OWASP ASVS Article

The Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS) is new – *really* new. Late second quarter of 2009 kind of new. It is *not possible* that one's applications could have *already* been tested using ASVS. ASVS users and adopters have already figured out though that what they have been doing all along maps *very* closely to the different ASVS levels. With a little elbow grease, ASVS levels can be met without significantly increasing the amount of overall work that you would otherwise be doing. The net result being, you and your customers, whether internal or external, will now be using a common yardstick to measure your applications' trust. Results will be repeatable, and expectations will be clearly set.

While there are four ASVS levels, there are only three types of Web application verification techniques that are covered:

- *Use tools* – Using tools to perform vulnerability scans and code scans,
- *Use your eyeballs* – Manually testing and reviewing results of scans, to build upon tool findings, and
- *Use your brain* – Examining designs to see if technical security controls such as access controls are being used everywhere they need to be

The table below is a summary of what you would additionally have to do to meet an ASVS level, for each of the different techniques.[1]

Table 1 – What you'll need to do to meet ASVS requirements

What you do today	What you would additionally have to do to using ASVS
Dynamic scan	Add security tests for ASVS detailed verification requirements that your tools don't test for.
Source code scan	Add an additional pass through the code for ASVS detailed verification requirements that your tools don't test for.
Manual code review	After you perform your review as you have always done, add an additional pass through the code for ASVS detailed verification requirements that your analysis didn't already cover. Perhaps consider for next time updating your methodology to include checking for those additional items.
Security testing	After you perform your testing as you have always done, add an additional set of tests for those ASVS detailed verification requirements that your testing didn't already cover. Perhaps consider for next time updating your methodology to include testing for those additional items.
Design review	You will likely need to do a little bit of extra reconnaissance (and at the higher levels, likely some additional deep thought) to meet ASVS security architecture requirements. But, ASVS does not prescribe techniques, and your approach to doing risk assessments *may* be enough.

[1] For each of the above, you'll then also need to *update* your report to include a description of the application, of its security architecture (but *only* to the degree required to meet the targeted ASVS level), and you *may* need to include some additional details about the results of your analysis.

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

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