Alliance Technology Partners

Acunetix Licensing, Training, and ScanAssist Services

Alliance Technology Partners

acunetix Expert Partner

Alliance Technology Partners

Acunetix Licensing, Training, and ScanAssist Services

Do you need to take a more proactive stance on web application security? Or have you already invested in Acunetix and are looking for the knowledge to utilize it fully?

Whether you are a new or a veteran user of Acunetix, our Acunetix Training courses are the answer.

Why Use Acunetix For Your Cyber Readiness Plan?

You need to protect your network and website from intrusion, and that requires knowledge and flexible tools. As threats become increasingly creative, it just adds to the endless checklist an engineer has to be concerned with. Acunetix Web Vulnerability Scanner has everything you need to keep your organization at the top of their game with the following features:

Incident Response

Don't be victim of leftover vulnerabilities in your applications. In cases where an incident may have occurred through a vulnerability within web applications, Acunetix is useful for understanding the vulnerability used, and provides a powerful set of manual penetration testing tools to assist in understanding the threat and potential damage more fully.

Vulnerability Analysis

Acunetix WVS is a vulnerability scanner that scans websites, web applications, and web servers for vulnerabilities, allowing them to be addressed prior to exploitation by hackers attempting to infiltrate IT infrastructures. It's able to find a much greater number of vulnerabilities because of its intelligent analysis engine and Deep Scan technology – Capable of scanning complex Javascript

libraries, mobile and Single Page Application (SPAs), understanding AJAX, SOAP/WSDL, SOAP/WCF, WADL, XML, AJAX, & JSON, Google Web Toolkit (GWT), and CRUD operations. Acunetix DeepScan Technology provides greater support for Java Frameworks (including Java Server Faces (JSF), Springs and Struts) and Advanced detection of DOM-Based Cross Site Scripting.

Penetration Testing

Better understand your vulnerabilities. Exercise specific attacks (or blended attacks) to verify vulnerabilities, structure more advanced attacks, uncover the extent of a threat, determine what information can be gleaned, or determine how threats can be customized to performed more advanced attacks.

Network Mapping

While Acunetix is not known as a network mapping tool, it does provide port scanning, subdomain searching, and scanning for ranges of IP addresses within a network.

Compliance

Show your compliance. This is the core of the Acunetix focus. The vulnerability analysis populates a database that can be used to generate a number of compliance reports: CWE/SANS, HIPAA, ISO 27001:2013, ISO 27001:2005, NIST Special Publication 800-53, OWASP TOP 10 2013, PCI 3.1, Sarbanes-Oxley Act of 2002, DISA (DoD) Application Security and Development STIG, and Web Application Security Consortium: Threat Classification. Additionally, Acunetix provides standard reports for developers, summaries, and comparisons. The database is also accessible for generating queries to customize your own reporting needs.

About Us

Alliance Technology Partners is an Acunetix Expert Licensing Partner and a provider of Acunetix Training Courses and Consulting services in the United States/Canada. Our security consultants have been exclusively trained by Acunetix Management and Software Development Teams. They are actively engaged with Acunetix Management as advocates for our customers, always communicating potential improvements to the WVS tool with each version released.

What's Our Training Like?

- Learn fundamental factors of leveraging the Acunetix WVS tool as a platform between the application developers and web risk/security teams at the foundation layer/creation point of an application.
- Each course is instructor-led using a web-based Join.me remote desktop session and secure conference bridge phone number. This provides the greatest flexibility for all users engaged in the session and provides significant cost savings.
- Have up to 5 team members attending each course for one fixed price. Additional courses will be need to be purchased to accommodate teams larger than 5 members.
- Course(s) Duration: 3-hours with one 15-minute break
- Course completion certificates are always issued for the latest version of Acunetix.
- Training Courses are only available for the latest version release.

Introductory Training Overview

Course-The class provides an overview of the features and additional tools within the Acunetix WVS Tool, as well as demonstrates these features within an active scan. Below are the key areas of focus in this course.

