• Answer the following question:

– Give one reason (there are many) OAuth tokens should not be granted in the main flow, assuming the user has sent in the correct credentials.

**Answer:**

* OAuth 2 is an authorization framework that enables applications to obtain limited access to user accounts on an HTTP service, such as Facebook, GitHub, and DigitalOcean. It works by delegating user authentication to the service that hosts the user account, and authorizing third-party applications to access the user account. OAuth 2 provides authorization flows for web and desktop applications, and mobile devices.
* The implicit grant type is used for mobile apps and web applications (i.e. applications that run in a web browser), where the *client secret* confidentiality is not guaranteed. The implicit grant type is also a redirection-based flow but the access token is given to the user-agent to forward to the application, so it may be exposed to the user and other applications on the user's device. Also, this flow does not authenticate the identity of the application, and relies on the redirect URI (that was registered with the service) to serve this purpose.
* The implicit grant type does not support refresh tokens.
* With the resource owner password credentials grant type, the user provides their service credentials (username and password) directly to the application, which uses the credentials to obtain an access token from the service. This grant type should only be enabled on the authorization server if other flows are not viable. Also, it should only be used if the application is trusted by the user (e.g. it is owned by the service, or the user's desktop OS).
* After the user gives their credentials to the application, the application will then request an access token from the authorization server. If the user credentials check out, the authorization server returns an access token to the application. Now the application is authorized