DB에 데이터를 조회하는 기능에 대한 보안요구항목 적용

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | | | SP‐READ‐02 | | | | | | | |
| 업무시스템 | | | 전자정부 프레임워크  공통컴포넌트 | | | | | 화면명 | 아이디/비밀번호 찾기 화면 | |
| 업무기능 | | | 사용자 로그인 정보 입력 | | | | | 관련 TABLE |  | |
| 단위시스템 | | | 사용자 로그인 | | | | |  | |
| 화면 | | | | | | | | | | |
|  | | | | | | | | | | |
| 처리 개요 | | | | | | | | | | |
| 인증정보 조회 및 재설정을 위한 정보를 입력 받는 화면을 구성한다. 사용자에게 입력 받는 정보는 이름, 이메일 등 개인정보이다. 사용자 입력 후 아이디 및 비밀번호 찾기 버튼을 누르면 시스템은 그에 해당하는 사용자 인증정보를 조회한다. | | | | | | | | | | |
| 화면 입/출력 정보일람 | | | | | | | | | | |
| 번호 | I/O | | | 이벤트 | | 포인트 | 기능(링크 포함) | | | |
| 1 | I | | | 입력 | | 이름 |  | | | |
| 2 | I | | | 입력 | | 이메일 |  | | | |
| 3 | I | | | 클릭 | | 아이디 찾기 | 아이디 조회 | | | |
| 4 | I | | | 입력 | | 아이디 |  | | | |
| 5 | I | | | 입력 | | 이름 |  | | | |
| 6 | I | | | 입력 | | 이메일 |  | | | |
| 7 | I | | | 선택 | | 비밀번호 힌트 |  | | | |
| 8 | I | | | 입력 | | 비밀번호 정답 |  | | | |
| 9 | I | | | 클릭 | | 비밀번호 찾기 | 임시비밀번호 발송 | | | |
| 10 | I | | | 출력 | | 아이디 찾기 결과 | 조회된 아이디 출력 | | | |
| 11 | I | | | 출력 | | 비밀번호 찾기 결과 | 임시비밀번호 발송결과 출력 | | | |
| 업무 흐름 | | | | | | | | | | |
| 1. 사용자는 이름과 이메일을 입력하여 아이디를 조회한다.  2. 시스템은 해당 정보와 매칭되는 아이디 정보를 사용자에게 제공한다.  3. 사용자는 아이디, 이름을 포함한 개인정보를 입력하여 비밀번호 조회를 시도한다.  4. 시스템은 해당 정보와 매칭되는 계정의 존재여부를 확인하고, 계정이 존재할 경우 이메일 주소로 임시비밀번호를 발송한다. | | | | | | | | | | |
| 보안요구항목 | | | | | | | | | | |
| 구분 | | 보안요구항목 | | | 중점점검항목 | | | | | 비고 |
| SR1‐1 | | DBMS 조회 및 결과 검증 | | | 아이디/비밀번호 찾기시 검색을 위한 사용자 이름, 이메일, ID에 쿼리를 조작할 수 있는 입력값으로 SQL 삽입공격이 시도될 수 있으므로 입력값 검증이 필요함. | | | | | 공통필터적용 |
| SR1‐5 | | 웹 서비스 요청 및 결과 검증 | | | 아이디/비밀번호 찾기시 입력정보에 악의적인 스크립트가 포함될 수 있으므로 입력값 검증이 필요함. | | | | | 공통필터적용 |
| SR2‐3 | | 비밀번호 관리 | | | 비밀번호 찾기시 사전에 등록된 이메일 주소로만 임시 비밀번호가 전송되도록 제한해야 함.  임시비밀번호로 첫 로그인시 반드시 신규비밀번호로 변경하도록 관리해야 함. | | | | |  |
| SR2‐4 | | 중요자원 접근 통제 | | | URL을 변조하여 중요페이지 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. | | | | |  |
| SR2‐8 | | 중요정보 전송 | | | 사용자가 입력한 정보는 암호화하여 전송하거나, 암호화된 통신 채널을 통해 전달해야 함. | | | | |  |
| SR3‐1 | | 예외처리 | | | 사용자 정보 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 해야 함. | | | | |  |