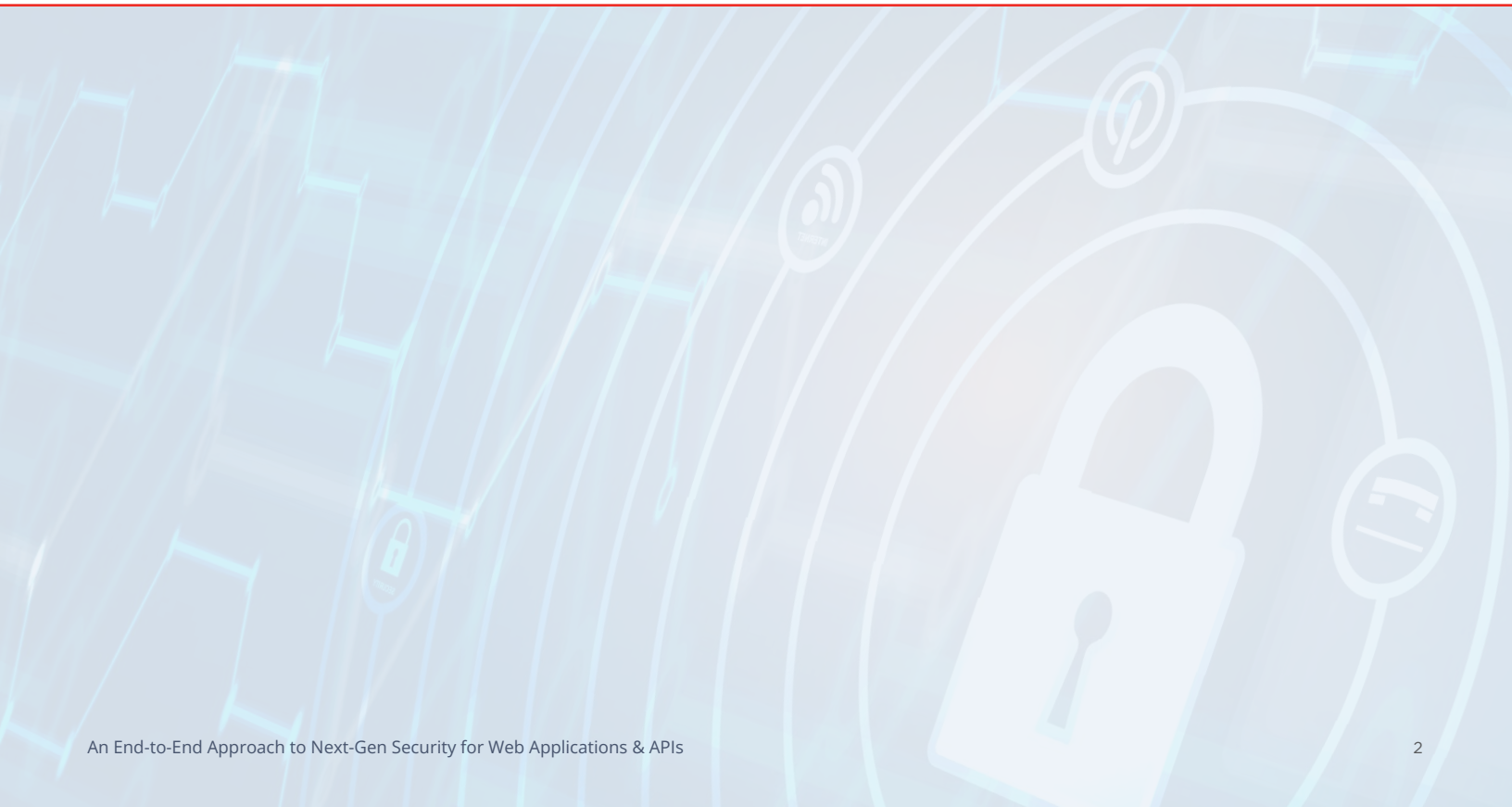
Qualys.

