□ 단국대학교 > 사이버보안 학과 > 인터넷 보안 > 보고서 템플릿

25년 1학기 인터넷 보안 수업

# File Download

**2025년 4월 29일**

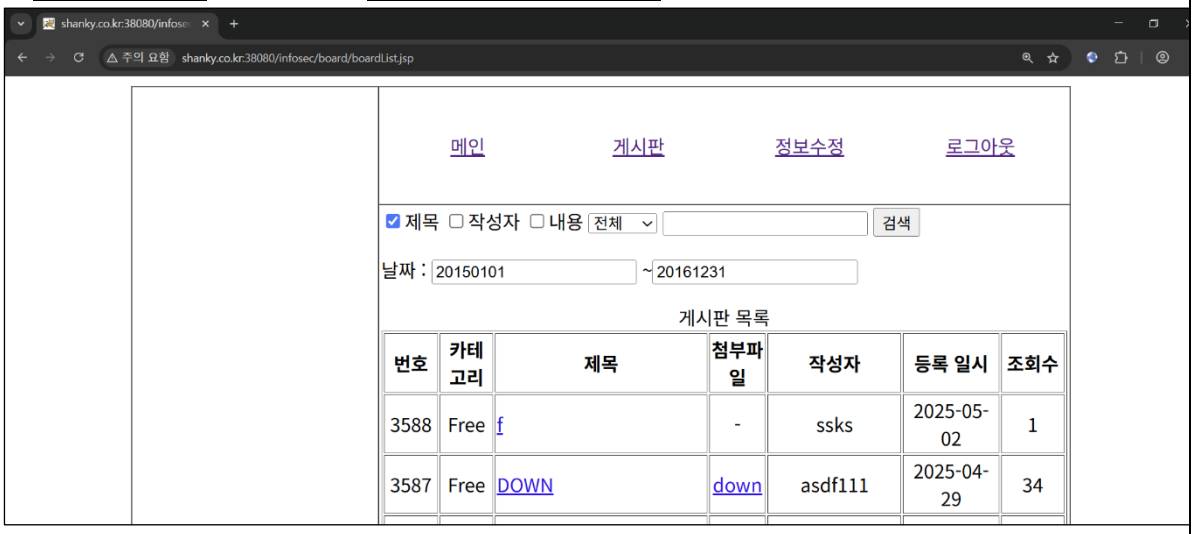
학번 : 32231594
이름 : 박기쁨

**<과정 설명>**

File Download 취약점 공격은 파일을 다운로드하는 과정에서의 취약점을 이용하여 원하는 정보를 탈취하는 행위를 말한다. 본 실습에서는 File Download 취약점을 이용해 DB 접근 관련 파일을 찾고, DB 에 접속해보고자 한다.

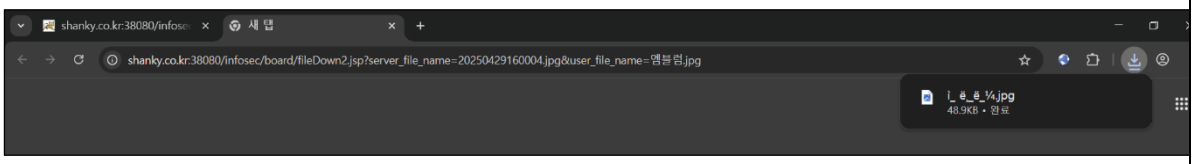
**Step 1. File Download 가 가능한 취약한 페이지 찾기**

Step 1-1. File Download 가 가능한 **취약한 페이지** 찾기
: 파일경로 및 파일명이 노출되는 취약한 페이지를 찾는다.
: 게시판 페이지에 접속하여 첨부파일 다운로드 기능을 확인한다.




: 링크를 URL 창에 복사하여 확인한 후 붙여넣기 해본다.

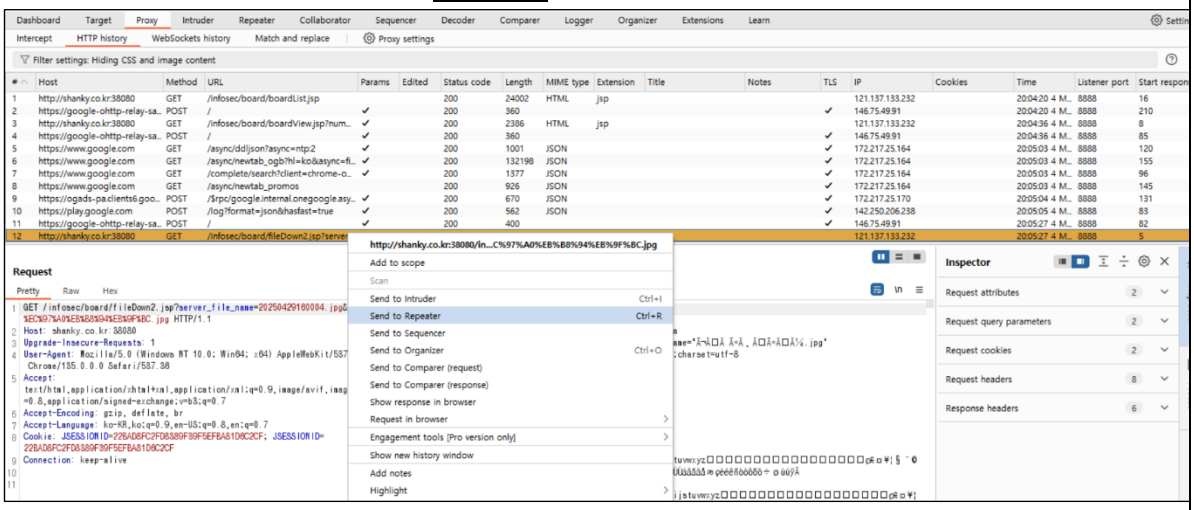
(URL(파라미터) 확인, 파일 다운로드 되는 것 확인)




