CyberSecurity MALAYSIA

MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

LGMS

SECURE DEVELOPMENT ANALYST

LEVEL
INTERMEDIATE

DURATION
3 DAYS

SiberKASA

TARGET PARTICIPANTS

- Application Developers
- Application Security Engineers
- Members of the information security team
- Individuals interested in Secure Coding Practices

REQUIREMENTS

There are no pre-requisite entry requirements. However, participants are required to bring their own laptop.

Insecure web application is one of the biggest causes of organizational data breaches. The number of attacks against web applications increase year by year.

Start securing your web applications by integrating secure coding practices into the software development lifecycle (SDLC). In general, it is much less expensive to develop secure applications than to remediate security vulnerabilities inherent in completed and deployed applications which could be the cause of data breaches.

LGMS' OWASP Top 10 & Secure Coding Practices training will cover technology agnostic secure coding practices that, if implemented, will mitigate at least the top 10 most common web application vulnerabilities.

Additionally, with our unique and extensive penetration testing experience, we will guide you through hacking and securing your web application from a hacker's perspective.

TERMINAL OBJECTIVES

1. To provide awareness and overview of secure coding practices to develop secure applications
2. To provide awareness of the OWASP Top 10 Web Application Security Risks
3. To comply with PCI DSS secure coding training requirements

AGENDA

Day 1 - OWASP Top 10

1. **Injection**
   Understand why & how injection vulnerabilities exist from technical point of view with lab/ hands-on demo. Prevent against injection flaws, such as SQL and OS injection
2. **Broken Authentication**
   Secure Implementation of authentication and sessions management
3. **Sensitive Data Exposure**
   Proper protection of sensitive data, such as personally identifiable information (PII) and the authentication credentials
4. **XML External Entities (XXE)**
   Understand why & how XXE vulnerabilities exist from technical point of view with lan/hands-on demo. Avoid untrusted data processed by a weakly configured XML parser
5. **Broken Access Control**
   Access control checks or protection to prevent access to unauthorized data

Day 2 - OWASP Top 10

1. **Security Misconfiguration**
   Define, implement and maintain secure configurations
2. **Cross-Site Scripting (XSS)**
   Understand why & how XSS vulnerabilitis exist from technical point of view with lab/ hands-on demo. Input validation and output encoding to prevent XSS attacks
3. **Insucure Deserialization**
   Understand why & how insecure deserialization vulnerability exist from technical point of view with lab/hands-on demo. Identify and avoid the use of serialized objects from untrusted sources.
4. **Using Components with Known Vulnerabilities**
   Identify and avoid the use of components with known vulnerabilities
5. **Insufficient Logging and Monitoring**
   Proper implementation of logging & monitoring.

Day 2 - OWASP Top 10

1. **Security Misconfiguration**
   Define, implement and maintain secure configurations
2. **Cross-Site Scripting (XSS)**
   Understand why & how XSS vulnerabilities exist from technical point of view with lab/ hands-on demo. Input validation and output encoding to prevent XSS attacks
3. **Insecure Deserialization**
   Understand why & how insecure deserialization vulnerability

GET IN TOUCH

03 - 8800 7999

training@cybersecurity.my

www.cyberguru.my

exist from technical point of view with lab/hands-on demo. Identify and avoid the use of serialized objects from untrusted sources.

4. **Using Components with Known Vulnerabilities**

   Identify and avoid the use of components with known vulnerabilities

5. **Insufficient Logging and Monitoring**

   Proper implementation of logging & monitoring.

Day 3 - Secure Coding Practices (OWASP ASVS)

1. **Architecture, Design and Threat Modelling**

   Secure principles must be built in and be innate to all applications in aspects of any sound security, architecture, availability, confidentiality, processing integrity, non-repudiation, and privacy

2. **Authentication**

   Establishing or conforming someone (or something) as authentic and that claims made by a person or about a device are connect, resistant to impersonation, and prevent recovery of interception of password

3. **Session Management**

   Ensure session management is properly implemented

4. **Access Control**

   Ensure access control is tighten and align with business functional requirements

5. **Validation, Sanitization and Encoding**

   Proper implementation of validation, sanitization and encoding can eliminate more than 90% of all injection type vulnerabilities.

6. **Stored Cryptography**

   Ensure secured and proper cryptography algorithm is used in protection sensitive data

7. **Error Handling and Logging**

   High quality logs will often contain sensitive data, and must be protected as per local data privacy laws or directives

8. **Data Protection**

   Application is responsible for ensuring data stored in encrypted and cannot be easily illicitly obtained, altered or disclosed

9. **Communications**

   Secure communication configuration should be periodically checked to ensure that the configuration is always present and effective

10. **Malicious Code Verification**

    Best efforts should be undertaken to ensure that the code has no inherent malicious code or unwanted functionality

11. **Business Logic**

    High value business logic flows must consider abuse cases and malicious actors. Ensure business logic requirements are properly align with the technical implementation

12. **File and Resources**

    Ensure untrusted file is handled accordingly and in a secure manner

13. **API and Web Services**

    Effective security controls for all API types, including cloud and Serverless API

14. **Configuration**

    Configuration of the application out of the box (default configuration) should be safe to be on the internet, secure-by-default configuration.

GET IN TOUCH

03 - 8800 7999

training@cybersecurity.my

www.cyberguru.my