Introduction

This report documents a basic vulnerability assessment conducted on a deliberately vulnerable test website as part of a Cyber Security Internship. The purpose of this assessment is educational and focuses on identifying common web security issues using safe, non-intrusive methods.

Scope

The assessment was limited to manual observation and analysis of publicly accessible pages of the target website. No exploitation, brute-force attacks, or intrusive testing techniques were performed.

Vulnerability 1: Missing HTTPS (Unencrypted Communication)

Description:
The website uses HTTP instead of HTTPS. This means data sent between the user and the server is not encrypted.

Impact:
An attacker could intercept sensitive information such as usernames and passwords.

Risk Level:
Medium
Recommendation:
Enable HTTPS by installing an SSL/TLS certificate to encrypt communication between users and the website.

Vulnerability 2: Reflected User Input (Lack of Input Validation)

Description:
The search functionality reflects user input directly on the webpage and includes it in the URL without proper validation.

Impact:
Improper input handling may allow attackers to inject malicious content, potentially leading to client-side attacks such as Cross-Site Scripting (XSS).

Risk Level:
Medium
Recommendation:
Implement proper input validation and output encoding to ensure user input is handled securely.

Conclusion

This vulnerability assessment identified basic security issues related to unencrypted communication and improper input handling. Although the assessment was limited to non-intrusive methods, the findings highlight the importance of secure configuration and input validation to protect web applications from common security risks.