Introduction of Command Injection and Practice

Student Jeongmin Lee

Introduction

본 보고서는 명령어 삽입 공격(Command Injection)에 대해 다루며, 수업에서 제공된 강의자료 및 유튜브 영상들을 참고하여 작성되었습니다. 부족하다고 판단되는 부분은 추가적으로 인터넷에서 관련 자료를 조사하여 내용을 보완하였습니다.

이를 통해 명령어 삽입 공격의 개념, 유형, 실제 사례, 그리고 이를 방지하기 위한 모범 사례에 대해 심도 있게 이해하는 것을 목표로 합니다.

What is Command Injection?

명령어 삽입 공격이란 웹 애플리케이션의 취약점을 악용하여 공격자가 임의의 시스템 명령을 실행할 수 있도록 하는 보안 취약점입니다. 이러한 공격은 사용자 입력이 적절하게 검증되지 않거나 필터링되지 않는 경우에 발생합니다. 공격자는 악의적인 명령어를 입력하여 시스템에서 원하지 않는 작업을 수행하거나 민감한 정보를 탈취할 수 있습니다.

명령어 삽입 공격은 SQL 삽입 공격과 유사합니다. 그러나 주요 차이점은 SQL 삽입이 데이터베이스에 SQL 명령을 삽입하는 반면, 명령어 삽입은 호스트 운영 체제에서 시스템 수준 명령을 실행할 수 있도록 한다는 점입니다. 다시 말해, SQL 삽입은 SQL 쿼리를 조작하여 데이터베이스를 대상으로 하는 반면, 명령어 삽입은 OS 수준에서 임의의 명령 실행을 허용하는 취약점을 악용합니다.

Objectives

The primary objectives of this paper are to:

- Define command injection and its various forms.
- Analyze real-world examples of command injection attacks.
- Discuss best practices for preventing command injection vulnerabilities.

Plan

The plan for this paper includes a detailed examination of command injection vulnerabilities, including their causes and effects. We will also explore various case studies to illustrate the real-world impact of these vulnerabilities and provide actionable recommendations for developers and organizations to mitigate the risks associated with command injection.