WHITEPAPER

An End-to-End Approach to Next-Gen Security for Web Applications & APIs

Table of Contents



According to Verizon's 2022 Data Breach Investigations Report, web applications remain both the top hacking vector and data breach pattern, accounting for roughly 70% of security incidents. This is because web applications are everywhere and easily probed for weaknesses. A vulnerability in any small or seemingly insignificant web application or API can potentially serve as an entry point for intrusion into your network.

Securing your web applications and APIs starts with knowing what you have. All organizations have web applications and APIs in production, both Internet facing and internal. Some may be custom made by your developers and hosted in the public cloud, while others are vendor-supplied apps of unknown security posture. Additionally, web applications and APIs are constantly growing, expanding, and getting updated with new releases continuously pushed into production. Security cannot be ignored for any single one of them, but application security testing must not slow down the development process.

Web applications remain both the top hacking vector and data breach pattern, accounting for roughly 70% of security incidents.

About the Qualys Web Application Scanning Catalog

Having an up-to-date inventory of your web apps and APIs is crucial, and Qualys Web Application Scanning (WAS) can help. Web apps and APIs are essentially services that function over HTTP and/or HTTPS. The Qualys WAS catalog serves as a repository and triage area for these services, surfacing apps and APIs that the Cybersecurity team may or may not know about.

The Qualys WAS catalog is populated by three different sources:

- ✓ Vulnerability Management (VM) scans
- ✓ VM map scans
- ✓ WAS scans

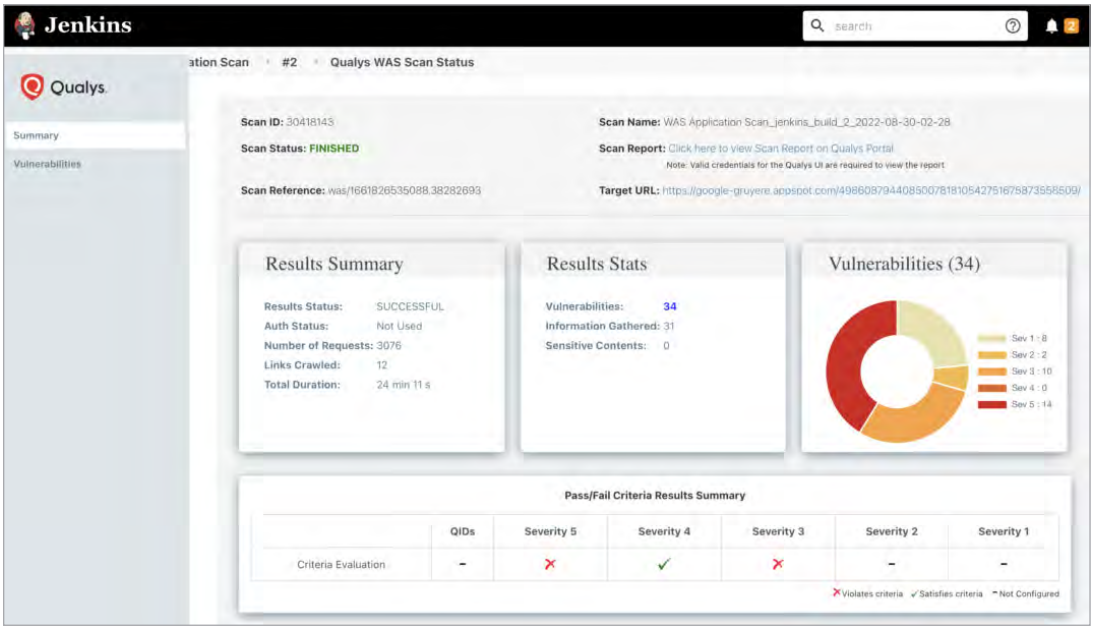
By using the WAS catalog, customers may find web apps or APIs that are absent from their current inventory. By selecting "Add to WAS Subscription" on any catalog entry, Qualys WAS users can quickly launch or schedule a WAS scan against that service. Significant enhancements coming to the WAS catalog include a subdomain discovery capability and integrations with Qualys CyberSecurity Asset Management to identify even more web applications and APIs in the organization's perimeter.

