# 파일 다운로드 취약점 및 기타 취약점

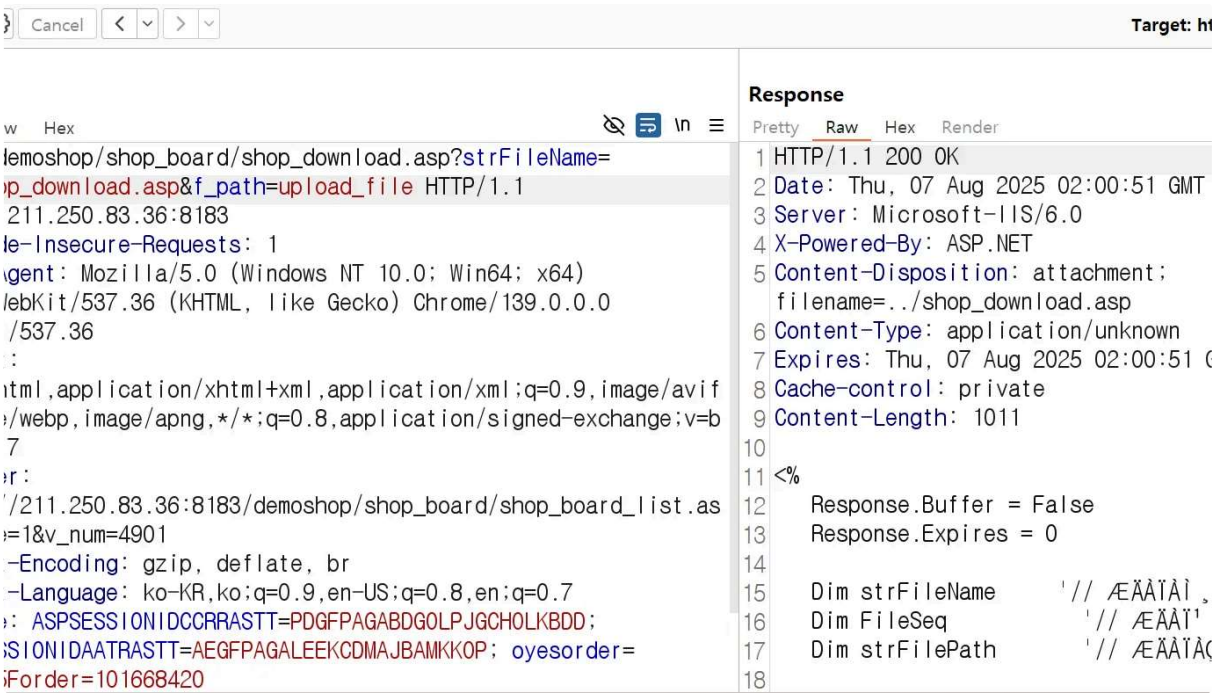
파일 다운로드 받는 과정에서 다운로드 담당하는 소스코드가 입력 값 검증이 되지 않아서, 상단에 있는 파일(소스코드, 환경설정 파일 등)을 접근해서 다운로드 받을 수 있는 취약점!!!!

strFileName에서 입력 값 검증이 되지 않아서 ../ 패턴을 이용해 상단의 디렉터리 및 파일에 접근 여부를 확인

shop_download.asp 서버 사이드 파일을 다운로드 받아 중요 코드 로직을 확인할 수 있다.

/demoshop/shop_board/shop_download.asp?
**strFileName=shop_download.asp**&f_path=upload_file

/demoshop/shop_board/upload_file/../shop_download.asp
/demoshop/shop_board/shop_download.asp




1. → **(대응) shop_download.asp?strFileName=2&f_path=1 (데이터베이스에서 정보를 가져옴)**

### LFI (Local File Inclusion) 취약점

LFI는 웹 애플리케이션이 **로컬 파일 시스템의 파일을 동적으로 포함**할 때, 사용자 입력을 적절히 검증하지 않아 공격자가 서버 내 임의의 로컬 파일을 포함시켜 읽거나 실행할 수 있는 취약점

발생 조건

- include(), require() 등의 함수가 사용자 입력을 기반으로 로컬 파일 경로를 지정.
- 디렉토리 이동 문자(../)나 절대 경로(/etc/passwd)를 필터링하지 않음.
- PHP 설정에서 open_basedir가 제한적으로 설정되지 않음.

공격 방식

- 공격자는 URL 매개변수를 조작해 서버 내 민감한 파일(예: /etc/passwd, config.php)을 포함.
- 디렉토리 이동(../)을 사용해 상위 디렉토리의 파일에 접근.
- PHP 래퍼(예: php://filter)를 활용해 파일 내용을 인코딩된 형태로 읽거나 실행.

결과

- 민감한 정보 유출(예: 사용자 계정, 데이터베이스 설정).
- 로그 파일이나 세션 파일에 악성 코드를 삽입해 RCE로 확장 가능.