Article - Getting Stated Using ASVS

The Open Web Application Security Project (OWASP) developed the Application Security Verification Standard (ASVS) to normalize the range in the coverage and level of rigor available in the market when it comes to performing Web application security assessments (also called "verification"). Web application developers typically initiate the verification process by contracting with an independent consulting firm (also called a "verification provider") to perform a verification according to ASVS requirements. The verification provider then documents verification findings according to application developer and ASVS reporting requirements. The verification provider then provides the findings to the application developer. ASVS verification is voluntary for Web applications that are acquired by United States Government (USG) civil agencies and non-USG entities, but as per the supplemental guidance for the RA-5 control ("Vulnerability Scanning") in NIST Special Publication 800-53, Revision 2, vulnerability scanning, source code review, or both may be required. In this case, using ASVS to perform vulnerability scanning, source code review, or both is one possible approach to meeting requirements based on the RA-5 control. Benefits include using a common yardstick to measure applications' trust, ensuring that results are repeatable, and ensuring that expectations are clearly set.

Approach

The OWASP ASVS defines verification and documentation requirements that are grouped on the basis of related coverage and level of rigor. The Standard defines four hierarchical levels (e.g. Level 2 requires more coverage and rigor than Level 1) as depicted in the figure below.

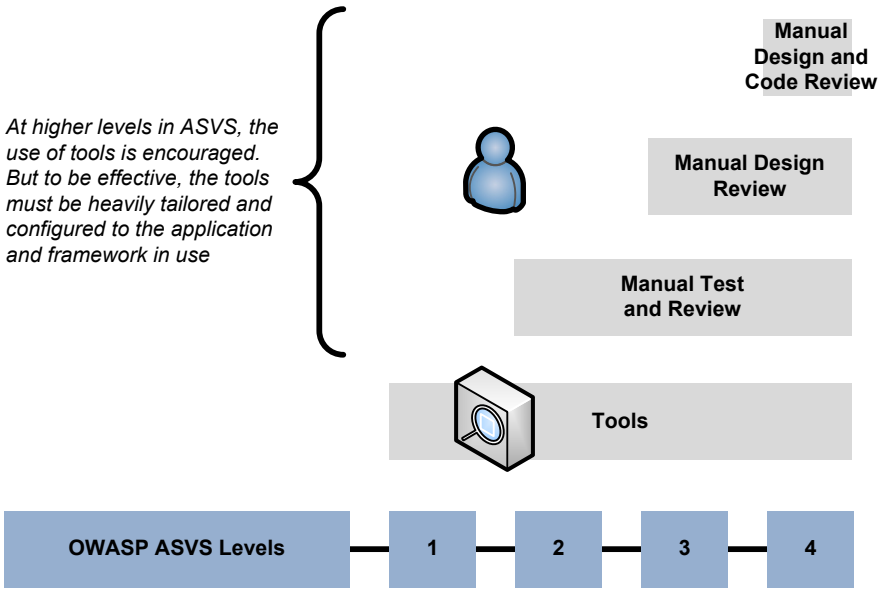

Figure 1 - OWASP ASVS Levels

Web application security verification is performed from a logical point of view by following (or attempting to follow) paths into and out of a targeted application (called the Target of Verification or TOV) and performing analysis along those paths. More complex applications typically take more time to analyze resulting in longer and more costly verifications. Lines of code are not the only factors that determine the complexity of an application – different technologies will typically require different amounts of analysis. Simple applications may include for example libraries and frameworks. Applications of moderate complexity may include simple Web 1.0 applications. Complex applications may include Web 2.0 applications and new/unique Web technologies.

ASVS defines constituent components for Levels 1 and 2 (e.g. verification at Level 1 requires meeting both Level 1A and 1B requirements). For example, applications may claim compliance to either Level 1A or 1B instead of Level 1, but making such claims is weaker than claiming Level 1. Verification and documentation requirements are defined in this Standard using three types of requirements: High-Level requirements, Detailed requirements, and Reporting requirements. The High-Level requirements define the overall application implementation and verification requirements. The Detailed requirements define low-level application implementation and verification requirements (i.e., specific items to verify). The Reporting requirements define how the results of performing an application verification according to the OWASP ASVS must be documented.

OWASP provides numerous resources, including ASVS, to help organization's develop and maintain secure applications. The OWASP ASVS, OWASP Contract Annex,[1] and OWASP ESAPI[2] can be used to support your Software Development Life Cycle (SDLC) as depicted in the figure below.

