OWASP ASVS –
An Application Security Treasure Chest

About the Speaker

DI Thomas Kerbl, MSc.

Principal Security Consultant

- 20+ years experience in information security
- 50+ speeches
- Service Owner for „Secure Software Development Consulting“
- Teamleader
- Security Analyst, Security Architect

Education

- MSc @ Technikum Vienna, Specialization in Multimedia & Software Development
- Dipl. Ing @ Hagenberg, Specialization in Computer- and Media Security

Certificates

- Accredited ÖNORM A 7700 Auditor
- ISTQB Certified Tester
- ISAQB Certified Professional for Software Architecture
- ISSECO Certified Professional for Secure Software Engineering
- PCiIAA Practitioner Certificate in Information Assurance Architecture

✉ t.kerbl@sec-consult.com

https://twitter.com/dementophobia

On the menu for today…

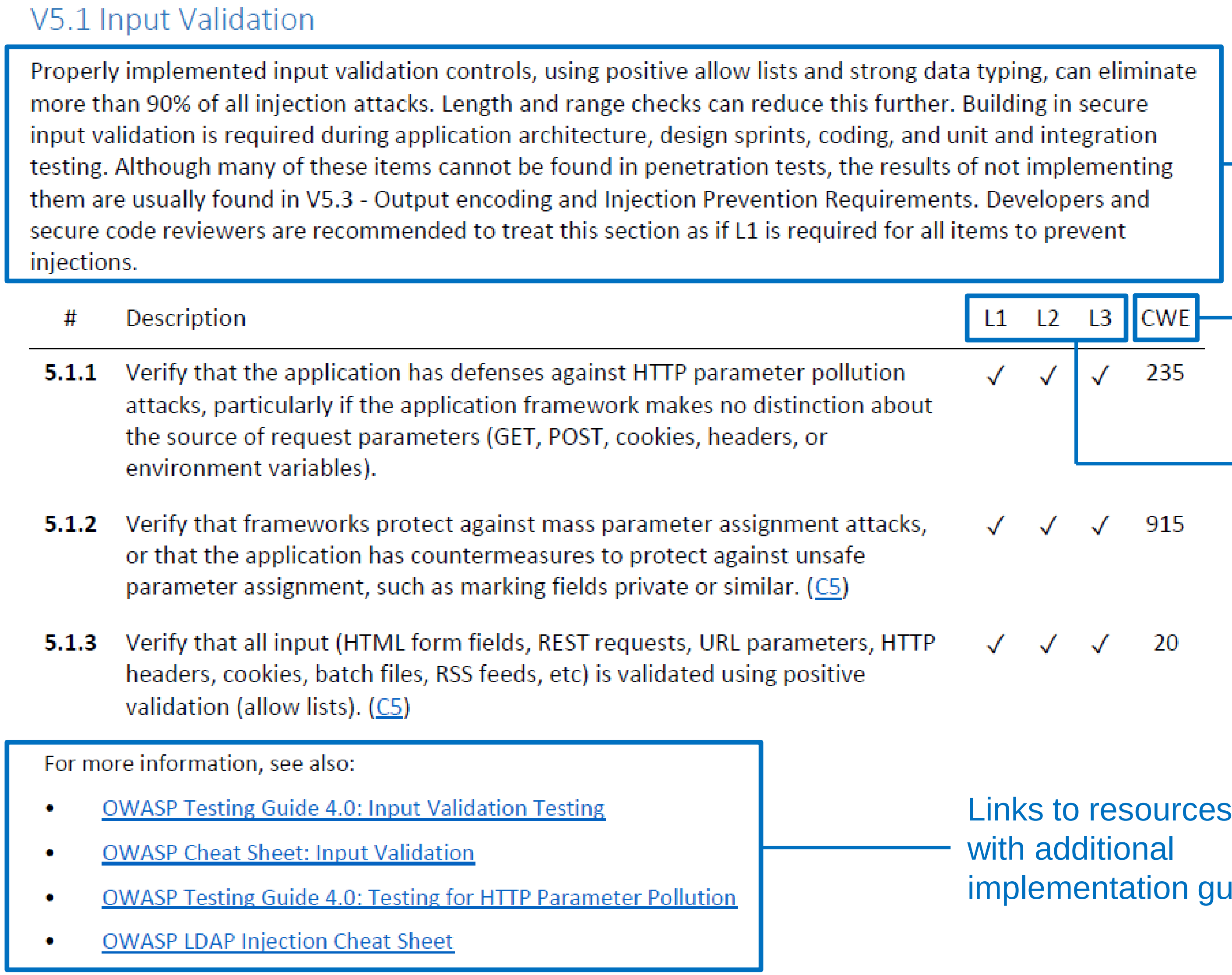
- **An introduction to OWASP ASVS**
- How to **fully integrate the ASVS in key activities** of your SSDL
- **Preparation and procedure for certification** according to the ASVS
- A **speculative outlook** into the future of the ASVS

