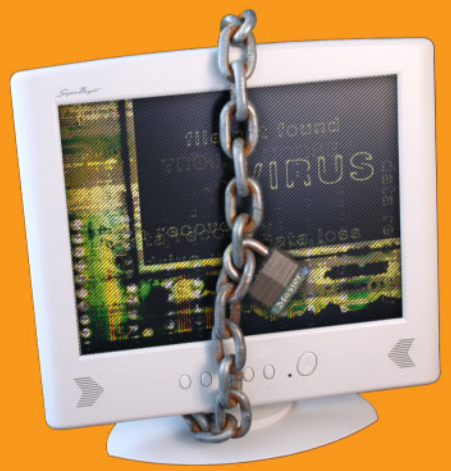
CyberSecurity MALAYSIA

An agency under MOSTI

ISMS SIRIM UKAS

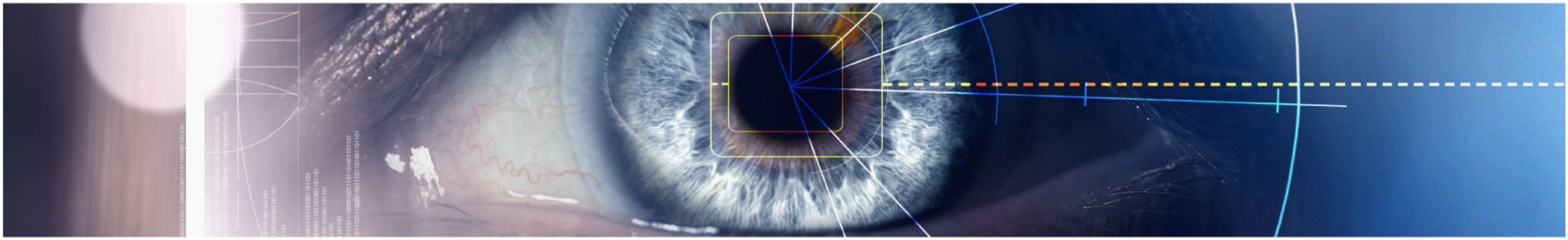


WEB APPLICATION SECURITY

Building Secure Web Applications in Java/J2EE

February 17 - 19 2009

CyberSecurity Malaysia, Kuala Lumpur Malaysia



WEB APPLICATION SECURITY

February 17 - 19 2009
CyberSecurity Malaysia, Kuala Lumpur Malaysia

Course Description

This course teaches the students how to develop secure web applications in today's complex internetworked environment. Students will receive a deep and thorough understanding of the most prevalent and dangerous security defects in today's applications. Additionally, they will learn practical and actionable guidelines on how to remediate against these common defects in Java/J2EE and how to test for them in their own applications.

This class starts with a description of the security problems faced by today's software developer, as well as a detailed description of the Open Web Application Security Project's (OWASP) "Top 10" security defects. These defects are studied in instructor-lead sessions as well as in hands-on lab exercises in which each student learns how to actually exploit the defects to "break into" a real web application. (The labs are performed in safe test environments.)

Remediation techniques and strategies are then studied for each defect. Practical guidelines on how to integrate secure development practices into the software development process are then presented and discussed.

Intended Audience

The ideal student for this tutorial is a hands-on web application developer or architect who is looking for a fundamental understanding of today's best practices in secure software development.

Presented by An IT Security practitioner with over 20 years of experience in the academic, military, and commercial sectors, including the U.S. Department of Defense and Carnegie Mellon University

To register and obtain further information, please contact Training Department
Tel: 03-8946 0999 Fax: 03-8946 0844 Email: training@cybersecurity.my

Curriculum

Day One

08:30 Registration & Morning Coffee

09:00 Preparation Phase: Understanding the Problem
- What are the issues that result in software that is susceptible to attack?
- Why do software developers continue to develop weak software?