Web Application Scanning in the Development Phase

According to Qualys customer surveys, enterprises indicate that they select Qualys for our expertise in vulnerability scanning. An IBM study reported that fixing vulnerabilities in production applications is up to 6X more expensive than fixing them during the software design and development phase. Other estimates put this cost even higher. When it comes to new web apps (and APIs), it is essential to perform application security testing early... and often. Not only is this proactive approach significantly cheaper, but it also reduces the risk of deploying software with coding errors!

Qualys is also a leading dynamic application security testing (DAST) provider. DAST is a type of testing that looks for security vulnerabilities by safely testing a running application from the outside. This type of testing is not dependent on the framework or programming language used. As a DAST solution, Qualys WAS requires only a running instance of the web app or API to scan for vulnerabilities.

We provide a variety of free plugins (called "WAS connectors") for Jenkins, Bamboo, TeamCity, and Azure DevOps to help application development teams build scans directly into their CI/CD pipelines. The plugins allow for unobtrusive security testing with scan results — and details of any offending vulnerability — pushed directly into the developer's CI/CD tool of choice. When used with a virtual scanner appliance inside your network, you can test your applications and APIs no matter where they are in your internal environments.



WAS Connectors let developers run vulnerability scans, get details right in CI/CD tools

The self-service model is another option with Qualys WAS for performing testing during the development phase. Developers can be given direct access to the WAS UI with the responsibility to complete regular vulnerability scans of the web apps and APIs they are building. With tagging and role-based access control (RBAC), Qualys WAS provides everything required for development teams to have separate and individualized control over their security testing.

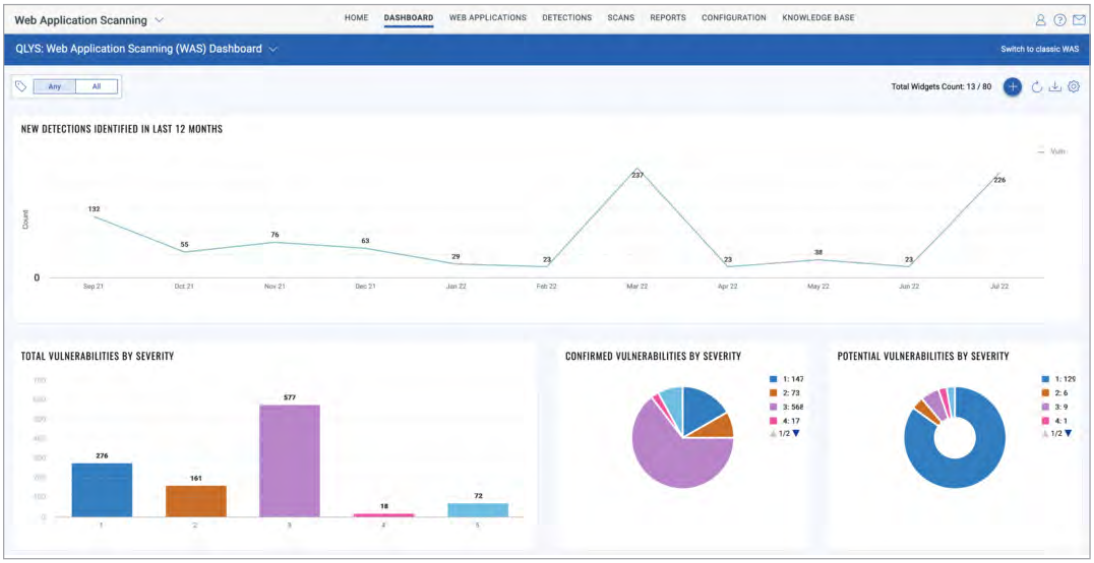
With developers managing their own DAST scans, the Cybersecurity team can then focus on successfully administering the testing program. This can include setting up user logins, configuring scan option profiles, and monitoring scanning activity to ensure scans are being executed properly.

