파일을 다운로드 하는기능에 대한 보안요구항목 적용

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | | | SP‐FILEDOWNLOAD‐05 | | | | | | | |
| 업무시스템 | | | 전자정부 프레임워크  공통컴포넌트 | | | | | 화면명 | 게시물 내 첨부파일 다운로드 화면 | |
| 업무기능 | | | 게시물 내 첨부파일 다운로드 | | | | | 관련 TABLE |  | |
| 단위시스템 | | | 게시물 내 첨부파일 다운로드 | | | | |  | |
| 화면 | | | | | | | | | | |
|  | | | | | | | | | | |
| 처리 개요 | | | | | | | | | | |
| 사용자가 조회하는 공지사항의 상세내용을 출력하는 화면 내 첨부파일을 누르면 다운로드 URL로 이동하여 해당 파일을 다운로드 받을 수 있도록 한다. | | | | | | | | | | |
| 화면 입/출력 정보일람 | | | | | | | | | | |
| 번호 | I/O | | | 이벤트 | | 포인트 | 기능(링크 포함) | | | |
| 1 | I | | | 입력 | | 첨부파일 | 첨부파일 다운로드 | | | |
| 업무 흐름 | | | | | | | | | | |
| 사용자는 첨부파일을 클릭하여 해당 파일을 다운로드 받을 수 있다. | | | | | | | | | | |
| 보안요구항목 | | | | | | | | | | |
| 구분 | | 보안요구항목 | | | 중점점검항목 | | | | | 비고 |
| SR1‐1 | | DBMS 조회 및 결과 검증 | | | 첨부파일 다운로드를 위한 URL 파라미터에 쿼리를 조작할 수 있는 입력값으로 SQL 삽입공격이 시도될 수 있으므로 입력값 검증이 필요함. | | | | | 공통필터적용 |
| SR1‐4 | | 시스템 자원 접근 및 명령어 수행 입력 값 검증 | | | 서버에서 명령 창을 실행해두는 경우 사용자가 시스템 명령어를 입력할 가능성에 대비하여 미리 정의된 인자 값의 배열을 통해 명령어를 선택하도록 해야 함. | | | | |  |
| SR1‐5 | | 웹 서비스 요청 및 결과 검증 | | | 첨부파일 다운로드시 입력정보에 악의적인 스크립트가 포함될 수 있으므로 입력값 검증이 필요함. | | | | |  |
| SR1‐10 | | 업로드·다운로드 파일검증 | | | 첨부파일 다운로드를 위해 요청되는 파일명에 경로를 조작하는 문자가 포함되어 있는지 점검해야 함.  첨부파일 다운로드시 사용자 입력 값을 검증하여 웹 루트 디렉터리를 벗어난 영역에서 파일을 다운로드 할 수 없도록 해야 함.  파일 다운로드를 처리하기 전에 파일에 대한 바이러스 및 악성코드 여부를 점검하고 다운로드 받은 파일의 무결성 검사를 실행함.  필요시 인증된 사용자만 파일을 다운로드 할 수 있도록 제한함. | | | | |  |
| SR2‐1 | | 인증 대상 및 방식 | | | 인증이 필요한 게시판, 관리자 전용 게시판 등 중요페이지 접근시 인증 절차가 부재이거나, 부적절하게 인증 과정을 우회할 수 있는지를 확인해야 함. | | | | |  |
| SR2‐4 | | 중요자원 접근통제 | | | URL/파라미터를 변조하여 중요페이지 또는 권한 없는 페이지 접근에 대한 인증을 우회할 수 없도록 해야 함.  SSI(Server‐Side Includes) 변수가 조작되어 명령실행을 통해 서버 데이터 정보가 누출되지 않도록 해야 함. | | | | |  |
| SR2‐7 | | 중요정보 저장 | | | 첨부파일 다운로드시 실제저장 명, 파일의 저장경로 등이 노출되지 않도록 함.  소스코드 내에 중요정보를 노출하는 주석문이 존재하지 않아야 함. | | | | |  |
| SR3‐1 | | 예외처리 | | | 첨부파일 다운로드 요청시 오류가 발생하는 경우 지정된 페이지로 리다이렉트 하여 에러 정보가 노출되지 않도록 해야 함. | | | | |  |
| SR4‐1 | | 세션통제 | | | 중복 로그인을 허용하지 않는 경우 이전에 생성된 로그인 세션을 종료하거나, 새로이 연결되는 세션을 종료해야 함.  로그인 상태인 사용자를 위해 해당 페이지에 로그아웃 인터페이스를 구현함.  세션 ID가 URL, 에러메시지, 로그 등에 노출되지 않도록 해야 함. | | | | |  |