보안 이슈 적용 전 미리 캡쳐 해둠(양갱)

SQL Injection

구현 전



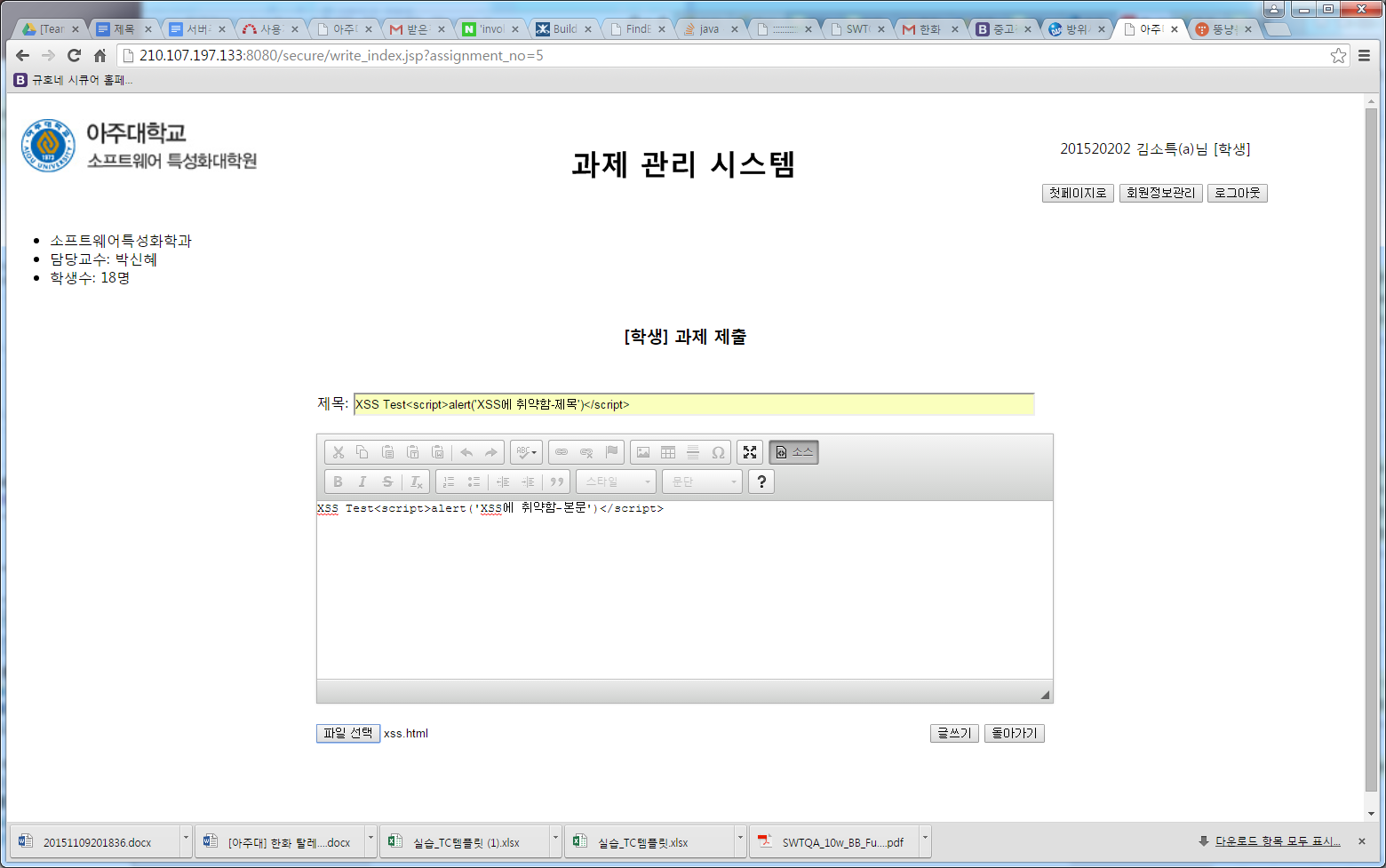
아이디에 ' or 1=1 # 입력



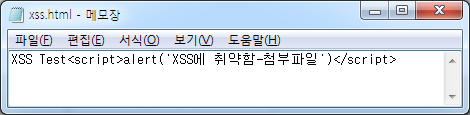
로그인 성공

XSS

-학생 과제제출에서 테스트

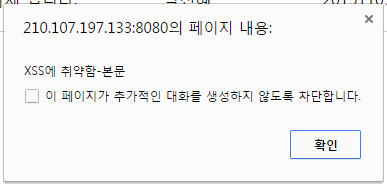
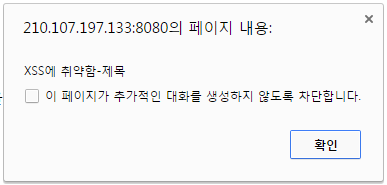


