Moniwell, SPC Communication Platform

Web Application Security Standards and Practices

Objective

This document outlines the comprehensive security standards and best practices implemented to safeguard the confidentiality, integrity, and availability of data for Moniwell web application. The security measures are designed to adhere to industry regulations, protect sensitive information, and ensure a robust defense against potential threats.

1. Data Encryption

All sensitive data, including customer information and login credentials, are encrypted in transit using industry-standard protocols such as TLS (Transport Layer Security). Furthermore, we have implemented AES256 encryption algorithm to encrypt data at rest. All the PII data that is being stored in the DB is being encrypted and provides data protection limiting exposure in breach scenarios.

2. Secure Development Practices

Adherence to secure coding practices and OWASP (Open Web Application Security Project) guidelines. Code reviews and static code analysis are conducted regularly to identify and remediate security flaws in the application code.

3. Security Headers and Configurations

Implementation of security headers, Content Security Policy (CSP), and other web server configurations to enhance the application's resistance against common web vulnerabilities like Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF).

4. Web Application Firewall (WAF)

Implementation of a Web Application Firewall to filter and monitor HTTP traffic between a web application and the Internet, providing an additional layer of security against various web-based attacks.

5. Security Incident Response Plan

A detailed incident response plan is in place to address and mitigate security incidents promptly. This includes a clear escalation path, communication plan, and post-incident analysis to prevent future occurrences.

6. Secure Third-Party Integrations

Thorough vetting and ongoing monitoring of third-party integrations to ensure they adhere to security standards. Regular security assessments are performed on third-party components.

7. Disaster Recovery and Business Continuity

Established processes for data backup, disaster recovery, and business continuity to minimize downtime and ensure the availability of critical services.

8. Continuous Improvement

Regular review of security policies and procedures to incorporate emerging threats and technologies. Continuous improvement initiatives to enhance the overall security posture of the application.

9. Continuous Monitoring

Continuous monitoring of the web application for security events, anomalies, and unauthorized activities. Security information and event management (SIEM) systems are utilized for real-time analysis.

10. Regular Software Updates

Prompt application of security patches and updates for all software components, including web servers, databases, and third-party libraries, to address known vulnerabilities.

11. Documentation and Knowledge Sharing

Comprehensive documentation of security policies, procedures, and best practices. Regular knowledge sharing sessions to keep the development team updated on emerging security threats and countermeasures.