See the Training Course Outline On the Following Page:

General	• Scan Templates • Scan Settings • Crawling Options • Login Sequence Recorder (form authentication) • HTTP Authentication • Setting up customized Scan Profiles • Throttling a Scan • Scan Progression/Alerts Node
Pentesting & Discovery Tools	• HTTP Editor • HTTP Sniffer • Site Crawler • HTTP Fuzzer • Authentication Tester • Compare Results Tool • Target Finder & Subdomain Scanner • Web Services Scanner/Editor
Scheduling, Automation & Integration	• Web-based Scheduler • Options for scheduling scans/excluded hours/scanning of list of targets import from CSV • Use of Selenium IDE for scanning complex business logic-driven applications • Import manual crawl data from third-party tools such as FIddler, BurpSuite, and HAR (HTTP Archive) files as well as the built-in Acunetix HTTP Editor • Dynamically pre-seed automated crawls using external or custom-built tools and scripts • XML and AVDL exports for machine readable outputs
Reporting & Compliance	• General reporting options – Executive Summary/Affected Items Report/Developer Report/Scan Comparison Report/Monthly Vulnerabilities Report • CVE/CVSS and CWE scoring in reports • Reporting customizations/export options and formats/database schema for extraction of results into DoD specialized reporting structures as required • Compliance reporting options: • NIST Special Publication 800-53 - Recommended Security Controls for Federal Information Systems • DISA (DoD) Application Security and Development STIG • OWASP Top 10 2013 • ISO 27001 • CWE SANS Top 25 • WASC • Sarbanes-Oxley Act 2002 • HIPAA

Advanced Training Overview

The focus of this course will be determined based on the results of a questionnaire completed at the end of the introductory training session. The trainee will have the opportunity to indicate the areas in which more in-depth instruction is desired. Below are the most common areas of focus.

Reducing Scan Times

A common challenge faced by many clients is reducing scan times without compromising the integrity of the scan. This is an important for all clients, but especially true for client faced with the following challenges:

- Clients with large web applications
- Clients working with template based websites
- Clients requiring scans for numerous sites within a limited window of time

Authenticated Scanning

Unauthenticated scanning typically yields very little in the way of crawl results. It is recommended that clients perform authenticated scans where possible. Many challenges may arise when performing authenticated scans including the following:

- Troubleshooting authentication errors and timeout issues
- Working with client-side certificates and multi-factor authentication

Understanding Common Vulnerabilities

Providing scan results to developers generally requires working with the development team to understand the true impact of the vulnerabilities found. The security team should be prepared to explain and work with the development team to verify and understand the impact of the findings. Understanding the vulnerabilities and working with the tools is a crucial step in this process:

- Understanding Cross-Site Scripting Vulnerabilities - Stored, Reflected and DOM Based XSS
- Understanding SQL Injection Vulnerabilities - Classic, Blind, and Compound SQLI

Troubleshooting and Tuning Scans

While scans may be automated and scheduled, due diligence should be taken to understand your results, verify findings, and tune your scans. Since websites and applications differ greatly there is not a one-size-fits-all approach. Time should be taken to understand the crawl and vulnerability scanning results. This can entail making several scan configuration changes, comparing results, and parsing logs. Training includes but is not limited to the following areas:

- Strategies for Logging and Comparing results
- Understanding and working with Parameter Exclusion, Inputs Fields, and Variations
- Utilizing the HTTP Sniffer to build a better Crawl

Looking For Something Hands-On?

We do provide a one-day onsite training session for military and government organizations that require it. Two Acunetix-trained onsite engineers will proctor the class, and provide the Introductory and Advanced Training courses in a single day. The instructors will also bring all necessary virtual test servers to perform different types of vulnerability scans in a stand-alone, private environment with no access to any government/DoD systems or networks. No work on your end or worry of breach!

Need Help With Your Scans?

Do you already own Acunetix but having problems with configuration for a particular application, or experiencing other issues? We offer Acunetix ScanAssist:

- ScanAssist allows active Acunetix users the ability to have an Acunetix Training engineer review current scanning challenges, strategies, and new release implementation questions.
- It is offered as a 5-hour individual user option or as a 50-hour Organization (team) option. Time is pooled for team use.
- All ScanAssist requests must be submitted via e-mail to websecsupport@alliancetechpartners.com. A ticket will be generated for tracking each request and resolution time will be deducted from the ScanAssist user/organization agreement.

18102 Chesterfield Airport Rd.
Suite E
Chesterfield, MO 63005

alliancetechpartners.com

314 649 8888 St. Louis
314 649 8889 Fax
888 891 8885 Toll Free