**Step 2. 취약점을 이용하여 중요 파일 다운로드 하기**

Step 2-1. File Download 관련 패킷 **Repeater** 로 보내기

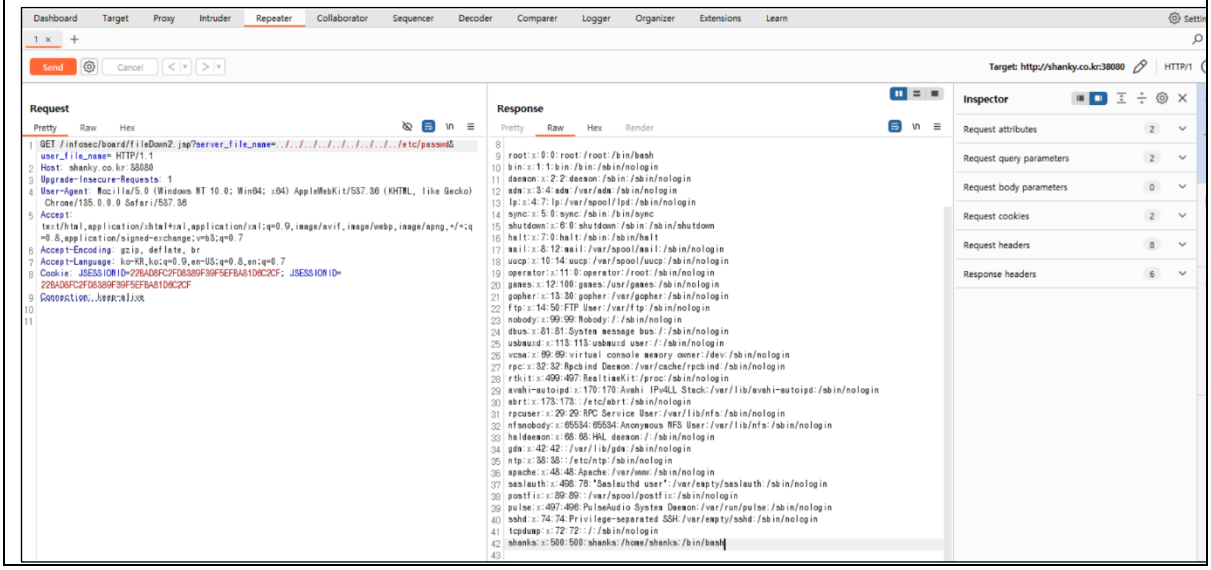
: 패킷을 반복해서 사용하기 위해 Repeater 로 보낸다.




Step 2-2. **/etc/passwd**, **/etc/shadow** 를 이용하여 **사용자** 알아내기

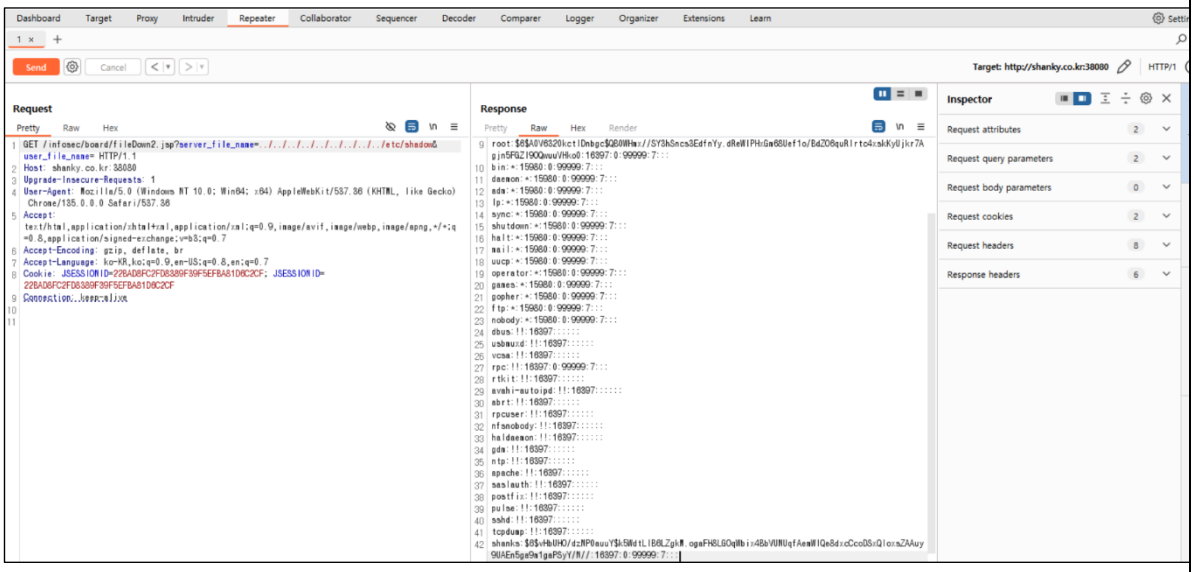
: server_file_name 파라미터에 /etc/passwd 의 경로를 삽입한 후 요청을 전송한다.

