More about OAuth2.0 grant

What is a grant?

When you sent a request to the authorization server you will sent a field that specify the type of grant that you would want:

1. implicit
2. authorization code
3. client credentials
4. password
5. refresh token

Think of the grant as the "method" that you would like to interact with the server to get the access token (after all the end goal is to get an access token to interact with the API server no?), you would usually use the authorization code grant to get the access token on the behalf of the user.

You would use client credentials to get access token on behalf of the application itself, not the user.

Authorization code

This grant type is the one that you typically see when you interact with an application on the web. Say an application online twitter-tweet-auto.com that advertise itself as a free tweeting tool that help you sent out scheduled tweets, you would then use the website will redirect you to a twitter page which asks for your permission for this application (twitter-tweet-auto.com) to access your account.

You would either approve or deny the request and you would be redirected back to the site. Then the site might "log you in" in the sense that they have your access token and can provide the "service" to you on your behalf. You achieved this without giving your password and username to the website.

Client credentials

Let's say an application itself is using the service then the grant type it will need to choose is client credentials. Through this grant type you would be getting back an access token for YOUR APPLICATION not on the behalf of any user.

You would be providing your client id and client secret in the request so that the authorization server / token server and provide the access token for you after authentication yourself.

There will not be any prompt to allow or deny the access because again it is not on behalf of any user anymore.

Implicit

The access token is returned immediately without needing to go through the token server to exchange the authorization code for a valid access token.

However, this is pretty deprecated and is kinda dangerous, use authorization code instead.

Password

First of all. Why?

This is the exact reason why OAuth is created in the first place which is to avoid user provided credentials to gain access to their resources.

Well, in this grant you would provide the user's username and password in the request in order to gain the access token, but why?

Revision #3
Created 29 April 2023 18:10:01 by Tamarine
Updated 29 April 2023 19:05:52 by Tamarine