

## WEB APPLICATION SECURITY

A recent study by the US-CERT indicated a diminishing correlation between vendor advisories and security incidents. One of the underlying factors for this trend was an increase in attacks against custom web applications. The successful execution of such attacks has an adverse impact on the company's reputation and the bottom line. This three-day course will provide the attendees an in-depth understanding of the threats faced by their web applications and the countermeasures to prevent their introduction. The course instructors utilize a combination of real world case studies, live demos and labs to reinforce the concepts.

<b>Duration</b>	3 days
<b>Who Should Attend</b>	Information security professionals, security auditors, penetration testers, and software architects.
<b>Prerequisites</b>	Students should have experience using Windows operating systems and the World Wide Web. Familiarity with computer security terminology and concepts is required.
<b>Students Will Learn</b>	<ul style="list-style-type: none"><li>▪ Architecture of web applications and the HTTP protocol</li><li>▪ Tools for manipulating the HTTP protocol and applications</li><li>▪ How web applications use cryptographic algorithms and protocols</li><li>▪ How web applications validate and restrict user input and how some forms of validation can be defeated</li><li>▪ How to tamper with data sent to a web application and use that process to discover and exploit the application</li><li>▪ How to discover, exploit and remediate SQL injection vulnerabilities in a web application</li><li>▪ How web applications manage user sessions and how to discover, exploit and remediate insecure session management</li><li>▪ How to discover, exploit and remediate Cross Site Scripting vulnerabilities in a web application</li><li>▪ How to discover, exploit and remediate Cross Site Request Forgery vulnerabilities in a web application</li><li>▪ How to discover, exploit and remediate assorted other vulnerabilities in web applications</li><li>▪ How Web 2.0 affects web application security</li><li>▪ How security can be integrated into the development cycle of a web application to prevent the introduction of vulnerabilities</li></ul>
<b>Labs</b>	<ul style="list-style-type: none"><li>▪ Trusting Data from the Client Lab</li><li>▪ Brute Force Lab</li><li>▪ Authorization Lab</li><li>▪ Cross Site Scripting Lab</li><li>▪ Cross Site Request Forgery Lab</li><li>▪ SQL SELECT Lab</li><li>▪ SQL Injection Lab</li><li>▪ Final Lab</li></ul>
<b>Course Materials</b>	<ul style="list-style-type: none"><li>▪ Student manual</li><li>▪ Class handouts</li><li>▪ Security book</li><li>▪ MANDIANT gear</li><li>▪ Free Tools CD with course tools and scripts</li></ul>
<b>Suggested Next Courses</b>	<ul style="list-style-type: none"><li>▪ Incident Response</li><li>▪ Network Traffic Analysis</li></ul>
<b>Contact</b>	1.800.647.7020 <a href="mailto:education@mandiant.com">education@mandiant.com</a> <a href="http://www.mandiant.com/education.htm">www.mandiant.com/education.htm</a>

### ***Introduction to HTTP and HTML***

- HTTP Defined
- NetCat Exercise
- HTTP Message Format
- Paros Exercise
- OPTIONS and TRACE Exercise
- Forms and Frames
- JavaScript and the DOM
- Dynamic HTML

### ***Introduction to Web Applications***

- Three Tier Architecture
- Web Servers
- Web Application Servers
- Frameworks
- Databases and Securing Database Connections

### ***Trusting Data from the Client***

- Hidden Field Tampering Demo
- Web Developer Extension
- Hidden Field Tampering Exercise
- Intro to target applications
- Bypassing Client Controls Exercise
- Trusting Data from the Client Lab

### ***Introduction to Cryptography***

- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Digital Signatures
- Secure Socket Layer (SSL)
- OpenSSL Client Demo
- Encrypted Storage

### ***Authentication***

- Authentication Technology
- HTTP Integrated Authentication
- Basic Authentication Demo
- Brute Force Lab
- Redirect on Login
- Login Redirection Demo

### ***Session Management***

- Technology Primer
- Cookies and Flags
- Cookie Eavesdropping Demo
- Predicting Session IDs
- Session Case Studies
- Leaking Session IDs

### ***Cross Site Request Forgeries***

- CSRF Defined
- CSRF in a GET Request
- GET CSRF Case Study
- POST to GET Exercise
- CSRF in a POST Request
- POST CSRF Case Study
- CSRF Lab
- CSRF on an Intranet

### ***Authorization***

- Definition
- Authorization Failures
- Forceful Browsing Exercise
- Parameter Manipulation
- Authorization Lab
- Authorization Enforcement Techniques

### ***Input Handling***

- Input Validation
- White vs Black List
- Encodings
- Input vs Output Encoding
- Dark Side of Encoding

### ***SQL Injection***

- SQL Syntax Basics
- SQL SELECT Lab
- Accessing Data
- SQL Injection Lab
- Bypassing Authentication
- Discovery and Prevention

### ***Cross Site Scripting***

- Stored XSS (with Exercise)
- Reflected XSS (with Exercise)
- DOM based XSS Demo
- XSS Impact Demos
- Discovery and Prevention

### ***Other Vulnerabilities***

- Header Injection (with Demo)
- Malicious File Execution
- URL Redirection (with Demo)
- Cache Control
- Content Type
- Denial of Service
- Command Injection
- Buffer Overflows

### ***Web 2.0 Security***

- Web 2.0 Defined
- MySpace Worm Case Study
- AJAX Security (with Case Study)
- Adobe Flash / Flex
- Client Reverse Engineering
- Mash Up Security
- Securing Web Services
- SOAP SQL Injection Demo

### ***Secure Web Application Development***

- Why Integrate Security Into Development?
- Compliance Issues
- Security During the Life Cycle
- Security Testing
- Security in Outsourcing (with Case Study)

### ***Setting Up***

- Configuring a system for web application testing
- Firefox Configuration and Extensions
- Proxy Set Up

### ***Final Lab***

- Tie all the concepts learned in the class into a final lab
- Students perform a full vulnerability assessment on a Mandiant-developed web application with a wide variety of security issues