10:30 Overview of available solutions
- Top-level discussion of best practices for developing secure software
- Security activities that can be integrated throughout a typical software development lifecycle

11:00 Morning Refreshments

11:15 Lab setup and demo
- Students install and configure software tools to be used in the upcoming exercises
- The instructor demonstrates the tools and runs through a sample exercise to ensure all students can use the tools correctly
- Review of web application basics
  - o HTTP methods (e.g., GET, POST)
  - o Identification and authentication
  - o Session management

12:00 Lunch

13:00 Exploiting web application weaknesses
- Introduction to OWASP top 10 (and other) security weaknesses in web applications
- How do attackers exploit these weaknesses?
- Class exercises of the most common web application weaknesses

15:00 Afternoon Refreshments

15:15 Exploiting web application weaknesses, continued
- Continued demonstration and class exercises of web application weaknesses

16:45 Questions and Answers

17:00 Close of Day One

Day Two

08:30 Registration & Morning Coffee

09:30 Secure development processes
- A detailed look at three common secure development methodologies, and their strengths and weaknesses
  - o Microsoft's SDL
  - o Cigital's Touchpoints
  - o OWASP's CLASP
- Group discussion of the feasibility of the processes

11:00 Morning Refreshments

11:15 Introduction to design review exercise
- Group exercise to review an example of a flawed design for security weaknesses

12:00 Lunch

13:00 Processes in depth – Design review
- Architectural risk analysis in detail
- Attack resistance
- Ambiguity analysis
- Weakness analysis
- Compare and contrast common processes for reviewing designs

15:00 Afternoon Refreshments

15:15 Architectural and design exercises
- Team exercise to review a flawed design using the processes described
- Abuse cases and design flaws

16:00 Processes in depth – Static code analysis
- Description of static code review processes
- Automated vs. peer review comparison of benefits and weaknesses
- Background of available automated static code review tool technology
- Integrating a static code review tool into a software development process effectively

16:45 Questions and Answers

17:00 Close of Day Two

Day Three

08:30 Registration & Morning Coffee

09:30 Static code analysis exercise
- Group exercise in which a simple program is analyzed using a commercial static code analysis tool
- The results are reviewed and analyzed by the class
- Group discussion about how to best utilize a static analysis tool

11:00 Morning Refreshments

11:15 Processes in depth – Security testing
- Black box vs. white box security testing of software
- Overview of common testing methodologies and tools
- Penetration testing
- Fuzz testing
- Dynamic validation

12:00 Lunch

13:00 Getting started
- Key elements to succeeding with a software security initiative
- Developing an action plan
- First steps

15:00 Afternoon Refreshments

15:15 Group discussion and questions
- Checklist of actions to be taken
- What questions remain unanswered?
- Lists, books, URLs, etc., for additional reading

17:00 Certificate of Attendance Presentation

17:30 Close of class

Program Facilitator

Mr. Kenneth Van Wyk is an internationally-recognized information security expert and author of the O'Reilly and Associates books, Incident Response and Secure Coding. Apart from providing consulting and training services through his company, he currently holds numerous positions: as a monthly columnist for the online security portal, eSecurity-Planet and is a Visiting Scientist at Carnegie Mellon University's Software Engineering Institute.

He is an IT Security practitioner with more than 20 years of experience in the academic, military and commercial sectors. He has held senior and executive technologist positions at Tekmark, Para-Protect, Science Applications International Corporation (SAIC), in addition to the U.S. Department of Defense and Carnegie Mellon and Lehigh Universities.

He also serves as an elected member of the Steering Committee and Board of Directors for the Forum of Incident Response and Security Teams (FIRST) organization. At the Software Engineering Institute of Carnegie Mellon University, he was one of the founders of the Computer Emergency Response Team (CERT®).

He holds an engineering degree from Lehigh University and is a frequent speaker at technical conferences. To date, Ken has presented papers and speeches for CSI, ISF, USENIX, FIRST and AusCERT, among others. Ken is also a CERT® Certified Computer Security Incident Handler.

