

WEB APPLICATION PENETRATION TESTING WITH CAIDO

Training Course



Course Highlights



40-Hour LIVE Instructor-Led Training



Hands-on Lab Experience



AI-Assisted Workflows



Advanced Vulnerability Coverage



Immersive Learning Schedule



Certified Experts



Dedicated Telegram Support Group



Access to Recorded Sessions



Career Guidance & Mentorship

About Course

The Web Application Penetration Testing with Caido Training course provides practical, hands-on learning for professionals who want to strengthen their web application security testing skills. The course introduces learners to Caido, a modern web security testing tool, and demonstrates how it can be used to intercept, inspect, modify, and analyze web traffic during penetration testing.

Learners will explore practical techniques for identifying and assessing common web application vulnerabilities, analyzing requests and responses, manipulating traffic, and validating security weaknesses. Through hands-on exercises and realistic testing scenarios, participants will gain experience with web application penetration testing workflows and learn how to document and report their findings effectively. By the end of the course, learners will be better prepared to use Caido as part of their web application security testing toolkit and apply structured penetration testing techniques to identify vulnerabilities and improve application security.

Course Objectives

You will be able to:

- ✔ Covers all Caido features: Intercept, Replay, HTTPQL, Plugins, Logging, Workspace.
- ✔ Integrates OWASP Top 10 vulnerabilities with PortSwigger Labs for practical exploitation.
- ✔ Includes advanced vulnerabilities beyond OWASP Top 10: SSTI, HTTP Request Smuggling, Race Conditions, Web Cache Poisoning, JWT attacks, GraphQL exploitation.
- ✔ AI-assisted pentesting workflows using MCP and the Chatio plugin.
- ✔ Professional reporting and collaboration modules.



Target Audience

- ✔ Security professionals preparing for OSWE/OSCP but wanting real-world exploitation practice with AI assistance.
- ✔ Penetration Testers and Red Teamers looking to modernize their workflows using AI.
- ✔ Developers and DevSecOps Engineers who want to understand web application flaws.
- ✔ Cybersecurity students seeking practical labs beyond theory.

Pre-Requisites

- ✔ Basic understanding of web technologies (HTTP, HTML, JavaScript).
- ✔ Familiarity with networking fundamentals.
- ✔ No prior pentesting experience required — beginners can start here, while advanced learners will benefit from the extended modules.

Course Content

Module 1

Introduction to Caido

- ✔ What is Caido?
 - ✔ Modern intercepting proxy for web application security testing
 - ✔ Comparison with Burp Suite and OWASP ZAP
- ✔ Installation and Setup
 - ✔ Windows, macOS, Linux installation
 - ✔ Proxy configuration and SSL certificate setup
- ✔ Interface Tour
 - ✔ Overview, Sitemap, Scopes, Filters
 - ✔ Proxy section: Intercept, HTTP History, WS History, Match and Replace
 - ✔ Testing section: Replay, Automate, Workflows, Assistant, Environment
 - ✔ Logging section: Search, Findings, Exports
 - ✔ Workspace section: Files, Plugins, Workspace
 - ✔ Plugins section: Drop, Scanner, Authorize, Screenshot Mode, Chatio, GraphQL Analyzer, Shift
- ✔ Modular design philosophy and workflow overview

Module 2

Core Features and Workflow

- ✔ Intercepting Traffic
 - ✔ Capturing HTTP/HTTPS requests
 - ✔ Filtering and modifying requests
- ✔ HTTP History and WS History
 - ✔ Reviewing captured traffic
 - ✔ Understanding timelines and WebSocket message flow
- ✔ Match and Replace
 - ✔ Automating payload substitution & header modification
- ✔ Replay Tool
 - ✔ Resending requests to endpoints
 - ✔ Crafting payloads and comparing responses
- ✔ Scope Management
 - ✔ Defining target domains
 - ✔ Excluding irrelevant traffic
- ✔ Session Handling and Environment
 - ✔ Managing cookies, tokens, and authentication
 - ✔ Setting environment variables for dynamic testing
- ✔ Data Visualization
 - ✔ Request timelines, response graphs, & performance metrics

Module 3

HTTPQL – Caido's Query Language

- ✓ What is HTTPQL and why it matters
- ✓ Structure: Namespace → Field → Operator → Value
- ✓ Namespaces
- ✓ Fields
- ✓ Operators
- ✓ Advanced Queries: chaining multiple conditions.



Module 4

Advanced Testing Techniques

- ✔ Automated Scanning (Scanner Plugin)
 - ✔ Configuring Caido's scanner
 - ✔ Severity levels and interpreting results
- ✔ Fuzzing and Parameter Tampering
 - ✔ Using Caido's Fuzzer
 - ✔ Creating custom wordlists
- ✔ Authentication Testing (Authorize Plugin)
 - ✔ Testing login flows, session fixation, & token validation
- ✔ API Testing (GraphQL Analyzer Plugin)
 - ✔ REST and GraphQL endpoints
 - ✔ JSON/XML payload handling
- ✔ WebSocket Testing (WS History)
 - ✔ Monitoring realtime traffic
 - ✔ Manipulating messages
- ✔ Match and Replace Automation
 - ✔ Dynamic payload injection and header rewriting

