Der Application Security Verification Standard (ASVS)

Matthias Rohr
SEC Consult Deutschland
Senior Security Consultant
m.rohr@sec-consult.com

SEC Consult

OWASP
10/2010

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

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

Der ASVS-Standard - Übersicht

- Erster offizieller Standard der OWASP
- Release 1.0 im August 2009
- Lead
  - Mike Boberski (bis 2010)
  - Dave Wichers (seit 2010)
- Deutsche Übersetzung
  - Initial: März 2010
  - Last Update: Oktober 2010
- Weitere Übersetzungen in Arbeit
  - Französisch, Spanisch, Japanisch, ... (5 weitere)

Motivation (1)

- Es existierte bisher kein Standard für die Verifikation der Sicherheit von Webanwendungen
- Folge: Wie kann ein Kunde zwischen einem toolbasierten Scan und einer aufwändigen Sicherheitsanalyse unterscheiden?
- Betroffene: Einkauf, Anbieter, QA

Die Philosophie hinter dem ASVS

- Unabhängigkeit in Bezug auf
  - Anwendung
  - Technologie
  - Tools
  - Lifecycle
- Anforderungen sollten direkt umsetzbar sein und keine zusätzliche Interpretation erfordern.
- Anforderungen sollten positiv formuliert sein

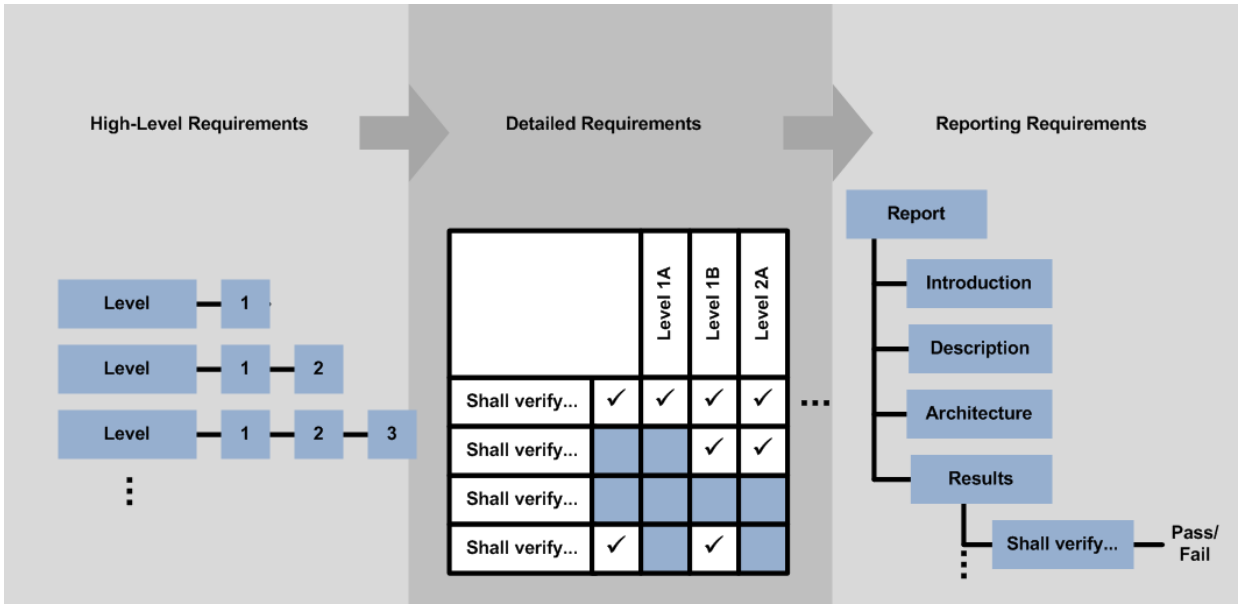
Die OWASP Top Ten stellen ein Beispiel für negative Anforderungen dar.

