OWASP

The Open Web Application Security Project

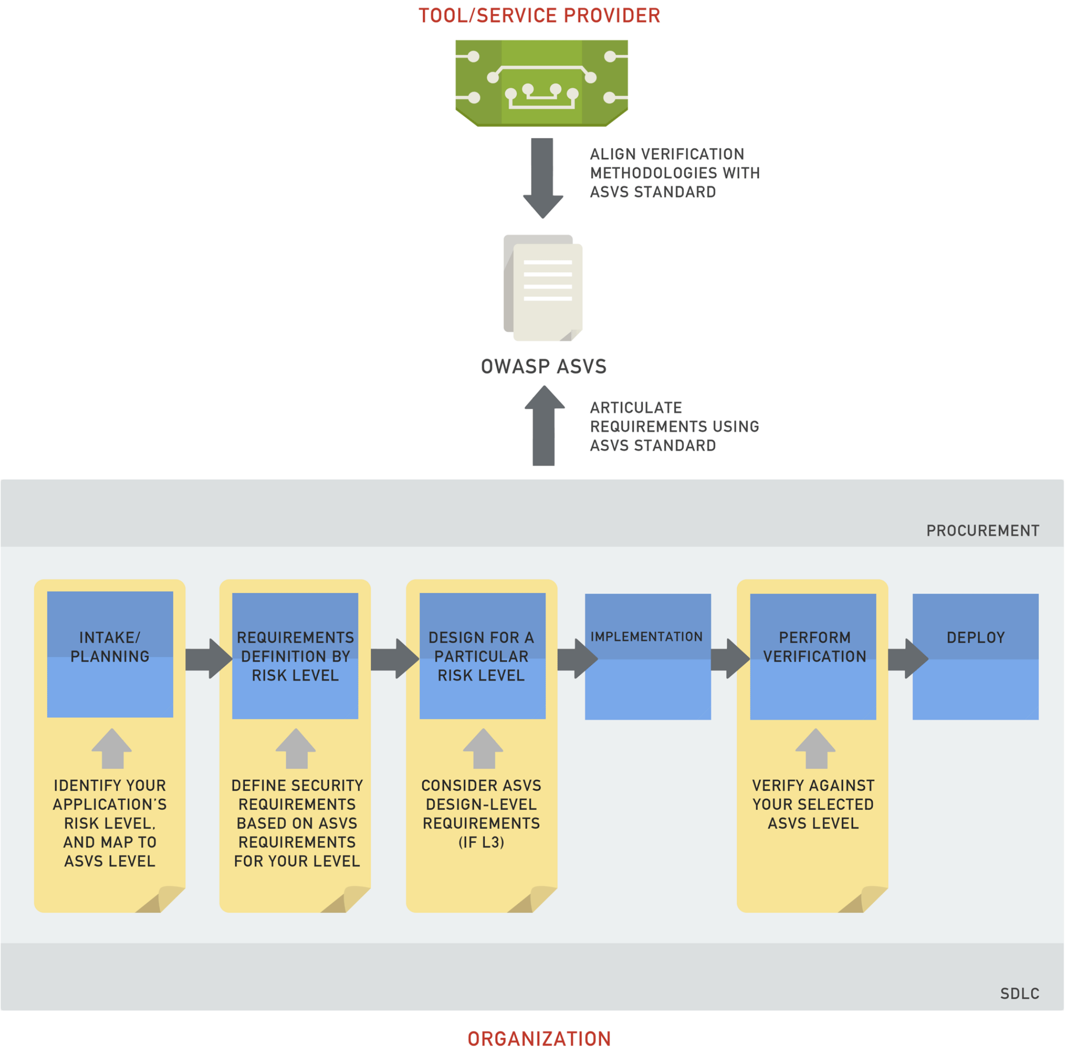
OWASP Application Security Verification Standard 2013

BACKGROUND

What is ASVS?

“The primary aim of the OWASP Application Security Verification Standard (ASVS) is to normalize the range in the coverage and level of rigor available in the market when it comes to performing web application security verification.”

