DB에 데이터를 입력하는 기능에 대한 보안요구항목 적용

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | | | SP‐CREATE‐01 | | | | | | | |
| 업무시스템 | | | 전자정부 프레임워크  공통컴포넌트 | | | | | 화면명 | 회원가입 화면 | |
| 업무기능 | | | 사용자 회원가입 신청 | | | | | 관련 TABLE |  | |
| 단위시스템 | | | 사용자 회원가입 | | | | |  | |
| 화면 | | | | | | | | | | |
|  | | | | | | | | | | |
| 처리 개요 | | | | | | | | | | |
| 사용자의 회원정보를 입력 받는 화면을 구성한다. 사용자에게 입력 받는 회원정보는 아이디/패스워드를 포함한 사용자의 개인정보이다.  사용자 입력 후 가입신청 버튼을 누르면 사용자의 회원정보가 DB에 추가된다. | | | | | | | | | | |
| 화면 입/출력 정보일람 | | | | | | | | | | |
| 번호 | I/O | | | 이벤트 | | 포인트 | 기능(링크 포함) | | | |
| 1 | I | | | 입력 | | 일반회원아이디 | 중복아이디 검색 | | | |
| 2 | I | | | 입력 | | 일반회원이름 |  | | | |
| 3 | I | | | 입력 | | 비밀번호 |  | | | |
| 4 | I | | | 입력 | | 비밀번호확인 |  | | | |
| 5 | I | | | 입력 | | 비밀번호힌트 | 비밀번호 힌트 선택 | | | |
| 6 | I | | | 입력 | | 비밀번호정답 |  | | | |
| 7 | I | | | 입력 | | 전화번호 |  | | | |
| 8 | I | | | 입력 | | 핸드폰번호 |  | | | |
| 9 | I | | | 입력 | | 이메일 주소 |  | | | |
| 10 | I | | | 입력 | | 소속정보 | 일반기업/공공기관 선택 | | | |
| 11 | I | | | 입력 | | 소속 명 |  | | | |
| 12 | I | | | 입력 | | 우편번호 | 우편번호 검색 | | | |
| 13 | I | | | 입력 | | 주소 |  | | | |
| 14 | I | | | 입력 | | 상세주소 |  | | | |
| 15 | I | | | 입력 | | 인증서DN | 인증서 등록 | | | |
| 16 | I | | | 클릭 | | 가입신청 | 입력된 회원정보로 가입신청 | | | |
| 업무 흐름 | | | | | | | | | | |
| 1. 사용자는 입력 창에 각각 자신의 회원정보를 입력한다.  2. 중복아이디 검색을 통해 입력한 아이디가 기존 회원정보에 존재하는지 확인한다.  3. 우편번호는 외부링크로 연결되어 값을 검색하고 검색된 결과가 입력된다.  4. 사용자는 첨부파일을 업로드 하여 인증서를 등록한다.  5. 회원정보 입력 후 가입신청 버튼을 누르면 시스템은 사용자의 회원정보를 데이터베이스에 추가한다. | | | | | | | | | | |
| 보안요구항목 | | | | | | | | | | |
| 구분 | | 보안요구항목 | | | 중점점검항목 | | | | | 비고 |
| SR1‐1 | | DBMS 조회 및 결과 검증 | | | 중복아이디 검색을 위한 사용자ID에 쿼리를 조작할 수 있는 입력값으로 SQL 삽입공격이 시도될 수 있으므로 입력값 검증이 필요함.  우편번호 검색을 위한 입력값을 조작하여 SQL 삽입 공격이 시도될 수 있으므로 입력값 검증이 필요함. | | | | | 공통필터적용 |
| SR1‐5 | | 웹 서비스 요청 및 결과 검증 | | | 회원가입을 위한 입력정보에 악의적인 스크립트가 포함될 수 있으므로 입력값 검증이 필요함. | | | | | 공통필터적용 |
| SR1‐6 | | 웹 기반 중요 기능 수행 요청 유효성 검증 | | | 스크립트를 이용하여 회원가입 요청이 처리될 수 있으므로, 실제 사용자의 유효한 요청인지 여부를 확인해야 함. | | | | | 공통필터적용 |
| SR1‐10 | | 업로드·다운로드 파일 검증 | | | 인증서 등록시 허가된 유형의 파일만 업로드 되도록 해야 함. | | | | |  |
| SR2‐3 | | 비밀번호 관리 | | | 사용자가 입력한 비밀번호에 대해 안전한 패스워드 설정 정책이 적용되어야 함.  비밀번호 힌트 및 정답은 예측 가능하지 않은 질문과 답변을 사용하도록 해야 함. | | | | |  |
| SR2‐7 | | 중요정보 저장 | | | 비밀번호는 솔트가 적용된 안전한 해시함수를 사용해서 암호화해서 저장해야 함.  소스코드내에 중요정보를 노출하는 주석문이 존재하지 않아야 함. | | | | | 공통함수hash()를 호출하여 비밀번호 암호화 |
| SR2‐8 | | 중요정보 전송 | | | 사용자가 입력한 회원정보는 암호화하여 전송하거나, 암호화된 통신 채널을 통해 전달해야 함. | | | | |  |
| SR3‐1 | | 예외처리 | | | 회원정보 입력 및 제출과정에서 오류가 발생하는 경우 지정된 페이지로 리다이렉트 하여 에러 정보가 노출되지 않도록 해야 함. | | | | |  |
| SR4‐1 | | 세션통제 | | | 세션 ID가 URL, 에러메시지, 로그 등에 노출되지 않도록 해야함. | | | | |  |