취약점 보고서

점검 요약

로그인 기능

- 검증 기능 및 쿼리 관리 부족, 그리고 유출하기 쉬운 관리자 계정 과 패스워드 사용으로 인한 관리자 계정 접근 성공.

검색 기능

- 입력 검증 기능 과 유효하지 않은 문자를 제거 또는 변경 하는 기능이 존재하지 않아 악의적인 작업 수행 가능.

발견한 취약점

1. 크리덴셜 스터핑 공격
2. SQL 인젝션 공격
3. 크로스 사이트 스크립팅(XSS)

취약점 분석

크리덴셜 스터핑 : ID : admin PW : admin

- 가장 잘 알려진 관리자 ID 및 PW 사용으로 인한 관리자 계정 접근 성공.

SQL 인젝션 : ID : admin’ OR 1=1 -- PW

- 상세한 에러 출력으로 인하여 사용자가 SQL 에러 메세지를 확인하고 공격 시도함.
- 입력 값이 SQL 명령어를 포함 하고 실행되면 원래의 쿼리가 조작되어 실행됨.

크로스 사이트 스크립팅 : <script> alert(document.cookie) </script>

- 검색 기능이 사용자의 입력 값을 출력함.
- 사용자의 입력 값이 HTML 스크립트 태그나 이벤트 핸들러일 경우 브라우저가 스크립트로 해석하고 실행함.

대응 방안

크리덴셜 스터핑

- 테스트나 관리를 위한 어드민 계정 생성시 잘 알려진 ID PW 사용을 지양하고 다중 요소 인증, 로그인 시도 모니터링, 기기 및 IP주소 기반 로그인 시도 제한 등을 구현하여 방어할 수 있습니다.

SQL 인젝션

- 사용자로부터 받은 입력을 검증하고 사전에 준비된 쿼리 사용, 또는 ORM을 사용하여 데이터베이스의 테이블을 클래스로, 레코드를 객체로 매핑하여 SQL 쿼리를 직접 작성하는 대신, 객체 지향적인 방식으로 데이터베이스 작업을 수행.

크로스 사이트 스크립팅

- 사용자의 입력 값을 검증하고 유효하지 않은 문자를 제거 또는 변경 후 실행하거나, 웹페이지에 사용자의 입력 값을 출력할 때 html 인코딩을 적용하여 브라우저가 스크립트로 해석하지 못하게 해야 합니다.