OWASP Application Security Verification Standard (ASVS) – Web Application Edition

Mike Boberski (Booz Allen Hamilton)
boberski_michael@bah.com

Jeff Williams (Aspect Security)
jeff.williams@aspectsecurity.com

Dave Wichers (Aspect Security)
dave.wichers@aspectsecurity.com

OWASP
03/09

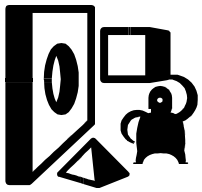
The OWASP Foundation
http://www.owasp.org

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

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

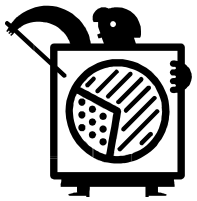
- 2/25/2009 – Proposed updates based on pilots being considered

- 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

OWASP Summer of Code 2008



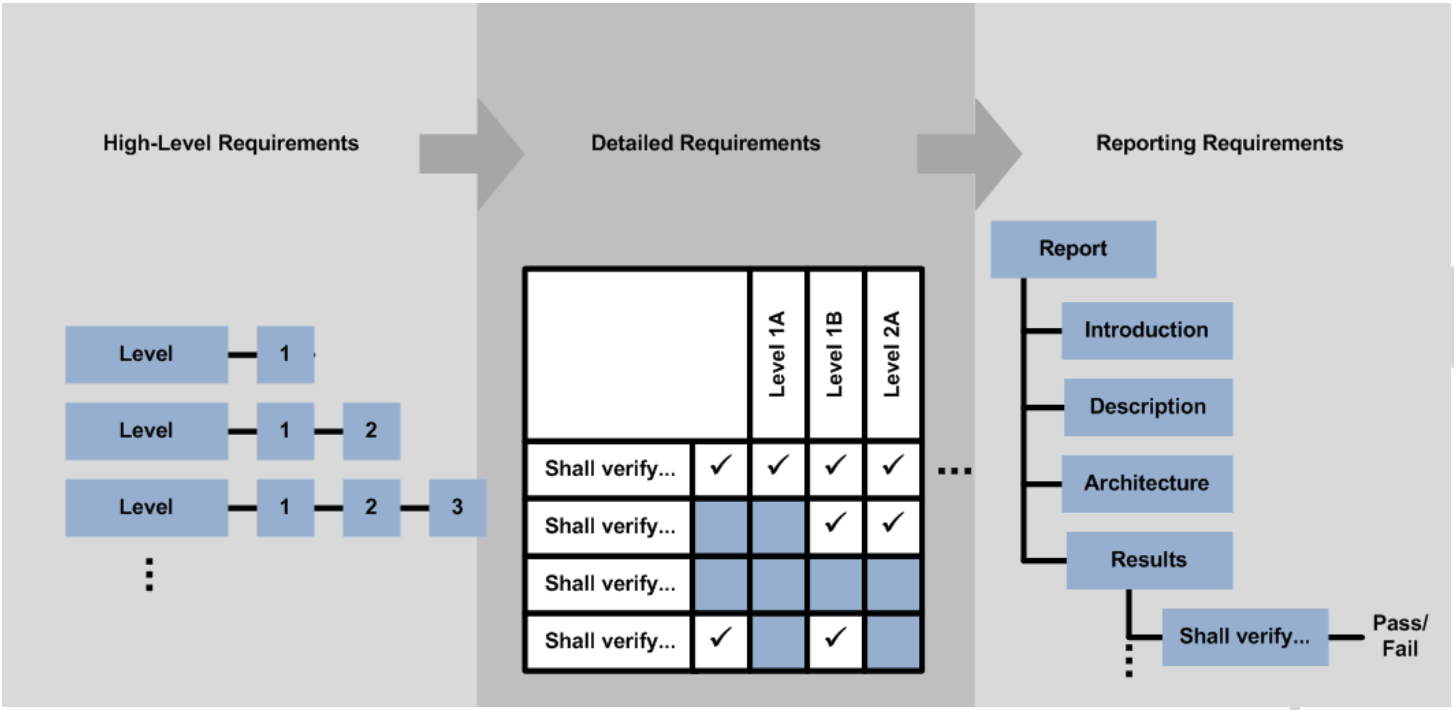
Check out the ASVS project page for the latest news:
http://www.owasp.org/index.php/ASVS#Announcements

Agenda

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

An Overview of ASVS

- "Verification Levels" section
- "Verification Requirements" section
- "Verification Reporting Requirements" section



What are ASVS Verification Levels?

