Agenda

- About ASVS
- Project Status
- Technical Details
- Getting Started
- Where to Go from Here
- Questions
Challenges...

- There is a huge range in coverage and rigor available in the application security verification market!

- Consumers have no way to tell the difference between:
  - Someone running a grep tool, and
  - Someone doing painstaking code review and manual testing!

*There are differences in coverage and rigor between types of tools, between tools and manual techniques, and between types of manual techniques!*
Philosophy of ASVS

- It is intended as a **standard** for how to **verify** the security of **web applications**

- It should be **application-independent**

- It should be **development life-cycle independent**

- It should define requirements that can be applied across web applications **without special interpretation**

---

Any such standard also needs to be **commercially-viable and therefore not overly burdensome**!
Design Goals of ASVS

- The standard should define functional verification requirements that take a white-list (i.e., positive) approach.
- The standard should define increasing levels of application security verification.
- The difference in coverage and level of rigor between levels should be relatively linear.

The standard should also be verification tool and technique independent!
What Questions Does ASVS Answer?

- What security features should be built into the required set of security controls?
- What are reasonable increases in coverage and level of rigor when verifying the security of a web application?
- How can I compare verification efforts?
- How much trust can be placed in a web application?

ASVS can answer these questions for applications ranging from minimum risk applications, to critical infrastructure applications.
Agenda

- About ASVS
- Project Status
  - Technical Details
- Getting Started
- Where to Go from Here
- Questions

The OWASP Foundation
http://www.owasp.org
What is the status of the ASVS as an OWASP standard?

- Web Application Edition of ASVS
  - It is the first OWASP standard
  - Current official release is Beta, released Dec 2008
  - Being piloted by Booz Allen Hamilton
    - Updates based on Booz Allen pilots under way
  - ASVS assessments being offered by Aspect Security

- Future Editions of ASVS
  - Web Services Edition under development
  - Translate to other languages
  - Additional architectures being considered (perhaps client-server, Cloud computing for example)
Project Plan and Status

- 2/25/2009 – Proposed updates based on pilots being considered

- 12/5/2008 - OWASP ASVS exits the Summer of Code 2008! The Beta draft of the Web Application Edition is released! Mike Boberski, Jeff Williams, and Dave Wichers primary authors

- 4/16/2008 - OWASP ASVS Summer of Code 2008 proposal submitted by Mike Boberski accepted!

- 2/20/2008 – Jeff Williams conceives of ASVS idea and encourages Mike to submit proposal

Check out the ASVS project page for the latest news: http://www.owasp.org/index.php/ASVS#Announcements
Agenda

- About ASVS
- Project Status
- Technical Details
- Getting Started
- Where to Go from Here
- Questions

The OWASP Foundation
http://www.owasp.org
An Overview of ASVS

- “Verification Levels” section
- “Verification Requirements” section
- “Verification Reporting Requirements” section
What are ASVS Verification Levels?

Increasing confidence in security:

1. Confidence in the correct use of security controls.
   - ✓

2. Confidence that security controls are working correctly.
   - ✓

3. Confidence that security controls are used everywhere within the application that they need to be.
   - ✓

4. Confidence that the security of the application was maintained during its development.
   - ✓

OWASP ASVS Levels: 1, 2, 3, 4
Application Security Verification Techniques

Find Vulnerabilities Using the Running Application

- Manual Application Penetration Testing
- Automated Application Vulnerability Scanning

Find Vulnerabilities Using the Source Code

- Automated Static Code Analysis
Level Definitions

■ Level 1 – Automated Verification
  ▪ Level 1A – Dynamic Scan (Partial Automated Verification)
  ▪ Level 1B – Source Code Scan (Partial Automated Verification)

■ Level 2 – Manual Verification
  ▪ Level 2A – Penetration Test (Partial Manual Verification)
  ▪ Level 2B – Code Review (Partial Manual Verification)

■ Level 3 – Design Verification

■ Level 4 – Internal Verification
Level 1 in more detail

- Automated verification of a web application treated as groups of components within a single monolithic entity.
Level 1 Options

- Level 1A
  Dynamic Scan (Partial Automated Verification)

- Level 1B
  Source Code Scan (Partial Automated Verification)

Need BOTH to achieve a full level 1…
MITRE found that all application security tool vendors’ claims put together cover only 45% of the known vulnerability types (695).

They found very little overlap between tools, so to get 45% you need them all (assuming their claims are true).
Level 2 in more detail

- Manual verification of a web application organized into a high-level architecture.
Level 2 Options

- Level 2A
  Manual Penetration Test

- Level 2B
  Manual Code Review

Need BOTH to achieve a full level 2…
Design verification of a web application organized into a high-level architecture.
Level 4 in more detail

- Internal verification of a web application by searching for malicious code (not malware) and examining how security controls work.
What are the ASVS Verification Requirements?

