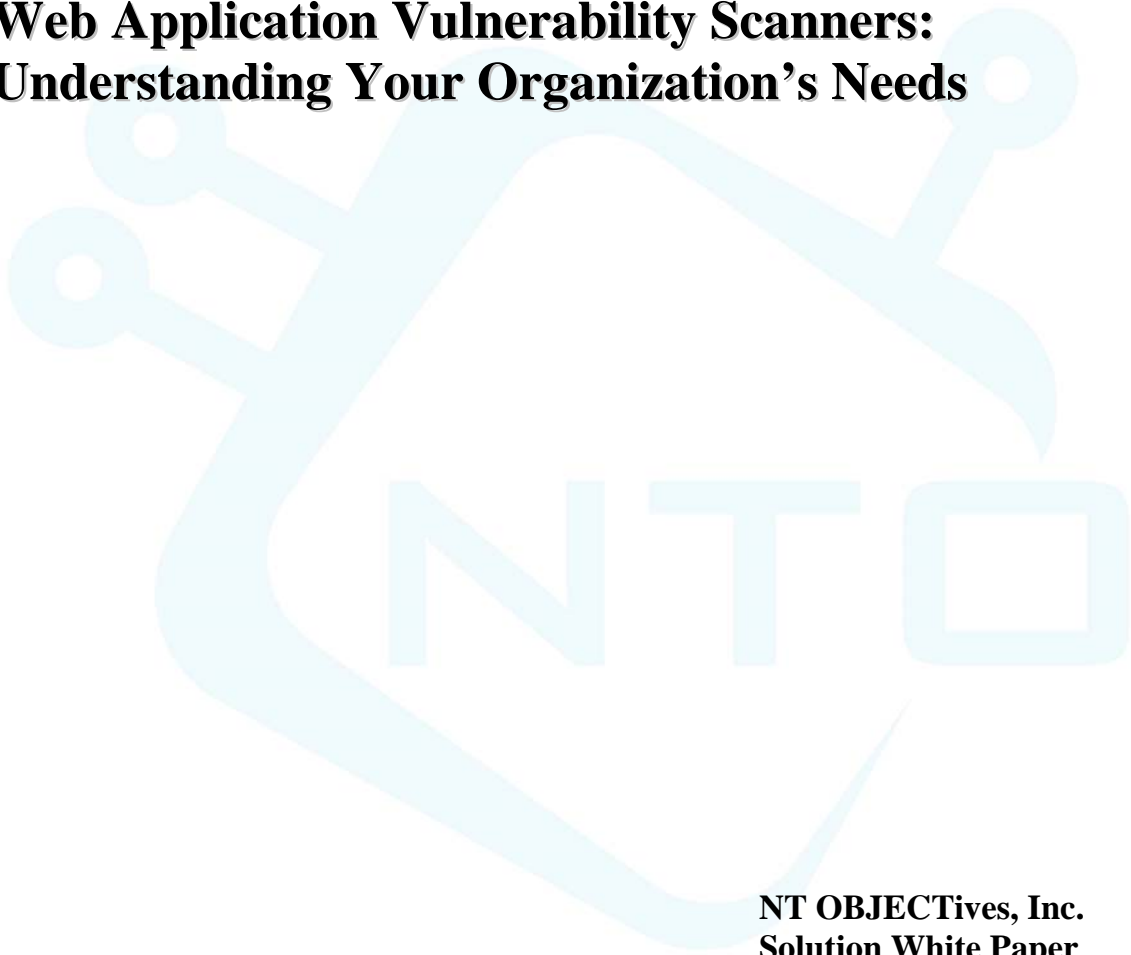


Web Application Vulnerability Scanners: Understanding Your Organization's Needs



**NT OBJECTives, Inc.
Solution White Paper
Authored by Erik Caso**

Web Application Vulnerability Scanners: Understanding Your Organization's Needs

Over the last year we've seen tremendous attention directed at application security, as if the world suddenly realized that no one hacks Windows over the Internet. In this time, many companies have come into existence and many solutions have come to market. And while application security is a young sector of the IT community, the technologies within it are even younger. Application vulnerability scanners, application firewalls, source code scanners and all the rest are incredible tools to help secure what Gartner says is the target of 70% of all Internet attacks – the web application.

As a quickly growing, albeit somewhat nascent, industry, however, there are many challenges to consumers today. How do application scanners work? How do you use them? Who in the organization should use them? Over the last few years, we've encountered all manner of personnel knowledge levels, corporate budgets and security priorities, but it seems the most important question has often not been answered – *What is it that you really need these things to do?*

With that in mind, this paper focuses on 10 important questions that aim to help you understand what your organization needs from an application vulnerability scanner. Before considering any vendor and all their wonderful features, it is critical to understand what you need, what you care about and how you will verify this. We have found that by understanding your organization, you can better evaluate and purchase a technology that will best serve you. As application security assessment needs are different than application security defense needs, this paper will focus on assessment, specifically as it applies to evaluating an application vulnerability scanner.

