

IBM Software Demos

Tivoli Application Security

Introduction:

Today, more than ever, organizations depend on the Internet to collect and deliver information, exposing companies to an increasing range and frequency of threats. In an effort to quickly bring new applications and services online, organizations have developed and deployed many new web applications with minimal attention given to the security risks that they may introduce. Unfortunately, this practice has resulted in a large number of web sites becoming surprisingly vulnerable to hackers.

Securing the applications which are used to collect sensitive data has understandably become a top priority for many information security professionals. Many organizations are adopting application security solutions from IBM to address these threats, and to strengthen their overall security posture.

Demo - Rational AppScan:

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.

AppScan allows a user to either automatically or manually scan a web application from top to bottom, and side to side in order to determine which tests need to be run. Once the exploration process is complete, the testing is done. You can see in the top right hand corner that this testing produces prioritized lists, which enable the user to understand which vulnerabilities were discovered during the scan.

The user is also allowed to drill down into each list to see exactly where each vulnerability was discovered. A developer would need to know the specific page and parameter where the vulnerability was discovered in order to begin fixing the security problems.

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

Once I understand where the problem exists, I may want to check to see why AppScan is telling me that the page is vulnerable to cross site scripting.

The request response tab provides the AppScan test details that showed the cross site scripting vulnerability in this example. There are all sorts of information in the request response tab to help validate

IBM Software Demos Tivoli Application Security

the vulnerability and do any additional custom testing. A unique advisory tab exists in the list of discovered issues to provide details on the nature of each vulnerability. The advisory tab includes a web lecture that helps you to visualize and better understand the vulnerability and the dangers it creates- all narrated by one of our security experts using a web based training module.

The remediation tab in AppScan helps you 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, J2EE, PHP, and a generic fix recommendation that will show you how to code or configure your environment more securely.

The remediation tasks view is your basic project plan. You can see a view with all of the issues, or you can modify the view to see the remediation steps necessary to fix the problems. This allows you to create a plan that will effectively help you fix the vulnerabilities.

By drilling down on one of the remediation tasks here, you will see exactly where a particular action needs to take place, and on the bottom you see exactly what issues that action will be addressing. You can generate a security report to share the information and send it to executives, developers, and Quality Assurance people. You can see that there are built in templates that help you auto select and customize reports for different audiences

If your organization needs to adhere to particular industry standards, here is a list of more than 40 pre-built reports that map your vulnerabilities to those standards. One of our most utilized reports is the PCI report, which is valuable in demonstrating how a web application's vulnerabilities might be pulling an organization away from compliance with its industry standards.

IBM Rational AppScan is a solution that can be used throughout the software lifecycle. Although it is more efficient and cost effective to scan for web application vulnerabilities earlier in the software lifecycle, organizations today use AppScan at all levels and phases

Demo - TAMeb:

IBM Software Demos Tivoli Application Security

As organizations enhance their overall security posture by leveraging AppScan to address their web application vulnerabilities, there is another problem that should be addressed – securing user access to web applications.

A few of the most pressing vulnerabilities out there today- cross site scripting and cross site request forgery- are successful because they attempt to bypass access controls to web applications.

One step in easing the remediation of these vulnerabilities is to deploy a web access management solution, like IBM Tivoli Access Manager for e-business. Tivoli Access Manager is used to define access control lists to web applications so that only the authenticated and authorized users can gain access to the web application.

The value of Tivoli Access Manager becomes more pronounced for organizations that have a large number of heterogeneous applications as they leverage different authentication and authorization formats. Tivoli Access Manager offers out-of-the-box integration with a number of leading 3rd party applications to enable flexible user authentication and centralized authorization.

Together, AppScan and Tivoli Access Manager complement each other. Tivoli Access Manager grants access to web applications and App Scan ensures that these applications are scanned and tested for vulnerabilities.

Conclusion:

The consequences of a security breach are great: increased regulatory scrutiny, fines, lawsuits, brand damage, consumer confidence erosion, and online channel decline. IBM's application security solutions allow companies to preemptively and actively protect applications from external and internal threats, increase efficiencies, support compliance and improve an organization's overall security posture. With the explosion of web-enabled applications, a new reality has emerged. Organizations should not neglect the important step of securing their web applications, the users that access them, and the data they collect. It only takes a single breach to ruin a reputation.