OWASP
The Open Web Application Security Project

OWASP Application Security Verification Standard 2008

– Web Application Edition

alpha

Creative Commons (CC) Attribution Share-Alike
Free version at http://www.owasp.org

FOREWORD

This document defines four levels of application security verification. Each level includes a set of requirements for verifying the effectiveness of security controls that protect web applications and web services.

The requirements were developed with the following objectives in mind:

- Provide web application and service application developers with a yardstick with which to assess the degree of trust that can be placed in their web applications and services,

- Provide guidance to security control developers as to what to build into their commercial products in order to satisfy web application and service security requirements, and

- Provide a basis for specifying web application and web service security requirements in contracts.

The requirements were designed to meet the above objectives by ensuring validation of how security controls are designed, implemented, and used by a web application or web service. The requirements ensure that the security controls used by a web application or web service operate using a deny by default strategy, are centralized, and are located on the server side.

TABLE OF CONTENTS

TABLES

TABLES

INTRODUCTION

The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. We advocate approaching application security as a people, process, and technology problem because the most effective approaches to application security include improvements in all of these areas. We can be found at www.owasp.org.

OWASP is a new kind of organization. Our freedom from commercial pressures allows us to provide unbiased, practical, cost-effective information about application security. OWASP is not affiliated with any technology company, although we support the informed use of commercial security technology. Similar to many open-source software projects, OWASP produces many types of materials in a collaborative, open way. The OWASP Foundation is a not-for-profit entity that ensures the project's long-term success.

The primary aim of the OWASP Application Security Verification Standard (ASVS) Project is to normalize the range in the coverage and level of rigor available in the market when it comes to performing application security verification using a commercially-workable open standard. This standard can be used to establish a level of confidence in the security of web applications and services.

APPROACH

The OWASP ASVS defines verification and documentation requirements that are grouped on the basis of related coverage and level of rigor. Web application security verification is performed from a logical point of view by travelling (or attempting to travel) paths into and out of the application, performing analysis along the path. The Standard defines four levels that are linearly hierarchical (e.g. Level 2 requires more coverage and rigor than Level 1) as depicted in the figure below.

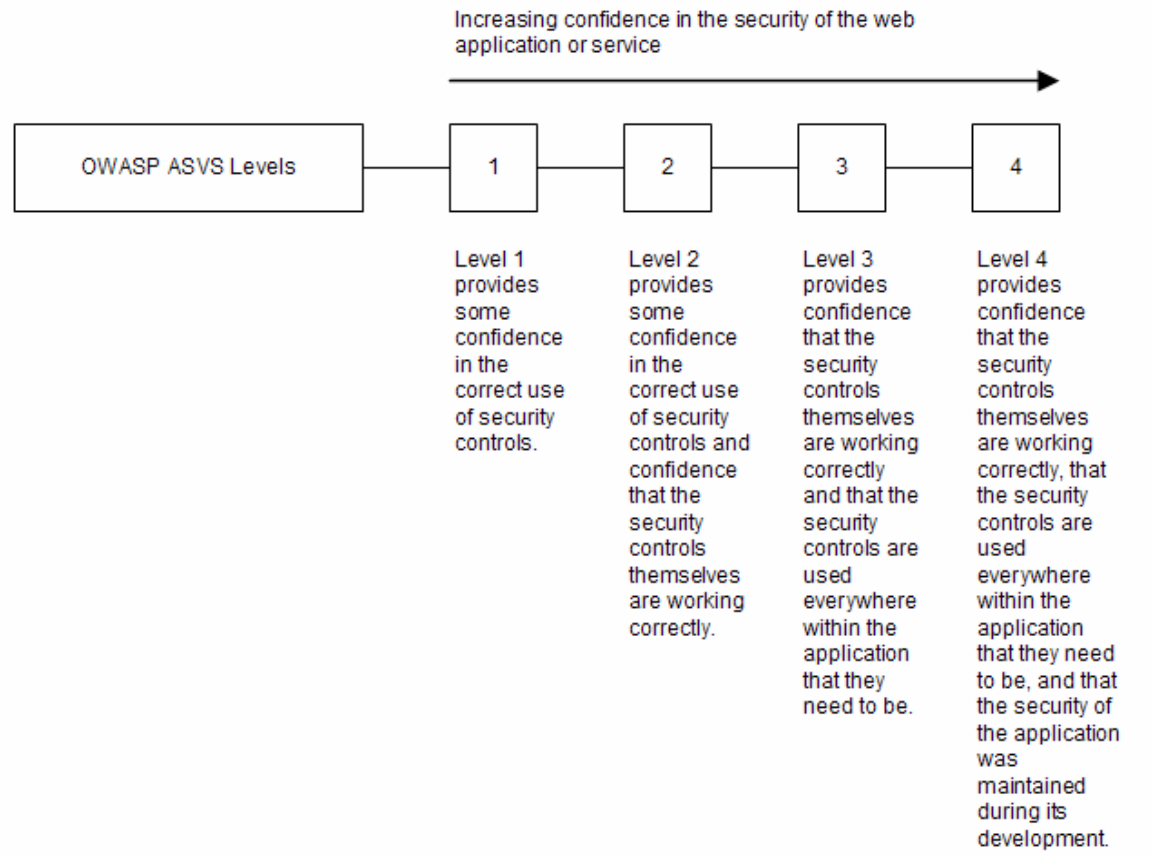

Figure 1 – OWASP ASVS Levels

The Standard further defines constituent components for Levels 1 and 2 (e.g. verification at Level 1 requires meeting both Level 1A and 1B requirements). Applications may claim compliance to either Level 1A or 1B instead of Level 1, but making such claims is weaker than claiming Level 1. Similarly, applications may claim compliance to either Level 2A or 2B instead of Level 2, but making such claims is weaker than claiming Level 2.

Verification and documentation requirements are defined in this Standard using three types of requirements: Level requirements, Derived Verification requirements, and Derived Reporting requirements. Level requirements define high-level web application and web service implementation and verification requirements according to OWASP ASVS. Derived Verification requirements define low-level web application and web service implementation and verification requirements (i.e. specific items to verify). Derived Reporting requirements define how the results of performing a web application or web service verification according to the OWASP ASVS must be documented. The relationship between these types of requirements is depicted in the figure below.

