Solution Brief

Scanning Web Applications for Vulnerabilities

Safeguarding your critical web applications

The clock is ticking as web applications take center stage as the point of entry for malicious activity and development teams are asked to deliver new applications at breakneck speed. It's only a matter of time before the two converge and your business has to do damage control. The number of websites infected with malware and malvertisements in the third quarter of 2010 is estimated at 1.2 million, double its estimate from the same time period last year. Also, operating system vulnerabilities are declining while web and database vulnerabilities, such as SQL injections and cross-site scripting (XSS), are on the rise—especially XSS, which, in 2010, was 17 times greater than it was in 2002.

Challenges of Web Application Security

- Reliance on and explosive growth of web applications
- Developers have little or no knowledge of creating secure web applications
- High cost of manually testing web applications for security holes

Reliance on Web Applications

If you're like most companies, you've come to rely on the web for serving up a good portion your critical applications, including those tied to commerce, and likely have plans to add even more web-based applications. The truth is that the rapid adoption and ease of deployment of web applications has left countless businesses open to attack by hackers. We've seen it over and over again—web application developers don't know that they've created vulnerable applications that are easily exploited, or because of pressure to get the application launched, they choose not to embed the proper security controls.

Think about the reliance of your business on your web presence. What would happen if your site was defaced or found to be distributing malware? How successful would you be if your customer data and credit card information were stolen? What would the financial impact be if your commerce site was maliciously taken offline? Are you in a regulated industry? As your business becomes more reliant on your web presence, these are just a few of the questions that we find ourselves facing on a daily basis.

Web Application Security Challenges

When you rely on the web for business-critical applications, it's essential that you consider the security implications just like you do for your other critical IT systems. With the number of web-based applications exploding and the new generation of developers and testers having little to no training or experience in designing secure applications, you now need—more than ever before—insights into which web applications are vulnerable.

It's understandable that security challenges exist, since, in most cases, these applications are under tremendous pressure to be up and running and generating revenue as fast as possible, but this often leads to poor design and errors. In addition, these applications are becoming increasingly complex. They usually involve multiple database systems, analytics, authentication, and even external third-party systems. The more complex these applications become, the higher the margin for error, especially when it comes to security controls.

Unlike the traditional operating systems and desktop applications, there are usually no commercial vendors to hold responsible for these applications. In most cases, no one is out there producing patches for your web applications. As our operationalized security models increasingly move to a "security=patching" mindset, these custom applications are often left in the dark. Not only is there no commercial vendor to hold accountable, but these applications are usually built with a plethora of technologies such as C/C++, .NET, Java, PHP, Perl, Python, Ruby, and others, making them even more difficult to test for weaknesses.

Key Benefits

McAfee Vulnerability Manager 7.0

- Proven, highly scalable architecture
- Extensive integration—authentication, asset management, ticket, security information and event management (SIEM), and more
- Discovery to remediation workflow
- Risk-based approach to vulnerability management
- Asset centric scanning—100 percent asset/result reconciliation of dynamic host configuration protocol (DHCP) systems
- Built-in customizable reporting
- Open application programming interface (API) and software development kit (SDK) for complete customization

Web Application Assessment Module

- Web applications are treated as manageable business assets
- Extensive coverage including OWASP, CWE, and more
- Scan for network, operating system, and web vulnerabilities in the same scan
- Discovery, crawling, and mapping
- Authenticated scanning
- Global and local exclusions and parameters
- Tunable performance
- Detection of sensitive content
- Integrated into ticketing for remediation workflow
- Full vulnerability documentation, description, and recommended remediation
- Evidence in reports—what was sent, what was received, and where the vulnerability was detected

