DB에 데이터를 수정/삭제하는 기능에 대한 보안요구항목 적용

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | | | SP‐UPDATE/DELETE‐03 | | | | | | | |
| 업무시스템 | | | 전자정부 프레임워크  공통컴포넌트 | | | | | 화면명 | 게시물 수정/삭제 화면 | |
| 업무기능 | | | 게시물 수정/삭제 | | | | | 관련 TABLE |  | |
| 단위시스템 | | | 게시물 수정/삭제 | | | | |  | |
| 화면 | | | | | | | | | | |
|  | | | | | | | | | | |
| 처리 개요 | | | | | | | | | | |
| Q&A 게시글을 수정/삭제하거나 목록을 출력하는 화면을 구성한다. | | | | | | | | | | |
| 화면 입/출력 정보일람 | | | | | | | | | | |
| 번호 | I/O | | | 이벤트 | | 포인트 | 기능(링크 포함) | | | |
| 1 | I | | | 클릭 | | Q&A ‐글 수정 |  | | | |
| 2 | I | | | 클릭 | | Q&A ‐글 삭제 |  | | | |
| 3 | I | | | 클릭 | | Q&A ‐글 목록 조회 |  | | | |
| 업무 흐름 | | | | | | | | | | |
| 1. 사용자가 조회한 Q&A의 게시글 내용을 수정한다.  2. 사용자가 조회한 Q&A의 게시글 내용을 삭제한다.  3. Q&A의 목록 조회 화면을 출력한다. | | | | | | | | | | |
| 보안요구항목 | | | | | | | | | | |
| 구분 | | 보안요구항목 | | | 중점점검항목 | | | | | 비고 |
| SR1‐1 | | DBMS 조회 및 결과 검증 | | | 목록 조회시 URL 파라미터에 쿼리를 조작할 수 있는 입력값으로 SQL 삽입공격이 시도될 수 있으므로 입력값 검증이 필요함. | | | | | 공통필터적용 |
| SR1‐5 | | 웹 서비스 요청 및 결과 검증 | | | 게시글 수정, 목록 조회시 입력정보에 악의적인 스크립트가 포함될 수 있으므로 입력값 검증이 필요함. | | | | | 공통필터적용 |
| SR1‐6 | | 웹 기반 중요기능 수행 요청 유효성 검증 | | | 스크립트를 이용하여 게시글 수정/삭제 요청이 처리될 수 있으므로, 실제 사용자의 유효한 요청여부를 확인해야 함. | | | | |  |
| SR1‐9 | | 보안기능 동작에 사용되는 입력 값 검증 | | | 쿠키·환경변수·Hidden 필드 값을 조작하여 게시글 수정/삭제 요청이 처리될 수 있으므로 실제 사용자의 유효한 요청여부를 확인해야 함. | | | | |  |
| 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 | | | URL을 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 | | | 소스코드 내에 중요정보를 노출하는 주석문이 존재하지 않아야 함. | | | | |  |
| SR3‐1 | | 예외처리 | | | 게시물 수정/삭제시 오류가 발생할 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. | | | | |  |