Introducing the OWASP ASVS – An application security treasure chest

1. Architecture, Design and Threat Modeling
2. Authentication
3. Session Management
4. Access Control
5. Validation, Sanitization and Encoding
6. Stored Cryptography
7. Error Handling and Logging
8. Data Protection
9. Communication
10. Malicious Code
11. Business Logic
12. Files and Resources
13. API and Web Service
14. Configuration

The 14 chapters of the ASVS (Version 4.0.3)

Anatomy of an ASVS chapter



V5.1 Input Validation

Properly implemented input validation controls, using positive allow lists and strong data typing, can eliminate more than 90% of all injection attacks. Length and range checks can reduce this further. Building in secure input validation is required during application architecture, design sprints, coding, and unit and integration testing. Although many of these items cannot be found in penetration tests, the results of not implementing them are usually found in V5.3 - Output encoding and Injection Prevention Requirements. Developers and secure code reviewers are recommended to treat this section as if L1 is required for all items to prevent injections.

#	Description	L1	L2	L3	CWE
5.1.1	Verify that the application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, or environment variables).	✓	✓	✓	235
5.1.2	Verify that frameworks protect against mass parameter assignment attacks, or that the application has countermeasures to protect against unsafe parameter assignment, such as marking fields private or similar. (C5)	✓	✓	✓	915
5.1.3	Verify that all input (HTML form fields, REST requests, URL parameters, HTTP headers, cookies, batch files, RSS feeds, etc) is validated using positive validation (allow lists). (C5)	✓	✓	✓	20

For more information, see also:

- OWASP Testing Guide 4.0: Input Validation Testing
- OWASP Cheat Sheet: Input Validation
- OWASP Testing Guide 4.0: Testing for HTTP Parameter Pollution
- OWASP LDAP Injection Cheat Sheet

Briefly explains, what the chapter is about

Mapping to the CWE database

Choose appropriate controls depending on your risk profile

Links to resources with additional implementation guidance

On the menu for today…

- **An introduction to OWASP ASVS**
- How to **fully integrate the ASVS in key activities** of your SSDL
- **Preparation and procedure for certification** according to the ASVS
- A **speculative outlook** into the future of the ASVS

3 Major Secure Software Development Pain Points

Unspecific or Missing Security Requirements

Lack of Security Guidance during Implementation

Missing Validation Criteria for Security Controls

OWASP

Application Security Verification Standard 4.0.3

Final

October 2021

Pain Point “Unspecific or Missing Security Requirements”

What we are used to:

```
Security Requirement #4:
“Ensure that confidentiality and integrity cannot be compromised.”
```

- ➢ What does this mean for me as an architect or developer?
- ➢ Are my homebrew security controls sufficient?
- ➢ What do I have to do?!

Wouldn’t it be great to have a complete list of all necessary technical security controls needed for every security-relevant functionality?

Pain Point “Lack of Security Guidance during Implementation”

What we are used to:

```
Our Collection of Coding Guidelines:
- General Style Guide
- Naming Conventions for Variables
- Rules for Code Complexity
```

- Where do I find **Secure** Coding Guidelines?
- Am I following best practices with my implementation?