: root 계정과 nologin 상태인 계정들, bash 쉘을 이용하는 shanks 계정을 확인할 수 있다.



: server_file_name 파라미터에 /etc/shadow 의 경로를 삽입한 후 요청을 전송한다.

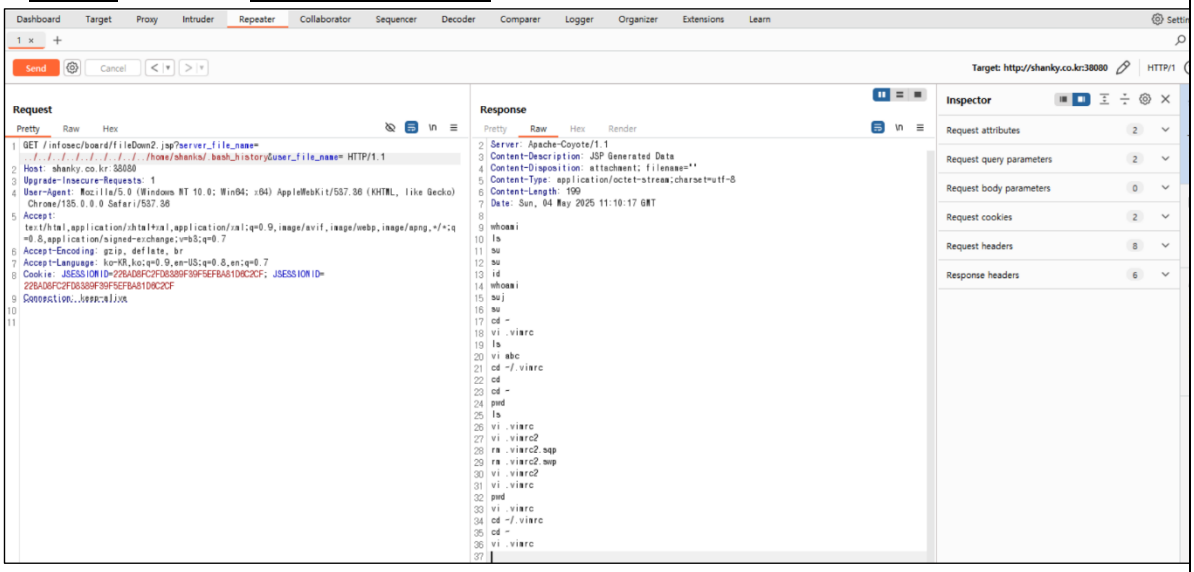
: root 계정과 shanks 계정의 해시 값 등을 확인할 수 있다.



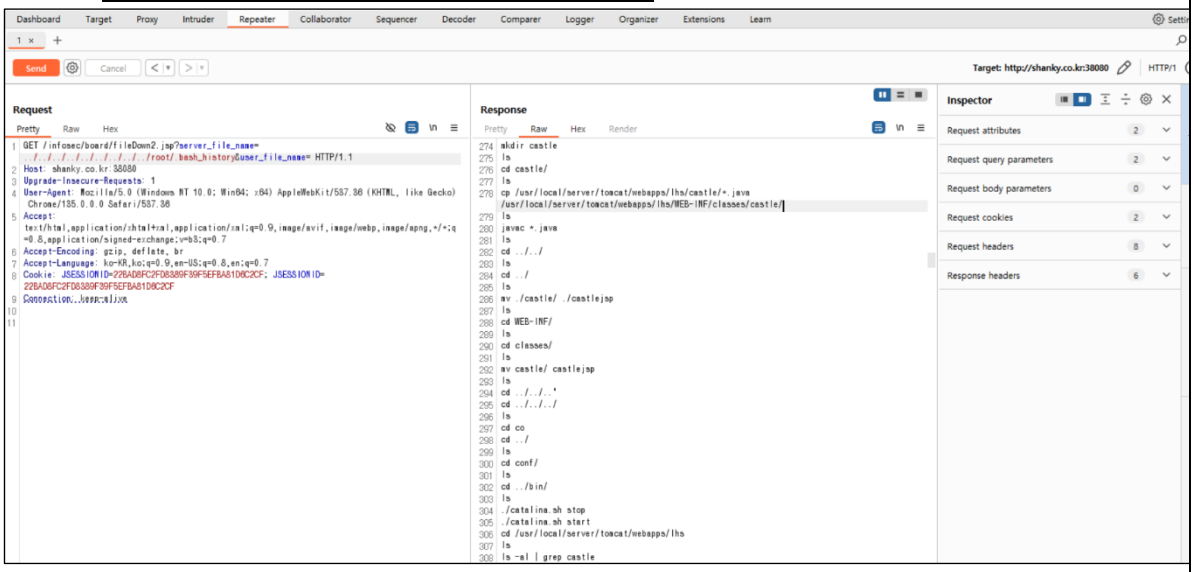
Step 2-3. **.bash_history** 를 이용하여 현재 접속되어 있는 사용자 **쉘 히스토리** 보기

: server_file_name 파라미터에 shanks 의 .bash_history 의 경로를 삽입한 후 요청을 전송한다.

: shanks 가 사용한 쉘 명령어 히스토리를 확인할 수 있다.