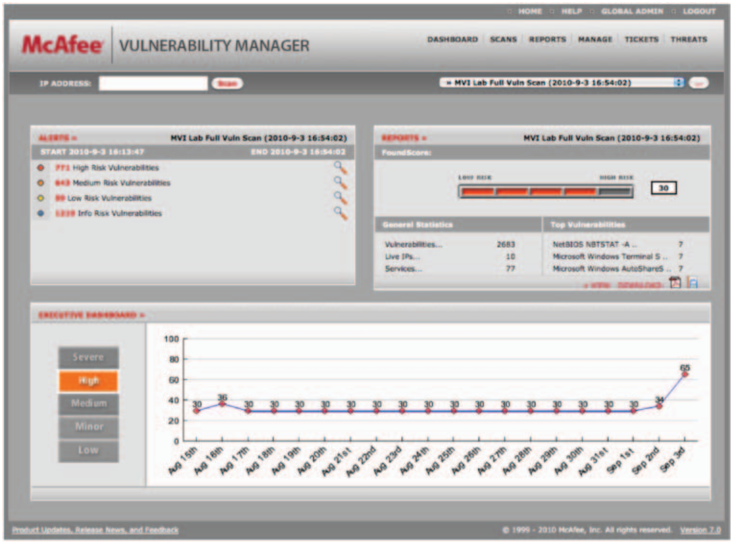
And to compound matters, the complexity of vulnerability detection in web applications is more art than science. Unlike the relatively black and white nature of traditional operating system vulnerabilities, web application vulnerabilities are more subjective and can be very subtle and difficult to detect. For example, a web page that outputs a directory of files might be perfectly allowable for your site, but for someone else, that is a huge vulnerability and results in a data breach. The subjectivity comes into play when determining whether or not the output received from the site was actually the desired output.

There are a few professional services organizations that can come in and manually test your applications for vulnerabilities and other coding issues. However, these specially trained people are usually very expensive, and their hands-on approach, while extremely effective, simply cannot scale to today's enterprise class environments. In addition, if you materially change an application or add new web applications, you'll need to invite them back for another round of testing. Perhaps they offer bulk discounts, but don't count on it.

If these security challenges sound manageable on one or two applications, multiply that by thousands. Today it's common to have tens of thousands of internal and external web applications that deliver revenue to your business and perform other incremental value to your customers and employees. With so many applications, you're faced with a daunting and seemingly insurmountable task of securing these applications. You can't just bury your head in the sand and hope that nothing bad happens.

Introducing: McAfee Vulnerability Manager 7.0

McAfee® Vulnerability Manager 7.0 was built specifically to easily enable companies of any size to scan assets (network devices and systems) for vulnerabilities. With the addition of the new web application scanning, McAfee Vulnerability Manager delivers its proven capabilities to web application vulnerability scanning. Existing customers that have migrated to McAfee Vulnerability Manager 7.0 have nothing further to deploy: no second consoles and no separate databases. They can leverage their existing expertise. New customers can conduct web application scans in a matter of minutes.



General Statistics		Top Vulnerabilities	
Vulnerabilities...	2683	NetBIOS NBTSTAT -A ...	7
Live IPs...	10	Microsoft Windows Terminal S ...	7
Services...	77	Microsoft Windows AutoShareS ...	7

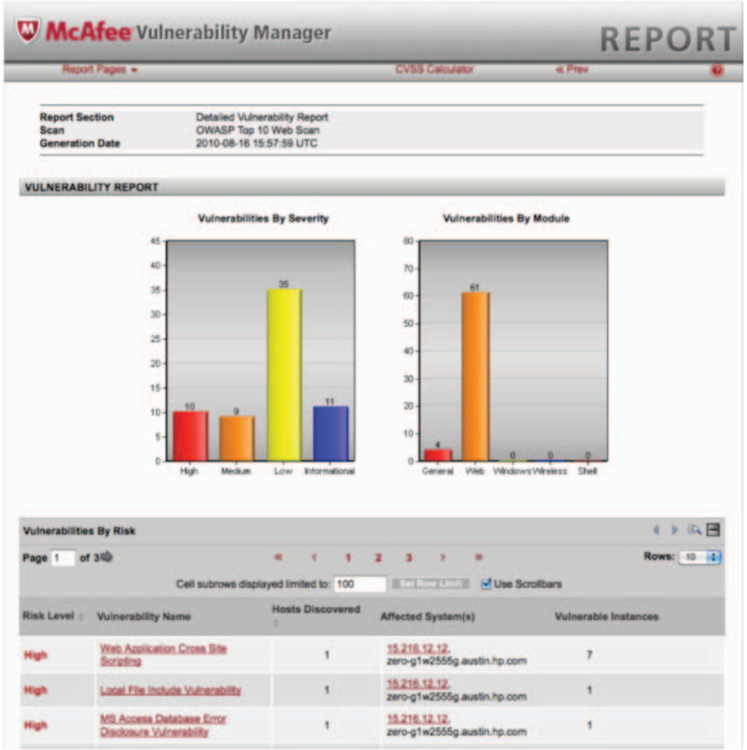
Figure 1. Executive dashboards let you quickly drill down into web vulnerabilities.

