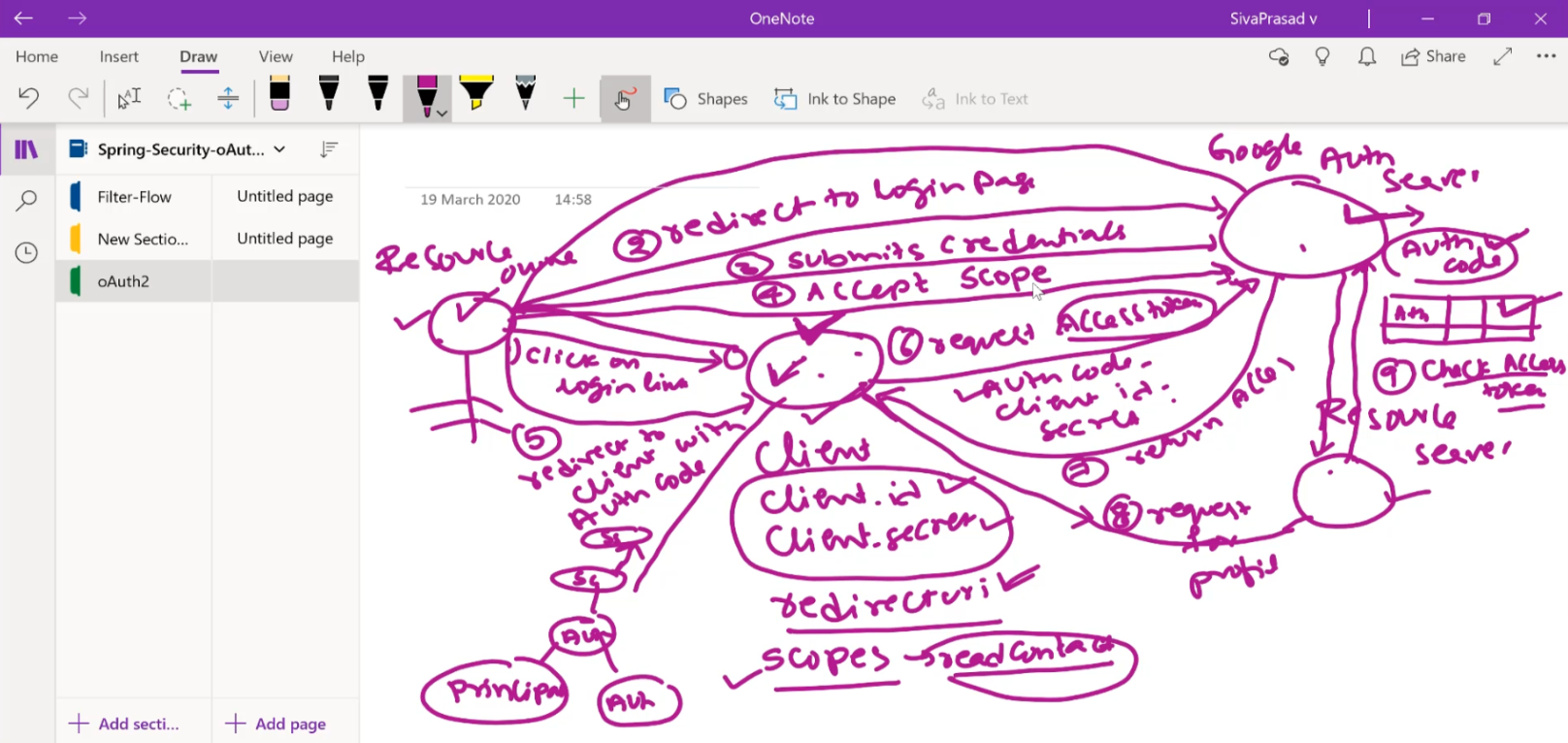
1. 
2. **For Example**:
   1. There are many resource servers such as one to expose Photos, another to expose Docs, still another to expose emails etc.
   2. Our resources are exposed by API.
   3. We’re the resource owner.
3.  
4. Let’s see the various ways a resource owner (user) can grant access to his resource to a client.
5. **Grant Types**:  
   
   1. Authorization Code Grant.
   2. Client Credential Grant Type
   3. Resource Owner password Grant Type.
   4. Implicit Grant.
6. **Authorization Code Grant**:
   1. Actually, in Oauth, there are 4 actors.
      1. Resource Owner (User).
      2. Client (App) wanting to access user’s resource.
      3. Resource Server.
      4. Authorization Server.
   2. 
   3. **Steps**:
      1. User tries to access client app (My App).
      2. Client App redirects the user to Authorization Server (Google).
      3. User submits the credentials.
      4. User then accepts the scopes.
      5. Google Authorization server generates Auth code; redirects the user to the client app with Auth Code.
      6. Client app then sends Client Id, Secrete and Auth Code to Google auth server to get an access token.
      7. Auth Server sends back access token.
      8. Using the access token, Client app requests for user’s profile from Google resource server.
      9. Resource server has to validate the access token by passing the token to Google Authorization Server.  
         NOTE: There are other ways. Such as There is a common DB to Auth Server and Resource Server
      10. Auth Server validates it and informs the Resource Server.
      11. Resource Server returns back the user’s profile to Client App.
      12. Then Client App stores the log in info inside the Http Session of the user.  
          Creates Principal, Authorization and stores inside authentication and that inside Security Context and that inside Http Session.