

WhiteHat Education Services

Education Services Overview & Course Offerings

courses

Web application security is critically important - today, over 70% of hacker attacks worldwide are actively targeting Web applications. In this rapidly evolving landscape, professionals in many roles, including developers, IT, management, and information security, all have an important part to play in Web application security. Our courses provide the up-to-date knowledge and skills required to understand and deliver meaningful security measures.

WhiteHat has a unique position within the industry – our WhiteHat Sentinel Service provides continuous, precise security assessments on hundreds of production Web applications on the Internet. Our experience in finding and analyzing vulnerabilities within such a broad and deep collection of real-world Web applications is unmatched. As a result, our courses incorporate the enormous wealth of experience from WhiteHat's core business.

Benefits

- Learn how to identify and fix website vulnerabilities
- Discover which coding errors make you vulnerable to attack
- Understand hacker's tools and techniques
- Experience hands-on training using real-world Web applications
- Learn how to make your code secure

About Our Instructors

Our classes are taught by seasoned Web application security professionals with many years of experience in developing Web applications for a variety of industries, providing security solutions to both large and small corporations. Our instructors are active contributors to the community, participating in standards bodies such as the Web Application Security Consortium (WASC) and the Open Web Application Security Project (OWASP). WhiteHat instructors leverage the unique insights offered by WhiteHat's continuous security assessment of hundreds of production Web applications. Our instructors have identified new classes of Web application attacks, published proof of concept attacks, books, articles, and blogs, and are frequent speakers at Web application security conferences.

Contact

WhiteHat Security also offers on-site education sessions for groups of 20 or more. Public courses are also available to individuals in cities across the country. To find out more about WhiteHat Education Services course curriculum, contact our corporate office at 408.343.8300.

Course Summaries

Introduction to Web Application Security

This workshop is available in a one or two-day format. It provides an overview of the fundamental principles of Web application security. It presents students with an understanding of how Web applications work, how vulnerabilities manifest in them, how to find and exploit those vulnerabilities, and solutions for protecting Web applications.

Secure Coding for Java Developers

This two-day course is designed to show Web application developers the dangers of insecure coding practices, specific ways their code can be exploited, and how to write code to avoid introducing vulnerabilities. This highly practical, interactive course will focus on secure coding techniques and methodologies that can be immediately applied in your applications. The class uses real-world examples, walking through real code samples, using live, feature rich applications, and showing how to hunt down, debug, and mitigate these flaws with better coding practices.

.NET

The two-day course is designed to implement security as a culture amongst the developers and will also include two main components: a review of the secure coding guidelines for .Net as well as .Net specific features like anti-XSS library. This highly practical, interactive course will focus on secure coding techniques and methodologies that can be immediately applied in your applications. The class uses real-world examples, walking through real code samples, using live, feature rich applications, and showing how to hunt down, debug, and mitigate these flaws with better coding practices.

WhiteHat Education Services

Secure Coding for Java Developers

overview

Course Summary

This two-day course uses a combination of theory, practical examples, and hands-on training. It is designed to show Web application developers:

- *The dangers of insecure coding practices*
- *Specific ways their code can be exploited*
- *How to write code to avoid introducing vulnerabilities*

This highly practical, interactive course will focus on secure coding techniques and methodologies that can be immediately applied in your applications. The class uses real-world examples, walking through real code samples, using live, feature rich applications, and showing how to hunt down, debug, and mitigate these flaws through better coding practices.

Benefits

- *Learn how hackers attack Web applications*
- *Discover how these attacks work*
- *See what coding mistakes make you vulnerable*
- *Learn how to make your code secure*

Who Should Attend

- *Java developers, architects, QA staff*

Duration

Available as a two-day workshop

Prerequisites

- *Must understand Java programming*
- *Familiarity with Web Application development (HTML, servlets, .JSP) is required*
- *Comfort with any major Java IDE (NetBeans, IntelliJ, Eclipse, etc.) is required*
- *Familiarity with TomCat, or comparable servlet container, is required*
- *Familiarity with Java command line interface is required*
- *Familiarity with encryption and SSL is helpful, but not required*

Structure

A combination of theory, practical examples, and hands-on training.

Contact

WhiteHat Security also offers on-site education sessions for groups of 20 or more. Public courses are also available to individuals in cities across the country. To find out more about WhiteHat Education Services course curriculum, contact our corporate office at 408.343.8300.

