Vulnerability Assessment with Application Security

Targeted attacks are growing and companies are scrambling to protect critical web applications. Both a vulnerability scanner and a web application firewall are required to properly secure web applications—and F5 BIG-IP Application Security Manager (ASM) offers both on a single platform.

by Peter Silva
Technical Marketing Manager, Security

Introduction

Protecting web applications is an around-the-clock job. Almost anything that is connected to the Internet is a target these days, and organizations are scrambling to keep their web properties available and secure. The ramifications of a breach or downtime can be severe: brand reputation, the ability to meet regulatory requirements, and revenue are all on the line. A 2011 survey conducted by Merrill Research on behalf of Verisign found that 60 percent of respondents rely on their websites for at least 25 percent of their annual revenue.[1]

And the threat landscape is only getting worse. Targeted attacks are designed to gather intelligence; steal trade secrets, sensitive customer information, or intellectual property; disrupt operations; or even destroy critical infrastructure. Targeted attacks have been around for a number of years, but 2011 brought a whole new meaning to advanced persistent threat. Symantec reported that the number of targeted attacks increased almost four-fold from January 2011 to November 2011.[2]

In the past, the typical profile of a target organization was a large, well-known, multinational company in the public, financial, government, pharmaceutical, or utility sector. Today, the scope has widened to include almost any size organization from any industry. The attacks are also layered in that the malicious hackers attempt to penetrate both the network and application layers.

To defend against targeted attacks, organizations can deploy a scanner to check web applications for vulnerabilities such as SQL injection, cross site scripting (XSS), and forceful browsing; or they can use a web application firewall (WAF) to protect against these vulnerabilities. However a better, more complete solution is to deploy both a scanner and a WAF. F5® BIG-IP® Application Security Manager™ (ASM) version is a WAF that gives organizations the tools they need to easily manage and secure web application vulnerabilities with multiple web vulnerability scanner integrations.

Web Security Challenges

As enterprises continue to deploy web applications, network and security architects need visibility into who is attacking those applications, as well as a big-picture view of all violations to plan future attack mitigation. Administrators must be able to

1   http://www.verisigninc.com/en_US/forms/ddosattentionreport.xhtml?loc=en_US?cmp=tw

2   http://www.symanteccloud.com/en/gb/mlireport/SYMCINT_2011_11_November_FINAL-en.pdf

understand what they see to determine whether a request is valid or an attack that requires application protection. Administrators must also troubleshoot application performance and capacity issues, which proves the need for detailed statistics. With the increase in application deployments and the resulting vulnerabilities, administrators need a proven multi-vulnerability assessment and application security solution for maximum coverage and attack protection. But as many companies also support geographically diverse application users, they must be able to define who is granted or denied application access based on geolocation information.

Application Vulnerability Scanners

To assess a web application's vulnerability, most organizations turn to a vulnerability scanner. The scanning schedule might depend on a change control, like when an application is initially being deployed, or other factors like a quarterly report. The vulnerability scanner scours the web application, and in some cases actually attempts potential hacks to generate a report indicating all possible vulnerabilities. This gives the administrator managing the web security devices a clear view of all the exposed areas and potential threats to the website. It is a moment-in-time report and might not give full application coverage, but the assessment should give administrators a clear picture of their web application security posture. It includes information about coding errors, weak authentication mechanisms, fields or parameters that query the database directly, or other vulnerabilities that provide unauthorized access to information, sensitive or not. Many of these vulnerabilities would need to be manually re-coded or manually added to the WAF policy—both expensive undertakings.

Another challenge is that every web application is different. Some are developed in .NET, some in PHP or PERL. Some scanners execute better on different development platforms, so it's important for organizations to select the right one. Some companies may need a PCI DSS report for an auditor, some for targeted penetration testing, and some for WAF tuning. These factors can also play a role in determining the right vulnerability scanner for an organization. Ease of use, target specifics, and automated testing are the baselines. Once an organization has considered all those details, the job is still only half done.

Simply having the vulnerability report, while beneficial, doesn't mean a web app is secure. The real value of the report lies in how it enables an organization to determine the risk level and how best to mitigate the risk. Since re-coding an application is expensive and time-consuming, and may generate even more errors, many organizations deploy a web application firewall like BIG-IP ASM. A WAF

enables an organization to protect its web applications by virtually patching the open vulnerabilities until it has an opportunity to properly close the hole. Often, organizations use the vulnerability scanner report to then either tighten or initially generate a WAF policy.

