CSCI 3800 – Spring 2016 **Hani Alghamdi**
Assignment #3 – OAuth

Some reasons why should not pass the access token in the main flow:

- It's a ietf.org specification

```
Don't pass bearer tokens in page URLs:  Bearer tokens SHOULD NOT be
      passed in page URLs (for example as query string parameters).
      Instead, bearer tokens SHOULD be passed in HTTP message headers or
      message bodies for which confidentiality measures are taken.
      Browsers, web servers, and other software may not adequately
      secure URLs in the browser history, web server logs, and other
      data structures.  If bearer tokens are passed in page URLs,
      attackers might be able to steal them from the history data,
      logs, or other unsecured locations.

For example, the client makes the following HTTP request using
   transport-layer security:

   POST /resource HTTP/1.1
   Host: server.example.com
   Content-Type: application/x-www-form-urlencoded

   access_token=vF9dft4qmT

   The "application/x-www-form-urlencoded" method SHOULD NOT be used
   except in application contexts where participating browsers do not
   have access to the "Authorization" request header field.  Resource
   servers MAY support this method.
```

- If bearer tokens are passed in page URLs, attackers might be able to steal them from the history data, logs, or other unsecured locations

Links:
https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2
http://tools.ietf.org/html/draft-ietf-oauth-v2-bearer-1