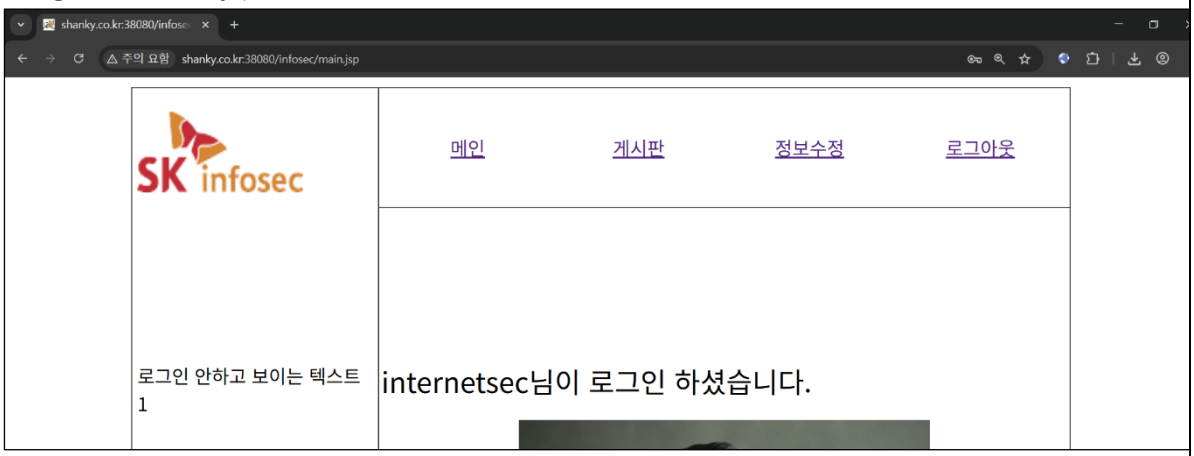


: server_file_name 파라미터에 root 의 .bash_history 의 경로를 삽입한 후 요청을 전송한다.
: root 가 사용한 쉘 명령어 히스토리를 확인할 수 있다.
: 특히, tomcat 폴더의 경로(/usr/local/server/tomcat)를 확인할 수 있다.

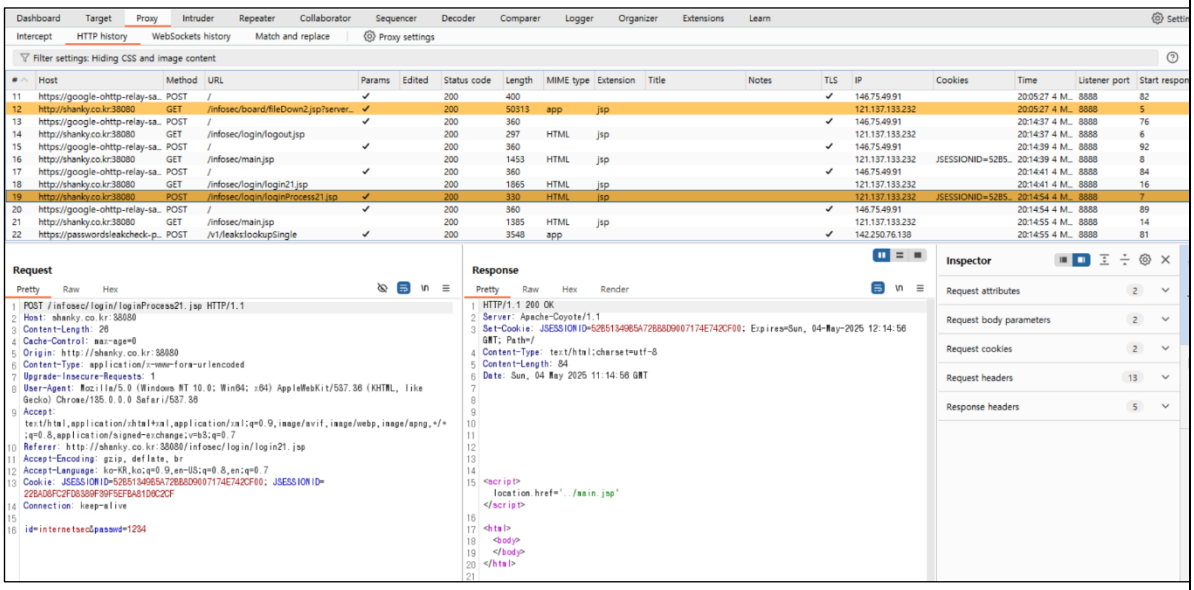



**Step 3. DB 접근 관련 파일 찾아내기**

Step 3-1. **login 프로세스 jsp 파일**을 다운로드 받아, **DB 접근**이 어떻게 구현되어 있는지 확인
: login 프로세스 jsp 파일을 다운로드 받기 위해, 로그아웃 후 재로그인 한다.

