

Assessing Assessment: Top 10 Questions When Evaluating Application Vulnerability Scanners

Over the last year, application security has received increasing attention. Organizations are realizing that no one hacks Windows over the Internet and that to truly protect private and business critical information, the application layer must be secured. There are a variety of application security scanning solutions available and many professionals have fundamental questions about the options. How do application scanners work? How are they used? Who within the organization should use them?

By understanding your organization's unique requirements, you can separate the fluff from the function and select solutions that will provide the best return on investment. Here are 10 important questions to address prior to selecting application security solutions:

1. How is your site constructed?

How big is your site? What types of Web technologies is it built with? What are the attack vectors, or the aspects of the site that create inherent site exposure? Understanding your site is the first step in knowing how to secure it.

2. Are you running complex authentication or session routines?

Software is inherently dumb. Unexpected responses generally result in failure. Web-form authentication and session management are dynamic. Know your site authentication requirements and make sure the scanner is able to handle such complexities on its own. If it can't, one of two things will be required: run it manually or ignore that part of your site.

3. Can the scanner look at your entire site?

It is important to have a solid understanding of your site size, architecture and content in order to verify the scanner is exercising the entire site. If a scanner can't interact with certain types of content, part of your site is getting ignored.

4. Does your site include common features such as custom error pages, Web server obfuscation, forced session changes, or URL-based cookies?

All error pages are not created equal. Some divulge immediately destructive information, some provide useful information and some are benign. Tactics like Web server obfuscation, session routines that force token changes and URL-based cookies make it even harder. Verify that the scanner can manage whatever processes may likely trip it up.

5. Automation?

Got links? If a scanner requires you to manually manage the scan to authenticate, identify custom error pages, execute JavaScript, or determine if something is vulnerable, you are faced with a losing battle. Identify your tolerance for manual features vs. manual requirements.

6. How will you evaluate accuracy?

Do you have a previously audited application with which to compare results? If you know what is secure and what is vulnerable, you can verify the scanner's accuracy.

7. What types of vulnerability assessment are you looking for?

While scanning for known vulnerabilities is an important aspect of security, it is distinct from checking dynamic, unknown vulnerabilities such as input validation, authentication/authorization, session strength and client-side code. Make sure the assessment features target your security concerns.

8. What are your reporting and data requirements?

The security team, development and QA teams, and executives each require different data to engage the issues. Make sure resulting data is consumable and useful to all involved.

9. Who should be on the evaluation team?

Make sure you know who will use the solution and integrate them into the evaluation process.

10. Does your evaluation plan accurately represent how you will use the solution?

Does your test environment realistically represent actual complexity, size, content and architecture? Make sure you test it in a manner that reflects future use.

All vendors claim to solve the problem. The truth is, though, that not all problems are the same. Make sure you have all the necessary information to select technology that addresses your challenges. Remember, technology alone is not a solution. It is only through the proper use of the right technology that people can successfully address the challenges at hand.

As you seek out the best application security solutions for your organization, arm yourself with information to make informed technology decisions and hold your vendors accountable.

About the Author

Erik Caso is vice president of product development at NT OBJECTives (www.ntobjectives.com) in Irvine, CA. He is on the board of the Web Application Security Consortium and is an advisor to numerous industry groups. He holds degrees in business and economics from Cal Poly San Luis Obispo.