제목, 본문(소스), 첨부파일(xss.html)에 각각 script 삽입

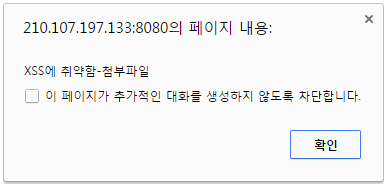


결과

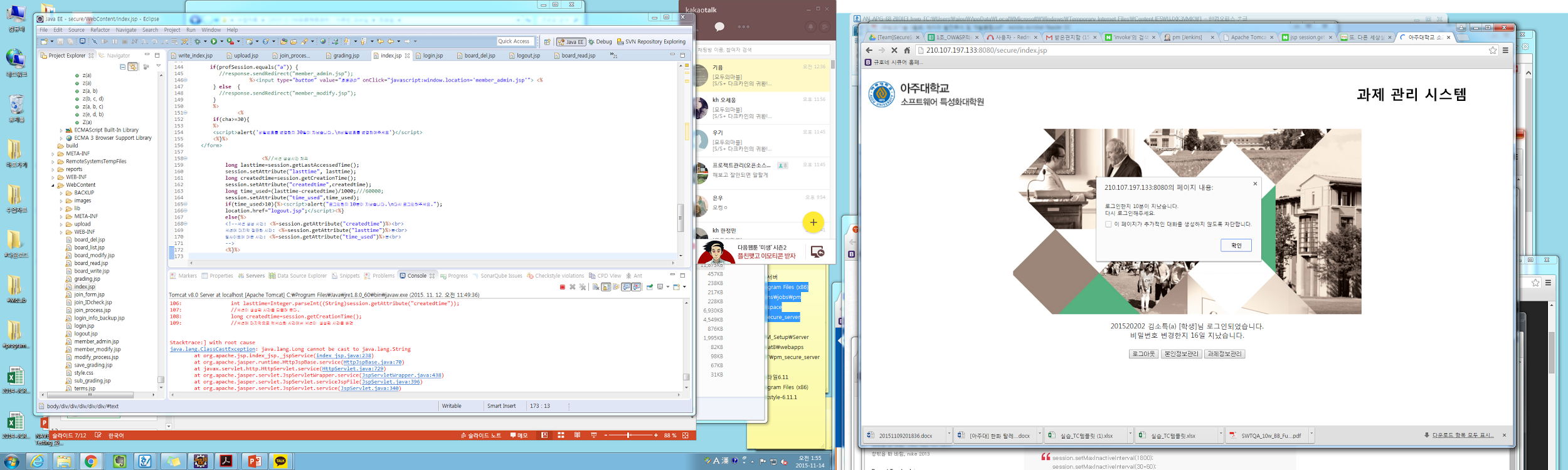
script가 실행되어 XSS에 취약함을 알 수 있음



html파일은 교수 아이디로 html파일을 열어볼 때 실행이 되도록 되어있음



10분 이상 경과시 세션 삭제-로그인한지 10분 지났다는 메시지 창 띄우고 로그아웃



홈페이지 오류메시지 표시되지 않도록 조치

/WEB-INF/web.xml에 아래의 코드를 삽입

모든 에러메시지에 errorpage.html로 이동

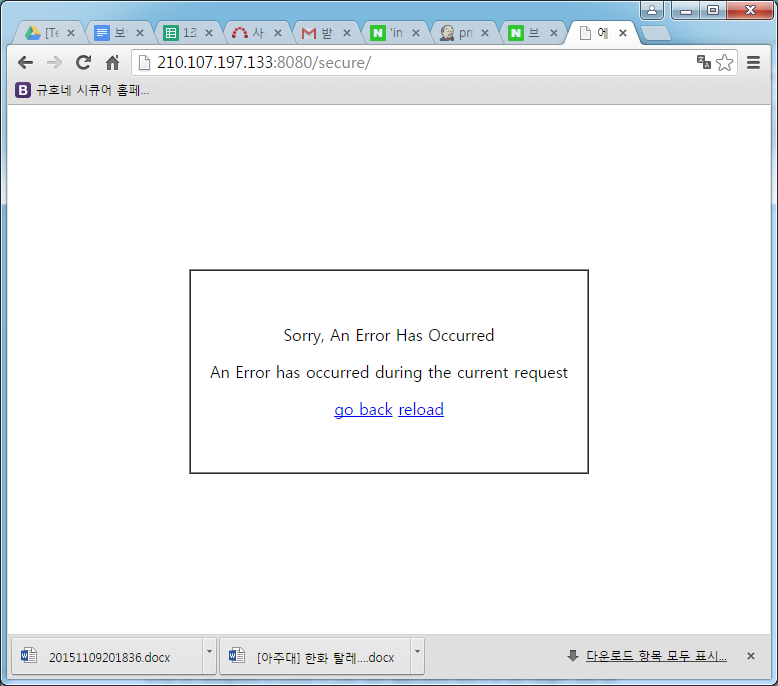
