OWASP 2025 GLOBAL AppSec

BARCELONA

MAY 26-30

ELAR LANG

INTRODUCING THE 5.0 RELEASE OF THE ASVS

FRIDAY MAY 30 | 11:30AM - 12:15PM

What is the latest status of the ASVS v5.0?

https://github.com/OWASP/ASVS/releases

The release from the stage

https://www.linkedin.com/feed/update/urn:li:activity:7334154966875406339/?actorCompanyId=102250617

APPLICATION SECURITY
VERIFICATION STANDARD

OWASP ASVS v5.0

Elar Lang, co-lead for OWASP ASVS

Background

- 10 years of Web app developer
- 13 years web application security tester and trainer
  - Clarified Security OÜ, Estonia
  - Web Application Penetration Tester
  - Analysing, building, and implementing pen-test process and requirements
  - Main author (and previously lector) of 4-day Web Application Security training (2800+ hours)

Co-leader in OWASP ASVS

- v4.0 - contributor and reviewer
- v4.0.2 - major contributor
- v4.0.3 - co-leader
- v5.0.0 - co-leader
- 1200+ contribute hours + summit and conferences

clarified security
we break security to bring clarity

Estonia
elar@clarifiedsecurity.com
linkedin.com/in/elarlang
x.com/elarlang
github.com/elarlang
security.elarlang.eu
cs/elar-lang/

Starting point - ASVS v4.0

Major release 4.0, 4.0.1 2019

- Patch release 4.0.2 2020
- Patch release 4.0.3 2021
- No breaking changes for 6+ years

Challenges ahead

- Define a clear scope for ASVS
  - What goes in and what does not?
- Define what is requirement
  - The concept of the requirement
  - What are the conditions for the verification requirement
- Rethink the requirement levels
  - Rationale for level evaluation
  - Balance between levels
- Development
  - Public discussion for changes
  - Agreement in the issue first, then PR

Defining the scope of ASVS

What is in, what is out

Scope of ASVS

Application - a product as the end result

- What must be implemented, developed, built, configured

Security - clear security problem to address

- It must be clear how it decrease the likelihood or impact component of risk

Verification - security verification "fail or pass" requirement

- Verifiable with full access to the application components and documentation

Standard - *"What security principle must be achieved"*

- Verification requirement oriented.
- Not a testing guide (*"How to test"*), not a implementation guide (*"How to implement"*)

> *"That is out of scope"*
> *- Said no attacker ever*

> *"Out of scope for ASVS"*
> does not mean
> *Not important (for security)*

Requirement

Security goal to achieve

- Not being too implementation or technology-specific
- Not describing how to implement or how to verify

Focus and message

- Self-explanatory as to why they exist
- Must be understandable independently out of context

True-or-false requirement

- "Verify that" == "The application MUST do that"
  - RFC2119
    - MUST = REQUIRED, SHALL
    - SHOULD = RECOMMENDED
  - Used in lowercase in ASVS.

> *"Verify that the security principle X is achieved to prevent attack Y."*

https://datatracker.ietf.org/doc/html/rfc2119

Documented Security Decision

Documentation requirement

- Actionable, verifiable
- Required only when needed for implementation or verification

Starting point for ASVS

- Analysis, before implementation
- Outcome from analysis is input for implementation

Flexibility mechanism

- Every application and organization may have its own needs and risks

> *Precondition for implementing and verifying*
> *A flexibility mechanism*

Requirement level

General

- Should be taken as an indication
- Priority-based evaluation
- Values from 1 to 3
- Verification requirement is "must have" from that level
  - Before that it can be considered a recommendation
- Sometimes different levels (L1, L2, L3) are described into a requirement

Definitions

- Level 1 - first step to prioritize
  - Without that it is not possible to provide security, the first layer of defense
- Level 2 - standard security level
  - Every application should have this as a goal
- Level 3 - advanced level of security
  - Extra step forward

> *L1 - first step in*
> *L2 - standard security*
> *L3 - an extra step*

Example based on V5 File Handling

V5 File Handling

Control Objective

The use of files can present a variety of risks to the application, including denial of service, unauthorized access, and storage exhaustion. This chapter includes requirements to address these risks.