Requirements

Each student will need to provide a laptop computer for the hands-on lab exercises. Recommended configurations include the following:

- Windows, Linux, or Mac OS X
- Local administrative privileges for installing and configuring software
- Java development environment (Sun SDK and Eclipse IDE recommended, although other SDKs and IDEs will work)
- Approximately 5 gigabytes of available disk space
- 1 gigabyte of RAM is recommended

Participant Mix

Advanced Web Application Security Essentials is designed for software developers who design, implement and / or test web applications using Java and related web application technologies.

CyberSecurity MALAYSIA

WEB APPLICATION SECURITY

Date : February 17 - 19 2009
Venue : Training Lab 1,
CyberSecurity Malaysia,
Mines Waterfront Business Park
Time : 9:00am - 5:00pm

Please complete this registration form and fax it back to [03] 8946 0844 or e-mail it to training@cybersecurity.my

Fee

- Investment Fee RM3,500 per delegate

The registration fee is payable in advance and inclusive of luncheon(s), refreshments, program materials, and certificate of attendance.

Due to limited seats reserved, an early confirmation of the reservation is HIGHLY advised. CyberSecurity Malaysia will only be able to confirm your reservation after the payment has been received.

To register

Contact Training Department:
Tel: [03] 8946 0999
Fax: [03] 8946 0844
E-mail: training@cybersecurity.my

Venue & Accommodation

Hotel accommodation and travel expenses are not included in the program fee.
If you have any physical access or dietary restrictions, please contact us at training@cybersecurity.my to notify us of your needs.

Training Registration Form

Designation: Mr. / Ms. / Mrs. / Dr. / Prof. / Other_____

Name
_____
Email
_____
Designation
_____
Fees(RM)
_____
Course/Programme
_____
Course Date
_____
Name of Organization
_____
Type of Organization(Goverment/Non-Goverment/Other)
_____
Address Of Organization
_____
_____
_____
Tel
_____
Fax
_____
Contact Person For Billing
_____
Email(Person For Billing)
_____
Billing Address(if different from above)
_____
_____
_____

_____ _____
Authorised Signatory/Name Company Stamp

_____
Date

For Official Use

Registration No: _____ Business Partner:_____
Promotion Index: _____ ☐ Tier 1 ☐ Tier 2
Your ***Training*** is
☐ Confirmed
☐ Postpone to _____
☐ To be advised _____

Term and Conditions

Confirmation of Reservation:

1. Reservation will only be confirmed upon receipt of a Purchase Order or Full Payment of Course Fee.
2. Cheque should be crossed and made payable to **"CyberSecurity Malaysia".**
3. Electronic Bank Transfer

Please remit the transfer to:

Account Name	: CyberSecurity Malaysia
Bank Name	: Malayan Banking Berhad
Account Number	: 5644 1870 5280
Swift Code	: MBBEMYKL
Bank Address	: Lot. No 1, G-1, G-2, Ground Floor, Support Services Building, 57000, Bukit Jalil, Kuala Lumpur, Malaysia

Withdrawal of Reservations:

1. If written notice of withdrawal is given 7 calendar days before course/program commencement, full refund of course fee will be entitled.
2. If written notice of withdrawal is given less than 7 calendar days before course/program commencement, a 50% penalty charge will be levied.*
3. Refund will not be entertained for **No Show** cases.* - * Replacement is allowed.

Cancellation of course:

1. CyberSecurity Malaysia reserves the right to amend or postpone courses.

Award of Certificates:

1. Certificate of Attendance will be awarded to participants with a minimum 75% attendance.
2. Certificates MUST be collected within three months upon notification.

Others

1. All participants are to observe the Copyright Law on intellectual properties such as software and courseware.
2. All classes will be conducted at our training venue, from 9am to 5.00pm, unless specified.

ACCEPTANCE

We hereby agree to abide by the terms and conditions and the course schedule as stipulated by CyberSecurity Malaysia.

CyberSecurity Malaysia (726630)
Level 4, Block C
Mines Waterfront Business Park
No. 3, Jalan Tasik, The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
MALAYSIA
Tel: 603-8946 0999
Fax: 603-8946 0844
www.cybersecurity.my

An agency under
MOSTI

ISMS SIRIM
UKAS