



# Tenable.io Web Application Scanning for K2

## Enhance Web Application Security Testing

### Business Challenge

Today's web applications have seen a rise in the complexity and deployment frequency to keep pace with demands of the modern business. Even with an increased focus on security development, web applications are still making it to production with critical vulnerabilities that are exploitable by cyber criminals. Oftentimes, when a vulnerability is found in production it's too late which drastically increases risk for exploitation and requires more time and resources to fix.

### Solution

The K2 integration with Tenable.io Web Application Scanning (WAS) enhances the visibility and information by monitoring the application execution directly on the application server, while Tenable.io WAS launches its scans. K2 supplement's Tenable.io WAS by providing additional detail on discovered vulnerabilities, including exact filename and line of code where the vulnerability exists to help organizations locate the vulnerability and remediate the issue. K2 has developed an innovative technology to detect "hidden" vulnerabilities in web applications during a scanning run by Tenable.io. The integration between K2 and Tenable gives organizations the ability to generate a single unified report using Tenable.io APIs, reducing the time that would otherwise be needed to correlate two separate reports.

### Value

By combining Tenable and K2 for the web application testing process, organizations benefit by reducing the remediation time needed to fix discovered vulnerabilities and releases the web applications to production. In addition, the integration of K2 with Tenable.io offers organizations the ability to discover additional hidden vulnerabilities, reducing the number of vulnerabilities that make it to production, and cutting down the number of successful attacks by cyber criminals when the application is in production.



### Technology Components

- Tenable.io Web Application Scanning
- K2 Security Platform
- K2 Report Generator

### Key Benefit

- Get web applications to production in less time
- Remediate discovered vulnerabilities quickly
- Pinpoint location of discovered vulnerabilities quickly
- Reduce the amount of vulnerabilities that make it to production in web applications
- Help quickly identify possible false positives

## ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at [www.tenable.com](http://www.tenable.com).

## ABOUT K2

K2 Cyber Security delivers the Next Generation Application Workload Protection Platform to secure web applications and container workloads against sophisticated attacks including OWASP Top 10 and memory-based attacks, and provides additional vulnerability detection. K2's Platform is deployed on production servers for runtime protection of applications and on pen-testing/pre-production servers to identify the location of the vulnerable code in real-time. K2's solution generates almost no false alerts, eliminates breaches due to zero-day attacks, detects attacks missed by traditional security tools including Web Application Firewalls, and dramatically reduces security cost. K2 Cyber Security is located in the USA, and provides cyber security solutions globally. Learn more at [k2io.com](http://k2io.com)



# Features

With this integration, you can:

- View a single report of discovered vulnerabilities by both Tenable and K2
- Report on detailed vulnerability telemetry including vulnerable file name and specific line of code
- View a summary of vulnerable URLs and vulnerability type

## How It Works

1. Add the K2 agent to the application server
2. Use K2's Report Generator after the Tenable.io WAS scan

K2 & TENABLE JOINT REPORT	
	
Summary	
Total Critical/High Risk Vulnerabilities = 6	
Critical/High Risk Vulnerabilities (Found by Both K2 and Tenable) = 4	
Critical/High Risk Vulnerabilities (Found by Tenable Only) = 0	
Critical/High Risk Vulnerabilities (Found by K2 Only) = 2	
Vulnerable APIs	
URI	Vulnerabilities
/userSearch.action	SQL Injection Attack
/listProduct.action?searchQuery=782014s7es9%3cscript%3ealert(1)%3c%2fscript%3elub6cajz75	Reflected XSS Attack
/listProduct.action	Reflected XSS Attack SQL Injection Attack
/ping.action	Remote Code Execution
/register.action	Stored XSS Attack

Security teams can use reporting that combines Tenable.io web application vulnerability insights with K2 to pinpoint the location of discovered vulnerabilities

## More Information

Get the latest apps here:

<https://www.tenable.com/products>

<https://www.k2io.com/free-trial/>

For support please contact: [support@k2io.com](mailto:support@k2io.com)

COPYRIGHT 2020 TENABLE, INC. ALL RIGHTS RESERVED. TENABLE, TENABLE.IO, TENABLE NETWORK SECURITY, NESSUS, SECURITYCENTER, SECURITYCENTER CONTINUOUS VIEW AND LOG CORRELATION ENGINE ARE REGISTERED TRADEMARKS OF TENABLE, INC. TENABLE.SC, LUMIN, ASSURE, AND THE CYBER EXPOSURE COMPANY ARE TRADEMARKS OF TENABLE, INC. ALL OTHER PRODUCTS OR SERVICES ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS.