

## Persistent Attack and Exploitation: Secure Coding JAVA

### Course Summary

This 2-3 day course is custom designed to implement security as a culture amongst developers. 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. It includes two main components: (1) Review of secure coding guidelines for JAVA, (2) JAVA specific features. Custom content can easily be added based on client requirements. This course illustrates how web applications are attacked by hackers, shows how these attacks work, shows coding mistakes that make you vulnerable to attacks, demonstrates how to make your code secure.

### Course Outline

1. Defining Attacks
2. Inherent Problems and Limitations of Internet Architecture
3. Looking at Vulnerabilities in JAVA code
4. Components of Writing Secure Code
5. Theory and Basics for 1-4 above
6. Recommended security practices for 1-4 above
7. Gotchas and implementation concerns for 1-4 above
8. Example Exploits for 1-4 above

### Examples of Exercises and Labs

- HTTP request/response flow
- Session management
- Cookies
- Encoding/decoding URLs
- Encoding/decoding character sets
- Encoding/decoding HTML entities
- How web applications are exploited
- Why you should never trust anything
- Input handling
- Authentication and session management
- Access control/authorization
- Exception handling and logging
- Encryption
- General JAVA mechanics
- Bypassing business logic flow
- Custom labs defined by client

### Course Duration

2-3 days CUSTOM

### Delivery Modes

Onsite Instructor Lead Class

### Pre-Requisites

- Understand JAVA programming
- Familiar with Web Application Development, HTML, servlets, .JSP
- Comfortable with major JAVA IDE
- Familiar with Tomcat or comparable servlet container
- Familiar with SSL and encryption

### Who Should Attend

JAVA developers, architects and QA Staff

### Materials Provided

Student reference manual  
Lab sheets and lab solutions

### Next Steps

- Accuvant Secure Coding .NET
- Accuvant Threat Modeling
- Accuvant Web Hacking and Security

### For More Information

For more information about Accuvant's global education services, please contact us at [education@accuvant.com](mailto:education@accuvant.com) or visit our web site: [www.accuvant.com](http://www.accuvant.com).

### About Accuvant

Accuvant is the only research-driven information security partner delivering alignment between IT security and business objectives, clarity to complex security challenges and confidence in enterprise security decisions. Accuvant delivers these solutions through three practice areas: Risk and Compliance Management, Accuvant LABS and Solution Services. Based on our clients' unique requirements, Accuvant assesses, architects and implements the policies, procedures and technologies that most efficiently and effectively protect valuable data assets.

Since 2002, more than 3,900 organizations, including 65 of the Fortune 100, as well as 20 major federal U.S. agencies and thousands of mid-market businesses have trusted Accuvant with their data security challenges. Headquartered in Denver, Accuvant has offices in 36 cities across the United States and Canada. For more information, visit [www.accuvant.com](http://www.accuvant.com).