Module 5

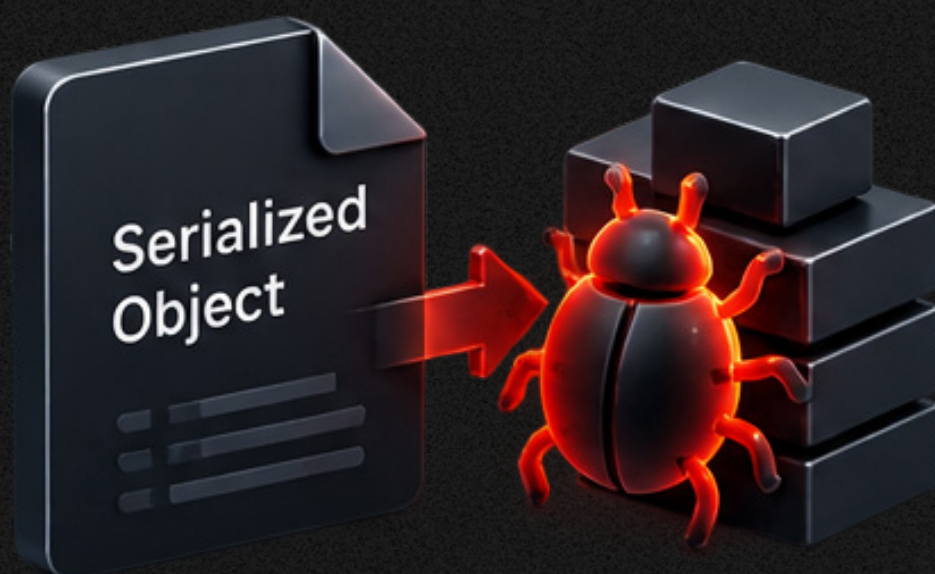
Exploiting OWASP Top 10 Vulnerabilities

- ✓ A01 Broken Access Control
- ✓ A02 Cryptographic Failures
- ✓ A03 Injection
- ✓ A04 Insecure Design
- ✓ A05 Security Misconfiguration
- ✓ A06 Vulnerable Components
- ✓ A07 Auth Failures
- ✓ A08 Integrity Failures
- ✓ A09 Logging Failures
- ✓ A10 SSRF

Module 6

Advanced Vulnerabilities Exploitation

- ✔ Server-Side Template Injection (SSTI)
- ✔ HTTP Request Smuggling
- ✔ Business Logic Exploits
- ✔ Race Conditions
- ✔ Web Cache Poisoning
- ✔ Clickjacking and UI Redressing
- ✔ XXE (XML External Entity Injection)
- ✔ Deserialization Attacks
- ✔ JWT Exploits
- ✔ Advanced XSS (DOM-based, CSP bypass)



Module 7

Plugins, Extensions and Customization

- ✔ Plugin Marketplace
 - ✔ Installing and managing plugins
 - ✔ Popular plugins: JWT Decoder, SQLi Helper, XSS Injector, Wordlist Generator
- ✔ Developing Custom Plugins
 - ✔ Plugin architecture
 - ✔ Writing plugins in JavaScript/TypeScript
 - ✔ Using Caido's API for automation
- ✔ Integration with External Tools
 - ✔ Nmap, Nikto, custom scripts
 - ✔ Exporting results (JSON, CSV)
- ✔ Automation Workflows (Automate and Workflows Tabs)
 - ✔ Scheduling scans
 - ✔ Triggering scripts based on responses
- ✔ Shift Plugin and Efficiency Tools
 - ✔ Streamlining repetitive tasks and workflow shortcuts

Module 8

Reporting and Collaboration

- ✔ Reporting Vulnerabilities (Findings and Exports)
 - ✔ Generating detailed reports
 - ✔ Custom templates and evidence collection (Screenshot Mode Plugin)
- ✔ Collaboration Features (Workspace Tab)
 - ✔ Sharing projects and findings
 - ✔ Team workflows and version control
- ✔ Best Practices
 - ✔ Ethical testing and responsible disclosure
 - ✔ Workspace hygiene and data management

Module 9

MCP Integration (Model Context Protocol)

- ✔ What is MCP and how it connects to Caido
- ✔ Benefits:
 - ✔ Automates repetitive tasks
 - ✔ Provides AI assisted traffic analysis
- ✔ Caido + MCP Use Cases
 - ✔ AI-driven request analysis
 - ✔ Automated HTTPQL query generation
 - ✔ Suggesting payloads for fuzzing
 - ✔ Summarizing scan results into human readable reports
- ✔ Chatio Plugin Integration
 - ✔ Using AI chat assistance within Caido
- ✔ Hands-on Demo: Connect Caido with MCP and use AI to interpret findings

Module 10

Logging and Data Management

- ✔ Search and HTTPQL Analyzer
 - ✔ Advanced filtering and query analysis
- ✔ Logging Best Practices
 - ✔ Using Search, Findings, and Exports for audit trails
- ✔ Drop Plugin Usage
 - ✔ Managing unwanted requests and cleaning traffic logs

Module 11

Assistant and Environment Configuration

- ✔ Assistant Tab
 - ✔ Using builtin helpers for quick actions
- ✔ Environment Tab
 - ✔ Setting variables, tokens, and dynamic parameters
- ✔ Workspace Files Management
 - ✔ Organizing captured data and reports



Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on

