관리자 페이지 기능에 대한 보안요구항목 적용

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | | | SP‐UPDATE/DELETE‐03 | | | | | | | |
| 업무시스템 | | | 전자정부 프레임워크  공통컴포넌트 | | | | | 화면명 | 관리환경 공지사항 관리 화면 | |
| 업무기능 | | | 관리환경 공지사항 관리 | | | | | 관련 TABLE |  | |
| 단위시스템 | | | 관리환경 공지사항 관리 | | | | |  | |
| 화면 | | | | | | | | | | |
|  | | | | | | | | | | |
| 처리 개요 | | | | | | | | | | |
| 관리환경에서 관리자만 접근 가능한 공지사항의 목록을 출력하는 화면을 구성한다. | | | | | | | | | | |
| 화면 입/출력 정보일람 | | | | | | | | | | |
| 번호 | I/O | | | 이벤트 | | 포인트 | 기능(링크 포함) | | | |
| 1 | I | | | 입력 | | 검색 창 |  | | | |
| 2 | I | | | 클릭 | | 검색 | 공지사항 검색 | | | |
| 업무 흐름 | | | | | | | | | | |
| 1. 관리자는 검색창에 검색어를 입력하여 공지사항을 조회한다.  2. 시스템은 검색 및 조회된 공지사항을 화면에 출력한다. | | | | | | | | | | |
| 보안요구항목 | | | | | | | | | | |
| 구분 | | 보안요구항목 | | | 중점점검항목 | | | | | 비고 |
| SR1‐1 | | DBMS 조회 및 결과 검증 | | | 공지사항 검색을 위한 검색어에 쿼리를 조작할 수 있는 입력값으로 SQL 삽입공격이 시도될 수 있으므로 입력값 검증이 필요함. | | | | | 공통필터적용 |
| SR1‐5 | | 웹 서비스 요청 및 결과 검증 | | | 공지사항 검색을 위한 입력정보에 악의적인 스크립트가 포함될 수 있으므로 입력값 검증이 필요함. | | | | | 공통필터적용 |
| SR2‐4 | | 중요자원 접근통제 | | | 인증이 필요한 게시판, 관리자 전용 게시판 등 중요페이지 접근시 인증 절차가 부재이거나, 적절하지 않은 인증 과정을 우회할 수 있는지를 확인해야 함. | | | | |  |
| SR2‐7 | | 중요정보 저장 | | | 소스접근통제 정책에 따라 관리자의 역할 및 접근권한에 기반한 올바른 접근이 이루어지도록 통제하여 인가 받은 사용자만을 허용하여야 함.  관리자 전용 페이지의 URL은 쉽게 추측될 수 없도록 설정함.  관리자 페이지를 원격으로 연결한 경우 암호화 통신채널을 사용해야 함. | | | | |  |
| SR3‐1 | | 예외처리 | | | 소스코드내에 중요정보를 노출하는 주석문이 존재하지 않아야 함. | | | | |  |
| SR4‐1 | | 세션통제 | | | 공지사항 조회시 에러가 발생하는 경우 지정된 페이지로 리다이렉트 하여 에러 정보가 노출되지 않도록 해야 함. | | | | |  |
| SR2‐1 | | 인증 대상 및 방식 | | | 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. | | | | |  |