Secure Coding for Java Developers

Defining the Attacks

Inherent Problems and Limitations of Internet Architecture

- *HTTP request/response flow*
- *Session management*
- *Cookies*
- *Encoding/Decoding URLs, character sets, and HTML entities*

Looking at Vulnerabilities in Java Code

- *How people exploit Web applications*
- *Why you can never trust anything that comes from the client*

Components of Writing Secure Code

The following modules cover seven core areas of concern for writing secure Java code for Web applications:

- *Input handling*
- *Authentication and session management*
- *Access control/authorization*
- *Exception handling and logging*
- *Encryption*
- *General Java mechanics*
- *Bypassing business logic flow*

For each of these areas, the course will cover:

- *Theory and basics*
- *Recommended security practices*
- *"Gotchas" and implementation concerns*
- *Example exploits*
- *Hands-on exercises, where the students will find, exploit, debug, and fix security flaws in Java code*

WhiteHat Education Services

.NET

overview

Course Summary

The two-day course is designed to implement security as a culture amongst the developers and will also include two main components:

- A review of the secure coding guidelines for .Net
- As well as .Net specific features like anti-XSS library

This highly practical, interactive course will focus on secure coding techniques and methodologies that can be immediately applied in your applications. The class uses real-world examples, walking through real code samples, using live, feature-rich applications, and showing how to hunt down, debug, and mitigate these flaws through better coding practices.

Benefits

- Illustrate how Web applications are attacked by hackers
- Show how these attacks work
- Show coding mistakes that make you vulnerable to attacks
- Demonstrate how to make your code secure

Who Should Attend

.NET developers, architects, QA staff

Duration

Available as a two-day workshop

Prerequisites

- Must understand .NET framework and ASP.NET programming
- Familiarity with Web application development (HTML, .NET framework)
- Comfort with Visual Studio
- Familiarity with IIS
- Familiarity with encryption and SSL is helpful, but not required

Structure

A combination of theory, practical examples, and hands-on training.

Contact

WhiteHat Security also offers on-site education sessions for groups of 20 or more. Public courses are also available to individuals in cities across the country. To find out more about WhiteHat Education Services course curriculum, contact our corporate office at 408.343.8300.

.NET Course Overview

Defining the Attacks

Inherent Problems and Limitations of Internet Architecture

- HTTP request/response flow
- Session management
- Cookies
- Encoding/decoding URLs, character sets, and HTML entities

Looking at Vulnerabilities in the Code

- How people exploit Web applications
- Why you can never trust anything that comes from the client

Components of Writing Secure Code

- Input handling
- Authentication and session management
- Access control/authorization
- Exception handling and logging
- Encryption
- .NET framework libraries
- Bypassing business logic flow

For Each Area, the Course will Cover:

- Theory and basics
- Recommended security practices
- “Gotchas” and implementation concerns
- Example exploits
- Hands-on exercises

WhiteHat Education Services

Introduction to Web Application Security

overview

Course Summary

This course is available as a one or two-day workshop. The course is taught using a combination of theory, practical examples, and hands-on training. It is designed to provide an overview of the fundamental principles of Web application security. This session presents students with an understanding of:

- How Web applications work
- How vulnerabilities manifest in them
- How hackers find and exploit these vulnerabilities
- Solutions for protecting Web applications

Benefits

- Identify elements that can make a Web application an easy target
- Learn about hackers' tools and techniques
- Understand how to identify vulnerabilities in Web applications
- Learn how to test and exploit vulnerabilities in your Web applications using freely available tools

Who Should Attend

Anyone interested in identifying vulnerabilities in Web applications, (IT staff, managers, system architects, information security professionals, etc.) and developers and QA professionals who want to understand Web application vulnerabilities and attack scenarios.

Duration

Available as a one or two-day workshop

Prerequisites

Be comfortable with Web browsers. Basic HTML familiarity is helpful.

Structure

A combination of theory, practical examples, and hands-on training.

Contact

WhiteHat Security also offers on-site education sessions for groups of 20 or more. Public courses are also available to individuals in cities across the country. To find out more about WhiteHat Education Services course curriculum, contact our corporate office at 408.343.8300.

Introduction to Web Application Security

Background

Evolution of Web applications, issues with Web applications, Web application vulnerabilities

Technologies

- HTTP protocol
- Hackers' Toolbox (HTML, JavaScript, AJAX)
- Request / response flow
- Encoding/decoding URLs, character sets, and HTML entities

Anatomy of an Attack

- How people exploit Web applications
- Why you can never trust anything that comes from the client

Top Web Application Attacks &

Vulnerabilities (topics vary depending upon duration of course selected – one or two-day)

- Overview of the top Web app vulnerabilities
- How those vulnerabilities were introduced and how they can be avoided
- Concepts, examples, case studies, and scenarios for each class of attack:
 - XSS (Cross Site Scripting)
 - SQL Injection
 - Blind SQL Injection
 - Authentication, Authorization and Session Attacks
 - CSRF (Cross Site Request Forgery)
 - Business Logic Flaws
 - HTTP Response Splitting

Solutions for Protecting Your Applications

- Solutions that can improve the security of your Web application
- Identifying the weaknesses in your Web app
- Remediation