

A MODERN APPROACH TO DYNAMIC APPLICATION SECURITY TESTING

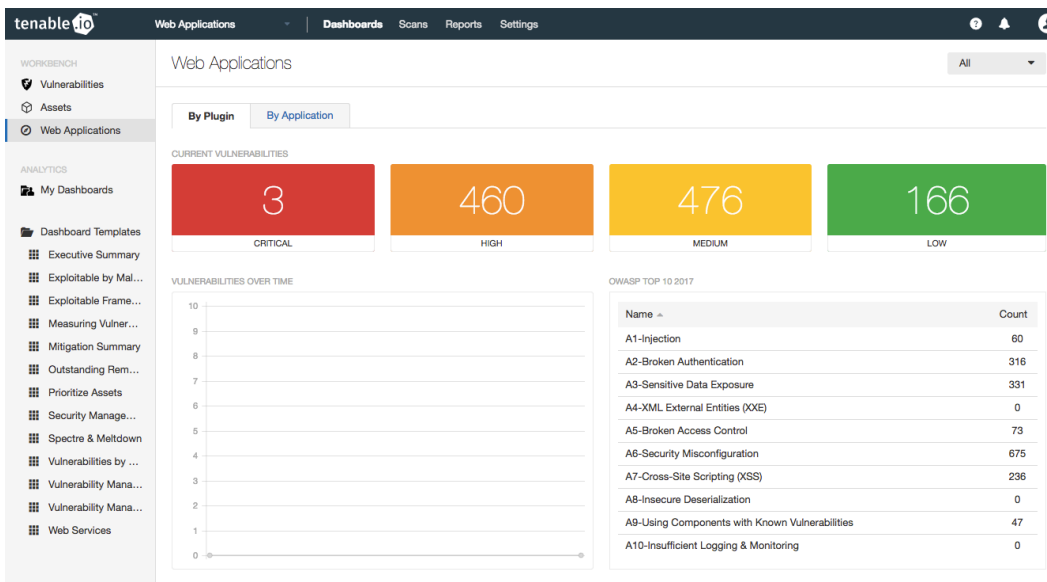
Modern web applications continue to be a challenge for organizations to secure as developers build increasingly complex business applications faster than ever. Many organizations are releasing new or updated web applications multiple times per day, each containing multiple vulnerabilities on average. Often outnumbered by developers by 100:1, security teams are struggling to keep up, and many web applications are not assessed for security issues until it's too late. Lack of application security skills and resources inhibit many organizations from adequately defending against cyberthreats.

But yet another standalone security product isn't the answer. Security leaders must have visibility into the security of all of their web applications as part of a comprehensive Cyber Exposure solution to gain a complete view of their security and compliance posture.

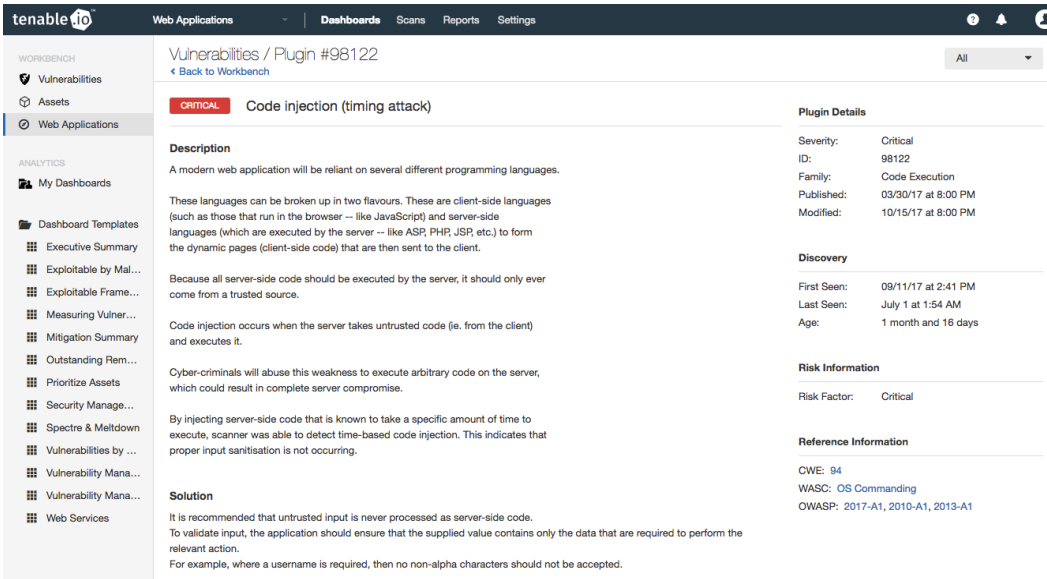
Tenable.io™ Web Application Scanning provides this visibility as part of a comprehensive Cyber Exposure solution. The product delivers safe and automated vulnerability scanning to cover the entire online portfolio, so security professionals can rapidly assess their web applications without heavy manual effort. Tenable.io Web Application Scanning provides high detection rates with minimal false positives, ensuring you understand the true cyber risks in your web applications.

