
OWASP Training Datasheet

# Application Security
# OWASP Training Datasheet

## APPLICATION SECURITY OWASP TRAINING

- Course overview
    - Students will gain valuable insight in to threats that are part of the OWASP Top 10 2013.
    - This is a language agnostic course that dives into the concepts around web application threats, vulnerabilities and strategies to mitigate them.
    - The course dives into each of the Top 10 items, providing easy to understand conceptual ideas, newsflashes demonstrating how these vulnerabilities have resulted in real exploits against organizations and recommendations to defending them.
- Learning Objectives
    - Express the vulnerabilities and exploits affecting modern web applications. Learn about the OWASP Top 10 2013 covering all aspects of the application.
    - Identify vulnerabilities; understand why they happen, what are exploits and what are defenses.
    - Evaluate how real organizations have been affected by these exploits.
    - Rise security awareness and get a good grasp on core security principles.

- Training may be provided on site, or online.
- A mini test is available to validate students understating of core principles.

## OUTLINE AT A GLANCE

### 1. Injection

- SQL injection
- OS and other types of injection
- Real world examples
- Defense tactics

### 2. Broken Authentication and Session Management

- Authentication and session management schema
- Targeting privileged accounts
- Real world examples
- Defense tactics

### 3. Cross-Site Scripting (XSS)

- What is XSS and why is it so persistent
- Different types of XSS
- Real world examples
- Defense tactics

### 4. Insecure Direct Object References

- What is it and why it occurs
- Direct references to restricted resources
- Real world examples
- Defense tactics

### 5. Security Misconfiguration

- Danger of default
- Misconfigurations across OSI model
- Real world examples
- Defense tactics

### 6. Sensitive Data Exposure

- Sensitive data in motion and rest
- Unintentional data exposure
- Real world examples
- Defense tactics

### 7. Missing Function Level Access Control

- Misconfigured systems
- Code checks
- Real world examples
- Defense tactics

### 8. Cross-Site Request Forgery

- Attacking authenticated users
- Security vs convenience
- Real world examples
- Defense tactics

### 9. User Components with Known Vulnerabilities

- 3rd party frameworks and libraries
- Why is it so widespread
- Real world examples
- Defense tactics

### 10. Unvalidated Redirects and Forwards

- How is it used for phishing
- HTTP response codes
- Real world examples
- Defense tactics

## WAT CAN WE DO FOR YOU?

We understand application security. We breathe it. We strive to provide you with the best training experience for your staff.

Our experience helping our clients research and manage real world security risks allows us to drive our training material with the latest threats and vulnerabilities seen in every day engagements.

What does that mean? It means that your staff is ready to respond to with forward thinking concepts to securing your business' most sensitive applications.

## HERE TO HELP

Reach out to Demyo advisor who can help.

Alan Kakareka, CISSP, GSEC, CEH, LPT
President @ Demyo, Inc.
Email: almaz@demyo.com
Viber, WhatsApp: +1 201 665 6666
Miami, Florida, USA.
www.demyo.com