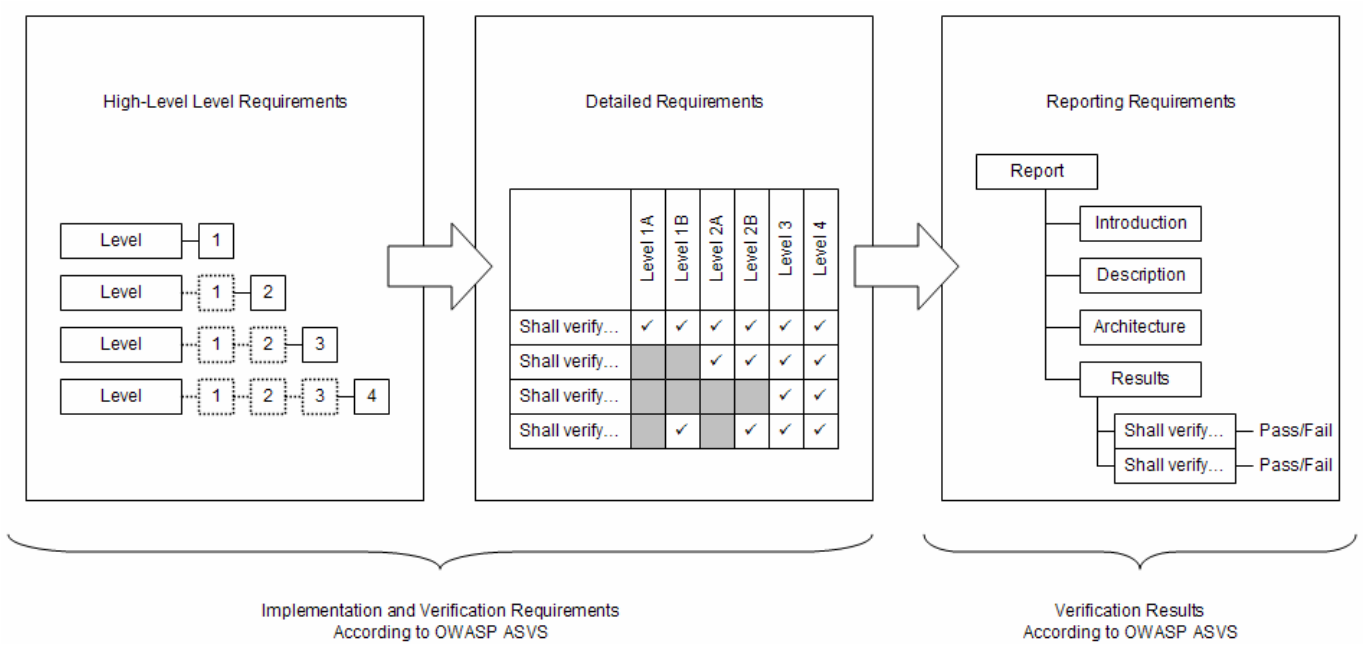

Figure 2 – Relationship between OWASP ASVS Requirements

ACKNOWLEDGEMENTS

We thank the OWASP Foundation for sponsoring the OWASP Application Security Verification Standard Project during the OWASP Summer of Code 2008. The project is led by Mike Boberski, an independent application security consultant.

Project Lead: Mike Boberski (Member, OWASP Foundation)

Authors: Mike Boberski (Member, OWASP Foundation)

Special recognition is extended to Jeff Williams, Dave Wichers, and Aspect Security, for providing extensive peer review throughout the production of this document.

Acknowledgement is also given for the contributions of: Pierre Parrend, who acted as an OWASP Summer of Code 2008 Reviewer; …TBD…; and finally, thanks are given to the application security verification community and others interested in trusted web computing for their enthusiastic advice and assistance throughout this effort.

APPLICATION SECURITY VERIFICATION LEVELS

The OWASP Application Security Verification Standard defines four levels of verification that increase in both breadth and depth. The breadth is defined in each level by a set of security requirements that must be addressed. The depth of the verification is defined by the approach and level of rigor required in verifying each security requirement.

LEVEL 1 – AUTOMATED VERIFICATION

Level 1 ("Automated Verification") is appropriate for minimum risk applications, where some confidence in the correct use of security controls is required, but the threats to security are not viewed as serious.

In Level 1, the verification involves the use of automated tools with manual verification. Because automated tools generally use vulnerability signatures to find problems, this level only provides partial coverage. The manual verification is not intended to make this level complete, only to verify that each automated finding is correct and not a false positive.

There are two constituent components for Level 1. Level 1A is for the use of automated vulnerability scanning (dynamic analysis) tools, and Level 1B is for the use of automated source code scanning (static analysis) tools. Verification efforts may use either of these components individually, or may perform a combination of these approaches to achieve a complete Level 1 rating. The structure of these levels is depicted in the figure below.

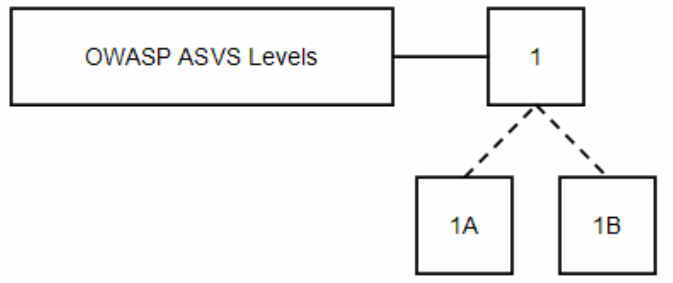

Figure 3 – OWASP ASVS Levels 1, 1A, and 1B

While it may be determined that an application meets either Level 1A or 1B, neither of these levels alone provide the same levels of rigor or coverage as an application that meets Level 1. An application that meets Level 1 must meet both Level 1A and 1B requirements.

The following are minimal requirements for Level 1, 1A, or 1B web applications or web services:

Security Control Behavior

There are no requirements for how web application or web service security controls make decisions at Level 1.

Security Control Use

There are no requirements for where web application or web service security controls are used within the application or web service at Level 1.

Security Control Implementation

There are no requirements for how web application or web service security controls are built at Level 1.

Security Control Verification

The tester shall dynamically scan the web application or web service as defined in Level 1A.

The tester shall perform source code scanning on the web application or web service as defined in Level 1B.

Requirements that allow the use of either technique do not have to be verified with both. These verification requirements can be verified with either technique at Level 1.

Documentation

The tester shall create a verification report that details the web application or web service security architecture, and the results of the verification. The web application or web service shall be defined by listing its components. Components may be defined in terms of either individual or groups of source files, libraries, and/or executables, as depicted in the figure below. The list need not be sorted or otherwise organized; the web application or web service shall be treated as groups of components within single monolithic entity. The path or paths a given end user request may take within the application are unknown.

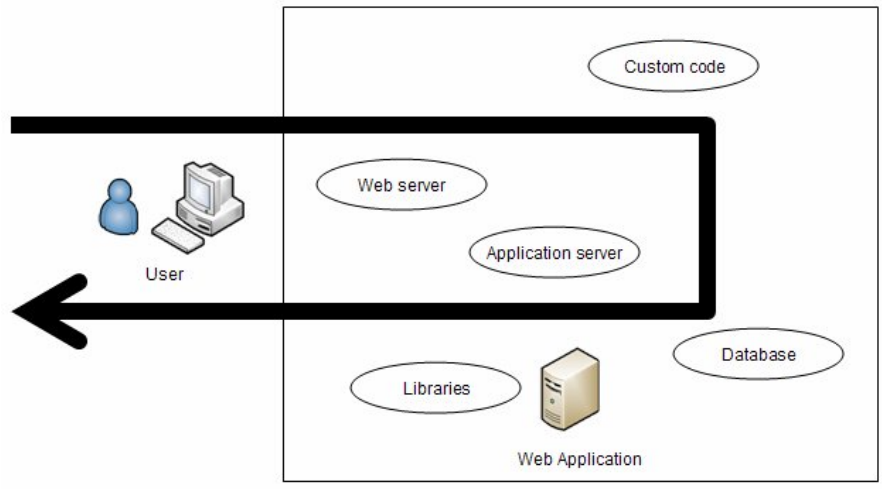

Figure 4 – OWASP ASVS Level 1 Security Architecture Example

LEVEL 1A – DYNAMIC SCAN (PARTIAL AUTOMATED VERIFICATION)

Option: Partial Security Control Verification

Dynamic scanning (a.k.a. “vulnerability scanning”) consists of using automated tools to access web application interfaces while the web application is running to attempt to circumvent the web application’s use of security controls. Note that this is not sufficient to verify the correct design, implementation, and use of a security control, but is acceptable verification at Level 1.