- Security architecture verification requirements
- Security control verification requirements

Security architecture information puts verification results into context and helps testers and reviewers to determine if the verification was accurate and complete.
A positive approach

- Negative
  - The tester shall search for XSS holes

- Positive
  - Verify that the application performs input validation and output encoding on all user input

Technology and threats change over time! ASVS takes a proactive a white-list approach.
# Requirement Summary

<table>
<thead>
<tr>
<th>Security Area</th>
<th>Level 1A</th>
<th>Level 1B</th>
<th>Level 2A</th>
<th>Level 2B</th>
<th>Level 3</th>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1 – Security Architecture Verification Requirements</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>V2 – Authentication Verification Requirements</td>
<td>3</td>
<td>2</td>
<td>9</td>
<td>13</td>
<td>13</td>
<td>14</td>
</tr>
<tr>
<td>V3 – Session Management Verification Requirements</td>
<td>4</td>
<td>1</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>V4 – Access Control Verification Requirements</td>
<td>5</td>
<td>1</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
</tr>
<tr>
<td>V5 – Input Validation Verification Requirements</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>V6 – Output Encoding/Escaping Verification Requirements</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>V7 – Cryptography Verification Requirements</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>V8 – Error Handling and Logging Verification Requirements</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>8</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>V9 – Data Protection Verification Requirements</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>V10 – Communication Security Verification Requirements</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>V11 – HTTP Security Verification Requirements</td>
<td>3</td>
<td>3</td>
<td>6</td>
<td>6</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>V12 – Security Configuration Verification Requirements</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>V13 – Malicious Code Search Verification Requirements</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V14 – Internal Security Verification Requirements</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td>22</td>
<td>12</td>
<td>51</td>
<td>83</td>
<td>96</td>
<td>112</td>
</tr>
</tbody>
</table>
What are ASVS reporting requirements?

- R1 – Report Introduction
- R2 – Application Description
- R3 – Application Architecture
- R4 – Verification Results

Is the report sufficiently detailed to make verification repeatable? Is there enough information to determine if the verification was accurate and complete?
Agenda

- About ASVS
- Project Status
- Technical Details
- Getting Started
- Where to Go from Here
- Questions

The OWASP Foundation
http://www.owasp.org
How do I get started using ASVS?

- Buyer and seller: agree how technical security requirements will be verified by specifying a level from 1 to 4,

- Perform an initial review of the application to be verified,
  - Minimum: Perform an ASVS Level 1 security architecture review!

- Develop a verification plan and a project schedule,

---

*Using ASVS requires planning and in that respect is just like any other testing exercise!*
How do I get started using ASVS? (continued)

- Perform a verification according to selected ASVS level requirements,
- Present findings,
- Develop and execute a remediation strategy,
- Re-verify after fixes are made (repeat as necessary).
- Ideally, develop a strategy to add verifications into the SDLC.

Tip: don’t scare people when you present your findings! Be specific. Propose a specific fix or a workaround, if able.
Agenda

- About ASVS
- Project Status
- Technical Details
- Getting Started
  - Where to Go from Here
- Questions

The OWASP Foundation
http://www.owasp.org
Where can I find help getting started using ASVS?

You can find information to help you get started using ASVS in two locations:

- Inside ASVS, section “Some Guidance on the Verification Process” in ASVS
- On the ASVS Project Page there are articles at the bottom of the page:

Articles in category “OWASP Application Security Verification Standard Project”

There are 32 articles in this category.

H cont.
- How to perform a security architecture review at Level 1
- How to perform a security architecture review at Level 2
- How to perform a security architecture review at Level 3
- How to perform a security architecture review at Level 4
- How to present findings without scaring people
- How to specify verification requirements in contracts
- How to use verification as a metric
- How to verify a cloud
- How to verify a web service
- How to verify business process management applications
- How to verify server requirements

M cont.
- Mapping ESAPI to ASVS Level 1
- Mapping ESAPI to ASVS Level 2
- Mapping ESAPI to ASVS Level 3
- Mapping ESAPI to ASVS Level 4
- Mapping NIST SP 800-53 to ASVS

W
- What is a TOV (Target of Verification)
- What is a TOV boundary
- What the differences are between malware and malicious code
- Where to draw the line between your application and the IT environment
- Why there are different bugs on different boxes
- Why you need to use a FIPS 140-2 validated cryptomodule

X
- XSS (Cross Site Scripting) Prevention Cheat Sheet
Where can I get a copy of ASVS, and talk to people using ASVS?

- You can download a copy from the ASVS Project page:
  - http://www.owasp.org/index.php/ASVS

- You can send comments and suggestions for improvement using the project mailing list:
  - See “Mailing List/Subscribe” link on project web page.
  - Tell us how your organization is using the OWASP ASVS. Include your name, organization's name, and brief description of how you are using the ASVS

Tip: Subscribe to the OWASP ASVS mailing list!
Owasp-Application-Security-Verification-Standard@lists.owasp.org
The OWASP Foundation
http://www.owasp.org
Questions?