<error-page>

<location>/errorpage.html</location>

</error-page>



<변경 전>



<변경 후>

글쓰기 write\_index.jsp

소스 제거

config.js를 작성

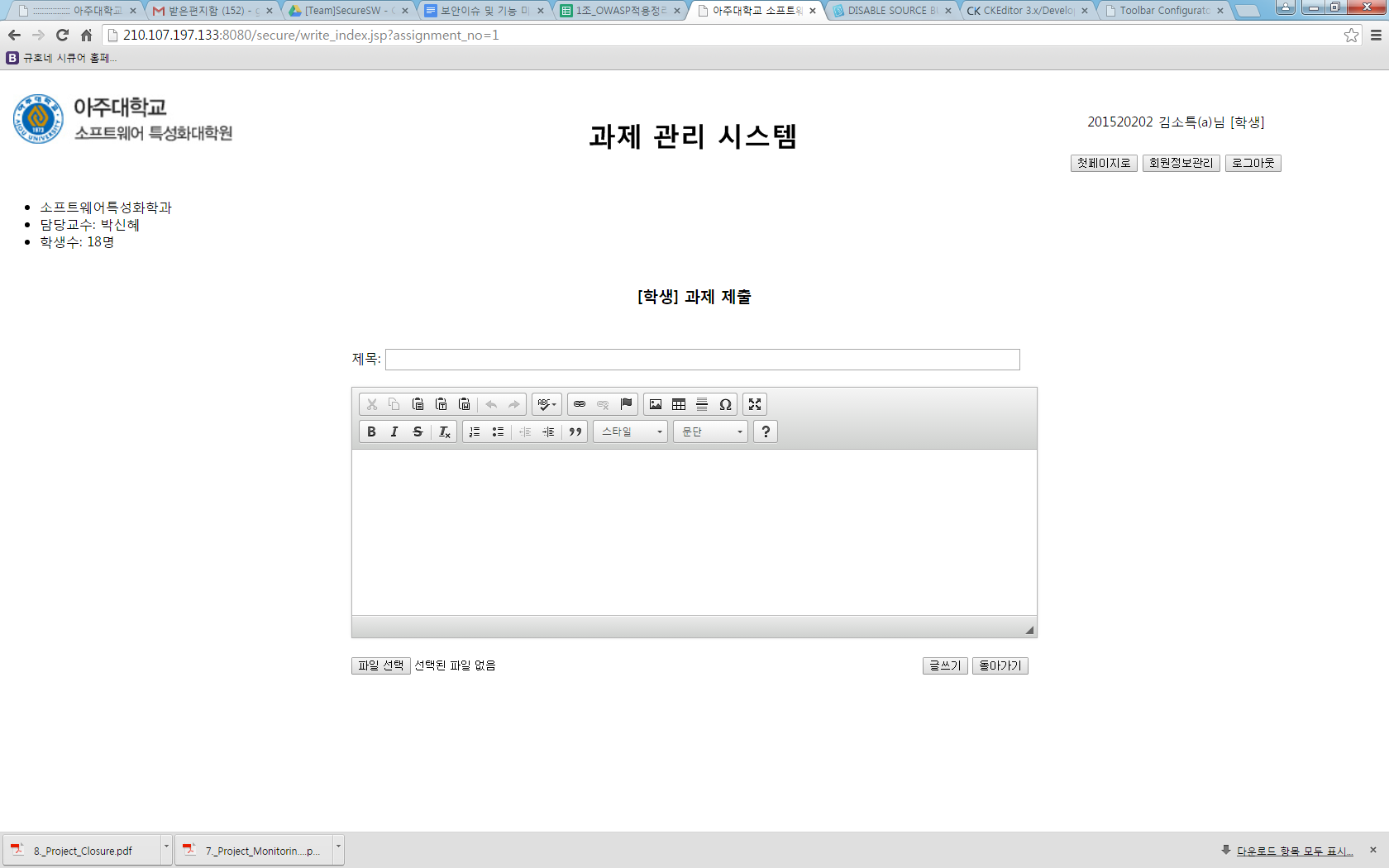
ckeditor의 config.js파일에 아래와 같은 코드를 삽입해줌

config.removeButtons = 'Source';

write\_index.jsp의 코드에 config.js파일이 반영되도록 수정

(반영전)CKEDITOR.replace('text\_content');

(반영후)CKEDITOR.replace(‘text\_content’,{toolbar: ‘’});