The tester shall dynamically scan the web application or web service according to the Level 1A requirements.

The tester shall verify all scan results using either manual penetration testing or code review. Unverified automated results are not considered to provide any assurance and are not sufficient to qualify for Level 1.

Multiple instances of a vulnerability pattern that can be traced to a single root cause should be combined into a single risk.

LEVEL 1B – SOURCE CODE SCAN (PARTIAL AUTOMATED VERIFICATION)

Option: Partial Security Control Verification

Source code scanning (a.k.a. “static analysis”) consists of using automated tools to search through web application source code to find patterns that represent a vulnerability. Note that this is not sufficient to verify the correct design, implementation, and use of a security control, but is acceptable verification at Level 1.

The tester shall perform source code scanning on the web application or web service according to the Level 1B requirements.

The tester shall verify all scan results using either manual penetration testing or code review. Unverified automated results are not considered to provide any assurance and are not sufficient to qualify for Level 1.

Multiple instances of a vulnerability pattern that can be traced to a single root cause should be combined into a single risk.

LEVEL 2 – MANUAL VERIFICATION

Level 2 (“Manual Verification”) is appropriate for applications that handle transactions up to $100,000 or personally identifiable information, where a low to moderate level of assured security is required. Level 2 provides some confidence in the correct use of security controls and confidence that the security controls themselves are working correctly. There are two constituent components for Level 2, as depicted in the figure below.

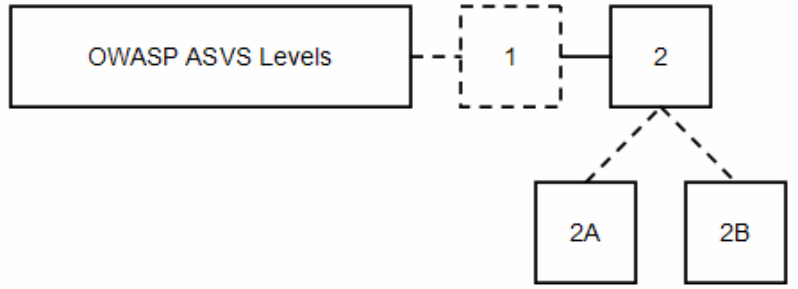

Figure 5 – OWASP ASVS Levels 2, 2A, and 2B

While it may be determined that an application meet either Level 2A or 2B, neither of these levels alone provide the same levels of rigor or coverage as an application that meets Level 2. Further, while Level 2 is a superset of Level 1, there is no requirement to run an automated tool to meet the Level 2 requirements. Instead, the tester has the option of using manual techniques for all requirements. If automated tool results are available, the tester may use them to support the analysis. However, even passing a requirement at Level 1 does not automatically indicate passing the same requirement at Level 2. This is because automated tools rely on signatures for problems, and do not provide sufficient evidence that the positive requirement has been met.

The following are minimal requirements for Level 2, 2A, or 2B web applications or web services:

Security Control Behavior

The tester shall verify that all security controls make decisions using a whitelist approach and that security controls cannot be bypassed.

Security Control Use

There are no requirements for where web application or web service security controls are used within the application or web service at Level 2.

Security Control Implementation

There are no requirements for how web application or web service security controls are built at Level 2.

Security Control Verification

The tester shall perform manual penetration testing on the web application or web service as defined in Level 2A.

The tester shall perform manual source code review on the web application or web service as defined in Level 2B.

Requirements that allow the use of either manual penetration testing or manual code review do not have to be verified with both. These verification requirements can be verified with either technique at Level 2.

The tester may optionally perform source code or dynamic scanning on the web application or web service as defined in Level 1. This automated verification cannot be used in place of the manual review of each requirement. However, if the scan

results help the tester perform their work more quickly, they can be used. Note that because a negative signature cannot verify the proper design, implementation, or use of a security control, even a verified automated result for a requirement does not mean that the manual review has passed.

Documentation

The tester shall create a verification report that describes the web application or web service security architecture, and the results of the verification. The web application or web service shall be defined by grouping its components organized into a high-level architecture (for example MVC controller components, business function components, and data layer components). Components may be defined in terms of either individual or groups of source files, libraries, and/or executables. The relationship between components or sorted groups of components need not be defined. For example, the diagram below depicts a web application that consists of a web server application, an application server application, custom code, libraries, and a database application that are grouped according to a MVC architecture. The path or paths a given end user request may take within the application are known, as depicted in the figure below. However, not all paths may be either identified or examined.

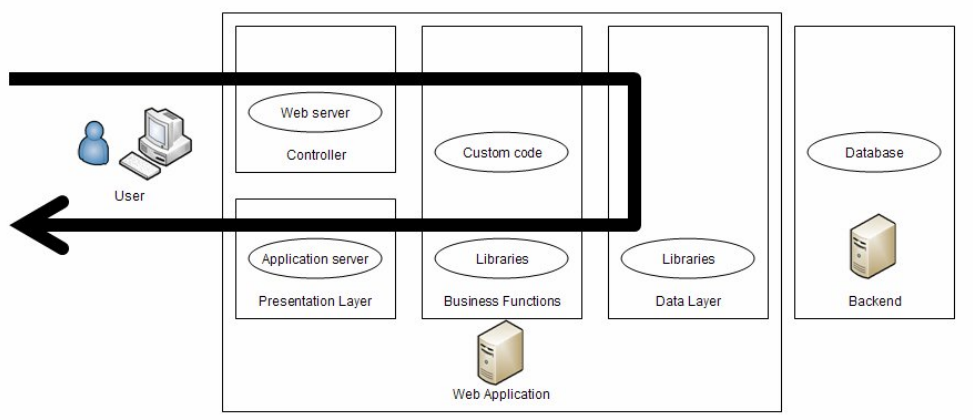

Figure 6 – OWASP ASVS Level 2 Security Architecture Example

LEVEL 2A – PENETRATION TEST (PARTIAL MANUAL VERIFICATION)

Option: Partial Security Control Verification

Manual penetration testing consists of creating dynamic tests to verify an application's proper design, implementation, and use of security controls.

The tester shall perform manual penetration testing on the application to verify the Level 2A requirements.

Where appropriate, the tester may use sampling to establish the effective use of a security control. The tester may choose to document a vulnerability pattern that will allow developers to confidently find and fix all instances of the pattern in the software baseline.

Multiple instances of a vulnerability pattern that can be traced to a single root cause should be combined into a single risk.

LEVEL 2B – CODE REVIEW (PARTIAL MANUAL VERIFICATION)

Option: Partial Security Control Verification

Manual code review consists of human searching and studying web application source code to verify the web application's design, implementation, and use of security controls.

The tester shall perform manual code review on the application to verify the Level 2B requirements.

Where appropriate, the tester may use sampling to establish the effective use of a security control. The tester may choose to document a vulnerability pattern that will allow developers to confidently find and fix all instances of the pattern in the software baseline.

Multiple instances of a vulnerability pattern that can be traced to a single root cause should be combined into a single risk.

LEVEL 3 – DESIGN VERIFICATION

Level 3 ("Design Verification") is appropriate for applications that handle transactions up to $1,000,000, process credit card information, process healthcare information, implement business critical or sensitive functions, or process other sensitive assets.

