OWASP AppSec Asia Pacific 2012 Training

Building Secure Web Applications

Web application security breaches on websites of major corporations and government entities have received significant media attention due to large number of users affected and the leaking of sensitive personal information.

This training will show how to develop secure Web applications and covers security aspects of the full software development life cycle (SDLC). Participants will learn about general security concepts and review common risks, including OWASP's Top 10 list, assess the technical and business impact of security risks and apply mitigation strategies. The training includes several hands-on labs covering implementation, white-box analysis and black-box testing for security. While most code examples use PHP, MySQL and JavaScript, the content is equally applicable to other programming languages and database engines.

Participants are welcome to bring Web applications or code samples for review during the training also.

Training outline

I. Introduction

Topics covered:
Security concepts
Real-world examples of successful attacks
Security in the software development life cycle
Infrastructure vs. application security
Layers of protection

Learning objectives:
Understand the security landscape, the impact of security breaches in Web applications, the types of attack vectors and methods of protection at different layers.

II. Common risks explained

Topics covered:
Attack types and common risks, including OWASP's Top 10 list and how multiple relatively harmless vulnerabilities can be combined to form an effective attack. Detailed exploration of Cross-Site Scripting

(XSS), Cross-Site Request Forgery (CSRF), HTTP Response Splitting, SQL injection, command injection, path traversal, and insecure direct object references.
Learning objectives:
Understand common risks in Web applications and what risks they present to the user and the website owner. Understand the most frequent and serious attacks in detail and know how to secure Web applications against these.

III. Tools to the rescue

Topics covered:
Overview of how tools help with building and running secure Web applications, including code libraries and frameworks, penetration testing and static code analysis tools intrusion detection systems/intrusion prevention systems (IDS/IPS).

Learning objectives:
Understand what tools are available to help during the full life cycle of a Web application, from specification and design, development and testing to protecting against common attacks at runtime.

Course materials

Presentation slides and supporting materials will be made available in PDF format.

Instructor

Klaus Johannes Rusch is a certified IT architect and manager at IBM, heading the Web Effectiveness group in the Global Web Services organization, which provides consulting services to business units in IBM for optimizing the Web experience as an in-house agency. Previously he was a team leader on the IBM Corporate Webmaster team that manages www.ibm.com.

Klaus Johannes Rusch has over 20 years of application development experience and a track record of hacking web applications. He received an award for best website back in 1995. He holds an MSc

degree in computer science from Vienna University of Technology and was an adjunct professor of computer science at Webster University, where he taught web development and web animation. He lives in Vienna, Austria with his wife and two kids, and online at http://klausrusch.atmedia.net/.