*2025년 CIA\_Web\_Sites 모의해킹*

*2025 / 01 / 20*

2024년 XXXX 모의해킹

모의해킹 결과 보고서 v0.1

목 차

1. 모의해킹 수행 정보 2

1.1. 개요 2

1.2. 대상 2

1.3. 수행 기간 2

1.4. 수행 인력 2

2. 모의해킹 결과 3

2.1. 총평 3

2.2. 결과 요약 4

3. 취약점 상세 내용 5

3.1. [대상 이름] (URL) 5

3.1.1. SQL Injection 5

4. 보안 권고안 7

4.1. SQL Injection 7

1. 모의해킹 수행 정보
   1. 개요

본 프로젝트는 [XXX]의 웹 애플리케이션에 대한 모의 해킹을 수행한 후 발견된 취약점에 대한 대응 방안을 제시함으로써 차후 발생할 수 있는 침해 사고를 예방하고 정보 보호 수준을 향상할 수 있는 대책을 수립하는 데 기여하는 것을 목적으로 합니다.

* 1. 대상

본 프로젝트 점검 대상은 다음과 같습니다.

|  |  |  |
| --- | --- | --- |
| No | Platform | URL |
| 1 | **WEB** | **~~~** |

* 1. 수행 기간

🡪 2022년 01월 1일 ~ 2022년 01월 2일

* 1. 수행 인력

|  |  |  |
| --- | --- | --- |
| 소속 | 성명 | 담당 업무 |
| SegFault | **xxx** | **- 웹 모의해킹** |

1. 모의해킹 결과
   1. 총평

본 시스템은 블라블라블라 뭐가 위험하다!

어떤 취약점이 존재하며, 이런저런 시나리오의 공격으로 어떤 위험이 발생할 수 있다!

니네 진짜 위험하거든?

(정중하게) 빨리 고치렴!

* 1. 결과 요약

|  |  |  |  |
| --- | --- | --- | --- |
| No | 대상 | 취약점 | 위치 |
| 1 | **XXX** | **SQL Injection** | **~~~** |
| 2 | **XXX** | **XSS** | **~~~** |

1. 취약점 상세 내용
   1. SFEnergy (http://normaltic.com:10000/)
      1. SQL Injection

|  |  |  |  |
| --- | --- | --- | --- |
| 구분 | 설명 | | |
| 발견URL | **URL** | **파라미터** | **메뉴** |
| https://r | num | 채용공고> 사무/영업 지원 |
| https://r | num |  |
| https:// | num |  |
| https:// | num |  |
| 취약점 상세내역 | 파라미터 값을 처리하는 애플리케이션에서 SQL 구문을 실행시킬 수 있는 문자에 대한 필터링 로직이 미흡하여 데이터베이스 정보를 조회하는 SQL 구문을 삽입 후 실행을 통해 데이터베이스에 저장된 정보 추출이 가능합니다. | | |

**1.** 로그인 페이지에 접속합니다.

텍스트이(가) 표시된 사진

자동 생성된 설명

**2.** 블라블라

텍스트이(가) 표시된 사진

자동 생성된 설명

**[보안 권고안]**

~~~~~ 잘 처리해야합니다.

1. 보안 권고안
   1. SQL Injection

|  |  |  |
| --- | --- | --- |
| 취약점 항목 | SQL Injection | |
| 취약점 개요 | 대화형 웹 사이트는 사용자의 입력 값을 이용하여 데이터베이스 접근을 위한 SQL 쿼리를 만들어 구현됨. SQL인젝션은 사용자의 입력 값으로 웹 사이트 SQL 쿼리가 완성되는 약점을 이용하며, 입력 값을 변조하여 비정상적인 SQL 쿼리를 조합하여 실행함. 비정상적인 SQL 쿼리로 DBMS 및 데이터(Data)를 열람하거나 조작 가능하므로 사용자의 입력 값에 대한 필터링을 구현하여야 함. | |
| 보안 조치 방법 | | |
| * 보안 조치 방법  1. 사용자 입력값 변수화 (PreparedStatemente)   ~~~~~~ | |