Week 3 – Vulnerability Introduction

This document introduces the concept of vulnerabilities in information systems and provides an overview of the OWASP Top 10, which lists the most critical security risks to web applications.

What is a Vulnerability?

A vulnerability is a weakness in a system, application, network, or process that can be exploited by an attacker to gain unauthorized access, disrupt services, or compromise data.

OWASP Top 10 (Overview)

- Broken Access Control – Failures in enforcing user permissions properly.
- Cryptographic Failures – Weak or missing encryption protecting sensitive data.
- Injection – Untrusted data sent to interpreters such as SQL or OS commands.
- Insecure Design – Lack of security controls in application design.
- Security Misconfiguration – Improperly configured servers, services, or apps.
- Vulnerable and Outdated Components – Using software with known vulnerabilities.
- Identification and Authentication Failures – Weak login and session handling.
- Software and Data Integrity Failures – Lack of integrity checks and updates.
- Security Logging and Monitoring Failures – Inadequate detection and response.
- Server-Side Request Forgery (SSRF) – Server fetching remote resources without validation.

Why the OWASP Top 10 Matters

The OWASP Top 10 helps developers, security professionals, and organizations understand the most common and impactful web application security risks, enabling them to prioritize mitigation efforts.