RoadMap Based on 2017

1. **Awareness and Training**

- **Objective:** educate all stakeholders about web security risks.
- **Actions:**
  - Conduct training sessions for developers, testers, and management on the OWASP Top 10.
  - Create awareness programs to highlight the importance of secure coding practices.

2. **Risk Assessment**

- **Objective:** Identify and assess the specific risks to your applications.
- **Actions:**
  - Perform a risk assessment to understand the unique threat landscape of your organization.
  - Prioritize risks based on the OWASP Top 10 and your specific business context.

3. **Secure Development Lifecycle (SDLC) Integration**

- **Objective:** Incorporate security into every phase of the software development lifecycle.
- **Actions:**
  - Implement security requirements in the design phase.
  - Use threat modeling to identify potential vulnerabilities early in the development process.
  - Integrate security testing (SAST, DAST) into CI/CD pipelines.

4. **Addressing OWASP Top 10 Risks**

- **Objective:** Mitigate the risks identified in the OWASP Top 10.
- **Actions:**
  - **A1:2017 - Injection:** Use parameterized queries and ORM tools to prevent injection attacks.
  - **A2:2017 - Broken Authentication:** Implement multi-factor authentication and secure session management.
  - **A3:2017 - Sensitive Data Exposure:** Encrypt sensitive data in transit and at rest; use strong cryptographic practices.
  - **A4:2017 - XML External Entities (XXE):** Disable DTD processing and validate XML inputs.
  - **A5:2017 - Broken Access Control:** Enforce strict access controls and regularly review permissions.

- **A6:2017 - Security Misconfiguration:** Regularly audit configurations and apply security hardening practices.
- **A7:2017 - Cross-Site Scripting (XSS):** Sanitize and encode user inputs; implement Content Security Policy (CSP).
- **A8:2017 - Insecure Deserialization:** Avoid deserializing untrusted data; implement integrity checks.
- **A9:2017 - Using Components with Known Vulnerabilities:** Maintain an inventory of components; regularly update and patch.
- **A10:2017 - Insufficient Logging & Monitoring:** Implement comprehensive logging and monitoring; establish incident response plans.

5. **Testing and Validation**

- **Objective:** Ensure that security measures are effective.
- **Actions:**
  - Conduct regular security testing (penetration testing, vulnerability scanning).
  - Use automated tools to continuously monitor for vulnerabilities.
  - Perform code reviews focusing on security issues.

6. **Incident Response Planning**

- **Objective:** Prepare for potential security incidents.
- **Actions:**
  - Develop and document an incident response plan.
  - Conduct drills and simulations to test the effectiveness of the response plan.
  - Establish communication protocols for reporting and managing incidents.

7. **Continuous Improvement**

- **Objective:** Evolve security practices based on new threats and vulnerabilities.
- **Actions:**
  - Stay updated with the latest security trends and OWASP updates.
  - Regularly review and update security policies and practices.
  - Foster a culture of security within the organization, encouraging feedback and improvement.

8. **Compliance and Governance**

- **Objective:** Ensure adherence to relevant regulations and standards.
- **Actions:**
  - Identify applicable compliance requirements (e.g., GDPR, PCI DSS).
  - Implement necessary controls to meet compliance standards.
  - Conduct regular audits to ensure compliance and identify gaps.

Revision #1
Created 4 November 2024 19:35:20 by Admin
Updated 4 November 2024 19:36:24 by Admin