IBM Software Demos
Rational AppScan

Rational AppScann Demonstration Script

: It didn’t take long for savvy hackers to discover that while firewalls and authentication techniques were being successfully employed to keep them out of our corporate networks, a simple compromise of the web application could let them sneak in the back door to access or manipulate sensitive resources. So while organizations were investing time in firewall type technology, scanning their networks for network specific vulnerabilities, and engaging with third party experts to provide vulnerability assessments, there is a still a very grave danger to relying too heavily on these strategies to protect your web application environment.

IBM offers software and services to help manage the application security lifecycle, including IBM Rational AppScan. This market leading solution scans applications, identifies vulnerabilities, and generates detailed fix recommendations to ease remediation.

The first step in scanning a web application for security vulnerabilities is to explore the application. AppScan allows a user to either automatically or manually scan a web application from top to bottom, side to side in order to determine what tests need to be run. Once the exploration process is complete, the testing is done. And you can see on the top right hand corner that testing produces vulnerability lists that are prioritized, enabling the user to understand what vulnerabilities were discovered during the scan.

The user is also allowed to drill down on each of the vulnerabilities to see exactly where the vulnerability was discovered. A developer would definitely need to know what page and parameter the vulnerability was discovered on so that they can begin fixing the problems.

Drilling down here on the log in dot.USPX shows us that the user ID parameter on our log in page is vulnerable to cross site scripting.

Once I understand where the problem exists, I might want to check to see why AppScan is telling me that we’re vulnerable to cross site scripting.

The request response tab gives me details as to what did AppScan do to run the test and what did it look for in the response to the application that told it that yes, cross site scripting is definitely a vulnerability in this instance. There is all sorts of information in the request response tab to help validate the vulnerability and do any custom testing that you would like to do on top of what AppScan has done already.

The advisory tab helps to educate us on what is the vulnerability. A unique advisory tab exists for each vulnerability in the list of discovered issues. Also included in the advisory tab is a web lecture that helps you to visualize and understand how the vulnerability works, what the dangers are, all narrated by one of our security experts using a computer based training module.

The remediation tab helps you to understand in developer speak exactly how to fix the problem. So whether it's a configuration issue that you need to send to your IT team or a coding problem that you need to send to a developer, here are all of the different ways using ASP.net, G2EE, PHP, and a generic fix recommendation that will show you how to code more securely or configure your environment more securely.

The remediation task view is your basic project plan. Rather than showing you a view with all of the issues, you can change that so that it shows you a view of all of the remediation steps you need to take in order to fix the problems. This is the step in the right direction that _____ allows you to take that shows light at the end of the tunnel in creating a plan that will effectively help you fix the vulnerabilities.

By drilling down on one of the remediation tasks, you see exactly where a particular action needs to take place, and on the bottom you see exactly what issues that one action will be addressing.

The report wizard allows you to disseminate the information in a scan to many different types of audiences.

The security report can be generated to be sent out to your executives, developers, QA people. You can see that there are built in templates that help you auto select and customize reports for whatever audience you're looking to inform.

If your organization is following particular industry standards, here is a list of pre-built industry standard reports that map your vulnerabilities to those industry standards to show you how you may not be conforming to those particular standards. One of our most used reports is the PCI report, showing extreme value on how a web application's vulnerabilities might be pulling an organization away from a standard they want to comply with.

Here are some other examples of reports that fall under regulatory compliance standards.

The list includes many different reports, including Sarbanes Oxley, HIPAA, GOBA, and many others that can help an organization see how they are or aren't complying with a particular regulatory standard with that web application.

IBM Rational AppScan is a tool that can be used throughout the software development lifecycle. The earlier in the STLC that you use a tool to scan for web application vulnerabilities, the more efficient and cost effective it is, but organizations today use AppScan throughout all sorts of different levels of the STLC.

Please reference these links for information on how to download white papers, more information, or even a trial version of AppScan to take on a proof of concept against your own web applications.

END