KEY BENEFITS

- Improve Scanning Confidence**
 Deliver highly accurate results with minimal false positives and negatives, giving you and your developers confidence that your reports are accurate.
- Reduce Manual Work Efforts**
 No-touch automated scanning allows you to understand your web application security risks as your environment changes without the manual effort and time otherwise needed.
- Remove Security Blind Spots**
 Scan all of your applications, including those built using modern web frameworks, such as JavaScript, AJAX and HTML5.
- Eliminate Application Disruptions**
 Define the parts of your web applications that are safe to be scanned to prevent disruptions or performance latency in critical web applications due to scanning.
- Reduce Product Sprawl**
 Gain visibility into your true cyber risks across your modern attack surface as part of the Tenable Cyber Exposure platform to decrease complexity and product sprawl.



Tenable.io Web Application Scanning allows security teams to view identified vulnerabilities to ensure visibility and prioritize remediation.



Vulnerabilities / Plugin #98122

CRITICAL Code injection (timing attack)

Description
A modern web application will be reliant on several different programming languages. These languages can be broken up in two flavours. These are client-side languages (such as those that run in the browser -- like JavaScript) and server-side languages (which are executed by the server -- like ASP, PHP, JSP, etc.) to form the dynamic pages (client-side code) that are then sent to the client. Because all server-side code should be executed by the server, it should only ever come from a trusted source. Code injection occurs when the server takes untrusted code (i.e. from the client) and executes it. Cyber-criminals will abuse this weakness to execute arbitrary code on the server, which could result in complete server compromise. By injecting server-side code that is known to take a specific amount of time to execute, scanner was able to detect time-based code injection. This indicates that proper input sanitisation is not occurring.

Solution
It is recommended that untrusted input is never processed as server-side code. To validate input, the application should ensure that the supplied value contains only the data that are required to perform the relevant action. For example, where a username is required, then no non-alpha characters should not be accepted.

Plugin Details
Severity: Critical
ID: 98122
Family: Code Execution
Published: 03/30/17 at 8:00 PM
Modified: 10/15/17 at 8:00 PM

Discovery
First Seen: 09/11/17 at 2:41 PM
Last Seen: July 1 at 1:54 AM
Age: 1 month and 16 days

Risk Information
Risk Factor: Critical

Reference Information
CWE: 94
WASC: OS Commanding
OWASP: 2017-A1, 2010-A1, 2013-A1

Gain actionable insight into web application vulnerabilities and remediation instructions for developers to fix security issues.

KEY CAPABILITIES

Understand Your Web Applications

Tenable.io Web Application Scanning helps you understand the sitemap and layout of your web applications. You can perform a crawl that shows you parts of the web application that the scanner sees, providing more detailed information about the web applications you own.

“At-a-Glance” Dashboard Visibility

Dashboards in Tenable.io Web Application Scanning give you “at-a-glance” visibility into scanned web applications. View vulnerabilities over time and based on risk level, OWASP Top 10 security issues, and descriptions of all vulnerabilities with detailed remediation instructions for developers.

Safe Scanning of Web Applications

In order to prevent performance latency and disruptions, it's important to define parts of critical web applications that are safe to scan and define other parts that should never be scanned. With Tenable.io Web Application Scanning, you can exclude parts of the web application to be scanned by providing the URLs or file extensions to be excluded from the scan, ensuring the scanner is non-intrusive.

Automated Web Application Scanning

With the scarcity (and cost) of security professionals, it's important to find solutions that offer automation to help alleviate the lack of security resources. Tenable.io Web Application Scanning allows you to simply and rapidly assess all of your web applications with a highly automated solution that reduces your manual work effort.

Unified Web App Scanning and Vulnerability Management

Tenable.io Web Application Scanning delivers comprehensive and accurate web application scanning into the Tenable Cyber Exposure platform so you can gain a complete view of your security and compliance exposure. This helps eliminate data silos and minimize the burden of product sprawl, so you can understand your cyber risk and protect your organization with one solution.

Coverage of HTML5, JavaScript and AJAX Web Applications

Legacy web app scanners can't keep up with the modern applications that have exploded in development today. Tenable.io Web Application Scanning is not only able to scan traditional HTML web applications, but also supports modern web applications built using HTML5, JavaScript and AJAX frameworks.

Advanced Authentication Support

Many web applications implement authentication to control access to sensitive user data, which can inhibit the ability for vulnerability scanners to assess the application. Tenable.io Web Application Scanning supports a broad range of authentication options, such as form-based authentication, cookie-based authentication, NTLM support, and Selenium-based authentication, to address most web application requirements.

For More Information: Please visit tenable.com
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact