Session / Cookie 방식

"서버기반인증시스템" 보통, 서버의 RAM에 저장됨.

Session/Cookie 방식 인증은 기본적으로 세션 저장소를 필요로 합니다. 세션 저장소는 로그인시 사용자 정보를 저장하고, 열쇠로 사용할 수 있는 *세션 ID* 를 만듭니다. 그리고 HTTP 헤더에 실어 클라이언트에게 보냅니다. 브라우저는 세션 ID 를 포함하는 쿠키를 저장하고있습니다. 인증이 필요한 요청에 해당 쿠키를 끼워 서버에 request 를 보냅니다.

인증 절차

1. 사용자가 로그인을 합니다.

2. 서버에서는 계정 정보를 읽어 사용자를 확인 후, 사용자의 고유 ID 값을 부여한 후 세션 저장소에 저장하고, 이와 연결되는 *세션 ID* 를 발행합니다.

3. 클라이언트는 서버에서 해당 "세션 ID 를 받아 쿠키에 저장" 한 후, "인증이 필요한 요청마다 쿠키를 헤더에 끼워" 보냅니다.

4. 서버에서는 쿠키를 받아 세션 저장소에서 확인 한 후, 일치하는 정보를 가져옵니다.

5. 인증이 완료되고 서버는 사용자에 맞는 데이터를 보내줍니다.

Session 과 Cookie 의 차이점

- Session
  - 서버에서 가지고있는 **정보** ← 인증된 사용자 정보
- Cookie
  - 서버에서 발급된 세션을 열기 위한 **키** 값(세션 ID 라고 칭함) ← 브라우저의 쿠키에 저장됨.

즉, 세션을 활용하지 않는 쿠키

쿠키만으로 인증을 한다는 것은서버의 자원은 사용하지 않는다는 것 - 클라이언트가 인증 정보를 책임지는 것을 의미합니다.

쿠키만으로 인증을 할 경우, 해커가 HTTP 요청을 중간에서 뺏어갈 때, **모든 정보가 탈취됩니다**.
또한 쿠키는 조작된 데이터일 수 있으므로 실제 정보가 존재하는 database 를 사용해서 작업합니다.
따라서 보안과는 관련 없는 장바구니, 자동로그인 설정 같은 경우에 유용하게 사용됩니다.