Level 3 ensures that security controls themselves are working correctly, and that security controls are used everywhere within the application that they need to be used to enforce application-specific policies. There are no constituent components for Level 3, as depicted in the figure below.

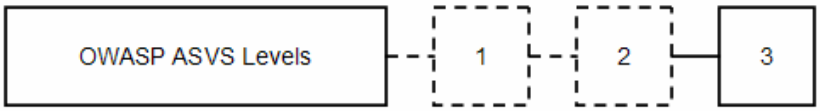

Figure 7 – OWASP ASVS Level 3

The following are minimal requirements for Level 3 web applications or web services:

Security Control Behavior

The tester shall verify that all security controls make decisions using a whitelist approach and that security controls cannot be bypassed.

Security Control Use

The tester shall verify that all security controls are centralized within the web application or web service, on the server side.

Security Control Implementation

There are no requirements for how web application or web service security controls are built at Level 3.

Security Control Verification

A prerequisite for Level 3 is that the tester shall perform manual verification of the web application or web service as defined in Level 2.

A threat model is an enhanced security control architecture that indicates threat agents, security zones, security controls, and important technical and business assets.

The tester shall create a threat model and use it to verify the design and use of all security controls as defined in the Level 3 requirements.

Documentation

The tester shall create a verification report that describes the web application or web service security architecture, and the results of the verification. The web application or web service shall be defined by sorting lists of its components organized into a high-level architecture (for example MVC controller components, business function components, and data layer components), and the relationship between components or sorted groups of components need must be defined. Components may be defined in terms of either individual or groups of source files, libraries, and/or executables. Supporting threat model information about threat agents and assets must be provided. The path or paths a given end user request may take within the application are known, as depicted in the figure below. All paths through the application are identified and examined.

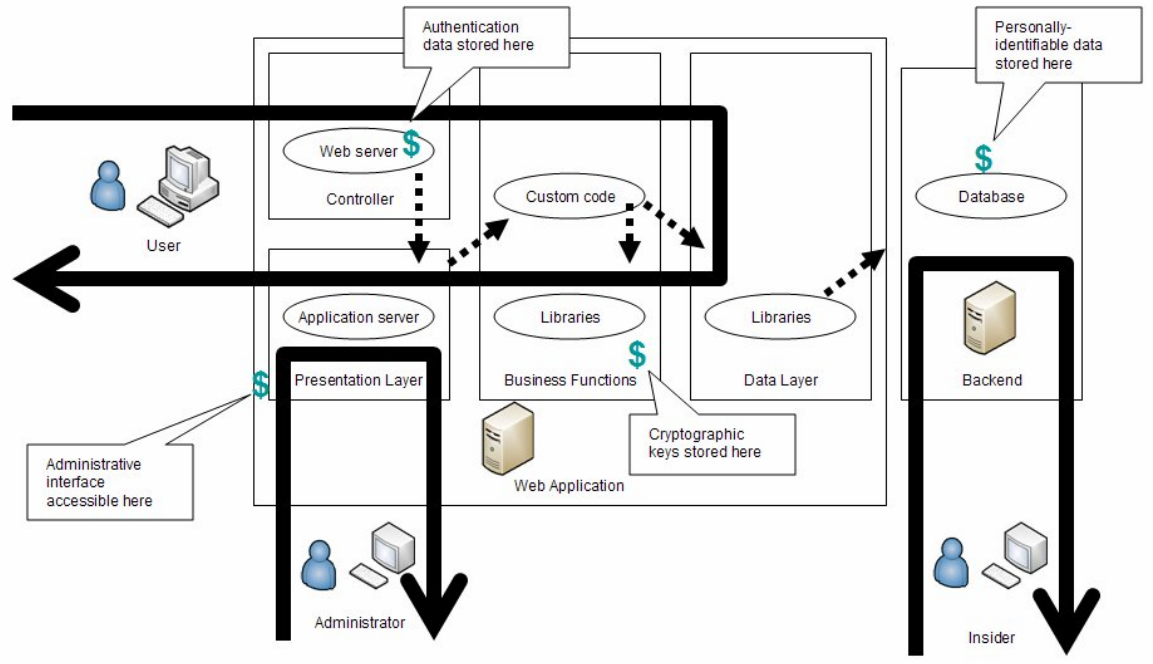

Figure 8 – OWASP ASVS Level 3 Security Architecture Example

LEVEL 4 – INTERNAL VERIFICATION

Level 4 ("Internal Verification") is appropriate for critical applications that protect life and safety, critical infrastructure, or defense functions. Level 4 ensures that security controls themselves are working correctly, that security controls are used everywhere within the application that they need to be used to enforce application-specific policies, and that secure coding practices were followed. There are no constituent components for Level 4, as depicted in the figure below.

Figure 9 – OWASP ASVS Level 4

The following are minimal requirements for Level 4 web applications or web services:

Security Control Behavior

The tester shall verify that all security controls make decisions using a whitelist approach and that security controls cannot be bypassed.

Security Control Use

The tester shall verify that all security controls are centralized within the web application or web service, on the server side.

Security Control Implementation

The tester shall verify that all security controls are easy to use correctly and are isolated, and that the web application or web service does not contain any malicious code.

Security Control Verification

A prerequisite for Level 4 is that the tester shall create a threat model and verify the security controls for the web application or web service as defined in Level 3.

The tester shall perform a manual line-by-line review to search for malicious code (which is not the same as malware), and security control interfaces must be examined to determine their isolation and ease of use as defined in the Level 4 requirements.

Documentation

The tester shall create a verification report that describes the web application or web service security architecture, and the results of the verification. The web application or web service shall be captured as defined in Level 3. Further, all previously unexamined code that was not identified as part of the web application or web service definition shall be identified, as depicted in the figure below.