[소스]가 사라짐

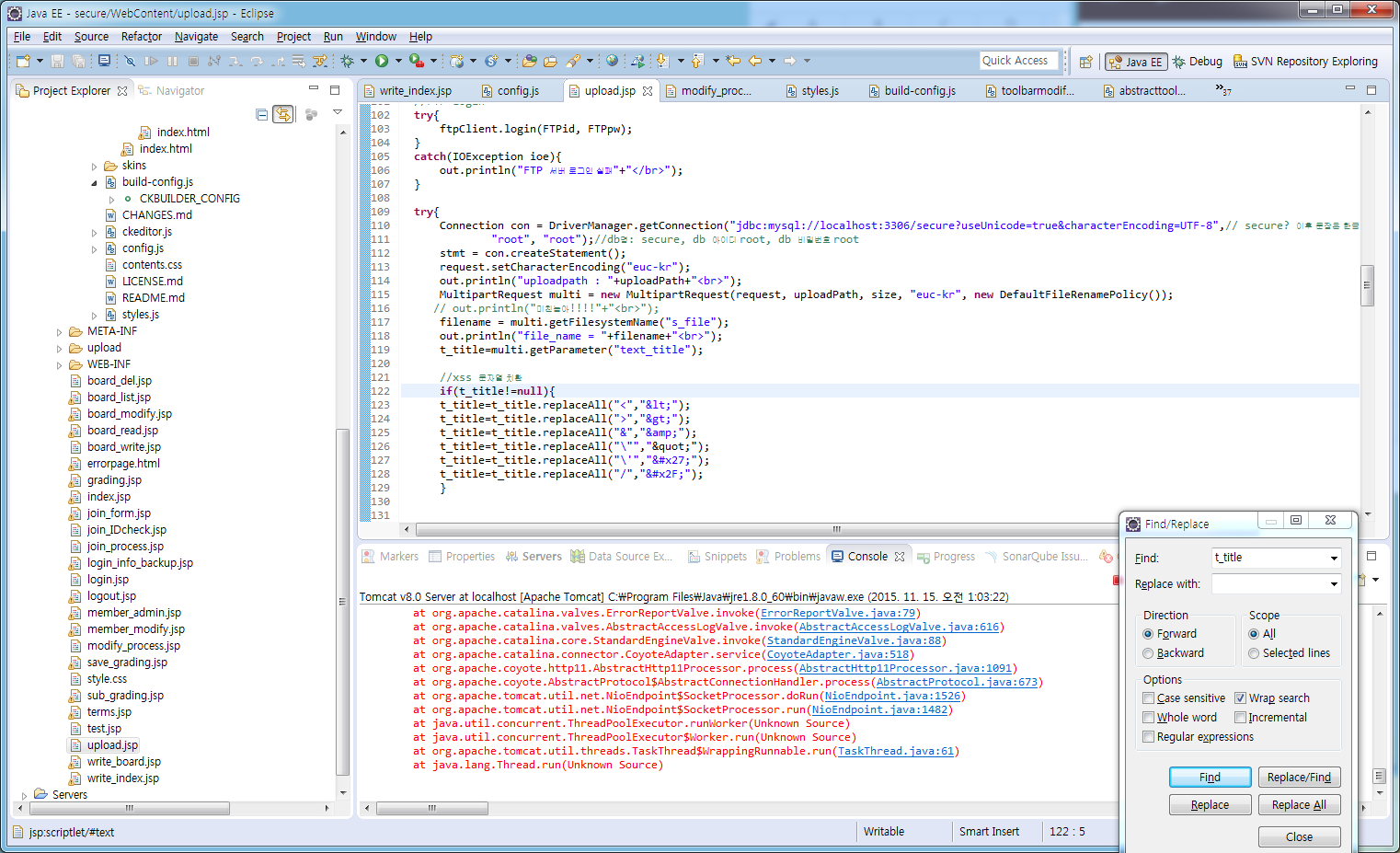


결과: 태그실행이 되지 않고, 스크립트 자체가 텍스트로 출력됨

제목에서 xss 문자열 치환

