|  |  |
| --- | --- |
| 대외비 | 수신자 외 열람 불가 |
| 관리번호 | **20220801174241-78P5** |

테스트 리포트

2022-08-01T17:42:41.433918

CERT팀

1. 총평 요약

여러모로 취약한거 같습니다.

1. 취약점 점검 결과 등급

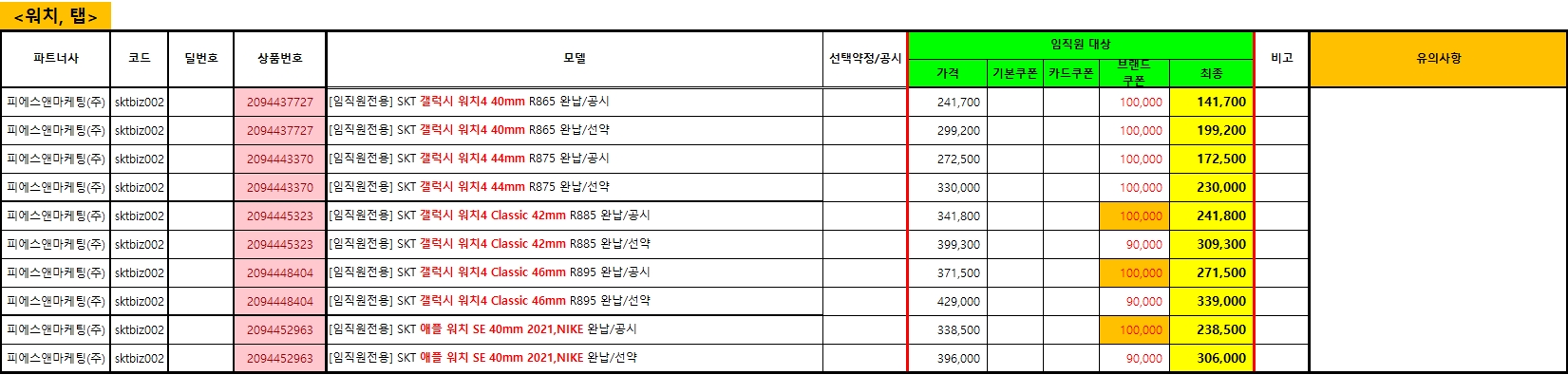
|  |  |
| --- | --- |
| **등급** | **FIRST** |
| **침해가능성[[1]](#footnote-1)** | **HIGH** |

1. 취약점 점검 결과 요약

|  |  |  |  |
| --- | --- | --- | --- |
| 분류 | 세부 진단 항목 | 취약점 등급 | 점검 결과 |
| XSS/CSRF 공격 가능성 | LOW | 취약 |
| SQL/Command Injection 공격 가능성 | LOW | 취약 |
| 검증되지 않은 리다이렉트와 포워드 | LOW |  |
| 입력 값 검증 부재 | CRLF 공격 가능성 | LOW |  |
| 악성코드파일 업로드 | LOW |  |
| 취약한 파일처리 | 중요 정보 파일 다운로드 가능성 | LOW |  |
| 요청 및 응답 파라미터 값 조작 가능성 | LOW |  |
| 비인증 상태 기능 사용 가능성 | LOW |  |
| 인증 값 중복/재사용 가능성 및 파기 여부 | LOW |  |
| 취약한 접근통제 및 인증 설정 | 관리자 서비스 분리 및 노출 여부 | LOW |  |
| 소스코드 내 주요 정보 저장 여부 | LOW |  |
| 주요 정보 저장/전송 처리 미흡 | 데이터 통신 간 정보 노출 여부 | LOW |  |
| 통신 구간 암호화 적용 여부 | LOW |  |
| 취약한 암호화 방식 사용 및 적용 관리 | 취약한 암호 알고리즘 사용 여부 | LOW |  |
| 오류페이지를 통한 정보 노출 여부 | LOW |  |
| 부적절한 오류 처리 | 일괄적인 오류 처리 페이지 존재 여부 | LOW |  |
| 패스워드 정책 유무 및 반영 여부 | LOW |  |
| 주요 기능 인증 실패 횟수 제한 | LOW |  |
| 서비스 기능 악용 가능 여부 | LOW |  |
| 백업 파일 및 테스트 파일 존재 여부 | LOW |  |
| 취약한 TLS 버전 사용 | LOW |  |
| HTTPS 통신 강제화 여부 | LOW |  |
| 쿠키 보호를 위한 설정 여부 | LOW |  |
| 파일 목록화 가능성 | LOW |  |
| 응답 헤더 내 서버 정보 노출 | LOW |  |
| 검색엔진 정보 노출 가능성 | LOW |  |
| 취약한 보안 기능 및 설정 | Client Request Method | LOW |  |
| 기타 취약점 | 취약점 진단 항목에 정의되지 않은 취약점 | LOW |  |

* + 1. 1-1. XSS/CSRF 공격 가능성
    2. 문제점

### 이슈를 작성합니다.

[그림1].캡션입력란

* + 1. 대응방안

### 잘 대응해야겠죠?

* + 1. 관련함수

### 환경설정 함수

### com.wemakeprice.com

### config()

* + 1. 1-2. SQL/Command Injection 공격 가능성
    2. 문제점

### 이슈를 작성합니다.

* + 1. 대응방안

### 리폰스를 등록합니다.

* + 1. 관련함수

### 환경설정 함수ㄴㄹㄴㅇㄹㄴㅇㄹㄴㅇㄹㅁㄴ

### com.wemakeprice.crpyto.com

### config()

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)