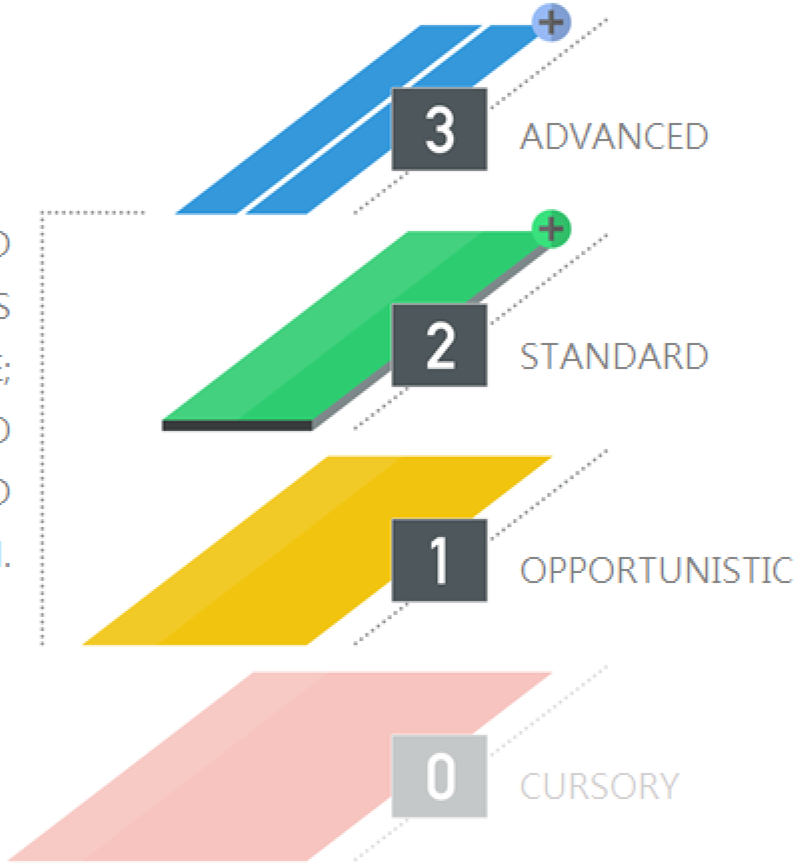
Why you should care


TOOL/SERVICE PROVIDER
ALIGN VERIFICATION METHODOLOGIES WITH ASVS STANDARD
OWASP ASVS
ARTICULATE REQUIREMENTS USING ASVS STANDARD
PROCUREMENT
INTAKE/ PLANNING
REQUIREMENTS DEFINITION BY RISK LEVEL
DESIGN FOR A PARTICULAR RISK LEVEL
IMPLEMENTATION
PERFORM VERIFICATION
DEPLOY
IDENTIFY YOUR APPLICATION'S RISK LEVEL, AND MAP TO ASVS LEVEL
DEFINE SECURITY REQUIREMENTS BASED ON ASVS REQUIREMENTS FOR YOUR LEVEL
CONSIDER ASVS DESIGN-LEVEL REQUIREMENTS (IF L3)
VERIFY AGAINST YOUR SELECTED ASVS LEVEL
SDLC
ORGANIZATION

Introducing ASVS 2013 Beta

At a glance

ASVS DEFINES DETAILED VERIFICATION REQUIREMENTS FOR LEVELS 1 AND ABOVE; WHEREAS LEVEL 0 IS MEANT TO BE FLEXIBLE AND IS CUSTOMIZED BY EACH ORGANIZATION.



OWASP ASVS LEVELS

Level 0: Cursory

Level 0 (or Cursory) is an optional certification, indicating that the application has passed some type of verification.

0
1
2
3
OWASP ASVS LEVELS

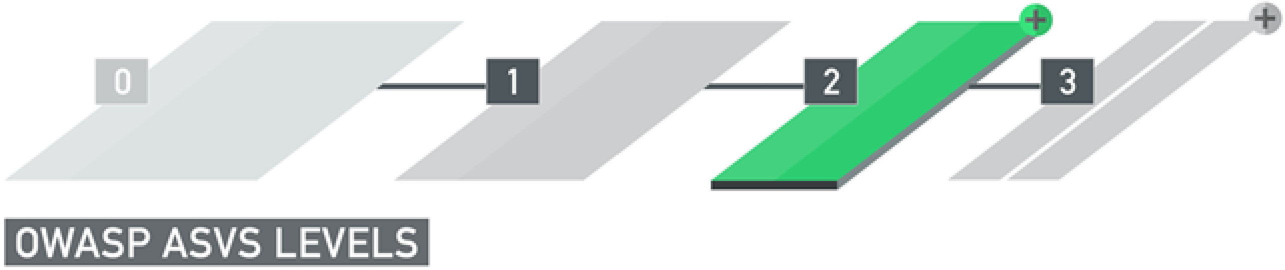
Level 1: Opportunistic

An application achieves Level 1 (or Opportunistic) certification if it adequately defends against application security vulnerabilities that are easy to discover.

0
1
2
3
OWASP ASVS LEVELS

Level 2: Standard

An application achieves Level 2 (or Standard) verification if it also adequately defends against prevalent application security vulnerabilities whose existence poses moderate-to-serious risk.



Level 3: Advanced

An application achieves Level 3 (or Advanced) certification if it also adequately defends against all advanced application security vulnerabilities, and also demonstrates principles of good security design.

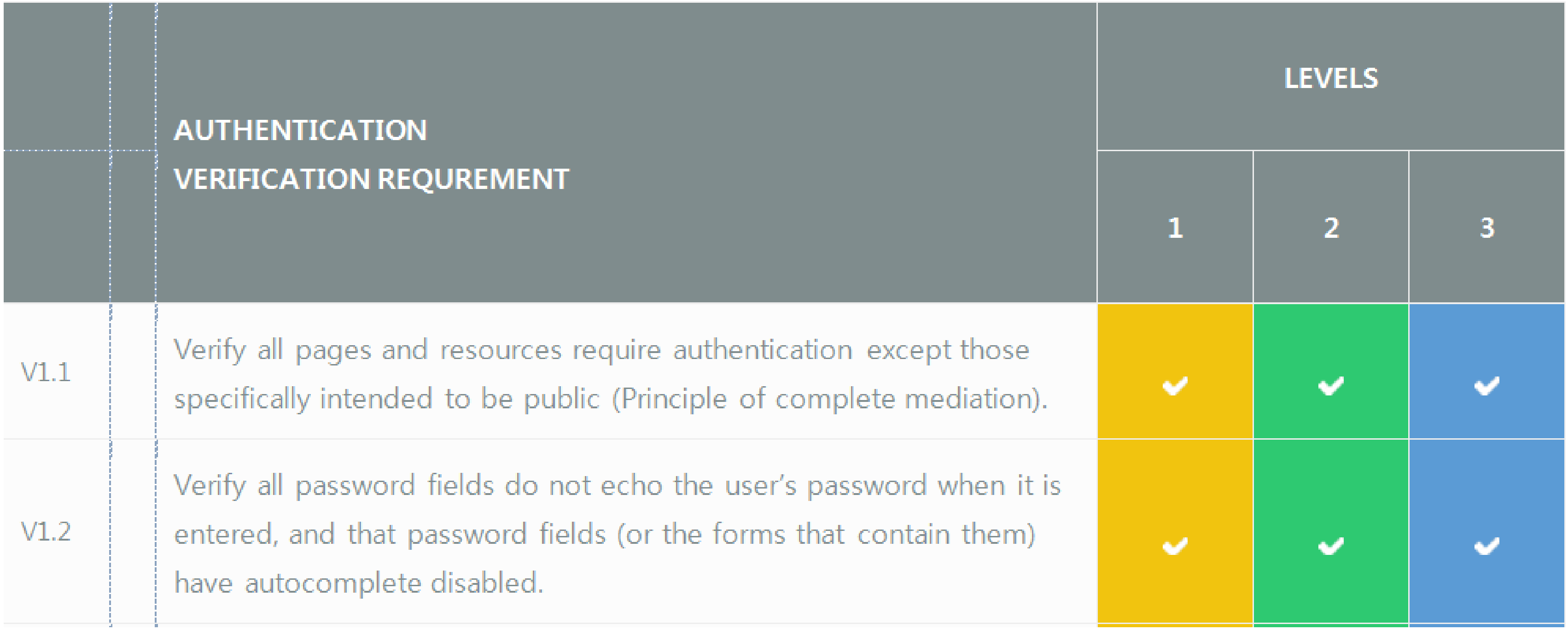
0
1
2
3
OWASP ASVS LEVELS

Scope of verification

The scope of the verification is separate from the requirements for achieving a level.

