Session Authentication (stateful)

(Standard) RFC 6265

1. The user **enters a login and password** and the frontend send them to the backend (POST request)
2. The backend **verifies the login/password** based on information stored on the server (usually in the database)
3. The backend **stores user information in a session**
4. The backend **grants access to resources** based on the information contained in the session

Do/Don't with passwords

- On the client side, do send passwords either:
  - ✓ in the headers (automatic with basic authentication) or
  - ✓ in the body (POST request with session authentication)
  - ◉ never in the URL
- On the server, do store passwords as
  - ✓ salted hash passwords only
  - ◉ never in clear or non-salted hash