Week-5

Asad Muhammad Channar

DHC-56

Task-1

Security Auditing

- Conduct a comprehensive security audit of the web application.
- Identify vulnerabilities using automated tools (e.g., OWASP ZAP) and propose mitigation strategies.

Security Auditing Report: Comprehensive Security Audit of Web Application

Introduction

This report presents the findings from a comprehensive security audit of the web application. The audit was conducted using automated tools, including OWASP ZAP, to identify potential vulnerabilities. Mitigation strategies are proposed to address the identified issues and enhance the overall security of the application.

Methodology

The security audit was conducted using the following methodology:
1. Automated Scanning: OWASP ZAP was used to scan the web application for common vulnerabilities.
2. Manual Verification: Identified vulnerabilities were manually verified to confirm their validity.
3. Risk Assessment: Each vulnerability was assessed for its potential impact on the application.
4. Mitigation Strategies: Recommendations were made to address each identified vulnerability.

Automated Scanning Results

The automated scan using OWASP ZAP identified several vulnerabilities. The following sections provide details on each vulnerability, including its description, risk level, and proposed mitigation strategies.

Vulnerability 1: Cross-Site Scripting (XSS)

Description: The application is vulnerable to Cross-Site Scripting (XSS) attacks, allowing attackers to inject malicious scripts into web pages viewed by other users.
Risk Level: High
Mitigation: Implement proper input validation and output encoding to prevent the injection of malicious scripts.

Vulnerability 2: SQL Injection

Description: The application is susceptible to SQL Injection attacks, enabling attackers to execute arbitrary SQL commands through input fields.
Risk Level: Critical

Mitigation: Use parameterized queries and prepared statements to prevent SQL injection attacks.

Vulnerability 3: Insecure Direct Object References

Description: The application allows direct access to objects based on user-supplied input, leading to unauthorized data access.
Risk Level: Medium
Mitigation: Implement access control checks to ensure users can only access resources they are authorized to view.

Vulnerability 4: Security Misconfiguration

Description: The application has misconfigured security settings, exposing it to potential attacks.
Risk Level: Medium
Mitigation: Review and update security configurations to follow best practices and reduce exposure to attacks.

Vulnerability 5: Sensitive Data Exposure

Description: Sensitive data is transmitted without proper encryption, making it susceptible to interception by attackers.
Risk Level: High
Mitigation: Ensure that sensitive data is encrypted during transmission using protocols like TLS.

Conclusion

The security audit identified several vulnerabilities in the web application. Implementing the proposed mitigation strategies will help to address these vulnerabilities and improve the overall security posture of the application. It is recommended to conduct regular security audits and continuously monitor the application for potential security issues.