Read More: Qualys WAS Self-Service Model white paper

Qualys WAS for DAST Scanning in Production

Even if your developers are performing routine cybersecurity testing in the development phase, your enterprise's production web applications and APIs cannot be ignored. Once in production, software enters maintenance mode. Security testing is still important since code changes will inevitably occur, and changes are most often where new vulnerabilities are introduced. Additionally, detection signatures are released for newly discovered software vulnerabilities all the time, so DAST scanning of production web applications and APIs is critical to maintain a strong security posture.

Qualys WAS provides the enterprise scalability required to make this possible. Customers enjoy unlimited scans, which means you can completely automate testing your production apps and APIs on a quarterly, monthly, weekly, or even daily basis. Qualys WAS can easily manage the scanning of thousands of production apps per week in bulk using its multi-site scan (aka "multi-scan") feature. Users can scan multiple web apps concurrently at a large scale. One Qualys customer was scanning 100,000+ web apps each week during the height of the Log4Shell disclosure in December 2021.



Track scan results easily right from Qualys WAS Dashboard

Tags are used to group applications in a logical way, and then scheduling/scanning is done on a tag basis rather than on a single application basis. This allows users to add or remove web applications or APIs to schedules by simply applying or removing the appropriate tag.

One caveat about scanning production apps and APIs: production data could be deleted or irreversibly corrupted, depending on the app or APIs functionality. Why? Because when Qualys WAS is testing a form, for example, we have no advance knowledge of the impact of our tests. The tests could result in spamming a "contact us" form or adding test data into a database. With this risk in mind, Qualys WAS has some features you can use to protect your production web applications or APIs during tests:

1. Do not run authenticated scans in production, or authenticate with least privilege (e.g. read-only) account credentials that cannot make changes to production data
2. Configure POST data blacklists to block tests against certain forms
3. Configure allow or deny list rules to only test specific URLs

Security Scanning for REST APIs with Qualys WAS

The new attack surface for malicious actors is your organization's APIs. Gartner predicts that 90% of web-enabled applications will have broader attack surfaces due to exposed APIs. If you are not testing your APIs for runtime vulnerabilities, know that malicious actors are certainly testing your defenses!

Scanning REST APIs has been a core capability of Qualys WAS since 2017. In that year we added initial support for API scanning by allowing customers to upload a proxy capture file containing the API calls (HTTP requests) for the various operations supported by the API.

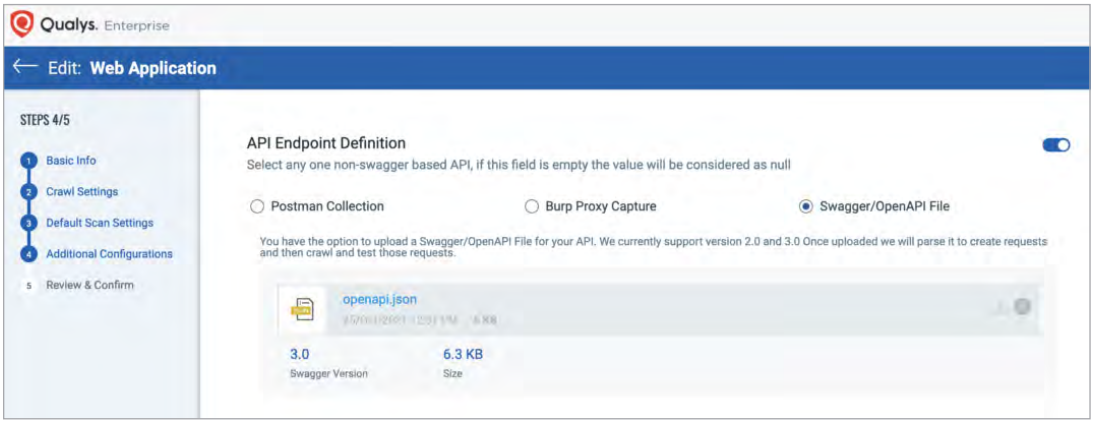
Unlike browser-based web applications, APIs do not have links to crawl or pages to view. They are simply endpoints that are designed for machine-to-machine communication. This makes testing APIs for runtime vulnerabilities challenging. The scanner needs to be given details about the API to know how to properly invoke the API calls and test endpoints for vulnerabilities. These details include operational methods like GET and POST, security mechanisms, POST parameters, URL query parameters, and URL path variables.