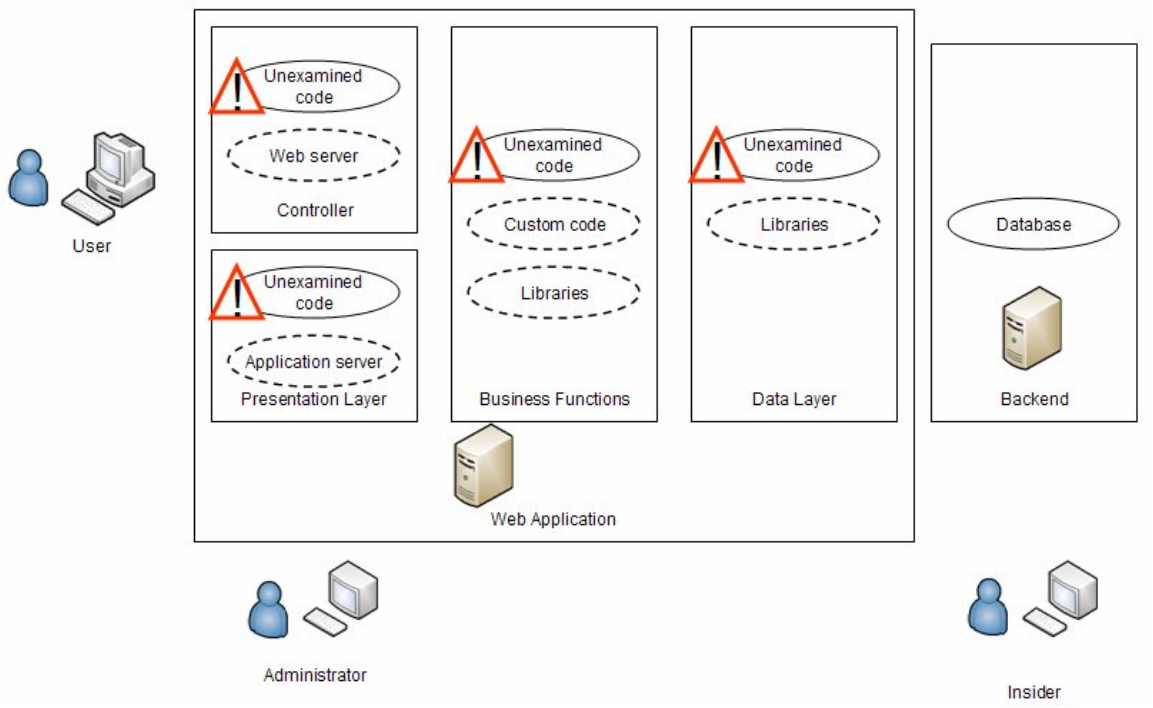

Figure 10 – OWASP ASVS Level 4 Unexamined Code Example

DETAILED VERIFICATION REQUIREMENTS

This section of the OWASP Application Security Verification Standard defines derived verification requirements that apply for each of the verification levels that the standard defines. Each section below defines families of verification requirements that are grouped on the basis of related assurance.

V1 – SECURITY ARCHITECTURE VERIFICATION REQUIREMENTS

For all levels, defining a security architecture is necessary to ensure both the completeness and accuracy (and repeatability when remediation is required) of the application security verification that is performed. Analysis can be directed and results can be traced back to an application's security architecture. However, while for all levels web applications must be defined using a security architecture, the information provided and level of detail necessary is different, depending on Level.

The table below defines the corresponding verification requirements that apply for each of the four verification levels.

Table 1 – OWASP ASVS Security Architecture Requirements (V1)

Verification Requirement	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V1.1: The tester shall identify application components (either individual or groups of source files, libraries, and/or executables).	✓	✓	✓	✓	✓	✓
V1.2: The tester shall verify the integrity of interpreted code, libraries, executables, and configuration files using checksums or hashes.				✓	✓	✓
V1.3: The tester shall verify all libraries, frameworks, and other supporting code meets OWASP ASVS requirements for the selected level.	✓		✓		✓	✓
V1.4: The tester shall define groups of application components organized into a high-level architecture.			✓	✓	✓	✓

V1.5: The tester shall identify the relationships between application components, groups of components, and external systems.					✓	✓
V1.6: The tester shall identify application threat model information including threat agents and assets.					✓	✓
V1.7: The tester shall identify all code not analyzed in a lower level.						✓

V2 – ACCESS CONTROL VERIFICATION REQUIREMENTS

The Access Control Verification Requirements define a set of requirements that can be used to verify an application's enforcement of access control. In most applications, access control must be performed in multiple different locations across the various application layers. These requirements define verification requirements for access controls for URLs, business functions, data, services, and files.

The table below defines the corresponding verification requirements that apply for each of the four verification levels.

Table 2 – OWASP ASVS Access Control Requirements (V2)

Verification Requirement	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V2.1: The tester shall verify that users can only access files for which they possess specific authorization.	✓	✓	✓	✓	✓	✓
V2.2: The tester shall verify that users can only access referenced functions for which they possess specific authorization.	✓	✓	✓	✓	✓	✓
V2.3: The tester shall verify that users can only access services for which they possess specific authorization.			✓	✓	✓	✓
V2.4: The tester shall verify that users can only access URLs for which they possess specific authorization.	✓	✓	✓	✓	✓	✓

V2.5: The tester shall verify that users can only access data for which they possess specific authorization.			✓	✓	✓	✓
V2.6: The tester shall verify that access controls fail securely.			✓	✓	✓	✓
V2.7: The tester shall verify that access control decisions are logged.			✓	✓	✓	✓
V2.8: The tester shall verify that the same access control rules are enforced in the presentation and business logic layers.			✓	✓	✓	✓
V2.9: The tester shall verify that all information used by access controls cannot be manipulated by end users.			✓	✓	✓	✓
V2.10: The tester shall verify that direct object references cannot be manipulated to access other objects without authorization.	✓		✓	✓	✓	✓
V2.11: The tester shall verify that for each access control type, there is a single implementation that is used by the application.				✓	✓	✓
V2.12: The tester shall verify that all access controls are implemented on the server side.			✓	✓	✓	✓
V2.13: The tester shall verify that all code implementing or using access controls is not affected by any malicious code.						✓

V3 – AUTHENTICATION VERIFICATION REQUIREMENTS

The Authentication Verification Requirements define a set of requirements that can be used to verify methods that generate and handle account credentials and session identifiers. These requirements define verification requirements for protecting credentials from disclosure to the maximum extent possible.

The table below defines the corresponding verification requirements that apply for each of the four verification levels.

Table 3 – OWASP ASVS Authentication Requirements (V3)

Verification Requirement	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V3.1: The tester shall verify that all pages require authentication except for pages that are specifically intended to be public.	✓	✓	✓	✓	✓	✓
V3.3: The tester shall verify that for each authentication control type, there is a single implementation that is used by the application.				✓	✓	✓
V3.4: The tester shall verify that all authentication controls are implemented on the server side.			✓	✓	✓	✓
V3.5: The tester shall verify that all code implementing or using authentication controls is not affected by any malicious code.						✓
V3.6: The tester shall verify that authentication controls fail securely.			✓	✓	✓	✓
V3.7: The tester shall verify that authentication decisions are logged.			✓	✓	✓	✓
V3.8: The tester shall verify that the strength of the authentication control is application- and/or data-specific.			✓	✓	✓	✓
V3.9: The tester shall verify that credentials are salted and hashed before storing.			✓	✓	✓	✓
V3.10: The tester shall verify that if a maximum number of authentication attempts is exceeded, the user is locked out.	✓		✓	✓	✓	✓

V3.11: The tester shall verify that that there are both user and administrator authentication control management interfaces and that they work correctly.			✓	✓	✓	✓
V3.12: The tester shall verify that credential reset mechanisms are as strong as credential setting mechanisms.			✓	✓	✓	✓
V3.13: The tester shall verify that all authentication credentials are stored in a centralized location (i.e. not hard-coded).		✓	✓	✓	✓	✓
V3.14: The tester shall verify that re-authentication is required before any sensitive operations are permitted.			✓	✓	✓	✓

V4 – SESSION MANAGEMENT VERIFICATION REQUIREMENTS

The Session Management Verification Requirements define a set of requirements that can be used to verify security related to HTTP requests, responses, sessions, cookies, headers, and logging.

The table below defines the corresponding verification requirements that apply for each of the four verification levels.