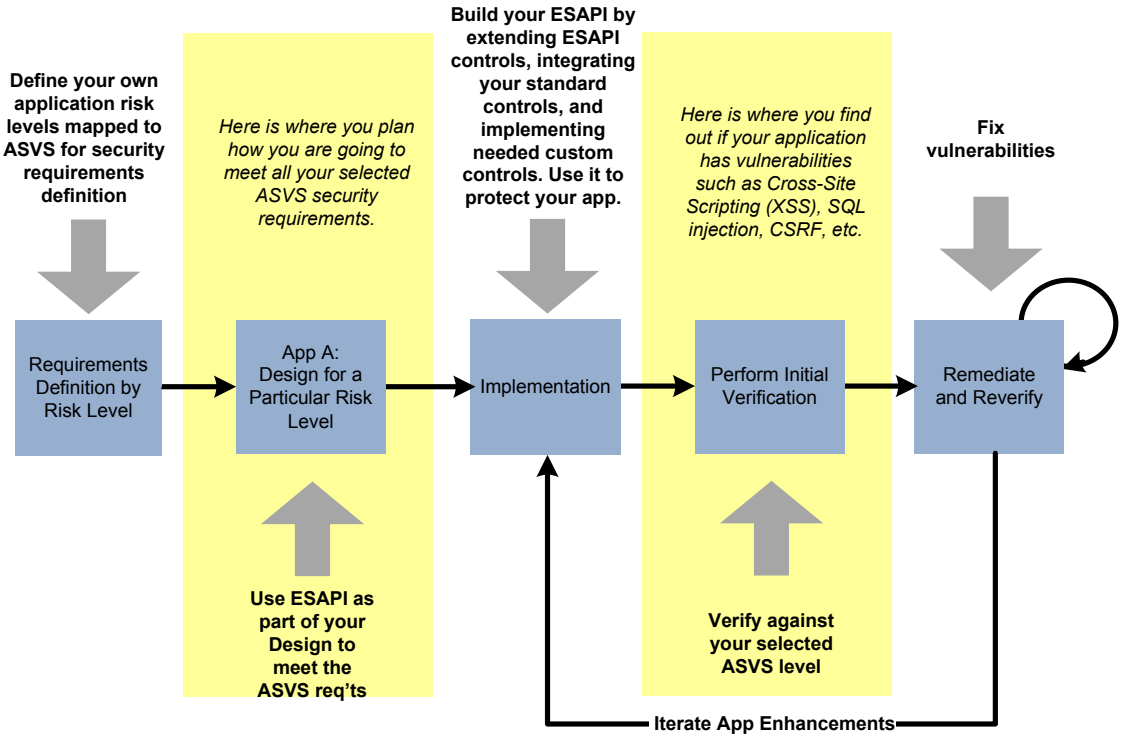

Figure 2 – One way to introduce verification as an activity into your SDLC[3]

Where To Go From Here

OWASP is the premier site for Web application security. The OWASP site hosts many projects, forums, blogs, presentations, tools, and papers. Additionally, OWASP hosts two major Web application security conferences per year, and has over 80 local chapters. The OWASP ASVS project page can be found here http://www.owasp.org/index.php/ASVS

[1] For information about how to specify an ASVS level in a contract, see the *OWASP Contract Annex*.
[2] For more information about how to ESAPI-Enable (ES-Enable) your application, see the OWASP *ESAPI* project (OWASP 2009).
[3] For more information about introducing security-related activities into your existing SDLC, see the *OWASP CLASP* (OWASP 2008) or *OWASP SAMM* Projects (OWASP 2009).

The following OWASP projects are most likely to be useful to users/adopters of this standard:

- *OWASP Top Ten Project* - http://www.owasp.org/index.php/Top_10
- *OWASP Code Review Guide* - http://www.owasp.org/index.php/Category:OWASP_Code_Review_Project
- *OWASP Testing Guide* - http://www.owasp.org/index.php/Testing_Guide
- *OWASP Enterprise Security API (ESAPI) Project* - http://www.owasp.org/index.php/ESAPI
- *OWASP Legal Project* - http://www.owasp.org/index.php/Category:OWASP_Legal_Project

Similarly, the following Web sites are most likely to be useful to users/adopters of this standard:

- *OWASP* - http://www.owasp.org
- *MITRE* - Common Weakness Enumeration – Vulnerability Trends, http://cwe.mitre.org/documents/vuln-trends.html
- *PCI Security Standards Council* - publishers of the PCI standards, relevant to all organizations processing or holding credit card data, https://www.pcisecuritystandards.org
- *PCI Data Security Standard (DSS) v1.1* - https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf

Copyright and License