**보안요구항목 적용 계획서**

|  |  |  |  |
| --- | --- | --- | --- |
| 요구사항분류 | 입력데이터 검증 및 표현 | 요구사항번호 | SR1‐1 |
| 요구사항이름 | DBMS 조회 및 결과 검증 | | |
| 요구사항내용 | ① 애플리케이션에서 DB연결을 수행할 때 최소권한의 계정을 사용해야 한다. | | |
| 보안요구항목 적용 계획 | 애플리케이션에서 DB연결을 위해 사용되는 계정은 "애플리케이션명\_시리얼번호"로 설정하며, 해당 계정에 대해서는 "애플리케이션명\_테이블명"에 대해 조회, 수정, 삭제, 업데이트 권한만 할당한다. | | |
| 비고 | 표준코딩정의서에서 정의 | | |

**유즈케이스 다이어그램**

|  |  |  |  |
| --- | --- | --- | --- |
| 유즈케이스 ID | 사용자 로그인 | | |
| 사전조건 | 포스트‐잇 프로그램을 가동한다. | | |
| 시나리오 | | | |
| [주요 이벤트 경로]  1. 사용자는 포스트‐잇 프로그램을 가동한다.  2. 자동 로그인이 실행되어 사용자는 바로 자신의 개인화된 화면으로 이동한다.  [대안 또는 예외 경로]  1. 로그인 옵션이 수동 로그인으로 적용되어 있을 때:  a. 프로그램은 아이디/비밀번호를 묻는 창을 띄운다.  b. 프로그램은 서버를 통해 아이디/비밀번호를 검증한다.  c. 아이디/비밀번호가 잘못되었을 경우 1.a로 돌아간다.  2. 첫번째 로그인일 경우  a. 프로그램은 아이디/비밀번호를 묻는 창을 띄운다.  b. 프로그램은 서버를 통해 아이디/비밀번호를 검증한다.  c. 아이디/비밀번호가 잘못되었을 경우 2.a로 돌아간다.  d. 사용자에게 자동 로그인 옵션과 수동 로그인 옵션 중 하나를 선택하도록 묻는다.  e. 사용자가 입력 옵션 선택을 하지 않을 경우, 기본적으로 자동 로그인 옵션을 선택하도록 한다. | | | |
| 사후조건 | | 사용자는 로그인에 성공한다. | |
| 보안요구항목 | | 중점점검항목 | 비고 |
| SR1‐1 DBMS 조회 및 결과 검증 | | 사용자가 입력한 아이디/비밀번호가 SQL삽입을 일으키지 않도록 해야 한다. | FR‐001 공통적용 |
| SR2‐2 인증수행제한 | | 인증시도 횟수가 제한되도록 해야 한다. | FR‐002 공통적용 |
| SR2‐8 중요정보전송 | | 아이디/비밀번호는 암호화된 통신채널을 이용하여 전송되어야 한다. |  |
| SR3‐1 에러처리 | | 에러메시지를 통해 시스템의 정보가 노출되지 않아야 한다. |  |

시퀀스 다이어그램

|  |  |  |
| --- | --- | --- |
| [순차 다이어그램: 사용자 로그인 – 수동 로그인] | | |
|  | | |
| 보안요구항목 | 중점점검항목 | 비고 |
| SR1‐1 DBMS 조회 및 결과 검증 | 사용자가 입력한 아이디/비밀번호가 SQL삽입을 일으키지 않도록 해야 한다. | FR‐001 공통적용 |
| SR2‐2 인증수행제한 | 인증시도 횟수가 제한되도록 해야 한다. | FR‐002 공통적용 |
| SR2‐8 중요정보전송 | 아이디/비밀번호는 암호화된 통신채널을 이용하여 전송되어야 한다. |  |
| SR3‐1 에러처리 | 에러메시지를 통해 시스템의 정보가 노출되지 않아야 한다. |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | | SP‐LOGIN‐01 | | | | | | | |
| 업무시스템 | | 포스트잇 클라이언트 | | | 화면명 | | | 사용자 로그인 화면 | |
| 업무기능 | | 사용자 로그인 정보 입력 | | | 관련 TABLE | | |  | |
| 단위 시스템 | | 사용자 로그인 | | |
| A. 화면 | | | | | | | | | |
|  | | | | | | | | | |
| B. 처리 개요 | | | | | | | | | |
| 사용자의 로그인 정보를 입력 받는 화면을 구성한다. 사용자에게 입력 받는 로그인 정보는 ID와 PASSWORD 이다. 사용자 입력 후  Login 버튼을 누르면 유즈케이스 '사용자 로그인' 의 대안 또는 예외 경로를 통해 로그인 정보를 검증한다. | | | | | | | | | |
| C. 화면 입/출력 정보일람 | | | | | | | | | |
| 번호 | I/O | | | 이벤트 | | 포인트 | | | 기능(링크 포함) |
| 1 | I | | | 입력 | | ID | | | - |
| 2 | I | | | 입력 | | PASSWORD | | | - |
| 3 | I | | | 입력 | | Login | | | 입력된 ID/PASSWORD로 로그인 시도 |
| D. 업무 흐름 | | | | | | | | | |
| 1. 사용자는 ID/PASSWORD 입력창에 각각 자신의 로그인 정보를 입력한다.  2. PASSWORD 입력창에 입력된 글귀는 바로 보이지 않고 점(dot) 또는 별(\*)로써 표시된다.  3. 개인 정보 입력 후 Login 버튼을 누르면 시스템은 사용자의 로그인 정보를 이용하여 로그인을 시도한다. | | | | | | | | | |
| 보안요구항목 | | | 중점점검항목 | | | | 비고 | | |
| SR1‐1 DBMS 조회 및 결과 검증 | | | 사용자가 입력한 아이디/비밀번호가 SQL삽입을 일으키지 않도록 해야 한다. | | | | FR‐001 공통적용 | | |
| SR2‐2 인증수행제한 | | | 인증시도 횟수가 제한되도록 해야 한다. | | | | FR‐002 공통적용 | | |
| SR2‐8 중요정보전송 | | | 아이디/비밀번호는 암호화된 통신채널을 이용하여 전송되어야 한다. | | | |  | | |
| SR3‐1 에러처리 | | | 에러메시지를 통해 시스템의 정보가 노출되지 않아야 한다. | | | |  | | |

**요구사항 추적표**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 분석 단계 | | | | 설계 단계 | | | 구현 단계 | | 시험 단계 | |
| 사용자 요구사항 명세서 | | 유즈케이스 명세서 | | 사용자 인터페이스 설계서 | 컴포넌트 설계서 | 데이터베이스 설계서 | 프로그램 코드 | 단위시험 결과서 | 통함시험 결과서 | 시스템 시험 결과서 |
| 요구 사항ID | 요구 사항명 | 유즈 케이스 ID | 유즈 케이스명 | 화면ID | 컴포넌트ID | 테이블ID | 파일 ID | 단위 시험 ID | 시나리오ID | 시나리오ID |
| FR‐001 | SQL 필터링 | - | - | - | CO‐001 | - | PG‐001 | UT‐001 | TT‐001 | TR‐001 |
| FR‐002 | 인증점검 | - | - | - | CO‐002 | - | PG‐002 | UT‐002 | TT‐002 | TR‐002 |
| .. | .. | .. | .. | .. | .. | .. | .. | .. | .. | .. |
| FR‐100 | 로그인 | UC‐100 | 로그인 처리 | UI‐100 | CO‐100 | DB‐100 | PG‐100 | UT‐100 | TT‐100 | TR‐100 |