Web Application Scanning

OWASP Top 10 2017 Coverage

November 2017

CONTINUOUS SECURITY

Introduction

The OWASP Top 10 is one of the most common ways to categorize web application risks and vulnerabilities. The vulnerability detections in Qualys Web Application Scanning (WAS) are consistent with, but more granular than, the OWASP Top 10. The WAS QIDs representing vulnerabilities do not always directly refer to a Top 10 item, but most of the QIDs fall under one or more of the Top 10 items. WAS also includes some QIDs for vulnerabilities not explicitly covered by the OWASP Top 10 but nevertheless pose a risk to web applications.

In most cases multiple QIDs are associated with a single Top 10 item. One reason is that the Top 10 item has such a broad scope that multiple detections provide more clarity on specific issues. A good example of this is Security Misconfiguration (A6), which can apply to many different weaknesses and vulnerabilities. Another reason is that some detections have complex testing methodologies and it's important to be able to distinguish between them in order to understand and fix the vulnerability. Examples of this are Injection (A1) and Cross-Site Scripting (A7).

Certain items in the Top 10 are more accurately identified by manual testing or code review. This is because they require knowledge of an application's users, business processes, workflows, or data context. For example, Broken Access Control (A5) greatly benefits from human analysis to understand different user roles and their permitted access levels within an application. In certain situations the scanner will make inferences regarding these types of vulnerabilities, but its scope is limited to minor issues or specific scenarios.

One of the new items for 2017 is Insufficient Logging & Monitoring (A10). This item represents a security risk, but not a vulnerability per se. Item A10 is essentially a special case requiring manual audit or review to understand a web application's back-end architecture and internal processes.

Overall, Qualys WAS vulnerability detections focus on problems that can be reliably automated, identified accurately, and lead to actionable results. The underlying scanning engine is updated several times a year and its payload/signature sets may be updated even more frequently. These approaches enable WAS to respond quickly as new vulnerabilities emerge, current detection capabilities are refined, and false positives or false negatives are reported from the customer base.

More information is available at the following links.

https://www.qualys.com/was

https://community.qualys.com/community/web-application-scanning

Qualys WAS Support Levels

The current status of WAS support for the risks and vulnerabilities in the OWASP Top 10 are classified into one of three levels:

1. **Comprehensive** – WAS implements several complementary approaches to identify a variety of vulnerabilities in this category. These tests largely mirror those used in manual analysis.
2. **General** – WAS addresses common vulnerabilities in this category, but has not yet implemented a more complete methodology covering all possible issues. Enhancements are being developed, but have not yet been released. Many of these tests can be complemented by manual analysis.
3. **Selective** – Certain vulnerabilities within this category can be tested in an automated manner and are supported, but others require in-depth knowledge of the back-end architecture, context of the data, or other information not available to a black-box/dynamic scanner such as WAS. The most effective testing methodology is manual analysis or internal architecture audit/review.

The table below provides the level of support for each Top 10 item (via color coding) as well as the associated WAS QIDs for each item.

OWASP Top 10 (2017)	Qualys WAS QID(s)	Notes
A1 – Injection	150003, 150012, 150047, 150055, 150093, 150114, 150156	
A2 – Broken Authentication	150032, 150045, 150049, 150053, 150068, 150069, 150120, 150121, 150129, 150151, 150160	Includes QIDs related to session management and insecure cookies.
A3 – Sensitive Data Exposure	150016, 150032, 150033, 150034, 150043, 150052, 150053, 150072, 150103, 150120, 150121, 150122, 150123, 150128, 150144, 150145, 150146, 150150, 150151, 150159, 150160, 150161	No determination is made regarding the security level of an application's data store.
A4 – XML External Entities (XXE)	150179, 150180	New item in 2017 Top 10.
A5 – Broken Access Control	150004, 150011, 150023, 150057, 150118, 150174	
A6 – Security Misconfiguration	150022, 150023, 150056, 150059, 150060, 150063, 150064, 150079, 150081, 150085, 150112, 150124, 150156, 150171	
A7 – Cross-Site Scripting	150000, 150001, 150002, 150013, 150046, 150048, 150062, 150076, 150084, 150090, 150092, 150117, 150158	
A8 – Insecure Deserialization	150157	New item in 2017 Top 10.
A9 – Using Components with Known Vulnerabilities	150127, 150134, 150153, 150154, 150155, 150162, 150163, 150165, 150166, 150173, 150175, 150178, 150188, 150189, 150190	Comprehensive coverage can be achieved with WAS and Qualys VM scanning.
A10 – Insufficient Logging & Monitoring	N/A	New item in 2017 Top 10. Requires manual audit/review of back-end architecture and processes.