Attackers can come from anywhere, so organizations need to quickly mitigate vulnerabilities before they become threats. They need a quick, easy, effective solution for creating security policies. Although it's preferable to have multiple scanners or scanning services, many companies only have one, which significantly impedes their ability to get a full vulnerability assessment. Further, if an organization's WAF and scanner aren't integrated, neither is its view of vulnerabilities, as a non-integrated WAF UI displays no scanner data. Integration enables organizations both to manage the vulnerability scanner results and to modify the WAF policy to protect against the scanner's findings—all in one UI.

Integration Reduces Risk

While finding vulnerabilities helps organizations understand their exposure, they must also have the ability to quickly mitigate found vulnerabilities to greatly reduce the risk of application exploits. The longer an application remains vulnerable, the more likely it is to be compromised.

BIG-IP Application Security Manager

F5 BIG-IP ASM, a flexible web application firewall, enables strong visibility with granular, session-based enforcement and reporting; grouped violations for correlation; and a quick view into valid and attack requests. BIG-IP ASM delivers comprehensive vulnerability assessment and application protection that can quickly reduce web threats with easy geolocation-based blocking—greatly improving the security posture of an organization's critical infrastructure.

BIG-IP ASM (version 11.1 and later) includes integration with IBM Security AppScan, Cenzic Hailstorm, QualysGuard WAS, and WhiteHat Sentinel, building more integrity into the policy lifecycle and making it the most advanced vulnerability assessment and application protection on the market. In addition, administrators can better create and enforce policies with information about attack patterns from a grouping of violations or otherwise correlated incidents. In this way, BIG-IP ASM enables

organizations to mitigate threats in a timely manner and greatly reduce the overall risk of attacks and solve most vulnerabilities.

IBM Security AppScan Scanner

IBM Security AppScan delivers security capabilities that allow enterprises to not only identify vulnerabilities, but to reduce overall application risk. The IBM Security AppScan portfolio includes white box (advanced static) and black box (dynamic) analysis—as well as run-time analysis that keeps current with the latest threats and produces precise, actionable results. IBM Security AppScan helps organizations manage risk throughout the application lifecycle and enables them to drive application security within BIG-IP ASM. Security AppScan service integration tests web application vulnerabilities and the latest Web 2.0 technologies, including AJAX based applications. Administrators can manage reporting and policy creation and enforcement through the BIG-IP ASM GUI.

Cenzic Hailstorm Scanner

Cenzic's scanning solution can scan websites and web applications in the enterprise to see how vulnerable they are to possible attack. Hailstorm scans against several default policy templates, and the results make it easy to see the overall status of the application, the number of URLs discovered, the forms discovered, and an overall site map. Hailstorm can also detect a link to an outside site, which other utilities can overlook. It can run different types of reports, for instance, a technician report or an executive report. Similar to the IBM Security AppScan, administrators can manage reporting and policy creation and enforcement through the BIG-IP ASM GUI.

QualysGuard WAS

One of the challenges of dynamic application security testing (DAST) is successfully authenticating the application during a scan. Built on Qualys's powerful SaaS platform, QualysGuard Web Application Scanning (WAS) 2.1 can perform authenticated web application scans and even complex authentication with multi-step login processes like client certificates to identify vulnerabilities. QualysGuard uses the power and scalability of the cloud to accurately discover, catalog, and scan large numbers of web apps to provide a high level of protection. QualysGuard WAS 2.1 identifies OWASP Top Ten web application vulnerabilities as well as emerging threats such as Slowloris. This automated solution reduces the complexity and cost of web application scanning.

Like with IBM Security AppScan and Cenzic Hailstorm, administrators can manage reporting and policy creation and enforcement through the BIG-IP ASM GUI.
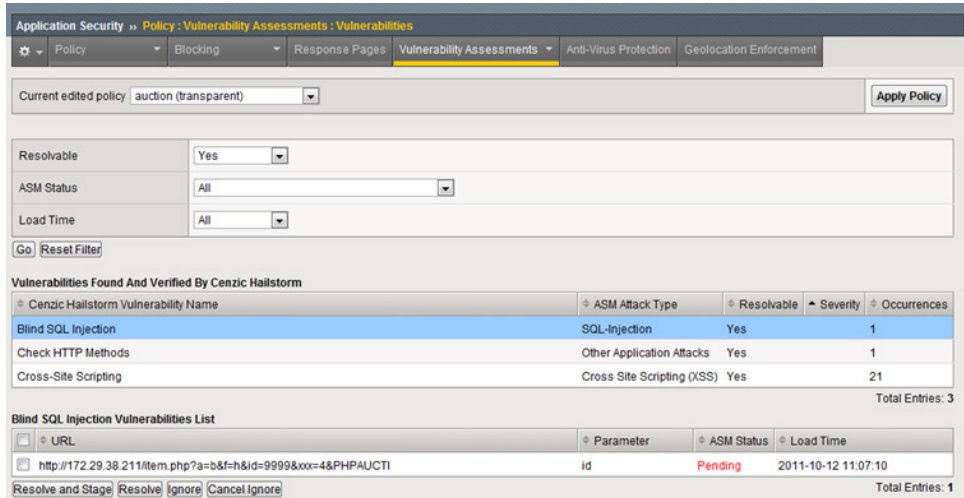