V5.1 File Handling Documentation

This section includes a requirement to document the expected characteristics of files accepted by the application, as a necessary precondition for developing and verifying relevant security checks.

#	Description	Level
5.1.1	Verify that the documentation defines the permitted file types, expected file extensions, and maximum size (including unpacked size) for each upload feature. Additionally, ensure that the documentation specifies how files are made safe for end-users to download and process, such as how the application behaves when a malicious file is detected.	2

V5.2 File Upload and Content

File upload functionality is a primary source of untrusted files. This section outlines the requirements for ensuring that the presence, volume, or content of these files cannot harm the application.

#	Description	Level
5.2.1	Verify that the application will only accept files of a size which it can process without causing a loss of performance or a denial of service attack.	1
5.2.2	Verify that when the application accepts a file, either on its own or within an archive such as a zip file, it checks if the file extension matches an expected file extension and validates that the contents correspond to the type represented by the extension. This includes, but is not limited to, checking the initial 'magic bytes', performing image re-writing, and using specialized libraries for file content validation. For L1, this can focus just on files which are used to make specific business or security decisions. For L2 and up, this must apply to all files being accepted.	1

Chapter

- V5 File Handling

Sections

- V5.1 File Handling Documentation
- V5.2 File Upload and Content

Requirements

- 5.1.1 - documentation requirement, L2
- 5.2.1 - implementation requirements, L1

(displayed partly)

Overview of changes

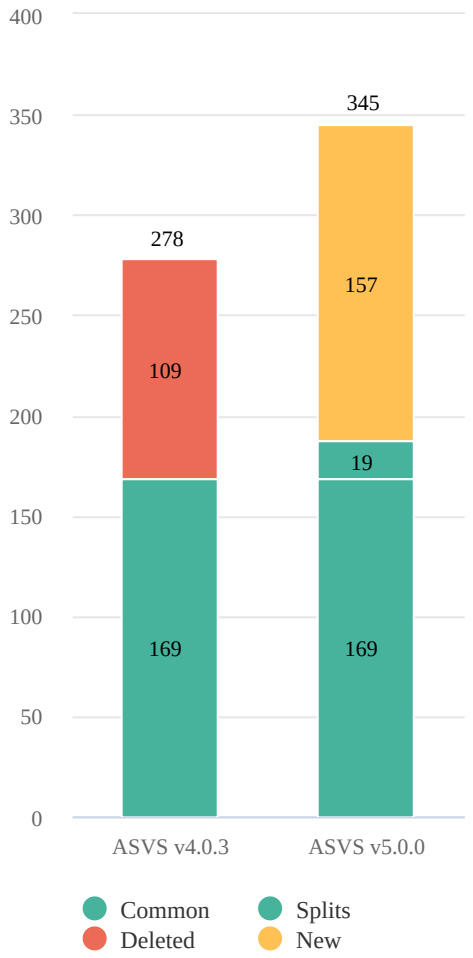
The scale of changes

In v4.0.3 - **278** requirements

- 109 requirements (38%) are no longer separate requirements in v5.0.0
  - 50 deleted due to redefined scope
  - 28 deleted as duplicates (or just covered by something else)
  - 31 requirements were merged into other one

In v5.0.0 - **345** requirements

- 157 new requirements
  - That do not originate (e.g, modify, split, or merge) from v4.0 requirements
- Split from old requirement
  - Different security principles, levels, sections
- Only 11 not changed, + 15 with grammar changes
- Every requirement has as new number



Two-way mapping for v4.0.3 and v5.0.0

Mapping files:

- `5.0/mappings`
- 🌐 `mapping_v4.0.3_to_v5.0.0.yml`
- 🌐 `mapping_v5.0.0_to_v4.0.3.yml`

Example output on

- 🌐 `https://asvs.dev`

Tags for v4.0.3

- `x.y.z` references to v5.0.0
- `MOVED TO x.y.z`
- `SPLIT TO x.y.z, i.j.k`
- `DELETED`
  - `DELETED, NOT IN SCOPE`
  - `DELETED, INCORRECT`
  - `DELETED, NOT PRACTICAL`
  - `DELETED, INSUFFICIENT IMPACT`
  - `DELETED, MERGED TO x.y.z`
  - `DELETED, COVERED BY x.y.z`

Tags for v5.0.0

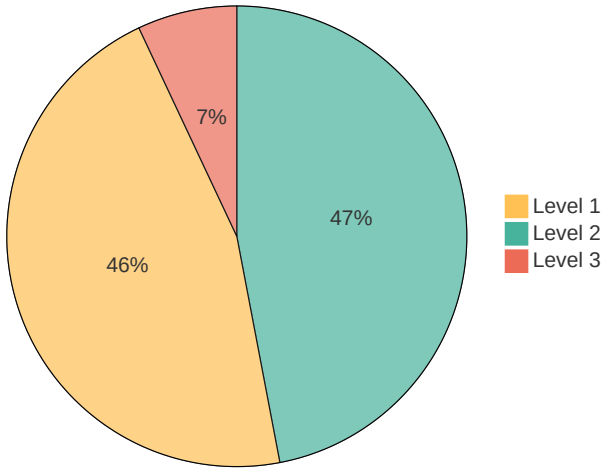
- `x.y.z` references to v4.0.3
- `MOVED FROM x.y.z`
- `SPLIT FROM x.y.z`
- `ADDED`
- `GRAMMAR`
- `MODIFIED`
- `MERGED FROM x.y.z`
- `COVERS x.y.z`

🌐 https://github.com/OWASP/ASVS/tree/master/5.0/mappings
🌐 https://asvs.dev/Mappings

Requirement levels balance

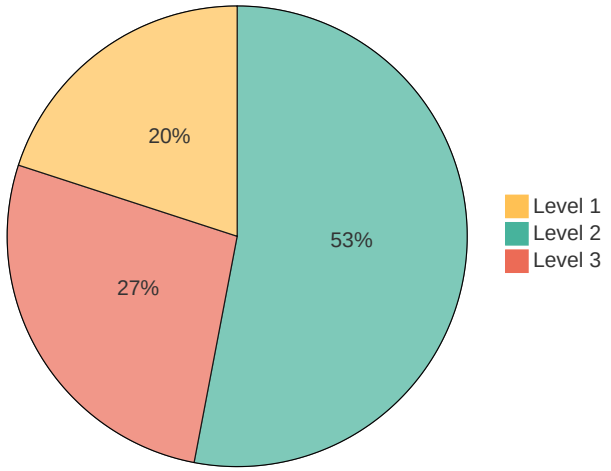
v4.0.3

- Total: 278
- Level 1: 128; 46%
- Level 2: +131; 47% (259; 93%)
- Level 3: +19; 7%



v5.0.0

- Total: 345
- Level 1: 70; 20%
- Level 2: +183; 53% (253; 73%)
- Level 3: +92; 27%



Changes in chapters and requirements

Requirements

- New requirements everywhere, in 67 different sections
- From old requirements, close to everything is modified
- Many movements to more suitable sections and categories
- Removed duplicates

Chapter and sections

- Can be skipped if not related
- You never need all 345 requirements

V1 Encoding and Sanitization

30 requirements, 8 new

Sections

- V1.1 Encoding and Sanitization Architecture
- V1.2 Injection Prevention
- V1.3 Sanitization
- V1.4 Memory, String, and Unmanaged Code
- V1.5 Safe Deserialization