Wouldn’t it be great to have detailed guidelines regarding the implementation of specific security mechanisms?

Pain Point “Missing Validation Criteria for Security Controls”

What we are used to:

```
Our Code Scanner gives us a green light and our test team
did not stumble over any severe vulnerabilities either.

Result: Security Test Passed!
```

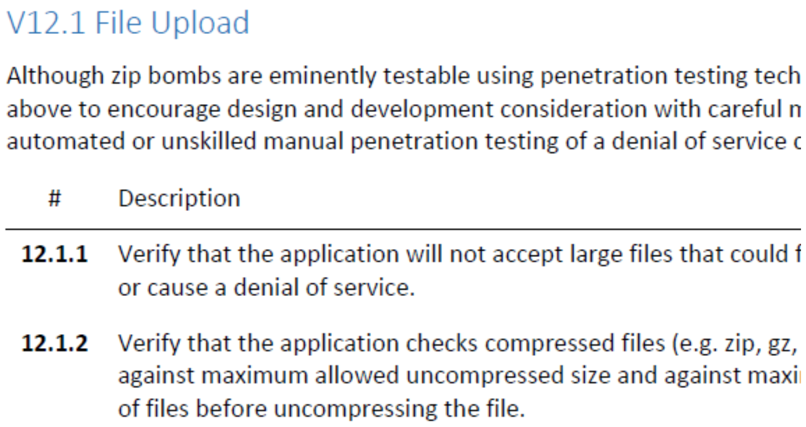
- ➢ Does our code scanner really cover everything that’s important?
- ➢ Is our test team assessing security in a structured manner?

Wouldn’t it be great to have a complete checklist with validation criteria to benchmark your security tools and guide your security test team?

Integration in your SSDL activities – Example

Implementing a file upload functionality:

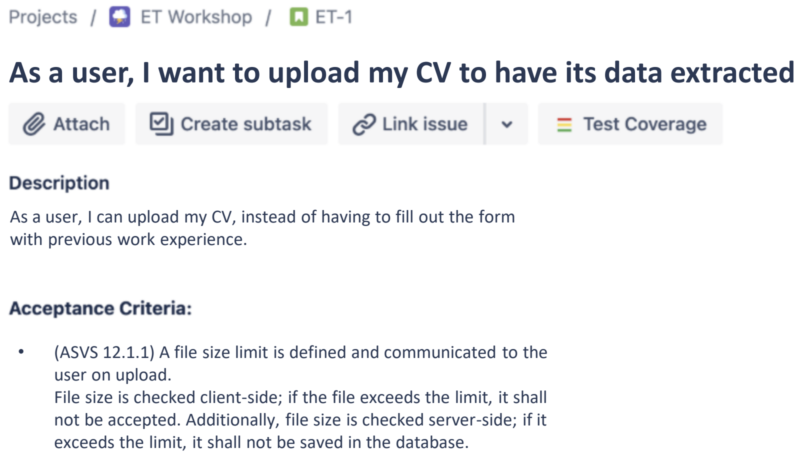
- Chapter 12: “Files and Resources”
  Immediately available complete list of implementation-ready technical security controls
- Add the ASVS controls to your user story as non-functional requirements / quality criteria / acceptance criteria
- Create (automated) test cases to verify relevant ASVS controls/requirements



V12.1 File Upload

Although zip bombs are eminently testable using penetration testing tech
above to encourage design and development consideration with careful n
automated or unskilled manual penetration testing of a denial of service c

#	Description
12.1.1	Verify that the application will not accept large files that could f or cause a denial of service.
12.1.2	Verify that the application checks compressed files (e.g. zip, gz, against maximum allowed uncompressed size and against maxi of files before uncompressing the file.



As a user, I want to upload my CV to have its data extracted

Description

As a user, I can upload my CV, instead of having to fill out the form with previous work experience.

Acceptance Criteria:

- (ASVS 12.1.1) A file size limit is defined and communicated to the user on upload.
  File size is checked client-side; if the file exceeds the limit, it shall not be accepted. Additionally, file size is checked server-side; if it exceeds the limit, it shall not be saved in the database.