Figure 1: Organizations can run a vulnerability assessment with IBM Security AppScan, Qualys, Cenzic, and WhiteHat.

WhiteHat Sentinel

WhiteHat Sentinel is the only solution that combines an advanced, cloud-based security platform with a team of security experts who act as an extension of an organization's internal team. WhiteHat Sentinel, which has been available in BIG-IP ASM since version 10, is designed to detect, prioritize, manage, and remediate application-based vulnerabilities using a web application firewall. It provides a user-friendly graphical representation of vulnerabilities and their threat scores. It does not use malicious payloads to identify vulnerabilities, which reduces the potential of infecting other systems, and because it's a SaaS-based platform, WhiteHat Sentinel is a completely turnkey solution.

WhiteHat Sentinel automatically scans web applications; a WhiteHat security specialist then validates the scan and provides a report about detected vulnerabilities. Administrators can then mitigate the vulnerabilities via BIG-IP ASM or by recoding them in the application itself.

The BIG-IP ASM and WhiteHat Sentinel integration is seamless. The BIG-IP configuration utility is a single vulnerability management point within the BIG-IP ASM GUI that prevents administrators from having to go back and forth between two UIs. The secure communication between the two solutions is enabled by

WhiteHat Sentinel's identification of BIG-IP ASM via an API key, which is available at the Sentinel admin site. Once vulnerabilities are found and mitigated, Sentinel retesting happens via the BIG-IP ASM GUI.

All interactions are conducted from the BIG-IP ASM user interface and there is seldom a need to access the Sentinel user interface to mitigate vulnerabilities. Vulnerabilities that cannot be automatically mitigated by BIG-IP ASM are presented to the user for manual mitigation. The results are available for download and can be viewed in both the WhiteHat Sentinel and BIG-IP ASM GUIs.

Improved Web Application Visibility

With multiple vulnerability scanner assessments in one GUI, administrators can discover and remediate vulnerabilities within minutes from a central location. BIG-IP ASM offers easy policy implementation, fast assessment and policy creation, and the ability to dynamically configure policies in real time during assessment. To significantly reduce data loss, administrators can test and verify vulnerabilities from the BIG-IP ASM GUI, and automatically create policies with a single click to mitigate unknown application vulnerabilities.

Additional Enhancements in BIG-IP ASM

In addition to the vulnerability scanner integration, BIG-IP ASM (version 11.1 and later) provides context that helps administrators understand attack methods, which better enables them to defend against attacks. And session-based enforcement and reporting gives security analysts an in-depth understanding of attack execution by user. For example, BIG-IP ASM will not only report that a SQL injection attack occurred on the website and the user name that executed it, but it will also associate the application user name with the session and specific violations.

With Violation Correlation, BIG-IP ASM administrators can make multiple violations appear as a single group according to a common rule or criteria. For example, multiple attacks that are coming from the same source IP address can be correlated into a single incident. Administrators can also define a blacklist or whitelist based on IP address geolocation information.

The BIG-IP ASM GUI includes a deployment wizard to secure virtual servers and dynamic reports that offers endless reporting scenarios. For instance, an administrator can receive a report of the top attacked URL of an enterprise's websites. And when there are application issues and web pages are rendering

slowly, virtual server CPU statistics show the CPU utilization per virtual server so operators can troubleshoot performance and capacity issues.

Conclusion

Security is a never-ending battle. The bad guys advance, organizations counter, bad guys cross over—and so the cat and mouse game continues. The need to properly secure web applications is absolute. Knowing what vulnerabilities exist within a web application can help organizations contain possible points of exposure. BIG-IP ASM offers unprecedented web application protection by integrating with many market-leading vulnerability scanners to provide a complete vulnerability scan and remediate solution.

BIG-IP ASM enables organizations to understand inherent threats and take specific measures to protect their web application infrastructure. It gives them the tools they need to greatly reduce the risk of becoming the next failed security headline.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119   888-882-4447   www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com