Web Application Scanning

McAfee Vulnerability Manager version 7.0's Web Application Assessment Module (WAAM) offers deep web application scanning to ensure that common coding mistakes and vulnerabilities are addressed as part of a vulnerability management lifecycle. What makes it unique is that it treats web applications as business assets, just like a server, router, or other high-value assets. This is important since web applications have business value and therefore have asset owners and varying levels of criticality. Treating them like traditional assets allows you to group and manage them like physical assets, allowing you to address web applications the same way you would handle other risk-prioritized assets in your environment. By using the Web Application Assessment Module's deep scanning capability and treating web applications as "first-class" citizens, you're able to more quickly deploy applications with a high level of confidence that hackers are not able to exploit those applications.

The Web Application Assessment Module covers commonly exploited web application vulnerabilities and weaknesses in the market today. Specifically, the Web Application Assessment Module includes the required checks for PCI DSS as well as coverage of the OWASP Top 10 and the CWE-25 categories. The Web Application Assessment Module is a completely integrated (user interface, reporting, engine, ticketing) module of McAfee Vulnerability Manager 7.0. It's ideally suited for customers wanting to extend the full vulnerability lifecycle management capabilities of McAfee Vulnerability Manager to deliver comprehensive, scalable, and recurring/schedulable web application vulnerability scanning of websites.

Instead of taking a piecemeal approach with your web application security, McAfee Vulnerability Manager allows you to take a risk-based approach to finding, assessing, and remediating web application vulnerabilities.



Report Section	Detailed Vulnerability Report
Scan	OWASP Top 10 Web Scan
Generation Date	2010-08-16 15:57:59 UTC

VULNERABILITY REPORT

Vulnerabilities By Risk

Page 1 of 3

« ‹ 1 2 3 › »

Rows: 10

Cell subrows displayed limited to: 100 Set Row Limit ☑ Use Scrollbars

Risk Level	Vulnerability Name	Hosts Discovered	Affected System(s)	Vulnerable Instances
High	Web Application Cross Site Scripting	1	15.216.12.12, zero-g1w2555g.austin.hp.com	7
High	Local File Include Vulnerability	1	15.216.12.12, zero-g1w2555g.austin.hp.com	1
High	MS Access Database Error Disclosure Vulnerability	1	15.216.12.12, zero-g1w2555g.austin.hp.com	1

Figure 2. Visual reports show you where to focus your attention.

