

Web Application Penetration Testing

Overview

From the first day to the last day, you will learn the ins and outs of Web App Pen Testing by attending thought provoking lectures led by an expert instructor.

Target Audience

Course Objectives

- Learn the Secrets of Web App Pen Testing in a totally hands-on classroom environment
- Learn how to exploit and defend real-world web apps – not just silly sample code
- Complete the 83 Step "Web App Pen Test Methodology", and bring a copy back to work with you
- Understand how to find Vulnerabilities in Source Code
- Take home a fully featured Web App Pen Test Toolkit
- Learn how to do OWASP Top 10 Assessments – for PCI DSS compliance and others

Course Outline

Web Application (In)security

The Core Security Problem: Users Can Submit Arbitrary Input
Key Problem Factors Immature Security Awareness In-House Development
Deceptive Simplicity
Rapidly Evolving Threat Profile Resource and Time Constraints Overextended
Technologies The New Security Perimeter
The Future of Web Application Security

Core Defense Mechanisms – OWASP Top 10

Injection
Cross-Site Scripting (XSS)
Broken Authentication and Session Management
Insecure Direct Object References Cross-Site Request Forgery (CSRF)
Security Misconfiguration
Insecure Cryptographic Storage Failure to Restrict URL Access Insufficient
Transport Layer Protection Unvalidated Redirects and Forwards

[Register Online](#)

Schedule

Class Length: 5 Days

G2R = "Guaranteed to Run" | OLL = "Online LIVE"
ILT = "Instructor-Led-Training"

This course is not currently available on the public schedule. Please contact us using the information in the footer below to inquire about future dates or to schedule a private class.

Web Application Technologies Relevant for Pen Testers

HTTP Requests, Responses, Methods, Headers
General, Request, Response Headers
Cookies Status Codes HTTPS
HTTP Proxies
HTTP Authentication
Server-Side Functionality
The Java, ASP.NET, PHP Platforms for Pen Testers
Client-Side Functionality
JavaScript
Thick Client Components
State and Sessions
Encoding Schemes, URL Encoding, Unicode Encoding

Bypassing Client-Side Controls

Transmitting Data via the Client
Auto-Discover Hidden Form Fields
HTTP Cookies
URL Parameter Injection
Manipulating The Referer Header
Tampering with Opaque Data
Hacking ASP.NET ViewState Capturing User Data: HTML Forms Length Limits
Script-Based Validation
Disabled Elements
Capturing User Data: Thick-Client Components
Java Applets
Decompiling Java Bytecode
Coping with Bytecode Obfuscation
Hacking ActiveX Controls Reverse Engineering ActiveX Manipulating Exported Functions Fixing Inputs Processed by Controls Decompiling Managed Code
Tampering with Shockwave Flash Objects Handling Client-Side Data Securely
Transmitting Data via the Client Validating Client-Generated Data
Logging and Alerting

Attacking Authentication

Authentication Technologies
Common Design Flaws in Authentication Mechanisms
Bad Passwords
Brute-Forcible Login
Exploiting Verbose Failure Messages
Exploiting Vulnerable Transmission of Credentials
Attacking Password Change Functionality & Forgotten Password Functionality
Exploiting "Remember Me" Functionality User Impersonation Functionality
Incomplete Validation of Credentials
Non-Unique Usernames
Predictable Usernames & Initial Passwords Insecure Distribution of Credentials
Implementation Flaws in Authentication Fail-Open Login Mechanisms
Defects in Multistage Login Mechanisms
Insecure Storage of Credentials
Securing Authentication
Use Strong Credentials
Handle Credentials Secretively Validate Credentials Properly Prevent
Information Leakage Prevent Brute-Force Attacks
Prevent Misuse of the Password Change Function Prevent Misuse of the
Account Recovery Function Log, Monitor, and Notify

