IBM Security AppScan Standard: Scan and analyze results

Go from configuration to scan and results analysis with this quick AppScan Standard editor reference

developerWorks security editors

This is a summary guide to getting started scanning for web application vulnerabilities with IBM® Security AppScan® Standard Edition and analyzing the results. Watch a video demonstration to learn how to configure AppScan for a dynamic scan of a new application. Follow a case study that demonstrates using AppScan Standard to scan and test two web applications. Watch a five-step process to help you analyze the results of your scan. Then watch a real-life scenario in which AppScan Standard is used (with AppScan Source) to establish embedded security analysis. A bonus is also included: An AppScan Standard guide to testing mobile applications.

IBM® Security AppScan® Standard automates application security testing by scanning applications, identifying vulnerabilities, and generating reports with intelligent fix recommendations to ease remediation. It provides static and dynamic application security testing throughout development.

In this article, watch video demonstrations to learn how to configure IBM Security AppScan for a dynamic scan of a new application, then analyze the results of a scan using a five-step process. You can also follow along with a case study that demonstrates using AppScan Standard to scan and test two web applications, then watch a real-life exploration of how an organization uses a combination of AppScan Standard and Source editions to provide the embedded security and analysis necessary to help developers eradicate source code vulnerabilities. There's also a resource for configuring AppScan to test mobile devices.

Configure your first scan with AppScan Standard

Technical support engineer Scott Hurd outlines the issues to consider when setting up your first Security AppScan Standard scan, including:

- The structure, configuration, language, platform, and purpose (production or test) of the site you're scanning
• The number of unique pages involved
• What types of security layers exist between the site and the server you're running AppScan on (Hint: Authentication can be an obstacle for first-time AppScan users when they're setting up a scan.)

The demo is performed on a test site, but the presenter includes information on scanning a production site.

Use AppScan Standard to test two web apps

In "Case study: AppScan security scan of Rational Focal Point," Shivakumar Patil, an IBM Rational Focal Point development team member who has been working on security using Rational AppScan for the last two years, details using IBM Security AppScan Standard edition to test web-based applications and their external endpoints, such as SOAP and REST web services.

Bonus: Test mobile apps and services with AppScan Standard

To add a mobile component to the mix, IT security professionals Daniel J. Anderson, Carlos Hoyos, and Nader Nassar help you explore different aspects of mobile application security using hands-on examples with AppScan Standard in the article "Secure your mobile applications with IBM Security AppScan Standard." For Android and iOS devices, they explain the types of mobile applications and web services; how to configure user agents, emulators, and the mobile device; how to perform recording and testing; and how to encrypt the transport layer.

Analyze your scan results with AppScan Standard

Rodney Ryan discusses a simple five-step process to analyze AppScan Standard scan results. Ryan uses a cross-site scripting vulnerability (XSS) as the example. XSS is a type of computer security vulnerability typically found in web applications. It enables attackers to inject client-side script into web pages so attackers may bypass access control restrictions (for example, same origin policy, which allows scripts originating from the same site to access each other's methods and properties but restricts scripts from other sites to do so).

The steps include:

1. Understand the issue: Read the advisory information on the advisory tab.
2. Understand the issue: Read the general and specific fix recommendations.
3. Request and response: Understand how AppScan is manipulating your server.
4. Request and response: Understand why AppScan's manipulation is considered a positive test.
5. Request and response: Do some manual verification of the test.

Using AppScan Standard in the real world

Sean Poris of The College Board discusses how his organization uses IBM Security AppScan Standard and IBM Security AppScan Source Editions to provide the embedded security and
analysis necessary to help developers eradicate source code vulnerabilities at the not-for-profit, membership-driven institution.

The College Board is best known through its flagship products, SAT and AP tests. The IT environment at the College Board supports approximately 200 different applications, custom and off the shelf; there is a broad infrastructure to support those applications. The infrastructure has hundreds of servers in a data center off site, and they are currently working on a virtualization initiative to reduce the physical footprint of those servers. The Board uses IBM Rational® products to enable the development life cycle of a variety of web applications and non-web applications, data warehouse, front-end applications, and mobile apps.

According to Poris, security is really crucial to consider upfront within the development life cycle. One of the challenges the Board has is to be able to empower the developers earlier in the life cycle to identify vulnerabilities and eradicate them from the source code.

The Board uses AppScan Standard to attack their site—to come into the website like an attacker, map out what an attacker could potentially do, and then run automated scripts to find out if there are any vulnerabilities in the site. It combines AppScan Standard capabilities with AppScan Source, which performs static analysis and essentially interrogates source code looking for vulnerability paths within that source code.
Related topics

- Visit the IBM Security AppScan Standard product site to learn how you can quickly identify, understand, and fix critical web application vulnerabilities.
- Uncover technical resources to help you get the most out of Security AppScan at developerWorks.
- Get details on how to download and evaluate IBM Security AppScan.