

22.12.1

HTTPS

Http의 보안 취약점을 보완, 암호화 웹 통신 프로토콜

- http : 브라우저와 서버가 정보를 교환하고 송통하기 위한 프로토콜

SSL

- Secure Sockets layer
- 인터넷을 통해 전달되는 정보 보안의 안전한 거래를 허용하기 위해 Netscape사에서 개발한 인터넷 통신 규약
- 90년대 중반 폐기된 프로토콜
- SSL 계층은 응용 프로그램 계층 과 전송 계층 사이에 위치

- 1) 응용 프로그램 계층 데이터가 SSL 계층에 전달
- 2) SSL 계층은 응용 프로그램 계층에서 수신 한 데이터에 대한 암호화를 수행
- 3) 암호화 된 데이터에 SSL 헤더 (SH)라는 자체 암호화 정보 헤더를 추가
- 4) SSL 계층 데이터는 전송 계층(TCP/UDP)에 대한 입력이 된다.

TLS

- Transfer Layer Security
- Transfer Layer Security
- SSL 3.0을 기초로 해서 IETF가 만든 프로토콜
- 보안 및 개인 정보 보호 기능이 강화 된 후속 인터넷 표준
- TLS는 단일 프로토콜이 아니고 2계층에 걸친 프로토콜

RequestBody vs ResponseBody

RequestBody

- Http요청의 본문 그대로 전달
- 일반적인 get/post가 아닌 xml이나 json기반의 메시지를 사용하는 요청의 경우 사용
- requestbody가 붙으면 http요청의 미디어타입(인코딩방식 ex. text, pdf,,,)과 파라미터 타입을 먼저 확인

ResponseBody

- xml, json기반
- messageconverter가 httpServletResponse의 출력스트림으로 넣는다.
- xml,json 형태의 데이터를 자바객체로 변환해서 객체에 저장한다.
- responsebody를 사용안하면 뷰이름으로 인식해서 파일을 찾는다(viewResolver)
- responsebody 하용시 응답으로 데이터 형태로 출력된다.