Table 4 – OWASP ASVS Session Management Requirements (V4)

Verification Requirement	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V4.1: The tester shall verify that TLS is required from login form to logout confirmation.	✓		✓		✓	✓
V4.2: The tester shall verify that the container's default session management control implementation is used by the application.	✓		✓	✓	✓	✓

V4.3: The tester shall verify that all code implementing or using session management controls is not affected by any malicious code.						✓
V4.4: The tester shall verify that sessions are invalidated when logging out.	✓		✓	✓	✓	✓
V4.5: The tester shall verify that the session id is changed on login/logout.	✓	✓	✓	✓	✓	✓
V4.6: The tester shall verify that the session id is never disclosed, particularly in URLs or logs.		✓		✓	✓	✓
V4.7: The tester shall verify that all pages have logout links.	✓		✓	✓	✓	✓
V4.8: The tester shall verify that only session ids generated by the application or web service are used.			✓	✓	✓	✓

V5 – INPUT VALIDATION VERIFICATION REQUIREMENTS

The Input Validation Requirements define a set of requirements that can be used to verify that input is encoded so that it will be safe for a variety of interpreters.

Table 5 – OWASP ASVS Input Validation Requirements (V5)

Verification Requirement	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V5.1: The tester shall verify that the character set for input is specified and that all characters are in a specified list of allowed characters.			✓	✓	✓	✓
V5.2: The tester shall verify that a specific, narrow, tailored, positive pattern is defined and applied to all input.	✓		✓	✓	✓	✓

V5.3: The tester shall verify that for each input validation control type, there is a single implementation that is used by the application.				✓	✓	✓
V5.4: The tester shall verify that all input validation controls are implemented on the server side.			✓	✓	✓	✓
V5.5: The tester shall verify that all input validation controls is not affected by any malicious code.						✓
V5.6: The tester shall verify that input validation control failures result in input rejection.			✓	✓	✓	✓
V5.7: The tester shall verify that input validation control failures are logged.			✓	✓	✓	✓
V5.8: The tester shall verify that input data is canonicalized for all downstream decoders or interpreters where user data might go before validation.					✓	✓
V5.9: The tester shall verify that user input is minimized.			✓	✓	✓	✓
V5.10: The tester shall verify that the environment is not susceptible to buffer overflows, or that security controls to prevent buffer overflows.			✓	✓	✓	✓

V6 – OUTPUT ENCODING/ESCAPING VERIFICATION REQUIREMENTS

The Output Encoding/Escaping Validation Requirements define a set of requirements that can be used to verify that output is encoded so that it will be safe for external applications.

Table 6 – OWASP ASVS Output Encoding/Escaping Requirements (V6)

Verification Requirement	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4

V6.1: The tester shall verify that output encoding/escaping controls encode all characters not known to be safe for the intended interpreter.				✓	✓	✓
V6.2: The tester shall verify that for each output encoding/escaping control type, there is a single implementation that is used by the application.					✓	✓
V6.3: The tester shall verify that all output encoding/escaping controls are implemented on the server side.			✓	✓	✓	✓
V6.4: The tester shall verify that all code implementing or using output validation controls is not affected by any malicious code.						✓
V6.5: The tester shall verify that output encoding/escaping controls fail securely.			✓	✓	✓	✓
V6.6: The tester shall verify that output encoding/escaping control failures are logged.			✓	✓	✓	✓
V6.7: The tester shall verify that operating system command parameters are escaped properly for the operating system in use.				✓	✓	✓
V6.8: The tester shall verify that all output to SQL interpreters use parameterized interfaces or the appropriate output encoding/escaping.			✓	✓	✓	✓
V6.9: The tester shall verify that all LDAP parameters that include untrusted user data are escaped.				✓	✓	✓
V6.10: The tester shall verify that all untrusted user data that is output to HTML (including embedded HTML and HTML attributes) is escaped.	✓	✓	✓	✓	✓	✓

V6.11: The tester shall verify that all output to CSS (including style tags) that include untrusted user data are escaped			✓	✓	✓	✓
V6.12: The tester shall verify that all output to Javascript (including event handlers and JavaScript object notation) that include untrusted user data are escaped		✓	✓	✓	✓	✓
V6.13: The tester shall verify that all output to XML that include untrusted user data are escaped			✓	✓	✓	✓

V7 – CRYPTOGRAPHY VERIFICATION REQUIREMENTS

The Encryption Verification Requirements define a set of requirements that can be used to verify a web application's encryption, random number, and hashing operations. Web applications should always use FIPS 140-2 validated cryptographic modules.

The table below defines the corresponding verification requirements that apply for each of the four verification levels.

Table 7 – OWASP ASVS Cryptography Requirements (V7)

Verification Requirement	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V7.1: The tester shall verify that cryptographic modules have been FIPS 140-2 validated.			✓	✓	✓	✓
V7.2: The tester shall verify cryptographic modules operate in their FIPS mode(s).			✓	✓	✓	✓
V7.3: The tester shall verify that algorithm modes and key sizes must be used in a consistent manner with the latest NIST guidance.			✓	✓	✓	✓

V7.4: The tester shall verify that access to the master secret (the application credential that is stored as plaintext on disk that is used to access the security configuration) is controlled.				✓	✓	✓
V7.5: The tester shall verify that hashes are salted when they are created.				✓	✓	✓
V7.6: The tester shall verify that for each cryptographic operation, the FIPS validated cryptographic module is used by the application.					✓	✓
V7.7: The tester shall verify that the cryptographic module is used on the server side.			✓	✓	✓	✓
V7.8: The tester shall verify that all code using the cryptographic module is not affected by any malicious code.						✓
V7.9: The tester shall verify that cryptographic modules fail securely.			✓	✓	✓	✓
V7.10: The tester shall verify that cryptographic module failures are logged.			✓	✓	✓	✓
V7.11: The tester shall verify that all random real numbers, random file names, random GUIDs, and random strings are generated using the cryptographic module's approved RNG.				✓	✓	✓

V8 – ERROR HANDLING AND LOGGING VERIFICATION REQUIREMENTS

The Error Handling and Logging Verification Requirements define a set of requirements that can be used to verify the tracking of security relevant events and the identification of attack behavior.

The table below defines the corresponding verification requirements that apply for each of the four verification levels.

Table 8 – OWASP ASVS Error Handling and Logging Requirements (V8)

Verification Requirement	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V8.1: The tester shall verify logging controls provide the ability to log both success and failure events that are identified as security-relevant, the identity of the user that caused the event, and a time stamp from a reliable source.				✓	✓	✓
V8.2: The tester shall verify that there is a single logging implementation that is used by the application.				✓	✓	✓
V8.3: The tester shall verify that all error handling and logging controls are implemented on the server side.			✓	✓	✓	✓
V8.4: The tester shall verify that all code implementing or using error handling and logging controls is not affected by any malicious code.						✓
V8.5: The tester shall verify that logging fails securely.			✓	✓	✓	✓
V8.6: The tester shall verify that that the application does not log sensitive data that would assist an attacker, including session id and personal information.			✓	✓	✓	✓
V8.7: The tester shall verify that that the application does not output error messages containing sensitive data that would assist an attacker, including session id and personal information.	✓	✓	✓	✓	✓	✓

V9 – DATA PROTECTION VERIFICATION REQUIREMENTS

The Data Protection Verification Requirements define a set of requirements that can be used to verify the protection of sensitive data (e.g. credit card number, SSN, privacy data).

Table 9 – OWASP ASVS Data Protection Security Requirements (V9)

Verification Requirement	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V9.1: The tester shall verify that sensitive data (e.g. credit card number, SSN, privacy data) is encrypted when it is stored persistently and when it is in transit.				✓	✓	✓
V9.2: The tester shall verify that external systems are accessed using a minimally privileged account.				✓	✓	✓

V10 – COMMUNICATION SECURITY VERIFICATION REQUIREMENTS

The Communication Security Verification Requirements define a set of requirements that can be used to verify that all communications with the web application or web service are properly secured.

