*2025년 모의해킹*

*2025 / 08 / XX*

2025년 모의해킹

모의해킹 결과 보고서 v1.0

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** | **http://192.168.128.128:1018/** |

* 1. 수행 기간

🡪 2025년 08월 06일 ~ 2025년 08월 10일

* 1. 수행 인력

|  |  |  |
| --- | --- | --- |
| 소속 | 성명 | 담당 업무 |
|  | **전예찬** | **- 웹 모의해킹** |

1. 모의해킹 결과
   1. 총평

본 시스템은 블라블라블라 뭐가 위험하다!

본 시스템은 SQL Injection으로 인한 DB 접근이 가능합니다.

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** |  |

1. 취약점 상세 내용
   1. Paint (http://192.168.128.128:1018/)
      1. SQL Injection

|  |  |  |  |
| --- | --- | --- | --- |
| 구분 | 설명 | | |
| 발견URL | **URL** | **파라미터** | **메뉴** |
| http://ctf.segfaulthub.com:4281/post.php | id | 게시판 |
| 취약점 상세내역 |  | | |

**[보안 권고안]**

**URL 파라미터 또는 XML 등 입력하는 부분에 SQL 구문 입력 후 서버에서 응답한 값에 대한 위험성 점검**

**SQL문으로 해석될 수 있는 값(글번호, 검색 내용 등)을 입력하여 데이터베이스내에 저장된 정보 열람 및 시스템 명령 실행가능 여부 점검**

**조작된 XPath 쿼리를 보내어 비정상적인 질의 가능 여부 점검 등**

Prepared Statement를 사용해 파라미터가 SQL 쿼리문에 동적으로 입력되지 않게 조치해야 합니다.

**또한 웹사이트 서버 동작을 위한 코드 작성이 마무리 되었을 경우에는 개발할 당시에 사용했던 에러 처리 구문으로 인해 내부 동작 로직이 노출되지 않게 삭제 처리를 하는 것이 좋습니다.**

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. SQL 쿼리에 사용되는 문자열의 유효성을 검증하는 로직 구현 2. 동적 SQL 구문 사용을 지양하며 파라미터에 문자열 검사 필수적용 (Prepared Statement) 3. 시스템에서 제공하는 에러 메시지 및 DBMS에서 제공하는 에러 코드가 노출되지 않도록 예외처리 4. 아래와 같은 특수문자를 사용자 입력 값으로 지정 금지  |  |  | | --- | --- | | 문자 | 설명 | | ‘ | 문자 데이터 구분기호 | | ; | 쿼리 구분 기호 | | --, # | 해당라인 주석 구분 기호 | | /\* \*/ | \*와 \*/ 사이 구문 주석 |   ~~~~~~ | |