**Authentication**

Sometimes, a website can have private pages or resources only accessible by certain users. When this happens, the server challenges the request to access, and the user has to provide the appropriate information to prove to the server that they should have access to it. This two-way process is *authentication*.

A framework by HTTP is available to be able to control access and authentication using defined mechanisms, namely:

1. Basic, which has the user give unencrypted information.
   1. Should only be used with HTTPS
2. Digest, which hashes the user’s password.
3. NTLM, which prevents capturing passwords.
   1. Through persistent connection

A common response status is the 401 Unauthorized status. It is sent when the user first tries to access the page, and the server sends a 401 status with **WWW-Authenticate**. This header field states which method to use for accessing.

The user then responds with information, typically a username/email and password, in the form of an **Authorization** request. It will either return a 200 OK status (the correct authorization was given, and access has been given), a 401 Unauthorized (the authorization was refused, and the Authorization request should be sent again), or a 403 Forbidden (the user has not been given proper access for the page or resource).

**References**

https://tools.ietf.org/html/rfc2616#section-11

https://www.httpwatch.com/httpgallery/authentication/

https://developer.mozilla.org/en-US/docs/Web/HTTP/Authentication