Vulnerability Assessment with Application Security

Peter Silva, 2012-31-01

The longer an application remains vulnerable, the more likely it is to be compromised.

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.

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.

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. BIG-IP Application Security Manager (ASM) version 11.1 is a WAF that gives organizations the tools they need to easily manage and secure web application vulnerabilities with multiple web vulnerability scanner integrations.

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 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

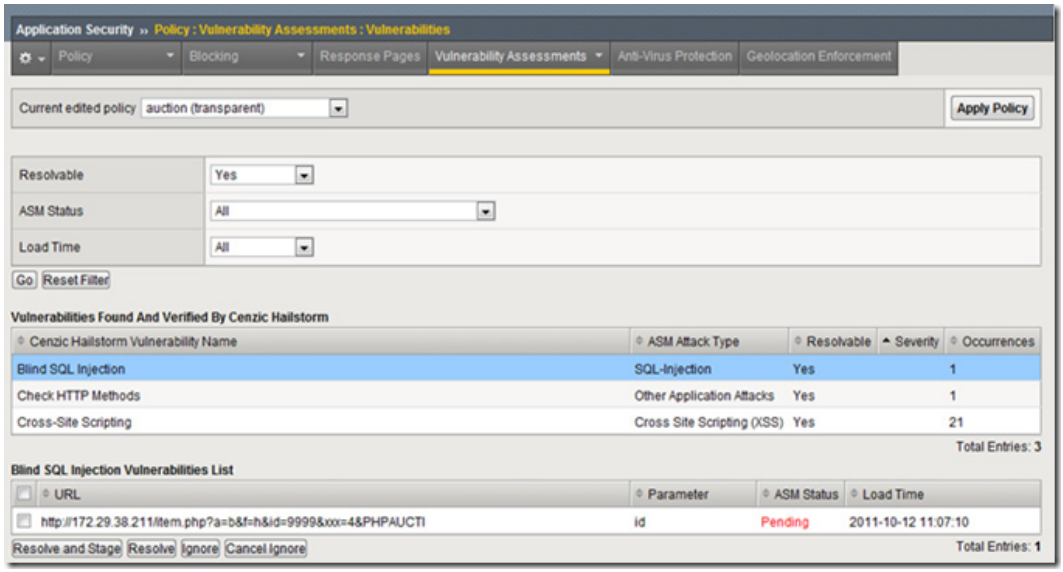
To assess a web application's vulnerability, most organizations turn to a vulnerability scanner. The scanning schedule might depend on a change control, like when an application is initially being deployed, or other factors like a quarterly report. The vulnerability scanner scours the web application, 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. 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 includes integration with IBM Rational 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.

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.

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 v11.1 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 v11.1 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.

ps

Resources:

- F5's Certified Firewall Protects Against Large-Scale Cyber Attacks on Public-Facing Websites
- IPS or WAF Dilemma
- F5 Case Study: WhiteHat Security
- Oracle OpenWorld 2011: BIG-IP ASM & Oracle Database Firewall
- Audio White Paper - Application Security in the Cloud with BIG-IP ASM
- The Big Attacks are Back…Not That They Ever Stopped
- Protection from Latest Network and Application Attacks
- The New Data Center Firewall Paradigm – White Paper
- Vulnerability Assessment with Application Security – White Paper
- F5 Security Vignette: Hacktivism Attack – Video
- F5 Security Vignette: DNSSEC Wrapping – Video

- Jeremiah Grossman blog

Technorati Tags: F5, big-ip, virtualization, cloud computing, Pete Silva, security, waf, web scanners, compliance, application security, internet, TMOS, big-ip, asm

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | 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