Final International University

“Software testing and validation” – Final Project

Nael Alyousefi - 1903060053

**Overview**

This report aims to address critical security issues discovered on your website related to authorization, input validation, and data deletion. These vulnerabilities pose a significant risk to your website's integrity, data confidentiality, and user trust. It is imperative to address these issues promptly to enhance the security posture of your website.

**1. Missing Authorization Checks**

Description: The website currently lacks proper authorization checks, which means that users may have access to functionalities and data they should not be able to access. This opens up a wide range of potential security vulnerabilities, such as unauthorized data access and misuse.

Suggestion: Implement a robust authorization system that verifies the identity and permissions of users before allowing them to access sensitive functionalities and data. Ensure that only authorized users can access, edit, or delete data.

**2. Acceptance of Invalid Input**

Description: The website currently accepts invalid input without adequate validation. This can lead to various security risks, including injection attacks (e.g., SQL injection, cross-site scripting), data corruption, and system instability.

Suggestion: Implement strict input validation for all user-generated content and user inputs. Use input validation libraries and frameworks to prevent malicious input from being processed by the application. Input validation should be applied both on the client and server sides.

**3.** **Unrestricted Data Deletion**

Description: The website allows users to delete approved data without sufficient checks and balances. This can result in the unauthorized removal of information, leading to data loss and compliance issues.

Suggestion: Ensure that only authorized users with appropriate permissions can delete data, and keep audit logs of all deletion activities for accountability and tracking.