서울교통 빅데이터 플랫폼 보안대책 이행여부 확인결과

점검항목	취약점	보안대책	이행여부 확인결과
취약한 세션관리 (1.1)	○ **쿠키 보안속성(Secure) 설정을 미적용한 경우, SSL 환경이 아닌 상황에서 자바스크립트를 통한 쿠키 값 읽기가 가능하여 일반 사용자의 검색 기록 및 세션 정보의 요청이 가능한 취약점** ○ 진단결과 - Chrome 〉 개발자 도구(F12) 확인 시 쿠키 값 중 Secure 속성 미적용	- 설정 파일에 쿠키 보안속성 HttpOnly, Secure 적용	**미이행** - 사유 : 오픈심의 이후 정식 도메인으로 변경되면 적용예정 - 조치 기한 : 정식 도메인 발급 후 1개월 이내 조치

관리번호	VR-S-20220105-002
외부유출 금지	

비공개

민감한 데이터 노출 (2.1)	○ **SSL/TLS v1.2 이상의 암호화 통신이 아닌 경우, 네트워크 기반의 평문 통신을 도청하는 스니핑이 가능한 취약점** ○ 진단결과 - 패킷 스니핑 도구(Wireshark)를 통해 홈페이지의 IP 기준으로 통신 확인 시 암호화 통신 미적용	- 클라이언트와 서버간 SSL/TLS (v1.2 이상) 암호화 통신	**미이행** - 사유 : 오픈심의 이후 정식 도메인으로 변경되면 적용예정 - 조치 기한 : 정식 도메인 발급 후 1개월 이내 조치
민감한 데이터 노출 (2.2)	○ **유효한 인증서 미적용의 경우, 스니핑 공격을 통한 통신 정보 탈취가 가능한 취약점** ○ 진단결과 - Chrome 〉 보안 연결(HTTPS) 미사용으로 인증서 미적용	- 인증서 갱신	**미이행** - 사유 : 오픈심의 이후 정식 도메인으로 변경되면 적용예정 - 조치 기한 : 정식 도메인 발급 후 1개월 이내 조치

불충분한 인증 메커니즘 (3.1)	○ **관리자 계정의 인증 절차가 미흡하여 계정 접근 및 홈페이지 위·변조가 가능한 취약점** ○ **에러에 대한 처리가 미흡하여 버전 노출된 경우, Exploit Code를 이용한 원격 명령어 실행 등이 가능한 취약점** ○ 진단결과 - 프록시 도구(BurpSuite) 〉 서버의 응답 값 내 관리자 권한 링크의 주석 처리 확인 - 교통빅데이터 〉 빅데이터 제공서비스 〉 데이터 목록 〉 파일데이터 〉 다운로드 진행 시, 프록시 도구(BurpSuite)를 이용하여 요청 값을 변조 할 경우 WebToB 사용 및 에러 반환 확인	- 관리자 페이지에 IP 접근제한 설정 - 관리자 페이지에 인가된 사용자만 접근가능 하도록 접근제한 설정 - 불필요한 기본 페이지 제거 - 통합 에러 페이지로 Redirect 설정	**이행완료** - 관리자 권한 접속링크 제거 · 소스코드 내역  - 인가된 사용자만 관리자용 페이지 접근가능 하도록 접근제한 설정 · 소스코드 내역 

관리번호	VR-S-20220105-002
외부유출 금지	

비공개

불충분한 인증 메커니즘 (3.3)	○ **로그인 후 중요 페이지 접근 시 재인증 절차가 없어 사회공학기법으로 인한 계정 정보 및 개인 정보 유출이 가능한 취약점** ○ 진단결과 - 항목 3.1에서 발견한 관리자 권한을 기반으로 시스템관리 〉 운영관리 〉 관리자 계정 추가의 경우, 기존 가입된 사용자 및 이메일 정보를 재인증 없이 열람 가능	- 중요 페이지(개인정보 취급 등)에 재인증 절차 추가	**이행완료** - 인가된 사용자만 관리자용 페이지 접근가능 하도록 접근제한 설정 · 소스코드 내역  - 개인정보(이메일 정보) 숨김처리 · 직접 확인 내역 

XSS (5.2)	○ **게시판에 악성 자바스크립트 삽입 후 실행이 가능하여 악의적인 사용자가 일반 사용자를 대상으로 쿠키 정보의 탈취 및 개인정보 등을 탈취하는 피싱 공격이 가능한 취약점** ○ 진단결과 - 이용안내 〉 대시민 질의답변 〉 글쓰기 진행 시 임의의 스크립트 삽입 및 실행 가능	- GET 방식 통신인 경우, 요청 파라미터의 특정 문자열(자바스크립트 정의어 및 Event Handler) 수동 필터링 - POST 방식 통신인 경우, XSS 방어 라이브러리 중 언어에 맞게 택하여 필터링 적용 · JSP : Lucy-XSS Filter, OWASP ESAPI XSS Filter · PHP : HTML Purifier Library · ASP : MS Anti XSS Library, HTML Sanitizer Library	**미이행** - 사유 : 서울시 통합게시판을 사용하므로 조치 불가

2022 년 01 월 05 일

※ 이행여부 확인자(보안관제요원),확인자(담당공무원)

이행여부 확인자 : 소속 ㈜윈스 직위 주임 성명 안승환 (서명)

확인자 : 소속 정보통신보안담당관 직위 주무관 성명 소관수 (서명)