<, >, &, “,’, / 등을 치환

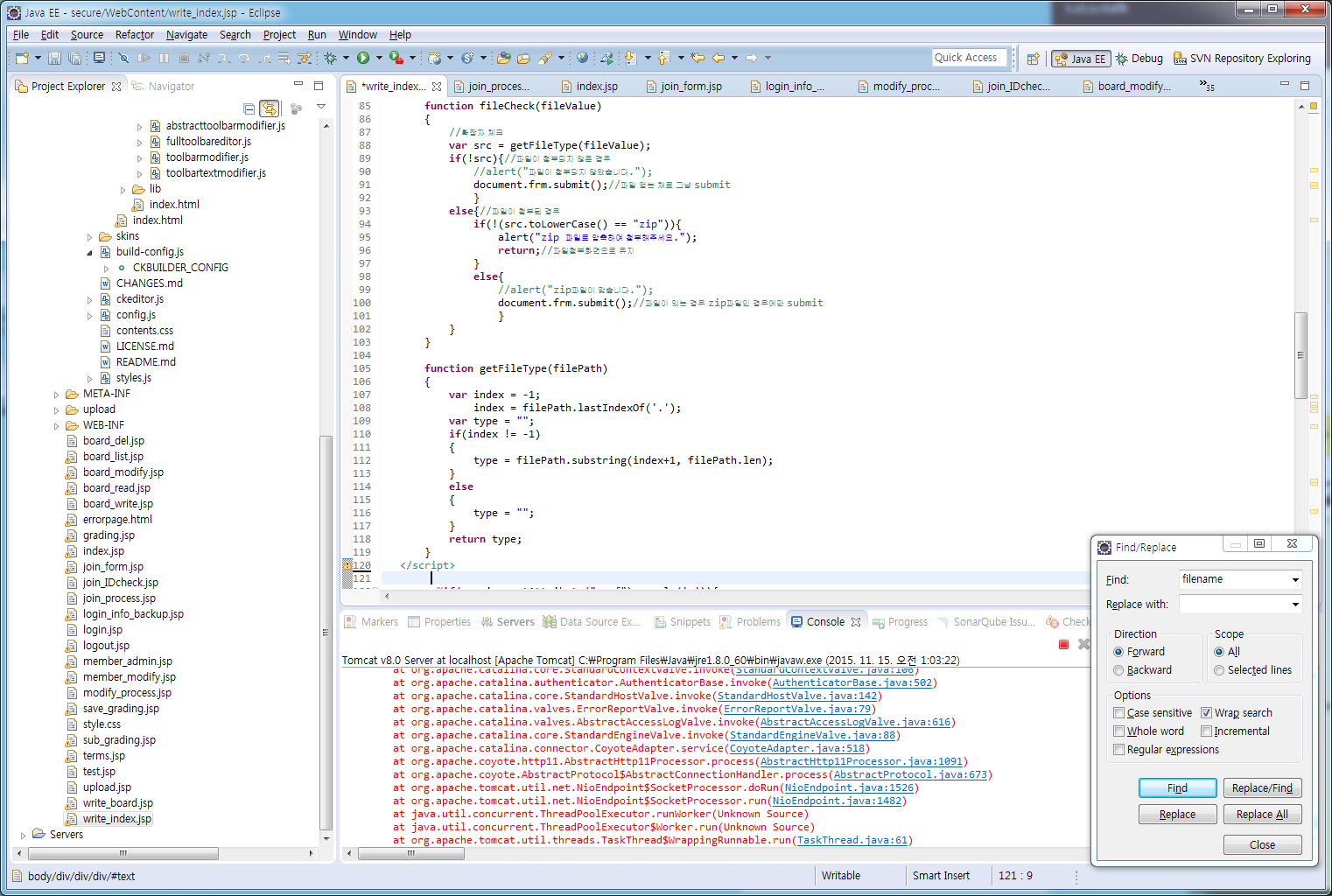
grading.jsp에서 제목문자열 변수인 t\_title에 문자를 치환해줌