The table below defines the corresponding verification requirements that apply for each of the four verification levels.

Table 10 – OWASP ASVS Communication Security Requirements (V10)

Verification Requirement	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V10.1: The tester shall verify TLS is used for all connections, including both front end and back end.			✓	✓	✓	✓
V10.2: The tester shall verify that there is a single standard TLS implementation that is used by the application.					✓	✓

V10.3: The tester shall verify that TLS controls fail securely.			✓	✓	✓	✓
V10.4: The tester shall verify that TLS control failures are logged.			✓	✓	✓	✓
V10.5: The tester shall verify that the TLS server certificate has been issued by a trusted CA.	✓	✓	✓	✓	✓	✓
V10.6: The tester shall verify that if client certificates are used that certificate paths are built and verified using configured trust anchors and revocation information.			✓	✓	✓	✓
V10.7: The tester shall verify that specific character encodings are defined for all connections.			✓	✓	✓	✓

V11 – HTTP VERIFICATION REQUIREMENTS

The HTTP Verification Requirements define a set of requirements that can be used to verify security related to HTTP requests, responses, sessions, cookies, headers, and logging.

The table below defines the corresponding verification requirements that apply for each of the four verification levels.

Table 11 – OWASP ASVS HTTP Requirements (V11)

Verification Requirement	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V11.1: The tester shall verify that all HTTP requests for transactions contain CSRF tokens.			✓	✓	✓	✓
V11.10: The tester shall verify that every HTTP response contains a content type header specifying a safe character set.	✓	✓	✓	✓	✓	✓

V11.10: The tester shall verify that every HTTP response containing sensitive data must contain a set of cache-control headers for various HTTP versions.	✓	✓	✓	✓	✓	✓
V11.10: The tester shall verify that redirects must not use unvalidated data.	✓	✓	✓	✓	✓	✓
V11.10: The tester shall verify that headers only use valid characters.		✓	✓	✓	✓	✓

V12 – SECURITY CONFIGURATION VERIFICATION REQUIREMENTS

The Security Configuration Verification Requirements define a set of requirements that can be used to verify the secure storage of all configuration information that directs the security-related behavior of the web application. Protection of this configuration information is critical to the secure operation of the application. Operating system access controls should be used to limit access to wherever the configuration information is stored.

The table below defines the corresponding verification requirements that apply for each of the four verification levels.

Table 12 – OWASP ASVS Security Configuration Requirements (V12)

Verification Requirement	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V12.1: The tester shall verify that all security-relevant configuration information is stored in a controlled location.				✓	✓	✓
V12.2: The tester shall verify that there is a single configuration store that is easy to audit.				✓	✓	✓
V12.3: The tester shall verify that the configuration store can be output in a human-readable format to facilitate audit.			✓	✓	✓	✓

V12.4: The tester shall verify that access to the web application's security configuration resources is controlled.			✓		✓	✓
V12.5: The tester shall verify that all changes to the security configuration are logged.			✓	✓	✓	✓
V12.6: The tester shall verify that all access is denied if the application cannot access the security configuration.			✓	✓	✓	✓

V13 – MALICIOUS CODE SEARCH VERIFICATION REQUIREMENTS

For Level 4, searching for malicious code in code that has been examined after performing Level 3 application verification is required.

The table below defines the corresponding verification requirements that apply for each of the four verification levels.

Table 13 – OWASP ASVS Malicious Code Search Requirements (V13)

Verification Requirement	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V13.1: The tester shall verify that there are no time bombs in any unexamined code by examining all system clock calls.						✓
V13.2: The tester shall verify that there are no back doors in any unexamined code by examining all code for functions unrelated to business requirements.						✓
V13.3: The tester shall verify that there are no Easter eggs in any unexamined code by examining all execution paths for extraneous code.						✓

V13.4: The tester shall verify that there are no salami attacks in any unexamined code by examining all transactions for incorrect logic.						✓

V14 – INTERNAL SECURITY VERIFICATION REQUIREMENTS

For Level 4, searching for malicious code in code that has been examined after performing Level 3 application verification is required.

The table below defines the corresponding verification requirements that apply for each of the four verification levels.

Table 4 – OWASP ASVS Self-Protection Requirements (V14)

Verification Requirement	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V14.1: The tester shall verify that the application protects all information used by security controls from misuse.					✓	✓
V14.2: The tester shall examine security control interfaces to determine that they are simple enough to use that developers are likely to use them correctly.						✓
V14.3: The tester shall verify that the application properly protects shared variables and resources from inappropriate concurrent access.						✓

VERIFICATION REPORTING REQUIREMENTS

An OWASP Application Security Verification Standard Report contains a description of the web application that was analyzed against the OWASP Application Security Verification Standard. The Report also documents the results of the analysis, including any remediation of vulnerabilities that was required.

An OWASP Application Security Verification Standard Report shall conform to the content requirements described in this section. A Report should include all necessary material necessary for a reader to understand the analysis that was performed and the results of the analysis, including configuration information and code snippets, as appropriate.

The contents of an OWASP Application Security Verification Standard Report are depicted in the figure below, which should be used when constructing the Report outline.

