OWASP Application Security Verification Standard 2013
Sahba Kazerooni

- Managing Director – Security Compass
- Specialist in secure software development
- Former SANS trainer & current OWASP ASVS project lead
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

PRODUCTION

INTAKE/PLANNING

IDENTIFY YOUR APPLICATION’S RISK LEVEL, AND MAP TO ASVS LEVEL

REQUIREMENTS DEFINITION BY RISK LEVEL

DEFINE SECURITY REQUIREMENTS BASED ON ASVS REQUIREMENTS FOR YOUR LEVEL

DESIGN FOR A PARTICULAR RISK LEVEL

CONSIDER ASVS DESIGN-LEVEL REQUIREMENTS (IF L3)

IMPLEMENTATION

PERFORM VERIFICATION

VERIFY AGAINST YOUR SELECTED ASVS LEVEL

DEPLOY

ORGANIZATION

SDLC
ASVS 2009 Challenges

• Document had not been updated since 2009 (some content was out of date)
• Uproar against automated level 1
• Many requirements were unclear/duplicates
• Document was not easy to read/interpret
• No clear-cut definition of levels
Initial Roadmap (Jan 2013)

• New Content
• Document segregation
• Case studies
• Mapping to other standards
• General quality control / cleanup of document
• (NTH) ASVS certification of automated scanners
• (NTH) Document design upgrade
Completed (Aug 2013)

- New Content
- Document segregation
- Case studies
- Mapping to other standards
- General quality control / cleanup of document
- (NTH) ASVS certification of automated scanners
- (NTH) Document design upgrade
At higher levels in ASVS, the use of tools is encouraged. But to be effective, the tools must be heavily tailored and configured to the application and framework in use.
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.
Level 0: Cursory

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

• No specific verification requirements
• Designed to be a flexible point-of-entry
• Organizations can define their own min. criteria, for example:
  – Automated scan of all externally-facing apps;
  – Established authentication policies;
Level 1: Opportunistic

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

• Login over HTTPS
• Session timeout implemented
• XSS, SQLi
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.
Includes

- OWASP Top 10
- Business Logic
- Basic crypto
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.
Includes

• Advanced cryptography
• Malicious code
• Advanced mobile device tests
Level 3 Design Elements

- Security controls are **centralized** within the application.
- Security controls that perform validation make decisions using a **whitelist** (“positive”) approach.
- Data validation controls are complemented by output **encoding** routines.
- All untrusted data that is output to SQL interpreters use **parameterized** interfaces, prepared statements, or are escaped properly.
Scope of verification

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

*e.g. ASVS L3+ certified*
## Detailed verification requirements

<table>
<thead>
<tr>
<th>AUTHENTICATION VERIFICATION REQUIREMENT</th>
<th>LEVELS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>V1.1 Verify all pages and resources require authentication except those specifically intended to be public (Principle of complete mediation).</td>
<td>✓</td>
</tr>
<tr>
<td>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.</td>
<td>✓</td>
</tr>
</tbody>
</table>
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
V12. Files and Resources
V13. Mobile
WHAT’S NEXT
Get it first!

Future direction

- Roadmap to update compliance from ASVS 2009 to ASVS 2013
- 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 me:
  Sahba@securitycompass.com
  Sahba.kazerooni@owasp.org

• Join the conversation:
  owasp-application-security-verification-standard@lists.owasp.org