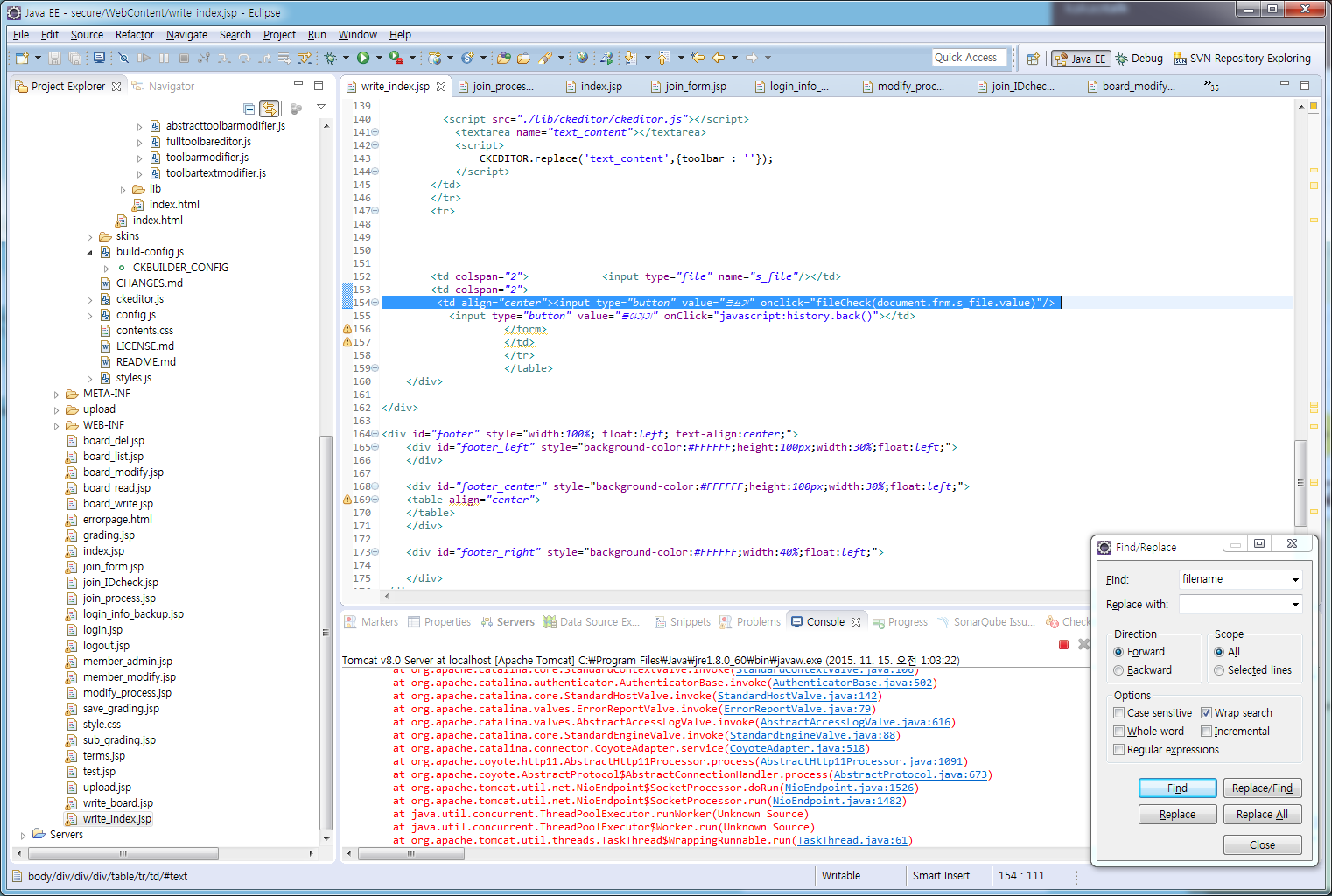


파일명 체크

jsp, html, php 등의 악성 스크립트 삽입이 가능한 파일 및 .exe 등의 실행가능한 프로그램으로 웹 어플리케이션에 악영향을 끼칠 수 있는 파일들의 첨부를 불가능하도록 조치

