



**NT OBJECTives, Inc.** offers in-depth training from some of the industry's top security experts. With backgrounds ranging from system hardening, network penetration testing, application testing and source-code review as well as compliance auditing, NTO is capable of educating developers, administrators, and security personnel about the security measures necessary to protect your web applications.

---

## **Web Application Security Training**

Training sessions present the most current methods for auditing and securing web applications. The course content follows a structure of tests, countermeasures, and coding practices that can be geared towards the needs of specific audiences such as application developers or security administrators. Real-life examples and in-depth coverage of the topic ensures that the information is relevant, detailed, and applicable to different web environments.

Courses are hands-on, and include real-world scenarios and targets to build exposure and understanding of these threats, far exceeding the typical academic instruction on security. Our instructors bring all necessary course materials and technical infrastructure to provide the most comprehensive, real-world training possible.

### **Course Highlights:**

- Top industry instructors
- Onsite instruction
- Hands-on lab exercises
- Customizable curriculum
- Comprehensive threat coverage

Courses are designed so that, upon completion, students will understand:

- ✓ The threat and nature of application security issues
- ✓ Processes to mitigate risk, including assessment and auditing application environments
- ✓ Secure architecture deployment, including secure coding practices and application layer countermeasures and defenses

## **Two-Day Course Content**

Course content is derived from NTO's comprehensive audit methodology that has been developed by the co-author of *Hacking Exposed: Web Applications* and author of *Hack Notes: Web Security*. The instruction includes techniques that would be performed by anonymous, unauthenticated users through privilege escalation attacks from authenticated users. Other topics cover techniques that target vulnerabilities in the application's handling of data syntax, semantics, and logic. Syntax-based attacks include invalid input, buffer overflows, SQL injection, and cookie poisoning. The semantic and logical techniques focus on the misuse of URL parameters, insecure session ID generation, and lack of robust access controls. Each test technique is accompanied by countermeasures that can be applied via code, the web server, or network devices.



Courses include these areas of application security:

**Application Architecture Security**

- Secure handling of session ID tokens, including resistance to session stealing, session guessing, and inadequate session expiration
- Secure database connection handling, resistance to SQL injection attacks
- Secure input validation functions, resistance to cross-site scripting and HTML injection attacks
- Separation of user and administrator roles, attributes, and capabilities
- Limit sensitive information available in client-side HTML

**Authorization Controls**

- Proper handling of user authentication tokens
- Proper identification of the user throughout the application
- Resistance to brute force credential-guessing attacks
- Secure transmission and storage of authentication tokens

**Encryption and Random Number Controls**

- Specific use of encryption as it applies to protecting user information, authentication tokens, and sensitive application information
- Specific use of encryption as it applies to protecting the confidentiality of user access to the application and SSL configuration
- Robustness of random numbers used for session ID generation and user tracking

**Platform Architecture Security**

- Defenses to prevent application vulnerabilities from executing arbitrary commands or accessing arbitrary files on the host operating system
- Implementation of platform components, including database, firewalls, and network devices to reduce the application's security risk

NT OBJECTives' training courses can be customized to offer 1 day, 2 day and 3 day instruction, and tailored to your organization's specific security concerns. Multiple instructors are present at all times to ensure personal attention and instruction is given to all students regardless of previous security knowledge or experience. Course curriculum and instruction performed by NT OBJECTives team of industry leading application security researchers and consultants, giving you exposure to the best talent in the industry.