> *"Process input safely"*

> *"Input Validation" moved away*

V2 Validation and Business Logic

13 requirements, 3 new

Sections

- V2.1 Validation and Business Logic Documentation
- V2.2 Input Validation
- V2.3 Business Logic Security
- V2.4 Anti-automation

"Accept only valid input"
"Provide expected business logic"

Documentation requirements

"Input Validation" moved here

V3 Web Frontend Security

31 requirements, 12 new

Sections

- V3.1 Web Frontend Security Documentation
- V3.2 Unintended Content Interpretation
- V3.3 Cookie Setup
- V3.4 Browser Security Mechanism Headers
- V3.5 Browser Origin Separation
- V3.6 External Resource Integrity
- V3.7 Other Browser Security Considerations

> *"If the browser is involved in attack scenario"*

> *"Cookie setup" moved here from "Session management"*

> *HTTP header-related requirements moved here "Configuration"*

V4 API and Web Service

16 requirements, 12 new

Sections

- V4.1 Generic Web Service Security
- V4.2 HTTP Message Structure Validation
- V4.3 GraphQL
- V4.4 WebSocket

> *General requirements for API and Web Service that are not browser-specific*

V5 File Handling

13 requirements, 5 new

Sections

- V5.1 File Handling Documentation
- V5.2 File Upload and Content
- V5.3 File Storage
- V5.4 File Download

> *Handle files safely*

V6 Authentication

47 requirements, 11 new

Sections

- V6.1 Authentication Documentation
- V6.2 Password Security
- V6.3 General Authentication Security
- V6.4 Authentication Factor Lifecycle and Recovery
- V6.5 General Multi-factor authentication requirements
- V6.6 Out-of-Band authentication mechanisms
- V6.7 Cryptographic authentication mechanism
- V6.8 Authentication with an Identity Provider

Identify the user

MFA is required from Level 2

Password-rules related requirement on L1 although not the first layer of defense

IdP for the future

V7 Session Management

19 requirements, 8 new

Sections

- V7.1 Session Management Documentation
- V7.2 Fundamental Session Management Security
- V7.3 Session Timeout
- V7.4 Session Termination
- V7.5 Defenses Against Session Abuse
- V7.6 Federated Re-authentication

Session management logic only

Security decision as an flexibility mechanism

"Cookie setup" moved away

"Token-based session management" moved away

Terminology update:
- Session Token
- Reference Token
- Session Identifier
- Self-contained Token

V8 Authorization

13 requirements, 9 new

Sections

- V8.1 Authorization Documentation
- V8.2 General Authorization Design
- V8.3 Operation Level Authorization
- V8.4 Other Authorization Considerations

> *Authorization*

> *Documentation requirements*

V9 Self-contained Tokens

7 requirements, 6 new

Sections

- V9.1 Token source and integrity
- V9.2 Token content

Independent technology layer

Base of "OAuth and OIDC"

V10 OAuth and OIDC

36 requirements, 35 new

Sections

- V10.1 Generic OAuth and OIDC Security
- V10.2 OAuth Client
- V10.3 OAuth Resource Server
- V10.4 OAuth Authorization Server
- V10.5 OIDC Client
- V10.6 OpenID Provider
- V10.7 Consent Management

> *"Standard in standard"*

> *"Area 51"*

> *Based on tens of RFCs and specifications*

V11 Cryptography

24 requirements, 9 new

Sections

- V11.1 Cryptographic Inventory and Documentation
- V11.2 Secure Cryptography Implementation
- V11.3 Encryption Algorithms
- V11.4 Hashing and Hash-based Functions
- V11.5 Random Values
- V11.6 Public Key Cryptography
- V11.7 In-Use Data Cryptography

> *"Standard in standard"*

> *"Massive Appendix"*

V12 Secure Communication

12 requirements, 5 new

Sections

- V12.1 General TLS Security Guidance
- V12.2 HTTPS Communication with External Facing Services
- V12.3 General Service to Service Communication Security