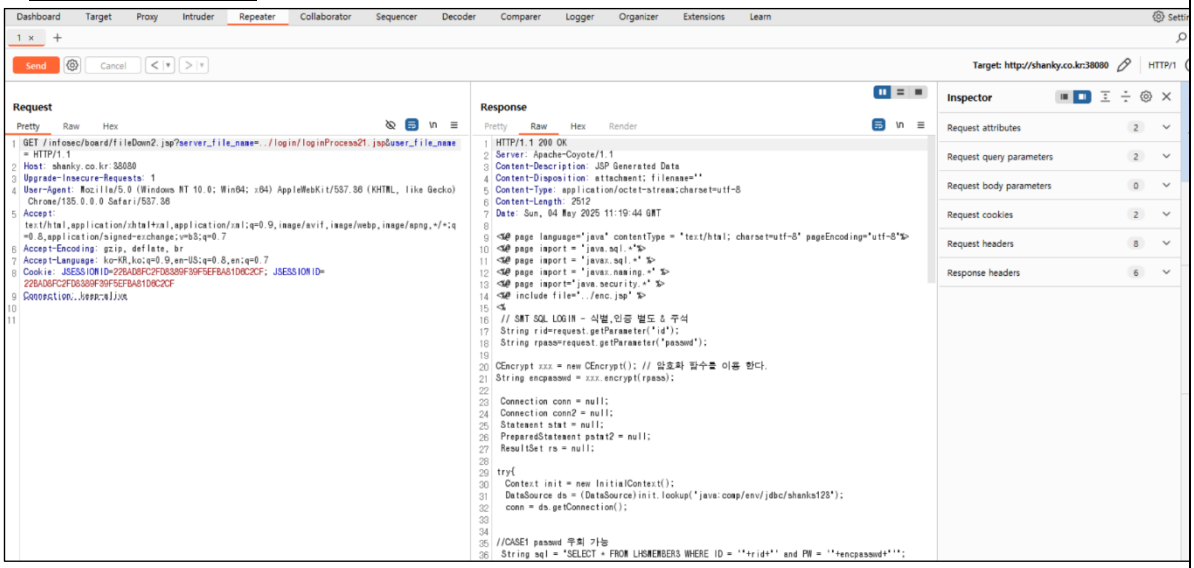


: Burp 를 이용하여 login 프로세스 jsp 파일의 이름과 경로를 확인한다.
(/infosec/login/loginProcess21.jsp)

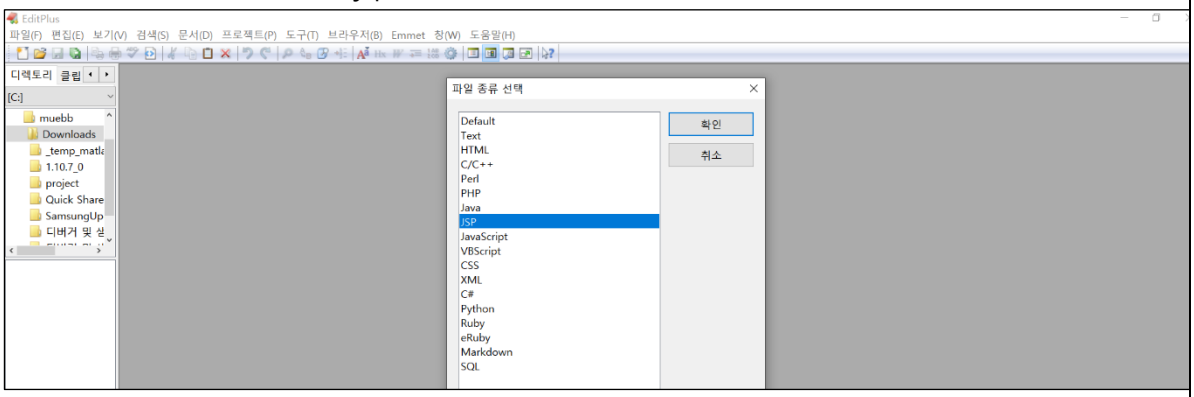


: server_file_name 파라미터에 loginProcess21.jsp 의 경로를 삽입한 후 요청을 전송한다.

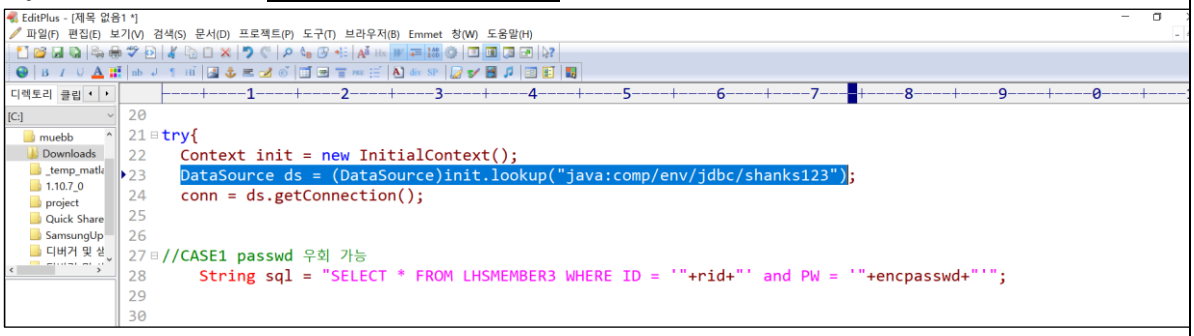
: loginProcess21.jsp 파일의 내용을 확인할 수 있다.



