HP WEBINSPECT AND HP ASSESSMENT MANAGEMENT PLATFORM

What's New with HP Application Security Center

Version 9.0

HP WebInspect 9.0 and HP Assessment Management Platform 9.0 enable security and application teams to evolve from managing scans and test results, to truly managing application security assessment programs that deliver the security intelligence necessary to manage application risk in context with the business.

Vulnerability Review with Retest

Dramatically reduce scan review times and create consistency across evaluations

- **Vulnerability Review** – Understanding and interpreting the results of an automated security scan is typically the most time consuming part of performing a security audit. HP WebInspect 9.0 simplifies and streamlines the review process with the new Vulnerability Review feature that enables users to interact with the results, rather than just read a report.
- **Reproduction Steps** – HP WebInspect 9.0 presents the steps to reproduce a vulnerability by displaying the sequence of requests through the application that produced the exploitable issue and shows how the scan identified the page. Simply right click a vulnerability and select "review vulnerability" for full reproducibility.
- **Retest** – With the Retest feature, HP WebInspect 9.0 users can easily reexecute the series of steps that discovered a specific vulnerability. Retest enables users to prove the reproducibility of a vulnerability and to confirm individual vulnerability fixes from developers without having to run an entirely new scan.

Better Handling of Complex Applications

Increase coverage, authentication and session handling of complex Web 2.0 and rich Internet applications

- **New macro recording technology** – HP WebInspect 9.0 introduces a dramatically different method for recording login macros, resulting in significantly improved authentication and session management. The new method works by recording user interactions within the browser instead of simplistic and error-prone proxying of HTTP requests. The resulting macros also provide feedback about their effectiveness in handling sessions properly during testing.
- **Flexible Authentication Handling** –New authentication handling can support dynamic security questions, multiple or substitute login credentials and parameterized login hostnames. Each of these capabilities makes session handling more consistent, reusable and resilient.
- **Post Scan Recommendations** – Post scan analysis provides users with recommendations on how to optimize and configure their scans by analyzing specific conditions in the scan results. This results in improved tuning and coverage of complex applications.

Efficient Vulnerability Management

Manage and reuse multiple sets of scan results in a single assessment workspace

- **Assessment Workspaces** – HP Assessment Management Platform 9.0 includes a new assessment workspace for managing your scans and vulnerability information across multiples sets of web application security testing into one centralized location. Within an assessment, you can combine the data from multiple scans, remove duplicate vulnerabilities, add manually found vulnerabilities, and attach documentation such as notes and screenshots. Assessments support import and reuse of findings and scan results from dynamic analysis, static analysis and manual findings.
- **Attachments and Screenshots** – Both HP WebInspect 9.0 and HP Assessment Management Platform 9.0 allow you to attach documents and screenshots to scan results for better context and communication on the vulnerabilities found.
- **Persist Results Across Scans** – You can now indicate that a test results should be ignored, such as with a false positive, and persist that across multiple scans.

Advanced Web Services Security Testing

Systematically and thoroughly security test web services for the first time

- **Support for Complex Data Types** – HP WebInspect 9.0 includes major improvements in understanding modern WSDLs, including support for complex data types, recursive types, and other advanced WSDL entities. As part of this effort a new tool has been created, Web Services Security Test Designer, to render advanced WSDLs and enables you to specify appropriate application data for your web service security test.
- **WS-Security (WSS) Improvements** – Expanded handling of WS-Security includes support for UserID and Password credentials at the application layer, as well as support for transport layer security (SSL/HTTPS) for Web Services.
- **New Attacks** – The new HP WebInspect 9.0 web service infrastructure has been integrated with the existing Smart Engine framework so that the Local File Include (LFI) and SQL Injection engines can agnostically deliver its attacks via web services, and subsequent future smart engines will easily plugin and enhance both web site and web service scanning.
- **Better Control** – As part of the new Web Services Security Test Designer you can now control which methods as well as which parameters per method get sent or attacked as part of the web service scan.
- **Web Services Auditing Automatically** – During a web site scan, if any web service traffic is detected, the associated web service is automatically audited as part of the web site scan, giving you automatic coverage of the larger attack surface of the web application
- **Web Service Security Designer** – The Web Service Security Designer is a new tool for configuring web service security scanning. It enables you to import advanced WSDLs and correctly render complex data types, control which methods and parameters get audited, and configure WS-Security options

New Complex Vulnerability Engines

Identify complex vulnerabilities with higher confidence

- **Blind SQL Injection** – A new time-based method for detecting Blind SQL Injection has been developed, which will send SQL Injection attacks aimed at slowing the performance of the database server for a specific period of time and sampling the response time of the web application to determine if the attacks were successful. This new method of Blind SQL Injection testing complements the preexisting Inferential testing method.
- **Cross Site Scripting and DOM-based Cross Site Scripting** – HP WebInspect 9.0 includes an improved Cross-Site Scripting audit engine that now has the ability to detect and report DOM-based Cross-Site Scripting (DOM-XSS) vulnerabilities. DOM-XSS differs from the stored and reflected XSS since malicious data is never sent to the server.
- **Cross Site Request Forgery (CSRF)** – A new CSRF engine significantly improves your ability to identify one of the most dangerous types of vulnerabilities in modern web applications. CSRF is exploited when a user interacts with a particular site and that site sends a request to another site using a previously established cookie to perform an action without knowledge or permission from the user.

Real-Time Hybrid Analysis

Observe dynamic attacks in the code as they happen

- **Real-Time Interaction with Runtime Analysis** – Users can correlate HP WebInspect or HP Assessment Management Platform results with the runtime analysis of HP Fortify Security Scope for a deeper understanding of potential security vulnerabilities in their applications. The dynamic and runtime analysis results are used together to produce more relevant and accurate test results displayed in HP Assessment Management Platform 9.0 or HP Fortify 360 Server. This greatly reduces the time required to determine the code changes needed to fix a vulnerability.

Streamlined Installation Process

Get started faster with easier installation

- **Bundled Prerequisites** –In HP WebInspect 9.0, prerequisites have been bundled into the installation package and can optionally be deployed as part of the HP WebInspect installation process.

Resources

For more information about the features in the release, consult the release notes for each product.