# **ASSIGNMENT - 1**

**NALADALA NAVYA**

**21BCE7791**

**WEB APPLICATIONS SECURITY RISKS**

1. **OWASP: A01: 2021 – Broken Access Control**

**CWE: CWE-285: Improper Authorization**

**Description:**

The product does not perform or incorrectly performs an authorization check when an actor attempts to access a resource or perform an action.When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information exposures, denial of service, and arbitrary code execution.

**Business Impact:**

CWE-285, Improper Authorization, poses a direct threat to businesses. It can expose sensitive data through unauthorized access, potentially leading to legal issues, revenue loss, and damaged reputation. Adhering to stringent authorization practices is pivotal for mitigating these risks and maintaining trust with stakeholders.



1. **OWASP: A09: 2021 – Security logging and monitoring failures**

**CWE: CWE-778: Insufficient Logging**

**Description:**

When a security-critical event occurs, the product either does not record the event or omits important details about the event when logging it.When security-critical events are not logged properly, such as a failed login attempt, this can make malicious behavior more difficult to detect and may hinder forensic analysis after an attack succeeds.For example, in Azure, the default value for logging is disabled.

**Business Impact:**

CWE-778, Insufficient Logging, carries significant business implications. Inadequate or absent logging hampers the detection of security incidents and breaches, delaying response efforts. This can result in prolonged unauthorized access, data compromise, and regulatory non-compliance. Robust logging practices are vital for prompt threat identification, reducing damage, and ensuring business continuity**.**

1. **OWASP: A08:2021 - Software and Data Integrity Failures**

**CWE: CWE-353: Missing Support for Integrity Check**

**Description:**

The product uses a transmission protocol that does not include a mechanism for verifying the integrity of the data during transmission, such as a checksum.If integrity check values or "checksums" are omitted from a protocol, there is no way of determining if data has been corrupted in transmission. The lack of checksum functionality in a protocol removes the first application-level check of data that can be used.

**Business Impact:**

CWE-353, Missing Support for Integrity Check, holds notable business consequences. Without mechanisms to verify data integrity, malicious tampering can go unnoticed, leading to compromised systems, erroneous decisions, and damaged trust. Establishing integrity checks is critical for upholding the reliability of operations and preserving customer confidence.

1. **OWASP: A03: 2021 – Injection**

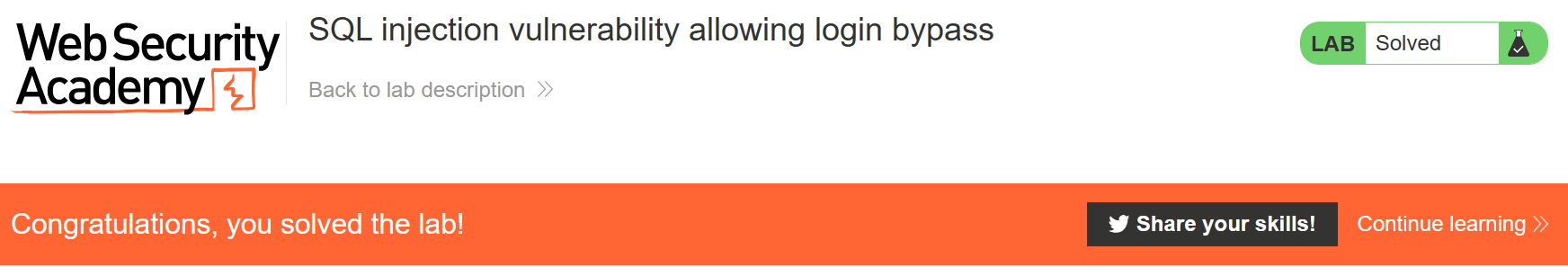
**CWE: CWE-94:Improper Control of Generation of code(‘code Injection’)**

**Description:**

The product constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.

**Business Impact:**

CWE-94, Improper Control of Generation of Code ("Code Injection"), poses critical business risks. Failing to control code generation can enable malicious code injection, leading to system manipulation, data breaches, and unauthorized access. This can result in operational disruption, compromised customer data, and legal consequences. Implementing strict input validation and secure coding practices is imperative to prevent code injection attacks and maintain the integrity of business operations.



1. **OWASP: A06: 2021 –Vulnerable and Outdated Components**

**CWE: CWE-1395: Dependency on Vulnerable Third-party Component**

**Description:**

The product has a dependency on a third-party component that contains one or more known vulnerabilities.For example, even an entire operating system might be from a third-party supplier in some hardware products. Whether open or closed source, these components may contain publicly known vulnerabilities that could be exploited by adversaries to compromise the product.

**Business Impact:**

CWE-1395, Dependency on Vulnerable Third-party Component, has substantial business implications. Relying on compromised external components can expose systems to security breaches, leading to data breaches, system downtime, and financial losses. Mitigating this risk through thorough component vetting and timely updates is crucial to ensure operational integrity and protect the company's reputation.