정보보안론 6주차 강의

HTTP 프로토콜 : 여러 프로토콜이 쓰이나 가장 많이 쓰이는 프로토콜은 HTTP

! 시험 - 전송 방식 !

GET 방식

가장 일반적인 HTTP Request 형태로, 요청 데이터의 인수를 웹 브라우저의 URL로 전송

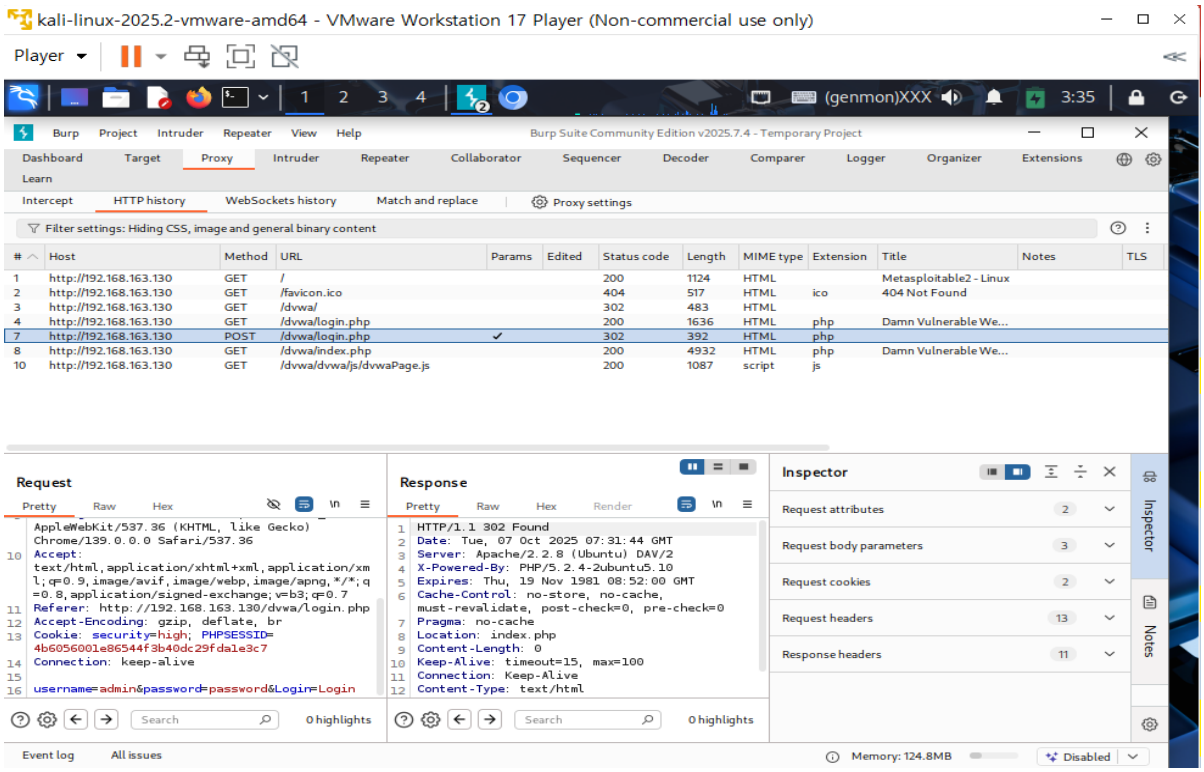
데이터가 주소 입력란에 표시되므로 최소한의 보안도 유지되지 않는 취약한 방식

POST 방식

URL에 요청 데이터를 기록하지 않고 HTTP 헤더에 데이터를 전송 (변수에 값을 넣어서 전송)

게시판의 경우: 목록이나 글 보기 화면은 접근 자유도를 위해 GET 방식을 사용

게시글을 저장·수정·삭제하거나 대용량 데이터를 전송할 때는 POST 방식을 사용



로그인 정보를 전송할 때는 POST 방식으로 전송됨

! 시험 HTTP Response !

클라이언트의 HTTP Request에 대한 응답 패킷

서버에서 쓰이는 프로토콜 버전, Request에 대한 실행 결과 코드, 간략한 실행 결과 설명문 내용이 담겨 있음

표 4-1 HTTP Response의 주요 실행 결과 코드

실행 결과 코드	내용	설명
100번대	정보 전송	HTTP 1.0까지는 계열에 대한 정의가 이루어지지 않았기 때문에 실험 용도 외에는 100번대 서버 측의 응답이 없다.
200번대	성공	클라이언트의 요구가 성공적으로 수신 및 처리되었음을 의미한다.
300번대	리다이렉션	해당 요구 사항을 처리하기 위해 사용자 에이전트가 수행해야 할 추가 동작이 있음을 의미한다.
400번대	클라이언트 측 에러	클라이언트에 오류가 발생했을 때 사용한다. 예를 들면 클라이언트가 서버에 보내는 요구 메시지를 완전히 처리하지 못한 경우 등이다.
500번대	서버 측 에러	서버 자체에서 발생한 오류 상황이나 요구 사항을 제대로 처리할 수 없을 때 사용한다.

디렉토리 이동 공격 실습

DVWA 보안은 low로 설정

URL을 이용한 디렉토리 이동 공격

http://192.168.163.130/dvwa/vulnerabilities/fi/?page=../../../../../etc/passwd