> *"Protect data in transit"*

V13 Configuration

21 requirements, 6 new

Sections

- V13.1 Configuration Documentation
- V13.2 Backend Communication Configuration
- V13.3 Secret Management
- V13.4 Unintended Information Leakage

> *"Build and deploy" - out of scope*

> *"HTTP Security headers" - moved*

> *"Dependency" - moved*

V14 Data Protection

13 requirements, 4 new

Section

- V14.1 Data Protection Documentation
- V14.2 General Data Protection
- V14.3 Client-side Data Protection

Define "sensitive data"

"Pure policy" - out of scope

"Backups" - out of scope

V15 Secure Coding and Architecture

21 requirements, 9 new

Sections

- V15.1 Secure Coding and Architecture Documentation
- V15.2 Security Architecture and Dependencies
- V15.3 Defensive Coding
- V15.4 Safe Concurrency

Inventory of used components

Define "risky component"

New section for Safe Concurrency

V16 Security Logging and Error Handling

17 requirements, 3 new

Sections

- V16.1 Security Logging Documentation
- V16.2 General Logging
- V16.3 Security Events
- V16.4 Log Protection
- V16.5 Error Handling

V17 WebRTC

12 requirements, all new

Sections

- V17.1 TURN Server
- V17.2 Media
- V17.3 Signaling

Removed mappings

Requirement-only scope

- To keep the releasable content as stable as possible

Removed mappings from requirement data

- ProActive controls
  - Were part of requirement text
- CWE
  - Not always good mapping available
  - Used for 1-to-1, in practice requires many-to-1 and 1-to-many
  - Disallows point to category
- NIST 800-63B v3, v4
  - Mostly paragraph level mapping, presented as part of section text in version 5

Open Common Requirement Enumeration (OpenCRE)

- No point to duplicate the work

> *Mapping is a display layer task*

The team behind ASVS v5.0

Leaders

- Elar Lang
- Josh C Grossman
- Jim Manico
- Daniel Cuthbert

Working Group

- Tobias Ahnoff
- Ralph Andalis
- Ryan Armstrong
- Gabriel Corona
- Meghan Jacquot
- Shanni Prutchi
- Iman Sharafaldin
- Eden Yardeni

Other Major Contributors

- Sjoerd Langkemper
- Isaac Lewis
- Sandro Gauci
- Mark Carney

Supporters behind ASVS v5.0

Maintaining Supporters

clarified security
we break security to bring clarity

Bounce SECURITY

MANICODE
SECURE CODING EDUCATION

Primary supporters

Google

Secondary supporters

Jit

Tertiary supporters

CREST

FWDSEC

omega point.

https://github.com/OWASP/ASVS/blob/master/SUPPORTERS.md

Post-Release

The release, the team and the future

Release strategy

Major.Minor.Patch

- Major (v4.0.3 > v5.0.0)
  - Full reorganization
- Minor (v5.0.3 > v5.1.0)
  - Requirement may be added or removed
  - Overall numbering stays the same
  - Reevaluation for compliance is necessary
- Patch (v5.0.0 > v5.0.1)
  - No changes for the meanings of the requirement
  - **If the application was valid of v5.0.0, it will be also valid for v5.0.1**

Patch release v5.0.1

- The actual feedback comes when v5.0.0 is in use

Stable

- Minor release (v5.0.x) is expected to be stable for years

The future, call for action

Take ASVS v5.0 into use

- Mapping from v4.0.3 helps to migrate
- Build on top of ASVS
  - Developer guidance
  - Testing guidance, automation
  - Align Cheat Sheet Series, and Testing Guide projects
  - Technology specific implementation and testing
  - OpenCRE

Contributing

- Feedback, improving the quality
- Translations
  - Previously in markdown...
- Web output
  - Can have dynamic changes now for mapping

Happy ASVS use!

`https://asvs.owasp.org`
`https://github.com/OWASP/ASVS/`