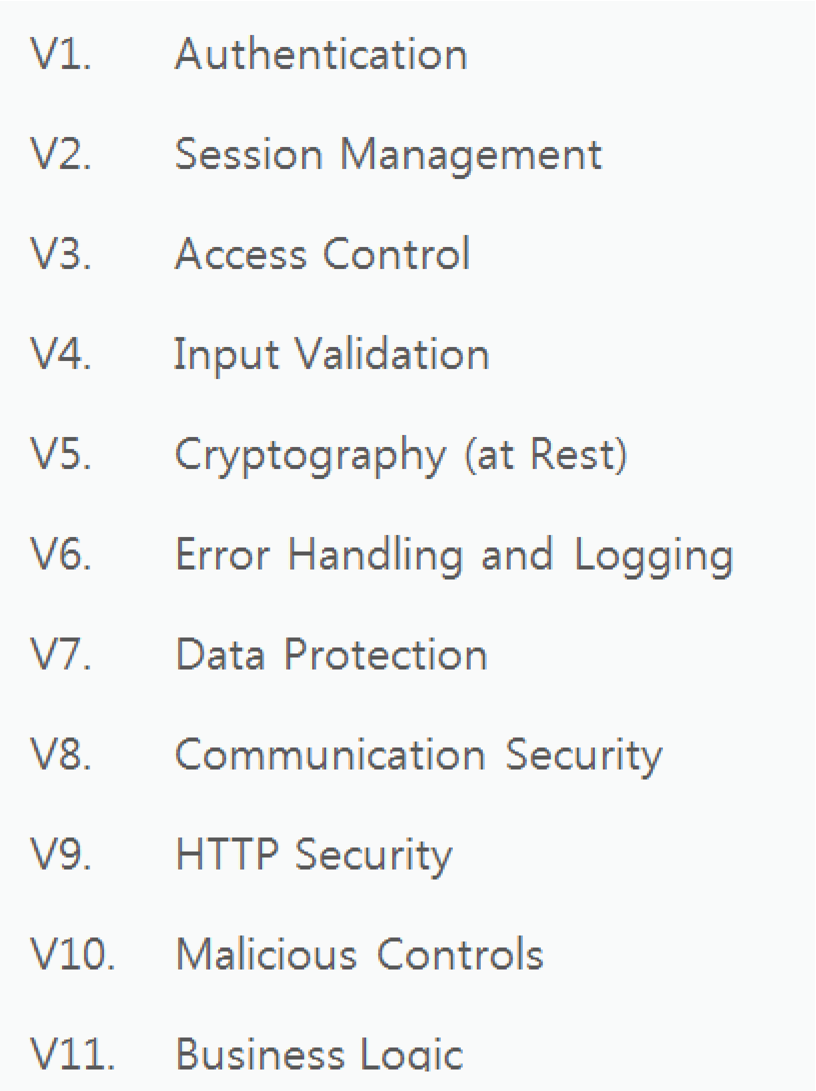
e.g. A [illegible] certified

Detailed verification requirements



		AUTHENTICATION VERIFICATION REQUREMENT	LEVELS		
			1	2	3
V1.1		Verify all pages and resources require authentication except those specifically intended to be public (Principle of complete mediation).	✓	✓	✓
V1.2		Verify all password fields do not echo the user's password when it is entered, and that password fields (or the forms that contain them) have autocomplete disabled.	✓	✓	✓

Detailed verification requirements



V1. Authentication

V2. Session Management

V3. Access Control

V4. Input Validation

V5. Cryptography (at Rest)

V6. Error Handling and Logging

V7. Data Protection

V8. Communication Security

V9. HTTP Security

V10. Malicious Controls

V11. Business Logic

What’s Next

Get it first!

OWASP ASVS 2013 (Beta)

http://
sourceforge.net/projects/owasp/files/ASVS/OWASP

Future direction

Map to other standards

- Remove detailed requirements?
- Makes ASVS more lightweight

Possibly two views: consumer and provider

Shoutout to…

Daniel Cuthbert, Andrew van der Stock, Krishna Raja, Evan Gaustad, Archangel Cuison, Etienne Stalmans

Authors and contributors of ASVS 2009

Thank you!

Any questions?

Email us:

Sahba.kazerooni@owasp.org

Daniel.cuthbert@owasp.org

Join the conversation:

owasp-application-security-verification-standard@lists.o