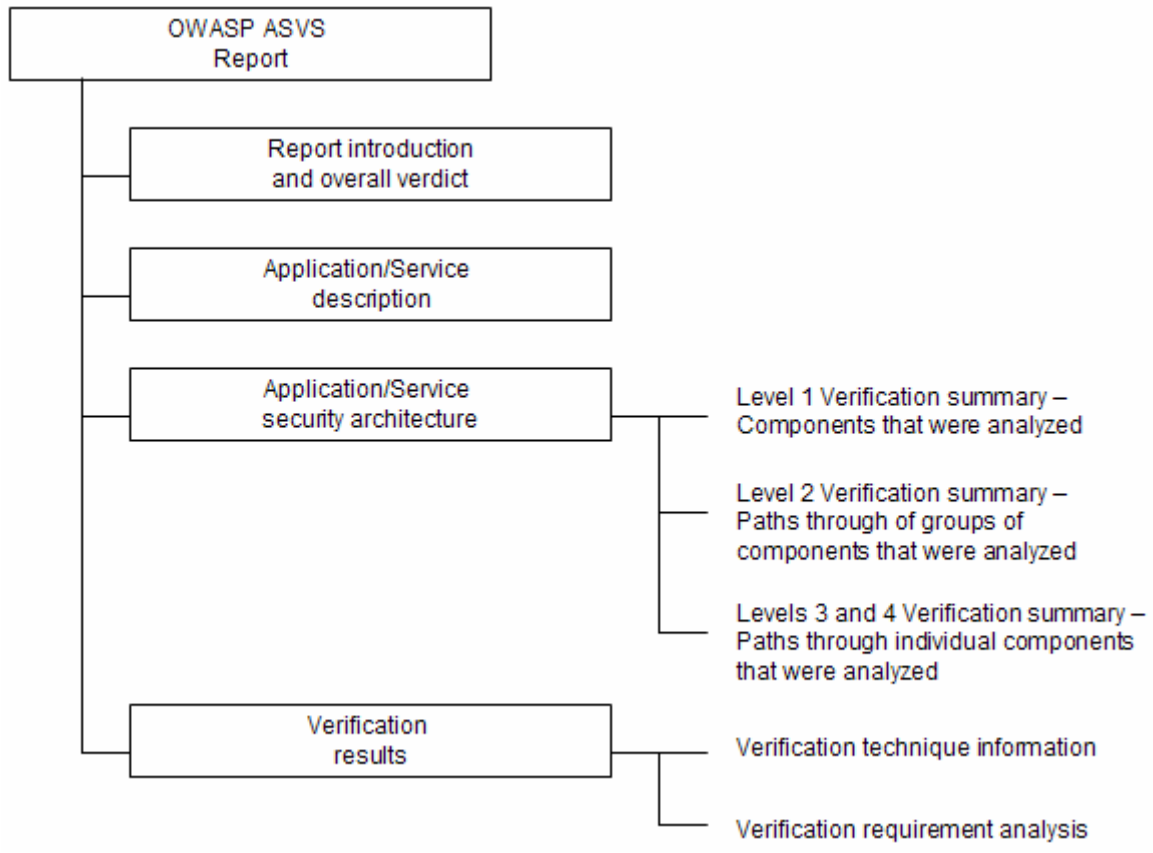

Figure 11 – OWASP ASVS Report Contents

R1 – REPORT INTRODUCTION

This part of the Report shall provide sufficient information to identify both the Report and the web application that is the subject of the report. The Report introduction shall also summarize the overall verdict.

R2 – APPLICATION/SERVICE DESCRIPTION

This part of the Report shall provide sufficient description of the web application to aid the understanding of its operation and the environment that it operates in.

R3 – APPLICATION/SERVICE SECURITY ARCHITECTURE

This part of the Report shall provide additional detail describing the web application as the first step in providing confidence to the reader of the report that the analysis that was performed was both complete and accurate. This part of the Report provides context for the analysis. The information presented in this section will be used in the course of the analysis to identify inconsistencies.

This part of the Report shall provide different levels of detail, depending on the OWASP Application Security Verification Standard Level that the analysis was performed. Details will vary according to Level as follows:

- Level 1 Verification – This part of the Report shall identify and describe components that were analyzed as defined in the Verification Level 1 section of the ASVS.
- Level 2 Verification Summary – This part of the Report shall identify and describe paths through of groups of components that were analyzed as defined in the Verification Level 2 section of the ASVS.
- Levels 3 Verification Summary – This part of the Report shall identify and describe paths through individual components that were analyzed as defined in the Verification Level 3 section of the ASVS.
- Levels 4 Verification Summary – This part of the Report shall identify and describe code analyzed as defined in the Verification Level 2 section of the ASVS.

R4 – VERIFICATION RESULTS

This part of the Report shall provide the results of the analysis that was performed according to section “Verification Requirements” of the Standard, including description of any remediation of vulnerabilities that was required, as follows:

Table 14 – OWASP ASVS Report Verification Results Contents

Level	Pass	Fail
Level 1 Automated Verification	• Verdict • Location (URL and/or source file path, name and line number) • Verdict justification (description of scan configuration)	• Verdict • Location (URL and/or source file path, name and line number) • Description (including configuration information as appropriate) • Risk rating (see the OWASP Risk Rating Methodology) • Risk justification
Level 2 Manual Implementation Verification	• Verdict • Location (URL and/or source file path, name and line number) • Verdict justification (an argument for completeness and correctness, providing specific evidence)	• Verdict • Location (URL and/or source file path, name and line number) • Description (including path through application components and steps to reproduce) • Risk rating (see the OWASP Risk Rating Methodology) • Risk justification

Level 3 Design Verification	• Verdict • Affected components and any relevant locations (URL and/or source file path, name and line number) • Verdict justification (an argument for completeness and correctness, providing specific evidence)	• Verdict • Affected components and any relevant locations (URL and/or source file path, name and line number) • Description (including path through application components and steps to reproduce) • Risk rating (see the OWASP Risk Rating Methodology) • Risk justification
Level 4 Internal Security Verification	• Verdict • Affected components and any relevant locations (URL and/or source file path, name and line number) • Verdict justification (an argument for completeness and correctness, providing specific evidence)	• Verdict • Affected components and any relevant locations (URL and/or source file path, name and line number) • Description (including path through application components and steps to reproduce) • Risk rating (see the OWASP Risk Rating Methodology) • Risk justification

GLOSSARY

Access Control – …

Application Security Verification – …

Application Security Verification Report – …

Application Security Verification Standard– …

ASVS – …

Authentication – …

Automated Analysis – …

Back Doors – …

CC – …

Code Scans – …

Common Criteria – …

Communication Security – …

Complete Automated Analysis – …

Complete Design Review – …

Complete Implementation Review – …

Cryptography – …

DOS Attacks – …

Dynamic Analysis – …

Easter Eggs – …

Error Handling – …

External Scans – …

External Systems – …

FIPS 140-2 – …

HTTP – …

Input Validation – …

Logging – …

Malicious Code – …

Malware – …

Open Web Application Security Project – …

Output Validation – …

OWASP – …

OWASP Enterprise Security API – …

OWASP ESAPI – ...

OWASP Risk Rating Methodology – ...

OWASP Testing Guide – ...

OWASP Top Ten – ...

Partial Automated Analysis – ...

Partial Implementation Review – ...

Salami Attacks – ...

Security Architecture – ...

Security Configuration – ...

Static Analysis – ...

Time Bombs – ...

WHERE TO GO FROM HERE

OWASP is the premier site for web application security. The OWASP site hosts many projects, forums, blogs, presentations, tools, and papers. OWASP hosts two major web application security conferences per year, and has over 80 local chapters.

The following OWASP projects are most likely to be useful:

- OWASP Top Ten Project
- OWASP Enterprise Security API (ESAPI) Project
- OWASP Risk Rating Methodology
- OWASP Testing Guide

Similarly, the following web sites are most likely to be useful:

- OWASP, http://www.owasp.org
- MITRE, Common Weakness Enumeration – Vulnerability Trends, http://cwe.mitre.org/documents/vuln-trends.html
- PCI Security Standards Council, publishers of the PCI standards, relevant to all organizations processing or holding credit card data, https://www.pcisecuritystandards.org/
- PCI DSS v1.1, https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf

THE BELOW ICONS REPRESENT WHAT OTHER VERSIONS ARE AVAILABLE IN PRINT FOR THIS TITLE BOOK.

ALPHA: "Alpha Quality" book content is a working draft. Content is very rough and in development until the next level of publication.

BETA: "Beta Quality" book content is the next highest level. Content is still in development until the next publishing.

RELEASE: "Release Quality" book content is the highest level of quality in a books title's lifecycle, and is a final product.

ALPHA
PUBLISHED

BETA
PUBLISHED

RELEASE
PUBLISHED

YOU ARE FREE:

to share - to copy, distribute and transmit the work

to Remix - to adapt the work

UNDER THE FOLLOWING CONDITIONS:

Attribution. You must aatribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Share Alike. - If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.

OWASP
The Open Web Application Security Project

The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. Our mission is to make application security "visible," so that people and organizations can make informed decisions about application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work.

On the cover: Braconid wasps are beneficial parasites. Braconids parasitize a broad range of hosts: caterpillars, flies, wasps, beetles, and aphids. After a female injects an egg into a host, the larva feeds slowly on that single host. By the time the host dies, the larva is fully grown. It pupates inside or near the dead host, sometimes in a silken cocoon, to emerge later as an adult wasp.