(텍스트 에디터를 이용하여 jsp 파일을 확인한다)



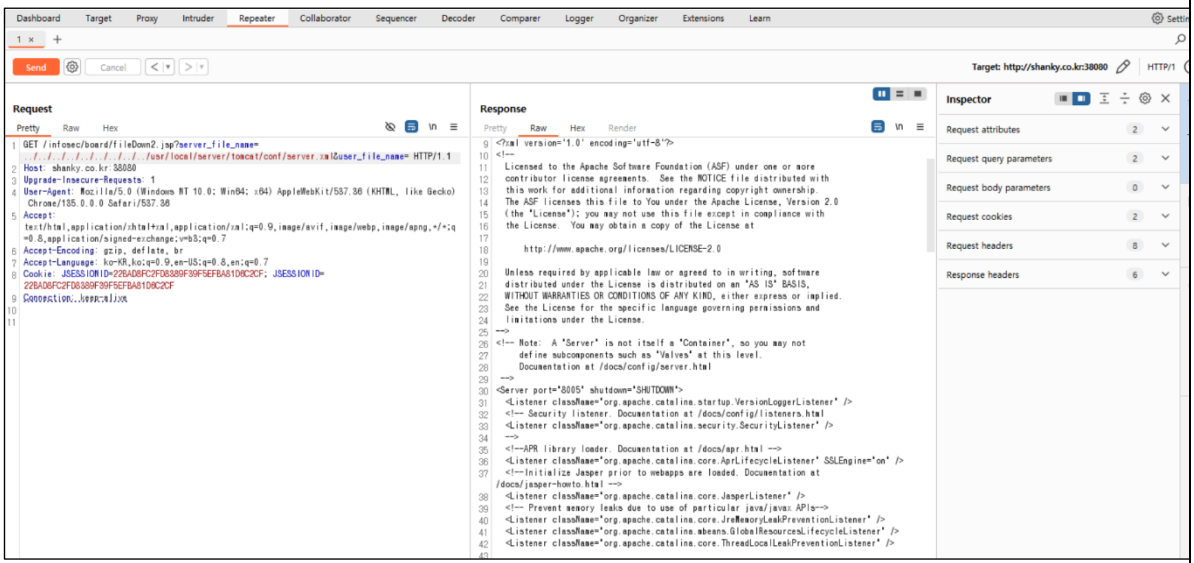

: jdbc 설정 파일 중 shanks123 의 설정 파일을 긁어오는 코드를 확인할 수 있다.




Step 3-2. **tomcat** 폴더 내의 **환경설정 파일(server.xml. context.xml)** 확인

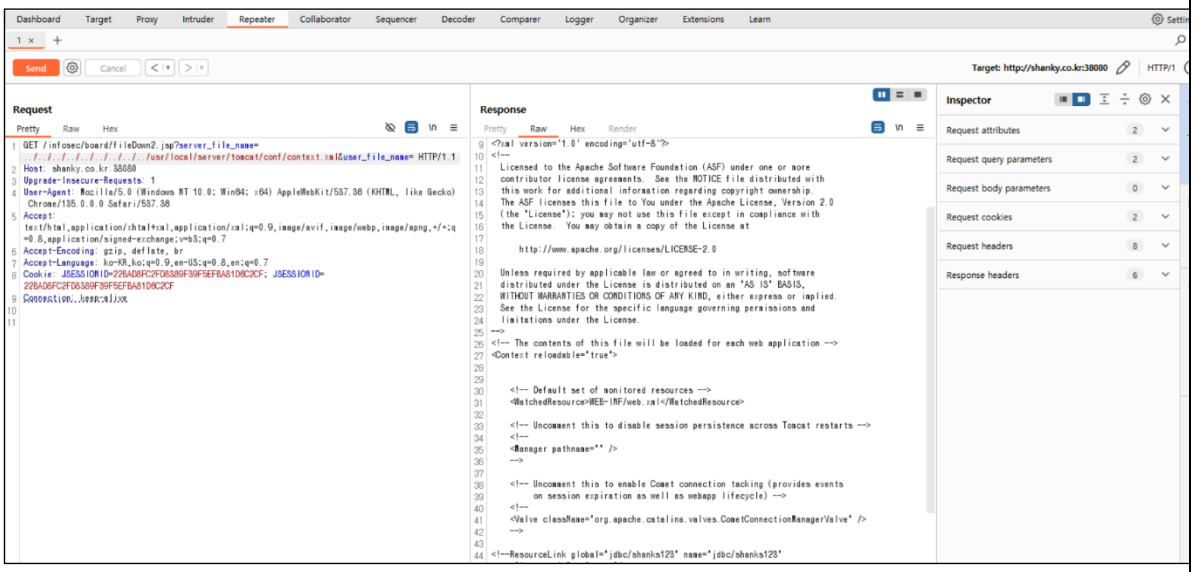
: server_file_name 파라미터에 /usr/local/server/tomcat/conf/server.xml 의 경로를 삽입한 후 요청을 전송한다.

: 원하는 정보가 없음을 확인할 수 있다.