Increasing confidence in security

OWASP ASVS Levels	1	2	3	4
Confidence in the correct use of security controls.	✓	✓	✓	✓
Confidence that security controls are working correctly.		✓	✓	✓
Confidence that security controls are used everywhere within the application that they need to be.			✓	✓
Confidence that the security of the application was maintained during its development				✓

Application Security Verification Techniques

Find Vulnerabilities
Using the Running Application

Find Vulnerabilities
Using the Source Code

Manual Application Penetration Testing

Automated Application Vulnerability Scanning

Manual Security Code Review

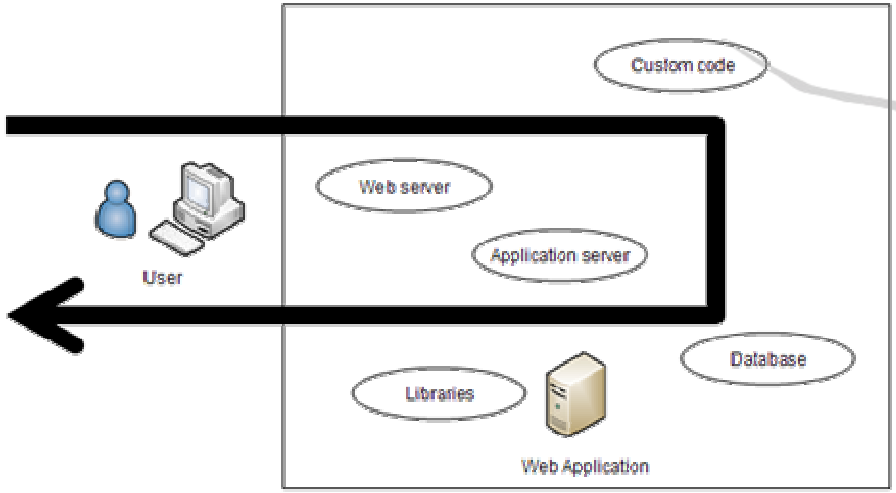
Automated Static Code Analysis

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 single monolithic entity



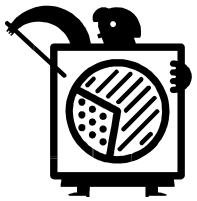
Level 1 Options

- Level 1A

  Dynamic Scan (Partial Automated Verification)

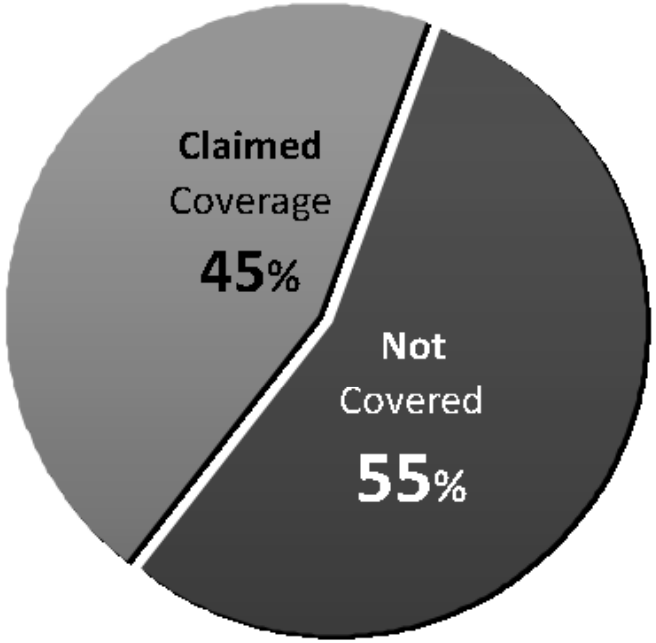
- Level 1B

  Source Code Scan (Partial Automated Verification)