1. How your site is 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 (i.e. risk to attack)? Your scanner should help you understand these issues. Application security is more than a work-list of things to fix. It is a dynamic, evolving problem that is almost infinitely complex. If your scanner doesn't help you build a long-term policy to address and solve this problem, you will find yourself continually facing the same work-list, year after year.

Net: Ignore the notion of discreet vulnerabilities here, and make sure the product assists you in your knowledge and security policy requirements going forward. This will result in fewer vulnerabilities down the road, because you have been able to translate site knowledge into business and security process.

2. Are you running complex authentication or session routines, and can the scanner manage through your session process?

Software is dumb. Unexpected responses generally result in failure. While network scanners have the luxury of interacting with primarily protocol-based technologies, application scanners absolutely do not. Complex web-form authentication, session management and encryption routines are entirely dynamic. Automating these routines is critical to the scanner's ability to interact with 100% of your site.

Net: Make sure your scanner is smart enough to handle such complexities by default on its own. If it can't one of two things will be required- you will have to manually manage the authentication process or whatever part of your site that is behind such authentication will not get examined.

3. Can the scanner look at your *entire* site?

Application-based content can utilize an innumerable amount of complicated, customized technology that is almost impossible to specifically account for. A prime example is

Web Application Vulnerability Scanners: Understanding Your Organization's Needs

dynamic pages created by JavaScript. JavaScript is a challenge for every application security vendor. It requires complex parsing routines to execute functions and interact with otherwise more complicated site content. Many scanners simply perform a source review of HTML to find the <href>s and execute the links. Dynamic content created with JavaScript is often entirely ignored. Remember, if these links can not be crawled, they will not be security tested. If a scanner can not execute JavaScript on your site you are faced with either assessing it manually or not assessing this portion of your site at all.

If your scanner can't utilize human interactive behavior to manage the scan on its own, you are left either having to run the scan manually or even precluded from scanning 100% of the site. Both cases are untenable in security. It is critical to first identify your entire site (servers, applications, technologies, resources, etc.) and then completely assess it for application specific threats (hint: this goes far beyond known vulnerability checks).

Net: When evaluating scanners, make sure you know how much of your site is being evaluated. Is anything getting missed? If something is getting missed, is there a work-around and is it acceptable? Most often the work-around is "manual scanning", where you tell the scanner what to do. This is obviously a problem for a site of any significant size, so make sure you are getting features that are most important to you doing your job (not the scanners!)

4. Can the scanner interact with common, often confusing, site features such as custom error pages, web server obfuscation, forced session changes, URL-based cookies and more?

All error pages are not created equal. Some divulge immediately destructive information, some provide useful information and some are benign. A good scanner must differentiate between these. Across the board we are confronted with dynamic issues that make this job harder: web servers are obfuscated (often times very well); session routines can force token changes; cookies can be token or URL-based; and the list goes on. An effective scanner must be able to prevent these issues from stopping the scan or from creating bad data (i.e. false-positives).

Net: Ensure that the scanner can manage whatever processes may trip it up. This can have a significant impact on scan accuracy and comprehensiveness.

5. Will the scanner run by itself, or are you required to operate it?

Got links? Automation is the only way to scan today's complicated enterprise sites, which can have tens of thousands of links. If your scanner requires you to manage the scan (e.g. in order to authenticate, identify custom error pages, execute JavaScript, or determine if something is vulnerable) you are faced with a losing battle. Furthermore, less-savvy departments within the organization may not have the time or technical knowledge to make sure the scans are operating properly. Your scanner is supposed to do that for you.

Net: There are manual requirements and manual features. One is a benefit, the other a burden. Make sure your scanner works for you, not the other way around.

6. Is it accurate?

We mean really accurate. Have you run it against a previously audited application and compared results? Does the scan provide results indicating that you may be "possibly vulnerable"? Remember, all error pages are not created equal. If a scanner utilizes rudimentary response analysis techniques, a complex site may generate arguably reliable data. Make sure the scanner provides useful, exact responses and is not generating false-positives or false-negatives.

Web Application Vulnerability Scanners: Understanding Your Organization's Needs

Net: Try to test systems that have recently been audited in order to compare results. If you know what is secure and what is vulnerable, you can verify accuracy.

7. Do you want to test for application vulnerabilities, known web server vulnerabilities, both?

Many scanners focus their vulnerability checking on the known, signature-based checks that primarily target CGIs and web server platforms. While scanning for known vulnerabilities is an important aspect of security, it does not help at all with dynamic, unknown application vulnerabilities such as input validation, authentication/authorization and session strength, encryption, client-side code, etc. Make sure your *application vulnerability* scanner is looking for *application* security risks, that it does it well and without compromise.