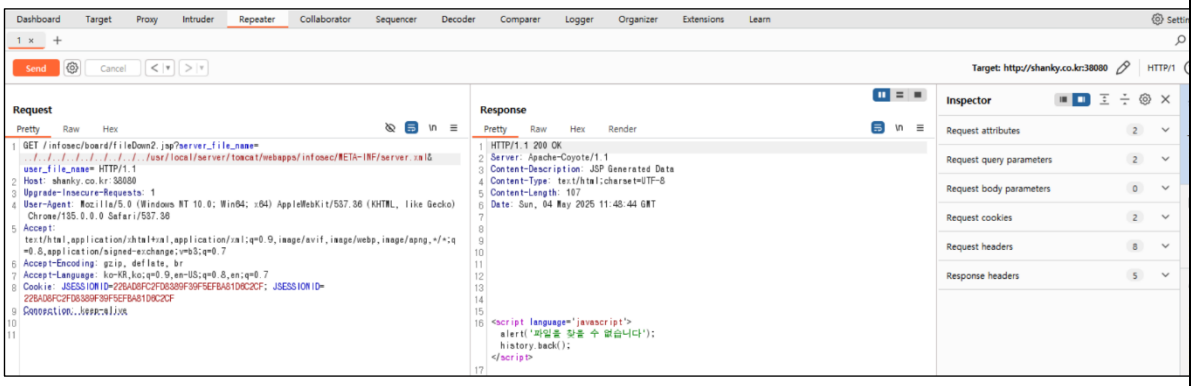
: server_file_name 파라미터에 /usr/local/server/tomcat/conf/context.xml 의 경로를 삽입한 후 요청을 전송한다.

: 원하는 정보가 없음을 확인할 수 있다.



: server_file_name 파라미터에 /usr/local/server/tomcat/webapps/infosec/META-INF/server.xml 의 경로를 삽입한 후 요청을 전송한다.

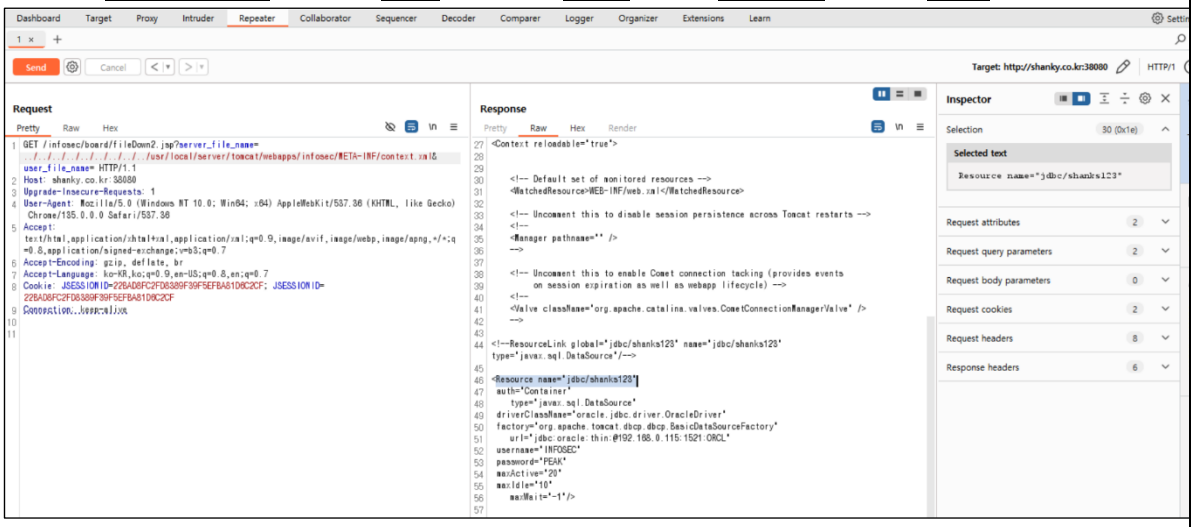
: 원하는 정보가 없음을 확인할 수 있다.



: server_file_name 파라미터에 /usr/local/server/tomcat/webapps/infosec/META-INF/context.xml 의 경로를 삽입한 후 요청을 전송한다.

: shanks123 파일의 내용을 확인할 수 있다.

(IP 는 192.168.0.115, Port 는 1521, DB 명은 ORCL, ID 는 INFOSEC, PW 는 PEAK)

