Introducing ASVS 2013 Beta

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
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 (or Cursory) is an optional certification, indicating that the application has passed some type of verification.
Level 1: Opportunistic

An application achieves Level 1 (or Opportunistic) certification if it adequately defends against application security vulnerabilities that are easy to discover.
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.
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
What’s Next
Get it first!

OWASP ASVS 2013 (Beta)

http://sourceforge.net/projects/owasp/files/ASVS/OWASP ASVS 2013 (Beta)
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 Cuisson, 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.owasp.org