**모의 컨설팅 (https://demo.testfire.net/)**

|  |  |
| --- | --- |
| 구분 | 상세 내용 |
| 사이트 이름 | https://demo.testfire.net/ |
| 취약점 명 | 1) SQL Injection  2) XSS(Cross Site Scripting) |
| 취약점 설명 | 1) demo.testfire.net/login.jsp에서 아이디에 1' or 1=1 --를 입력하여 입력되는 SQL 질의가 무조건 로그인  2) demo.testfire.net/index.jsp의 상단 오른쪽 검색 기능에서 <script>document.write(document.cookie)</script>를 입력해서 XSS 취약점이 노출되는 것을 확인 |
| 취약점 해결 방안 | 1) SQL Injection  - DB 쿼리에 영향을 주는 경우 입력 값을 검증하여 차단 유도  - 저장 프로시저 사용(사용하고자 하는 쿼리 형식을 미리 지정)  2) XSS(Cross Site Scripting)  - 입력 값 제한(입력 값을 제한해서 스크립트를 삽입 못하도록 함)  - 입력 값 치환(<script>태그를 자주 사용하기 때문에 <, > 등의 문자를 치환해서 script를 일반문자로 인식해서 실행되지 않음  - 스크립트 영역에 출력 자제  - PLURA V5 XSS 필터 사용(XSS 공격이 발생할 때 공격자 IP를 차단) |