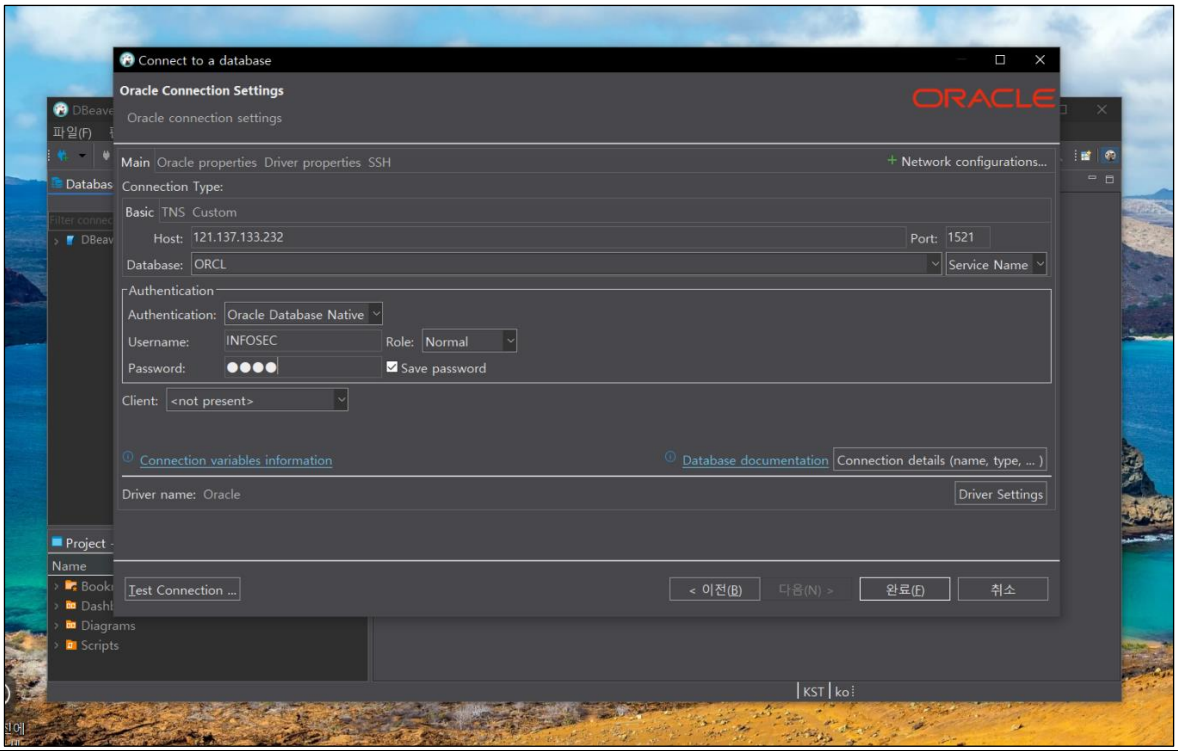



**Step 4. DB 접속**

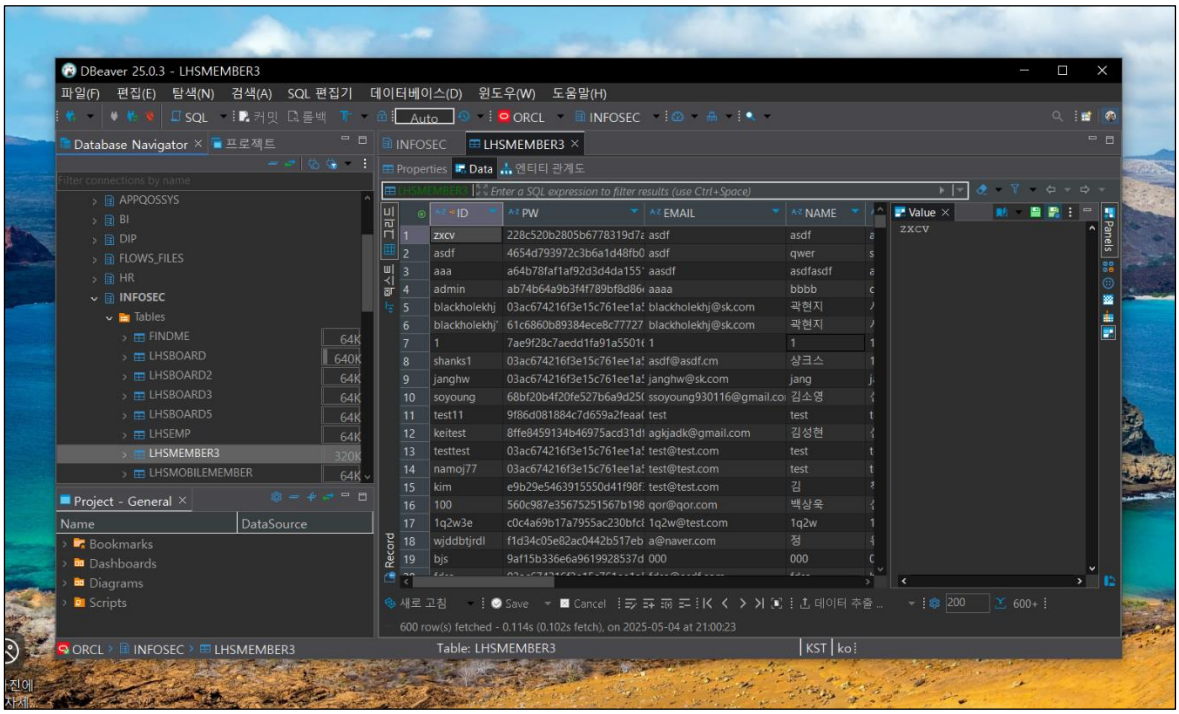
Step 4-1. 획득한 DB 정보를 이용하여 DB 접속

: Step 3 에서 획득한 IP, Port, DB 명, ID, PW 정보를 입력하여 DB 에 접속한다.

(IP 는 121.137.133.232 로 대체)



(DB 내 다양한 데이터에 접근 가능)




* 티스토리 '**서버 프로그래밍에 대한 이해 context.xml /server.xml / web.xml**' 참고 (https://sallykim5087.tistory.com/130)
* 티스토리 '**톰캣] Context 설정**' 참고 (https://parkcheolu.tistory.com/130)

| 성명 | 프로젝트 후 소감 |
|---|---|
| 박기쁨 | File Download 취약점 공격을 실습하며, 웹 서버 프로그래밍에 대한 이해가 부족하여 실습 과정에서 난관을 겪었다. 웹 서버에 대한 이해뿐만 아니라, 보호하고자 하는 분야, 해킹하고자 하는 분야에 대한 기본/기초적이면서도 정확한 지식을 갖고 있을 때, 비로소 주도적이고 창의적인 보호, 해킹을 수행할 수 있다는 것을 다시 한번 깨달은 실습인 것 같다.<br>한편, 실제 DB 에 접속해보는 과정을 수행해봄으로써 이론으로만 알고 있던 데이터베이스 관련 지식들을 눈으로 확인해볼 수 있어 좋았다. |