Attacking Access Controls

- Common Vulnerabilities
- Completely Unprotected Functionality Targeting Identifier-Based Functions
- Attacking Multistage Functions Locating Static Files
- Insecure Access Control Methods
- Attacking Access Controls
- Securing Access Controls
- A Multi-Layered Privilege Model

Injecting Code

- Injecting into Interpreted Languages
- Injecting into SQL
- Exploiting a Basic Vulnerability
- Bypassing a Login
- Finding SQL Injection Bugs
- Injecting into Different Statement Types
- The UNION Operator Fingerprinting the Database Extracting Useful Data
- An Oracle Hack
- An MS-SQL Hack
- Exploiting ODBC Error Messages (MS-SQL Only) Enumerating Table and Column Names Extracting Arbitrary Data
- Using Recursion
- Bypassing Filters
- Second-Order SQL Injection Advanced Exploitation Retrieving Data as Numbers Using an Out-of-Band Channel
- Using Inference: Conditional Responses
- Beyond SQL Injection: Escalating the Database Attack
- MS-SQL Oracle MySQL
- SQL Syntax and Error Reference
- SQL Syntax
- SQL Error Messages Preventing SQL Injection Partially Effective Measures
- Parameterized Queries Defense in Depth
- Injecting OS Commands Injecting via Perl Injecting via ASP
- Finding OS Command Injection Flaws
- Preventing OS Command Injection Injecting into Web Scripting Languages
- Dynamic Execution Vulnerabilities Dynamic Execution in PHP
- Dynamic Execution in ASP
- Finding Dynamic Execution Vulnerabilities
- File Inclusion Vulnerabilities
- Remote File Inclusion
- Local File Inclusion
- Finding File Inclusion Vulnerabilities Preventing Script Injection Vulnerabilities
- Injecting into SOAP
- Finding and Exploiting SOAP Injection
- Preventing SOAP Injection Injecting into XPath Subverting Application Logic
- Informed XPath Injection Blind XPath Injection
- Finding XPath Injection Flaws Preventing XPath Injection Injecting into SMTP
- Email Header Manipulation SMTP Command Injection Finding SMTP Injection Flaws Preventing SMTP Injection Injecting into LDAP
- Injecting Query Attributes Modifying the Search Filter Finding LDAP Injection Flaws

Exploiting Path Traversal

- Common Vulnerabilities
- Finding and Exploiting Path Traversal Vulnerabilities
- Locating Targets for Attack
- Detecting Path Traversal Vulnerabilities Circumventing Obstacles to Traversal
- Attacks Coping with Custom Encoding
- Exploiting Traversal Vulnerabilities
- Preventing Path Traversal Vulnerabilities

Attacking Web App Users – Reflected Attack

- Cross-Site Scripting
- Reflected XSS Vulnerabilities Exploiting the Vulnerability Stored XSS
- Vulnerabilities Storing XSS in Uploaded Files DOM-Based XSS Vulnerabilities
- Real-World XSS Attacks
- Chaining XSS and Other Attacks
- Payloads for XSS Attacks
- Virtual Defacement
- Injecting Trojan Functionality
- Inducing User Actions
- Exploiting Any Trust Relationships Escalating the Client-Side Attack Delivery
- Mechanisms for XSS Attacks
- Delivering Reflected and DOM-Based XSS Attacks
- Delivering Stored XSS Attacks
- Finding and Exploiting XSS Vulnerabilities
- Finding and Exploiting Reflected XSS Vulnerabilities Finding and Exploiting
- Stored XSS Vulnerabilities Finding and Exploiting DOM-Based XSS
- Vulnerabilities HttpOnly Cookies and Cross-Site Tracing
- Preventing XSS Attacks
- Preventing Reflected and Stored XSS Preventing DOM-Based XSS Preventing
- XST
- Redirection Attacks
- Finding and Exploiting Redirection Vulnerabilities
- Circumventing Obstacles to Attack Preventing Redirection Vulnerabilities
- HTTP Header Injection
- Exploiting Header Injection Vulnerabilities
- Injecting Cookies Delivering Other Attacks HTTP Response Splitting
- Preventing Header Injection Vulnerabilities
- Frame Injection
- Exploiting Frame Injection Preventing Frame Injection Request Forgery
- On-Site Request Forgery Cross-Site Request Forgery Exploiting XSRF Flaws
- Preventing XSRF Flaws JSON Hijacking
- JSON
- Attacks against JSON
- Overriding the Array Constructor Implementing a Callback Function Finding
- JSON Hijacking Vulnerabilities Preventing JSON Hijacking
- Session Fixation
- Finding and Exploiting Session Fixation Vulnerabilities
- Preventing Session Fixation Vulnerabilities
- Attacking ActiveX Controls Finding ActiveX Vulnerabilities Preventing ActiveX
- Vulnerabilities Local Privacy Attacks
- Persistent Cookies Cached Web Content Browsing History Autocomplete
- Preventing Local Privacy Attacks Advanced Exploitation Techniques
- Leveraging Ajax
- Making Asynchronous Off-Site Requests
- Anti-DNS Pinning
- A Hypothetical Attack
- DNS Pinning
- Attacks against DNS Pinning
- Browser Exploitation Frameworks