Need BOTH to achieve a full level 1…

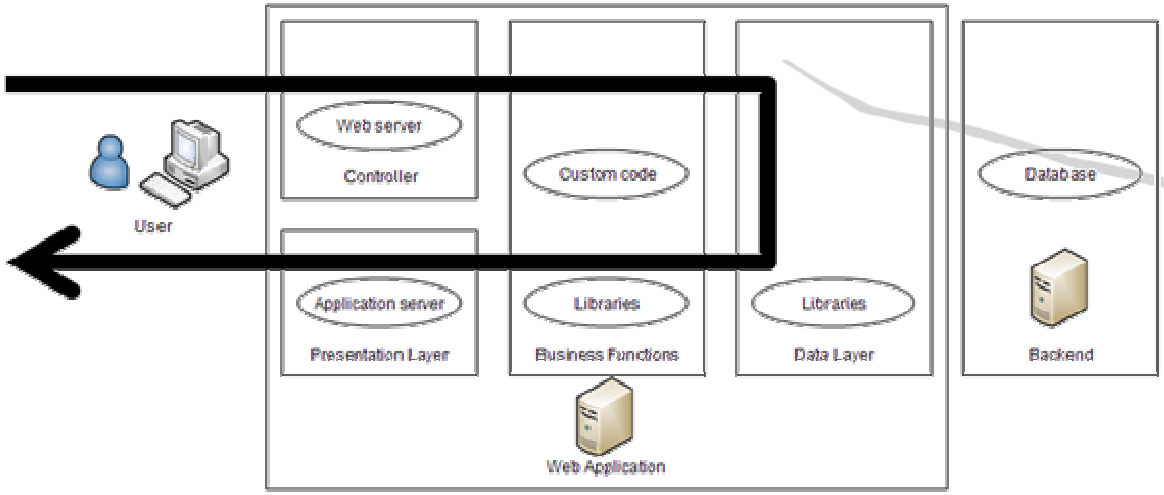
Tools – At Best 45%



- 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

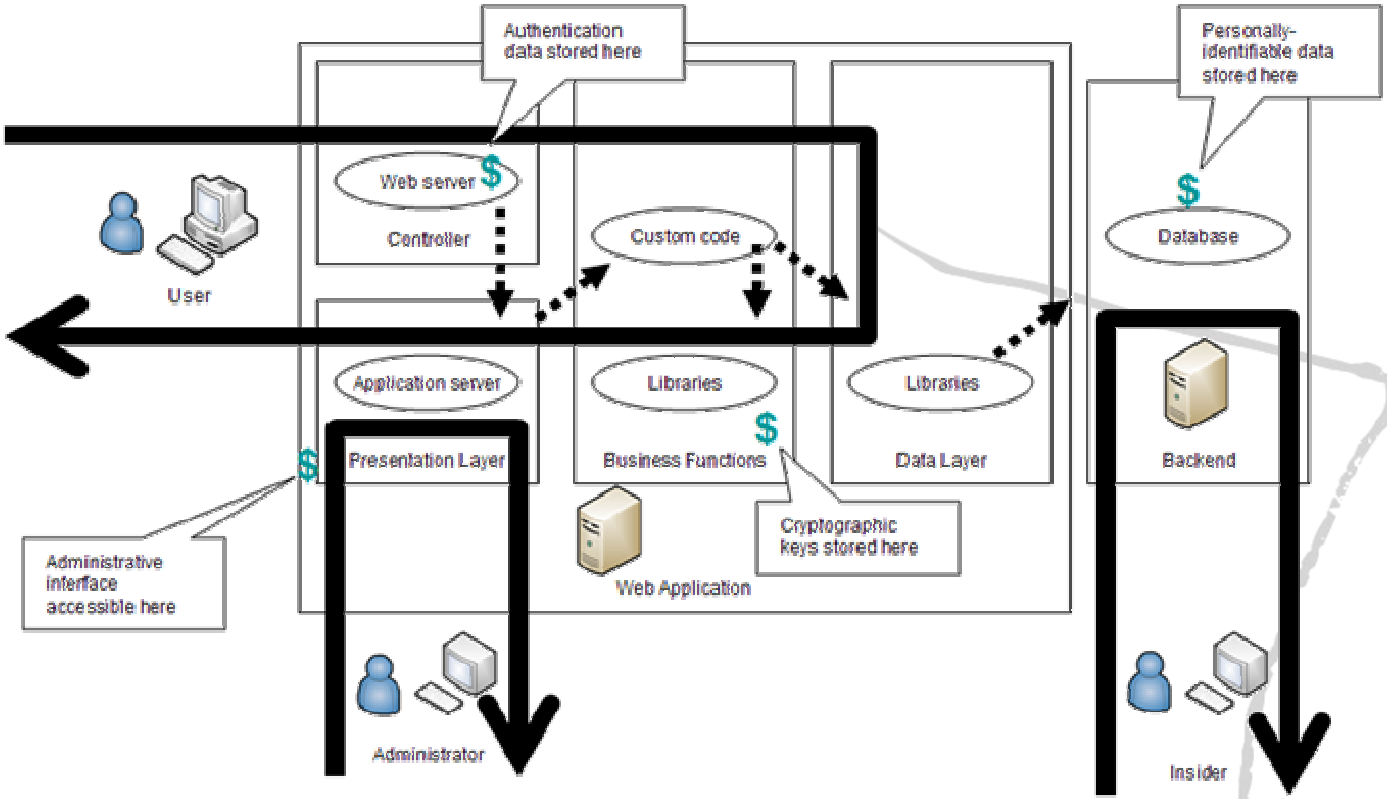
- Level 2B

  Manual Code Review

Need BOTH to achieve a full level 2…

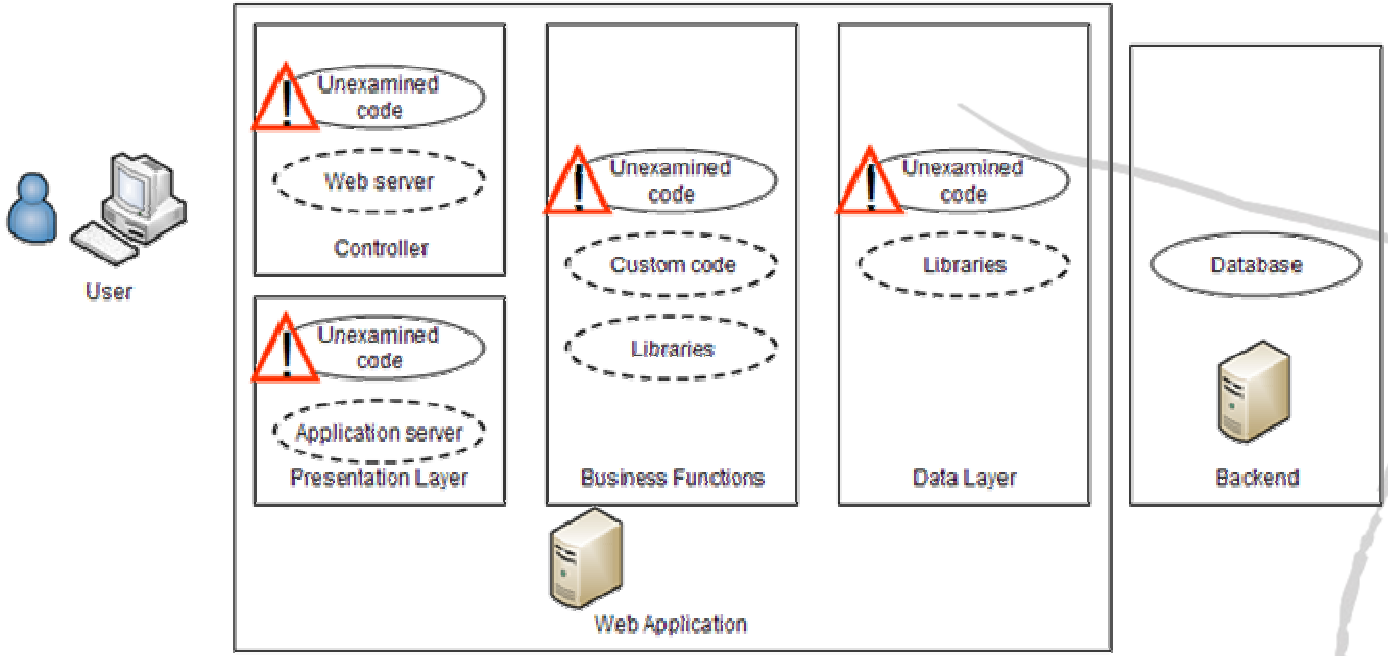
Level 3 in more detail

- Design verification of a web application organized into a high-level architecture.



Level 4 in more detail

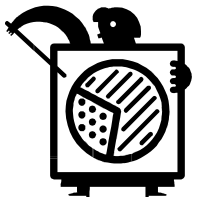
- Internal verification of a web application by searching for malicious code (not malware) and examining how security controls work.



What are the ASVS Verification Requirements?

- Security architecture verification requirements
- Security control verification requirements

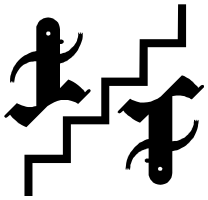
	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
Shall verify…	✓	✓	✓	✓	✓	✓
Shall verify…			✓	✓	✓	✓
Shall verify…					✓	✓
Shall verify…		✓		✓	✓	✓