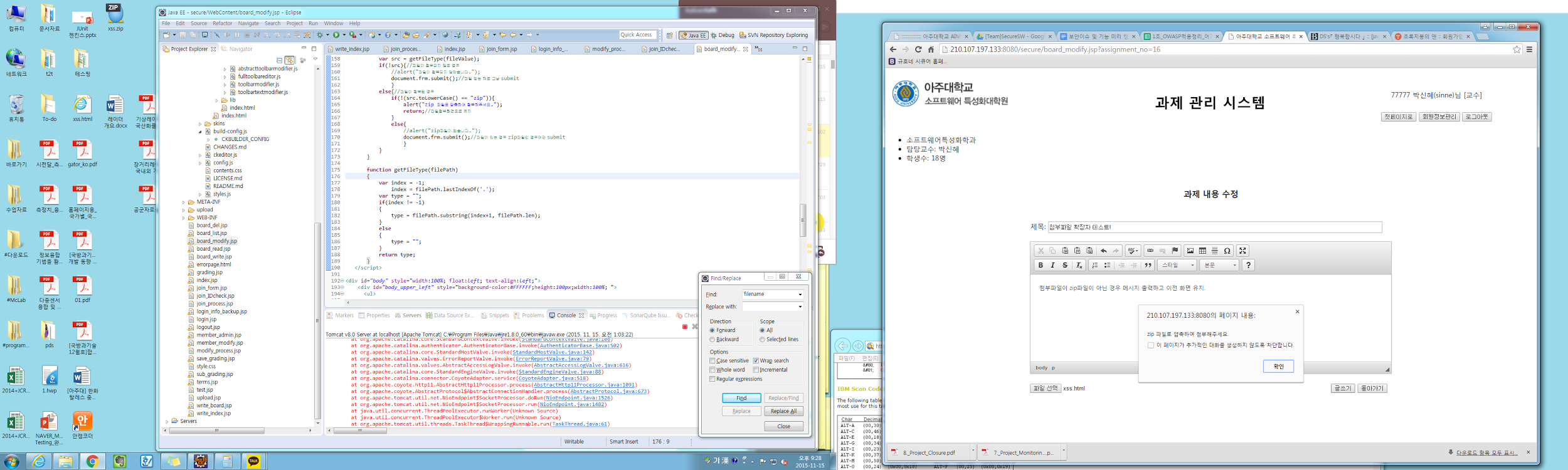
첨부파일을 모두 .zip파일로 압축하여 업로드하게 하여 일차적으로 웹브라우저에서 코드가 실행되는 것을 방지





javascript를 사용하여 파일을 form 전송시 파일이름을 체크하여 zip파일인 경우에만 전송하도록 함

write\_index.jsp(글쓰기), board\_modify.jsp(글수정)에 적용 완료



마지막

//소프트웨어 개발보안 가이드 98페이지 7. 하드코드된 비밀번호

|  |  |
| --- | --- |
| 적용전 | 적용 후 |
| String jdbcDriver = "jdbc:mysql://localhost:3306/secure";  String dbUser = "root";  String dbPass = "1";    String query1 = "select \* from member";  String query2= " where id='" + enId + "'";  String query3= "and pw='" + enPw + "'";    //데이터베이스 커넥션 생성  conn = DriverManager.getConnection(jdbcDriver, dbUser, dbPass); | String jdbcDriver = "jdbc:mysql://localhost:3306/secure";  //AES256 Encoding된 DB아이디, 패스워드  String dbUser = "K2amNtg+kL5xK23g7H3Znw==";  String dbPass = "CPnv7eGM8oJo4GvYbu3ySQ==";    String query1 = "select \* from member";  String query2= " where id='" + enId + "'";  String query3= "and pw='" + enPw + "'";    //데이터베이스 커넥션 생성  conn = DriverManager.getConnection(jdbcDriver, a256.AES\_Decode(dbUser), a256.AES\_Decode(dbPass)); |