Exploiting Information Disclosure Vulnerabilities

Exploiting Error Messages Script Error Messages Stack Traces
Informative Debug Messages Server and Database Messages Using Public Information
Engineering Informative Error Messages
Gathering Published Information
Using Inference
Preventing Information Leakage Use Generic Error Messages Protect Sensitive Information
Minimize Client-Side Information Leakage

Attacking Compiled Applications Buffer Overflow Vulnerabilities Stack Overflows

Heap Overflows
“Off-by-One” Vulnerabilities
Detecting Buffer Overflow Vulnerabilities
Integer Vulnerabilities Integer Overflows Signedness Errors
Detecting Integer Vulnerabilities
Format String Vulnerabilities
Detecting Format String Vulnerabilities

Attacking & Assessing Application Architectures

Tiered Architectures
Attacking Tiered Architectures
Exploiting Trust Relationships between Tiers
Subverting Other Tiers
Attacking Other Tiers
Securing Tiered Architectures Minimize Trust Relationships Segregate Different Components Apply Defense in Depth
Shared Hosting and Application Service Providers
Virtual Hosting
Shared Application Services Attacking Shared Environments Attacks against Access Mechanisms Attacks between Applications Securing Shared Environments Secure Customer Access
Segregate Customer Functionality
Segregate Components in a Shared Application

Source Code Auditing

Approaches to Code Review
Black-Box vs. White-Box Testing Code
Review Methodology
Signatures of Common Vulnerabilities
Cross-Site Scripting
SQL Injection Path Traversal Arbitrary Redirection OS Command Injection
Backdoor Passwords Native Software Bugs
Buffer Overflow Vulnerabilities
Integer Vulnerabilities Format String Vulnerabilities Source Code Comments
The Java Platform
Identifying User-Supplied Data
Session Interaction Potentially Dangerous APIs File Access
Database Access
Dynamic Code Execution OS Command Execution URL Redirection
Sockets
Configuring the Java Environment
ASP.NET
Identifying User-Supplied Data
Session Interaction Potentially Dangerous APIs File Access
Database Access
Dynamic Code Execution OS Command Execution URL Redirection
Sockets
Configuring the ASP.NET Environment
PHP
Identifying User-Supplied Data
Session Interaction Potentially Dangerous APIs File Access
Database Access
Dynamic Code Execution OS Command Execution URL Redirection
Sockets
Configuring the PHP Environment
Register Globals
Safe Mode Magic Quotes Miscellaneous Perl
Identifying User-Supplied Data
Session Interaction Potentially Dangerous APIs File Access
Database Access
Dynamic Code Execution OS Command Execution URL Redirection
Sockets
Configuring the Perl Environment
JavaScript
Database Code Components

Related Courses, Certifications, Exams

- Certified Web App Penetration Tester
- CWAPT