“Bulletproof Web – Securing Your Web Applications”
Course Version: 1.0

Instructor Admir Tuzovi

E-mail admirtuzovic@gmail.com

Web http://blog.dilla.ba

LinkedIn http://ba.linkedin.com/in/tuzza

Twitter https://twitter.com/xdiler

Version	Change description	Date
1.0	Course Agenda adjusted; Added Final Exam and Course Evaluation.	09.09.2014

Description:

Common aspect of web development that both developers new to the web and those with experience share in common is how to properly implement the security on server, framework, and application and user level.

Open Web Application Security Project (OWASP) defines some of the most frequent security exploits that web applications should be safe-guarded against, by teaching the developers on how to preemptively implement security best practices and thus prevent the attack long before it has even happened.

This course is focused on risks and challenges involved with development of web applications. Throughout all lessons, several important topics such as authentication, rights management, intrusion detection and prevention, protecting sensitive data, cryptography, securing communication, preventing information leakage, etc. will be covered.

During the course, at the end of each lesson, lesson-related attacks will be carried out on web application that is deployed in demo environment in order to demonstrate the damage risks that arise from lack of proper protection.

For each type of attack, one or more prevention methods will be explained. Furthermore, for .NET developers, source code for both unsafe and secure implementations will be available for download.

Goals:

Show practical demonstration on how some of the well-known exploits can be used to jeopardize safety and compromise the integrity of publicly available web applications.

Explain the origins and mechanisms behind each of the security threats in details.

Provide explanations of one or more methods that can be used to mitigate each of the attacks. Demonstrate the expected behavior when the attack has been successfully repelled.

Provide basic source code that can be used as first-aid (.NET only).

Raise awareness of attendees on lurking threats on the web and provide guidelines on where to look for help if needed.

Introduce latest security best-practices and standards.

Requirements:

Course is designed for both web developers who are actively working on projects that are available to broader audience (internet) and developers who are about to start developing for the web.

Elementary knowledge of HTTP, HTML, JavaScript, T-SQL and at least one of the languages for server-side web development is recommended for optimal understanding of course materials.

.NET framework is platform used for examples.

Number of attendees:

Minimum of 10 attendees are required for course to be scheduled.

Maximum of 20 attendees can be present at single session.

Course Agenda:

Course length spans to 12 lessons, encapsulating threats as defined in OWASP TOP 10 2013 specification, as well as new authentication/authorization mechanisms such as OAuth 2.0 and CBAC.

Below is overall description of each of the courses modules with topics that will be covered during each.

Lesson	Topic(s)	Day	Duration
SESS #1-1	Introducing Lecturer; Course Agenda Overview; Attacker Profiling; Introducing OWASP; Defense in Depth; Google Dorks; 0-Day;	Thu	1h
SESS #1-2	Broken Authentication and Session Management; HTTP Session Anatomy; Session Fixation; Dealing with the Passwords; Multi-Factor Authentication; Single Sign-On;	Thu	1h
SESS #2-1	Sensitive Data Exposure; Cryptography; Transport Layer Security; PKI; Man-In-The-Middle; PCI;	Sat	1h
SESS #2-2	Cross-Site Scripting (XSS); Content-Security-Policy; WYSIWYG Sanitizing;	Sat	1h
SESS #2-3	Cross-Site Request Forgery (CSRF); UI-Redress (Clickjacking);	Sat	1h
SESS #3-1	SQL Injection; ORMs;	Tue	1h
SESS #3-2	Unvalidated Redirects and Forwards; Phishing;	Tue	1h
SESS #4-1	Security Misconfiguration; Error Handling; Securing Cookies; Server Hardening; Using Components with Known Vulnerabilities; Heartbleed; Dependency Validation;	Thu	1h
SESS #4-2	Insecure Direct Object References; Parameter Tampering;	Thu	1h
SESS #5-1	Missing Function Level Access Control; Presentational Access Control; Introduction to Claims-Based Access Control (CBAC);	Sat	1h
SESS #5-2	Introduction to OAuth 2.0	Sat	1h
SESS #5-3	Final exam; Course evaluation;	Sat	1h

Resources:

Course materials => http://blog.dilla.ba

Evaluation:

Final exam will contain set of choice-based questions that will test general understanding of attacks and defense methods which will be covered in-depth during the course runtime. Exam will run for approximately 30 minutes.

Upon course completion, attendees will be provided with course evaluation inquiry sheet in order to provide feedback about quality of the course and lecturer.