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



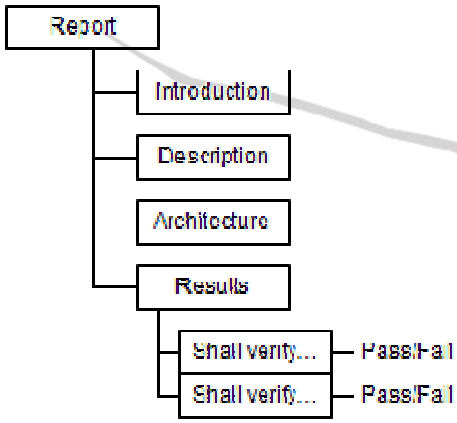
Technology and threats change over time! ASVS takes a proactive a white-list approach.

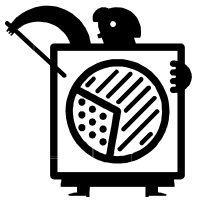
Requirement Summary

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

What are ASVS reporting requirements?

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





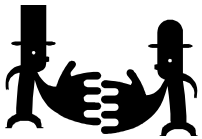
Is the report sufficiently detailed to make verification repeatable? Is there enough information to determine if the verification was accurate and complete?

Agenda

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

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

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.

A

- ASVS

H

- How to bootstrap your SDLC with verification activities
- How to build security controls
- How to create a verification service offering
- How to create catalogs of verified applications
- How to create verification project schedules
- How to document findings from a code review in a verification report
- How to handle problems caused by the IT environment
- How to meet verification reporting requirements
- How to perform a security architecture review at Level 1

H cont.

- 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 write verifier job requisitions

M

- Mapping ESAPI to ASVS Level 1

M cont.

- 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

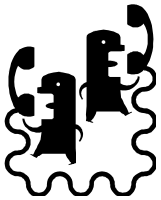
- What is a TOV (Target of Verification)
- What is a TOV boundary
- What the differences are between malware and malicious code
- Where to draw the line between your application and the IT environment
- Why there are different bugs on different books
- Why you need to use a FIPS 140-2 validated cryptomodule

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

Agenda

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

Questions?