On the menu for today…

- **An introduction to OWASP ASVS**
- How to **fully integrate the ASVS in key activities** of your SSDL
- **Preparation and procedure for certification** according to the ASVS
- A **speculative outlook** into the future of the ASVS

Software supply-chain security – ASVS to the rescue

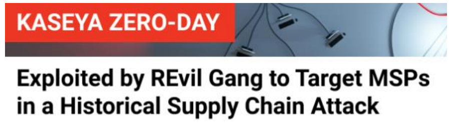
- Any software you buy and use may be vulnerable and compromised

- Require your suppliers to properly manage security in their software products

- The need for an international standard of application security requirements increases

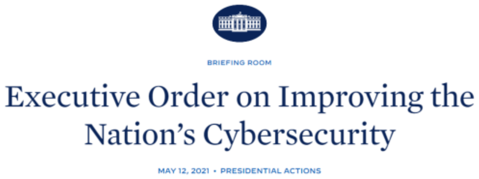
- Such a standard exists – the ASVS!
  But: Compliance with it cannot be certified…

solarwinds



KASEYA ZERO-DAY

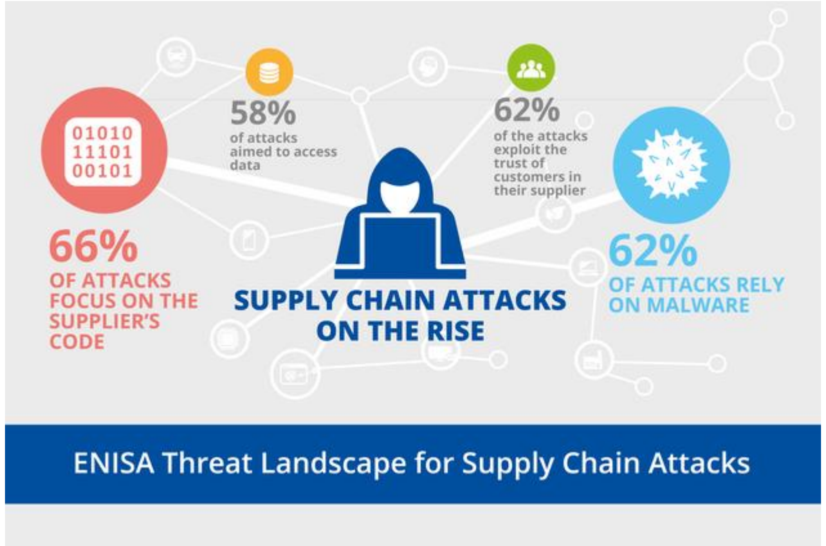
Exploited by REvil Gang to Target MSPs in a Historical Supply Chain Attack



BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

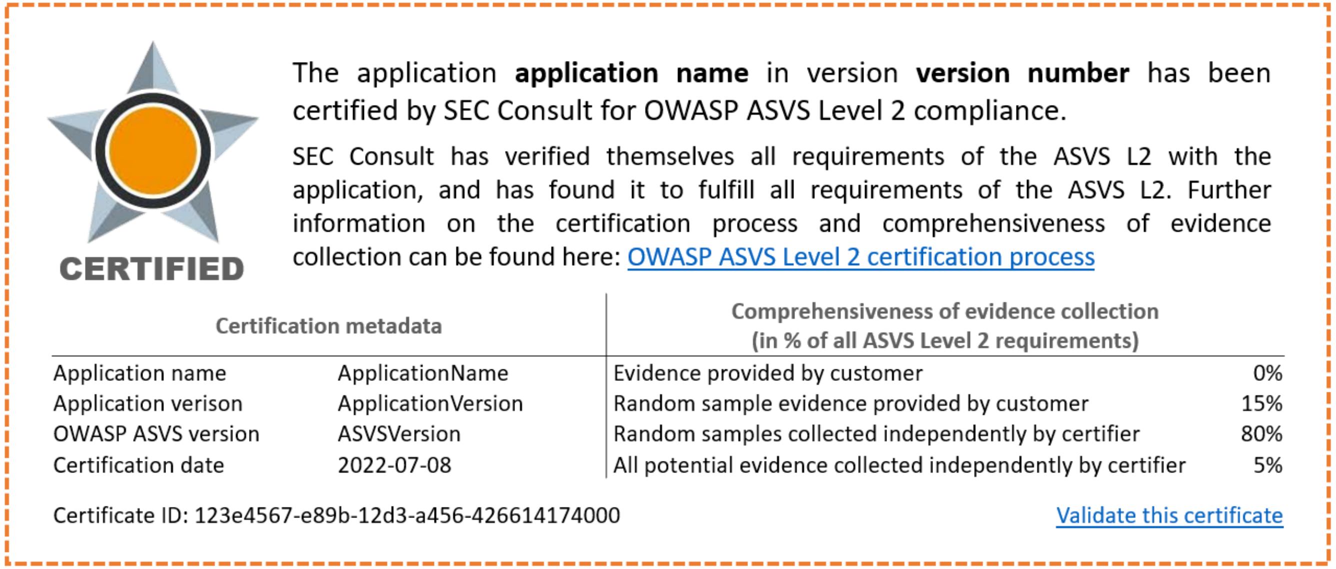

01010
11101
00101
58% of attacks aimed to access data
62% of the attacks exploit the trust of customers in their supplier
66% OF ATTACKS FOCUS ON THE SUPPLIER'S CODE
SUPPLY CHAIN ATTACKS ON THE RISE
62% OF ATTACKS RELY ON MALWARE

ENISA Threat Landscape for Supply Chain Attacks

ASVS certification

Proposed framework for certification standardization:

- Ease of verification of compliance by software buyers
- Ensure quality of certification process
- Open framework, allowing everyone to issue certifications
- Includes self-certification (and hybrid certification) schemes to allow software developers to self-certify their application in a trustable/reputable way



The application **application name** in version **version number** has been certified by SEC Consult for OWASP ASVS Level 2 compliance.

SEC Consult has verified themselves all requirements of the ASVS L2 with the application, and has found it to fulfill all requirements of the ASVS L2. Further information on the certification process and comprehensiveness of evidence collection can be found here: OWASP ASVS Level 2 certification process

Certification metadata		Comprehensiveness of evidence collection (in % of all ASVS Level 2 requirements)	
Application name	ApplicationName	Evidence provided by customer	0%
Application verison	ApplicationVersion	Random sample evidence provided by customer	15%
OWASP ASVS version	ASVSVersion	Random samples collected independently by certifier	80%
Certification date	2022-07-08	All potential evidence collected independently by certifier	5%

Certificate ID: 123e4567-e89b-12d3-a456-426614174000

Validate this certificate

Road to ASVS Certification – High-Level Process

- ✓ **Pre-assessment workshops** to assess readiness for certification of subject application
- ✓ **Knowledge transfer workshops** to transfer understanding of the application to reviewers for white box penetration testing and code reviewing
- ✓ **Conduction of penetration tests**, **code reviews** and **workshops** in order to assess and document the fulfillment of all security requirements
- ✓ **Creation of the certification package** containing all information and artefacts necessary for public disclosure of the successful certification
- ✓ **Reporting and final presentation** of the consolidated findings and audit report

On the menu for today…

- **An introduction to OWASP ASVS**
- How to **fully integrate the ASVS in key activities** of your SSDL
- **Preparation and procedure for certification** according to the ASVS
- A **speculative outlook** into the future of the ASVS

A speculative outlook into the future of the ASVS

New major version (v5) is in the making – Contribute now!

Certification based on ASVS L2 will become a recognized “Seal of Approval”.

Accreditation schemes for auditors will be defined (e.g., by CREST).

New flavors of ASVS – similar to the MASVS – will emerge.

AI based tool integration (e.g., language models like GPT-4).

Do you have
any further questions?

Don‘t hesitate to contact me:

✉ t.kerbl@sec-consult.com

https://twitter.com/dementophobia

CYBER INCIDENT? CALL +49 30 398 202 777