|  |  |
| --- | --- |
| 대외비 | 수신자 외 열람 불가 |
| 관리번호 | **${controlnumber}** |

테스트 리포트

2022-07-15T12:52:28.064083

CERT팀

1. 총평 요약

${review}

1. 취약점 점검 결과 등급

|  |  |
| --- | --- |
| **등급** | **${grade}** |
| **침해가능성[[1]](#footnote-1)** | **${possibility}** |

1. 취약점 점검 결과 요약

|  |  |  |  |
| --- | --- | --- | --- |
| **분류** | **세부 진단 항목** | **취약점 등급** | **점검결과** |
| 입력 값  검증 부재 | 1-1. XSS/CSRF 공격 가능성 | **중** |  |
| 1-2. SQL/Command Injection 공격 가능성 | **상** |  |
| 1-3. 검증되지 않은 리다이렉트와 포워드 | 하 |  |
| 취약한  파일처리 | 2-1. 악성코드파일 업로드 | **상** |  |
| 2-2. 중요 정보 파일 다운로드 가능성 | **중** |  |
| 취약한 인증  및  세션관리 | 3-1. 파라미터 값 및 쿠키 조작 가능성 | **중** |  |
| 3-2. 세션 재사용 가능성 및 타임아웃 설정 여부 | 하 |  |
| 3-3. 비인증 상태로 중요 page 접근 가능성 | 하 |  |
| 중요 정보  저장/전송  처리 미흡 | 4-1. 소스코드 내 주요정보 노출 여부 | 하 |  |
| 4-2. 요청 및 응답 값 내 주요정보 포함여부 확인 | **중** |  |
| 취약한 접근  통제 관리 | 5-1. 패스워드 정책 유무 및 반영 여부 | 하 |  |
| 5-2. 로그인 및 거래 시 인증 실패 횟수 제한 | **중** |  |
| 5-3. 관리자 페이지 노출 가능성 | 하 |  |
| 5-4. 검색엔진 정보 노출 가능성 | 하 |  |
| 5-5. 백업 파일 및 테스트 파일 존재 여부 | 하 |  |
| 부적절한  오류 처리 | 6-1. 오류페이지를 통한 정보 노출 여부 | 하 |  |
| 6-2. 일괄적인 오류 처리 페이지 존재 여부 | 하 |  |
| 취약한  보안설정 | 7-1. Client Request Method | 하 |  |
| 7-2. 파일 목록화 가능성 | 하 |  |
| 7-3. 취약한 TLS 버전 사용 여부 | **중** |  |
| 7-4. SSL/TLS Strip 가능 여부 | **중** |  |
| 기타 취약점 | 8-1. 취약점 진단 항목에 정의되지 않은 취약점 | 하 |  |

* **체크리스트 기준**

OWASP(Open Web Application Security Project) Top 10 – www.owasp.org

NIST(National Institute of standards and Technology) Web Application Check List – c/src.nist.gov

1. 침해 발생 시 서비스 장애 또는 개인정보 유출과 같은 기업의 이미지 또는 사업에 중대한 영향을 끼칠 수 있는 공격 방법의 난이도를 뜻함. *(난이도 단계: 쉬움->보통->어려움)* [↑](#footnote-ref-1)