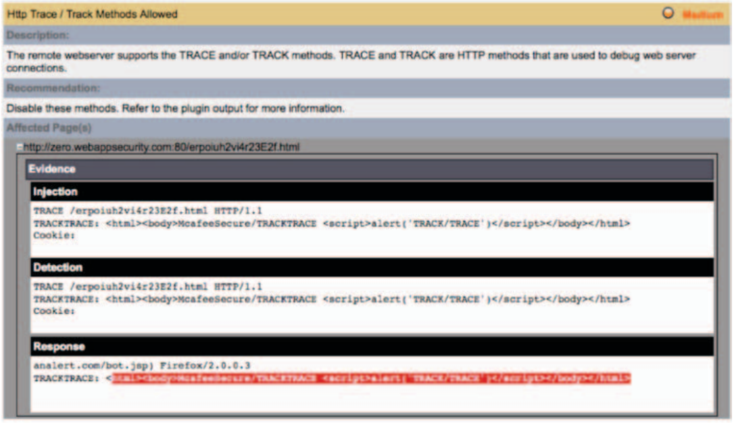
Web Application Vulnerability Reporting

Like most systems, reporting is a very important aspect of web application vulnerabilities. If you cannot view what's wrong, then you don't know what to remediate. Many web applications scanners either are too light (that is, they do not show enough beyond the vulnerability description) or go overboard and store hundreds of megabytes of raw data per application. Having too much raw data requires a very knowledgeable staff to sift through the data and determine what needs to be remediated. Neither option works. Too little data is useless, whereas too much data makes the storage and knowledge requirements too burdensome for scalable web application scanning.

McAfee Vulnerability Manager delivers an optimal mix of description and recommended remediation information that includes captured evidence from the site. It's careful not to go too far overboard in evidence so as not to negatively impact scalability, while still providing enough evidence to know where the vulnerabilities exist. This allows your less knowledgeable users to help developers pinpoint the vulnerability to speed remediation.

Summary-level graphs, delta, and trend data is readily available for web application vulnerability results, just as with traditional vulnerability data. McAfee Vulnerability Manager has both scan and custom reporting available straight out of the box. Supported direct access to the vulnerability database is also available for integration or enterprise extended reporting requirements.

Hyperlinked reports allow you to quickly drill down into detailed data either about the application or the vulnerability itself to see the evidence.



The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Disable these methods. Refer to the plugin output for more information.

http://zero.webappsecurity.com:80/erpoiuh2vi4r23E2f.html

```
TRACE /erpoiuh2vi4r23E2f.html HTTP/1.1
TRACKTRACE: <html><body>McafeeSecure/TRACKTRACE <script>alert('TRACK/TRACE')</script></body></html>
Cookie:
```

```
TRACE /erpoiuh2vi4r23E2f.html HTTP/1.1
TRACKTRACE: <html><body>McafeeSecure/TRACKTRACE <script>alert('TRACK/TRACE')</script></body></html>
Cookie:
```

```
analert.com/bot.jsp) Firefox/2.0.0.3
TRACKTRACE: <html><body>McafeeSecure/TRACKTRACE <script>alert('TRACK/TRACE')</script></body></html>
```

Figure 3. You can even review the vulnerable code.

Web Application Vulnerability Coverage

A web application scanner isn't much good if it cannot detect common and current vulnerabilities. While no automated scanner is as effective as a properly trained security tester, strong coverage of vulnerabilities is essential. The Web Application Assessment Module contains industry-leading vulnerability detection capabilities. In addition to out-of-the-box coverage, McAfee Vulnerability Manager is backed by the world's leading vulnerability and threat research organization, McAfee Labs™, with more than 400 dedicated researchers covering the globe. McAfee Labs continually feeds McAfee Vulnerability Manager new vulnerability information and content.

Conclusion

McAfee Vulnerability Manager is a proven, highly scalable, industry-leading vulnerability management solution. It offers traditional network, operating system, application, database, and now web application vulnerability scanning and management in one cohesive product. The new web scanning capability allows you to discover, crawl, assess, report, and manage the vulnerabilities discovered in any number of internal or external web applications. Treating web applications as the business assets that they are, combined with McAfee Vulnerability Manager's risk-based approach to vulnerability lifecycle management gives you the most powerful and scalable vulnerability management.

Next Steps

If you would like more information on McAfee Vulnerability Manager and the Web Application Assessment Module, please visit: http://www.mcafee.com/vm or contact your local McAfee representative or reseller near you.

About McAfee Risk and Compliance

McAfee Risk and Compliance products help you minimize risk, automate compliance, and optimize security. Our solutions diagnose your environment for real-time insight into your vulnerabilities and policies so that you can protect your most critical assets by focusing security investments where they matter most. To learn more, visit www.mcafee.com/riskandcompliance.

McAfee, Inc.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com