Net: Application vulnerabilities are tremendously complicated to test for. Get to know how your potential vendors design their assessment features in order to make sure they cover what you need and can get the job done. Assessment techniques can range from rudimentary string-replacement methods to intelligent, permutation-based assessment methodologies. The results can be staggeringly different.

8. Are the reports and the data usable?

Who are the reports designed for? The security team, the development and QA teams, and management are all very different audiences and need different results to make use of them. Do the reports indicate what is done well, in addition to what needs work? Do the vulnerability descriptions and recommendations educate the user to understand the security implication and fix it (step-by-step) immediately? Not all data is useful, so make sure that what you are getting helps you get your job done with minimal re-processing of the scan output.

Additionally, what do you plan to do with the raw data? Does it need to be integrated with other enterprise systems? Is it in a format that easily ports to other systems or products? What happens if a new version of the product comes out and the data format changes? Scan data transcends simple work-lists to fix discreet vulnerabilities. It plays a major role in understanding enterprise security. It is a part of numerous security datasets from other systems including firewalls, IDS, network scanners, anti-virus and more. Your data should be easily re-usable, whether the technology changes or not. It shouldn't take a team of consultants, a ton of time and money to make it work for you outside your scan reports.

Net: Make sure any and all people who will be using the reports are able to understand and act upon them easily. If you want to integrate scan data with other enterprise security datasets, make sure doing so is reasonably within reach of your data's native format.

9. Does your evaluation test site legitimately represent the complexity and content of your production environment(s)?

Do you have a test environment in which to run all technologies you are evaluating? Does that test environment realistically represent your enterprise (i.e. complexity, size, content, architecture, etc.)? Often times, people evaluate software by testing arbitrary servers lying around the office. Having answered the previous questions, you should be aware of how you will be using whatever technology you purchase and what it will be required to interact with. Make sure you test it in a realistic manner that allows you to feel confident it will really perform for you once you have made a purchase decision.

Net: Make sure you find a suitable test bed to evaluate technology in your organization. It should, as close as possible, match your enterprise production environments. This way you have a firm idea as to how the technology will perform when purchased.

Web Application Vulnerability Scanners: Understanding Your Organization's Needs

10. Upon purchasing a scanner, who will be using it and what will they be scanning?

Often times, this is an afterthought. The first part of this question is important to the evaluation process because you want the expected user-base (e.g. development, QA, IT/security, etc.) to understand the technology in order to make good use of it. Is the solution intuitive to all users? Do they understand the data, and can it fit into their work processes? Non-security specific personnel often times need mentoring in order to get the most out of an esoteric solution such as an application vulnerability scanner.

Secondly, and perhaps most important here, is what will you be scanning? A comprehensive application security program will review applications pre-production (i.e. during development and QA) as well as post-production. Production scanning is a tremendously important consideration during the evaluation due to the aggressive nature of certain types of security testing. Does the scanner issue malicious or dangerous requests to the target (e.g. issuing a <DELETE> statement to the database)? If so, can you easily disable these types of vulnerability checks; and if you do, will it negatively impact your production assessments? Can you force a scan attack policy to ensure no one ever uses such features when production scanning?

Net: Make sure you know who will be using the purchased technology and integrate them into your evaluation process. Most importantly, get to know what types of application assessment are being performed and determine how it will affect any production systems scanning.

At the end of the day, all vendors say they solve *the* problem. The truth is, though, that not all problems are the same. Furthermore, technology is not yet a solution in and of itself; rather, it is an enabler. Only through the use of the right technology can *people* solve the problem. Make sure you find the technology that helps solve your problems. To do that it is critical to understand your organization's needs. Be armed with the information necessary to buy the right technology to help you, and hold your vendor accountable.

Web Application Vulnerability Scanners: Understanding Your Organization's Needs

About NT OBJECTives, Inc.

NT OBJECTives, based in Orange County, California, brings together an unprecedented collection of this industry's top experts to offer a comprehensive suite of industry-leading technology and services to solve the application security problems of today's global business leaders. Through the synergy of the top security software developers and some of the industry's best consultants and researchers, NTO has created the first next-generation, automated technology capable of performing accurate application security audits. Coupled with a comprehensive service offering, including security training services, NTO is uniquely positioned to provide complete application security solutions to today's businesses.

About Erik Caso

Erik Caso is VP of Product Development and Marketing at NT OBJECTives, where responsible for driving NTO's' marketing and product strategies. Mr. Caso brings an extensive background in business strategy, product and business development to NT OBJECTives.

Prior to NT OBJECTives, Erik worked at Foundstone, where as Product Manager he led that company's flagship product, FoundScan, from a first generation technology to a third generation market leader. During this time he was instrumental in building product, sales and marketing strategies for the company. Prior to Foundstone, Erik led product and business strategies for companies such as Epoch Internet and The Boeing Company.

Mr. Caso is board member of the Web Application Security Consortium, and is an advisor to numerous industry groups and vendors. He holds degrees in business and economics from Cal Poly San Luis Obispo.