In 2018, we simplified the setup by adding support for Swagger version 2 specification files.

In 2019, we significantly increased the power of the cloud service's API testing capability by implementing support for Postman Collections. For example, this enabled defining a workflow within the API, such as having the output of one API call be used as input in another. This is similar to how Selenium scripts are used to have the scanner navigate through a workflow in a web application.

In 2020, we added support for OpenAPI version 3, the successor to Swagger V2.

Later in 2022, we will be introducing even more API security testing features.



Qualys WAS has built-in API scanning for runtime vulnerabilities

Qualys WAS Identifies Personally Identifiable Information

When scanning hundreds or even thousands of web applications or APIs, it is not always easy to know the full functionality of all those sites. This unknown becomes especially problematic when it comes to Personally Identifiable Information (PII). Qualys WAS has a built-in feature to identify where PII is being collected. This visibility allows Cybersecurity teams to assess:

- ✓ Why is this site collecting PII?
- ✓ Should this site be collecting PII?
- ✓ Where is this PII being stored?
- ✓ How is this PII being safeguarded?
- ✓ What controls are in place to monitor the PII against misuse?

Qualys WAS for Web Malware Detection

While Qualys WAS can discover vulnerabilities in web applications and APIs, what about sites that are already infected with malware? Your organization spent years building its brand and reputation. You can't risk losing it overnight if your customers are at risk by simply visiting your website.

Web Malware Detection Scanning (MDS) is an included service with Qualys WAS for external facing web applications. It is a separate scan that can be scheduled to run quarterly, monthly, weekly, or even daily against your web applications.

The testing consists of crawling your external web applications and hunting for malware using four methods:

1. **Signatures** — Are there known signatures in the embedded PDFs, media files, and other file types for known malware?
2. **Blacklists** — Are there any embedded links or 3rd party content providers to known blacklisted sites for malware?
3. **Heuristics** — Is there obfuscated code on the web application with functions that imply malicious intent?
4. **Behavioral Analysis** — What happens to the scanner as it crawls the site? Does it attempt any file read or write actions against the sandboxed server it runs on? Is memory usage or CPU usage increasing? Are there any behaviors to suggest malicious code is targeting client browsers?

What is especially useful is both the heuristics and behavior analysis can be used to identify unknown and zero-day threats to your site users.

What's Coming Next in Qualys WAS

When it comes to testing web applications and APIs, most tools start at the scanning stage... and stop there. Qualys WAS will expand its features and capabilities covering both before scans begin and long after they end, to turn your web application scanning into a web application vulnerability management program.

Today we already offer integrations into Splunk and ServiceNow AVR. Additionally, if you are a BugBounty user, you can export WAS scan reports right to their platform or import BugBounty vulnerabilities to centrally manage all web app and API vulnerabilities in Qualys WAS. The evolution of Qualys WAS is designed to fit within an enterprise's existing workflows and processes to seamlessly integrate into any enterprise's web application scanning program.

Not yet a WAS customer? Why not give us a look by signing up for a Free Trial today!

Related

An End-to-End Approach to Next-Gen Web Application and API Security

QSC18: API Security, Enabling Innovation Without Enabling Attacks and Data Breaches

Continuous Web Security Assessment for Production and DevOps Environments

v221005