Das ASVS-Design

- Der Standard definiert vier Level zur Differenzierung unterschiedlicher Prüfgrade der (Web-)Anwendungssicherheit.
- Die Unterscheidung hinsichtlich Prüfabdeckung und Prüfstrenge erfolgt relativ linear zwischen diesen Leveln.
- Der Standard definiert Vorgaben an den Ausbau des Ergebnisberichtes

Übersicht der ASVS-Struktur

- Abschnitt “Verifikationslevel für Anwendungssicherheit”
- Abschnitt “Anforderungen an detaillierte Verifikation”
- Abschnitt “Anforderungen an den Verifikationsbericht”

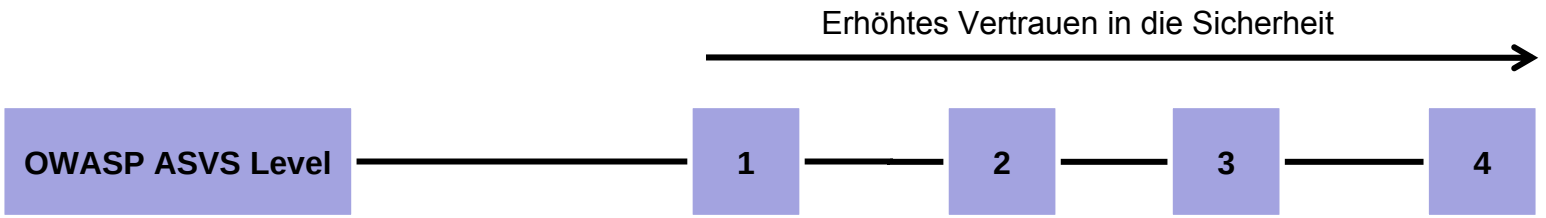


Welche ASVS-Level gibt es?

- Level 1 – Automatische Verifikation (Tools)
  - Level 1A – Dynamischer Scan (w3af, WebInspect, AppScan, etc.)
  - Level 1B – Source Code Scan (Fortify SCA, Ounce, etc.)
- Level 2 – Manuelle Verifikation
  - Level 2A – Penetrationstest
  - Level 2B – Code Review
- Level 3 – Design Verifikation
- Level 4 – Interne Verifikation

Eine Verifikation nach ASVS Level 2 beinhaltet die Durchführung von Penetrationstest und Codereview , bei Level 1 von dynamischen und Code-Scans

Eröhtes Vertrauen je Level



	1	2	3	4
...in die korrekte Verwendung von Sicherheitsmechanismen	√	√	√	√
... in die korrekte Funktionsweise der Sicherheitsmechanismen		√	√	√
... dass Sicherheitsmechanismen überall dort eingesetzt werden, wo dies erforderlich ist			√	√
.. in den Entwicklungsprozess und die Entwickler selbst.				√

Anforderungen im Einzelnen

- V1. Sicherheitsarchitektur
- V2. Authentisierung
- V3. Session Management
- V4. Zugriffskontrollen
- V5. Eingabevalidierung
- V6. Ausgabeenkodierung /-Escaping
- V7. Kryptographie
- V8. Fehlerbehandlung und Logging
- V9. Datensicherheit
- V10. Kommunikationssicherheit
- V11. HTTP-Sicherheit
- V12. Sicherheitskonfiguration
- V13. Identifikation von Schadcode
- V14. Interne Sicherheit

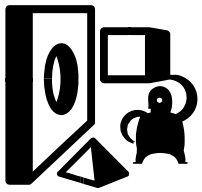
Verifikationsanforderung		Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V6.1	Verifiziere, dass nicht vertrauenswürdige Daten, welche in HTML ausgegeben werden (inklusive HTML-Elemente, Attribute, Javascript-Datenobjekte, CSS-Blöcke und URI-Attribute) für den jeweiligen Kontext entsprechend escaped wurden.		✓	✓	✓	✓	✓
V6.2	Verifiziere, dass sämtliche Ausgabeenkodierung /-Escaping serverseitig erfolgt.			✓	✓	✓	✓
V6.3	Verifiziere, dass sämtliche Methoden zur Ausgabeenkodierung alle Zeichen						

insg. 121 Anforderungen

Motivation (2)

- Es existieren kaum* Standards, die detailierte Vorgaben zur sicheren Implementierung von Webanwendungen liefern (Coding Guidelines)
- Folge: Sichere Implementierung ist meist nur abhägig vom Know How des jeweiligen Entwicklers
- Betroffene: Einkäufer, Anforderer, Entwickler

* Ausnahme z.B. tw. A7700

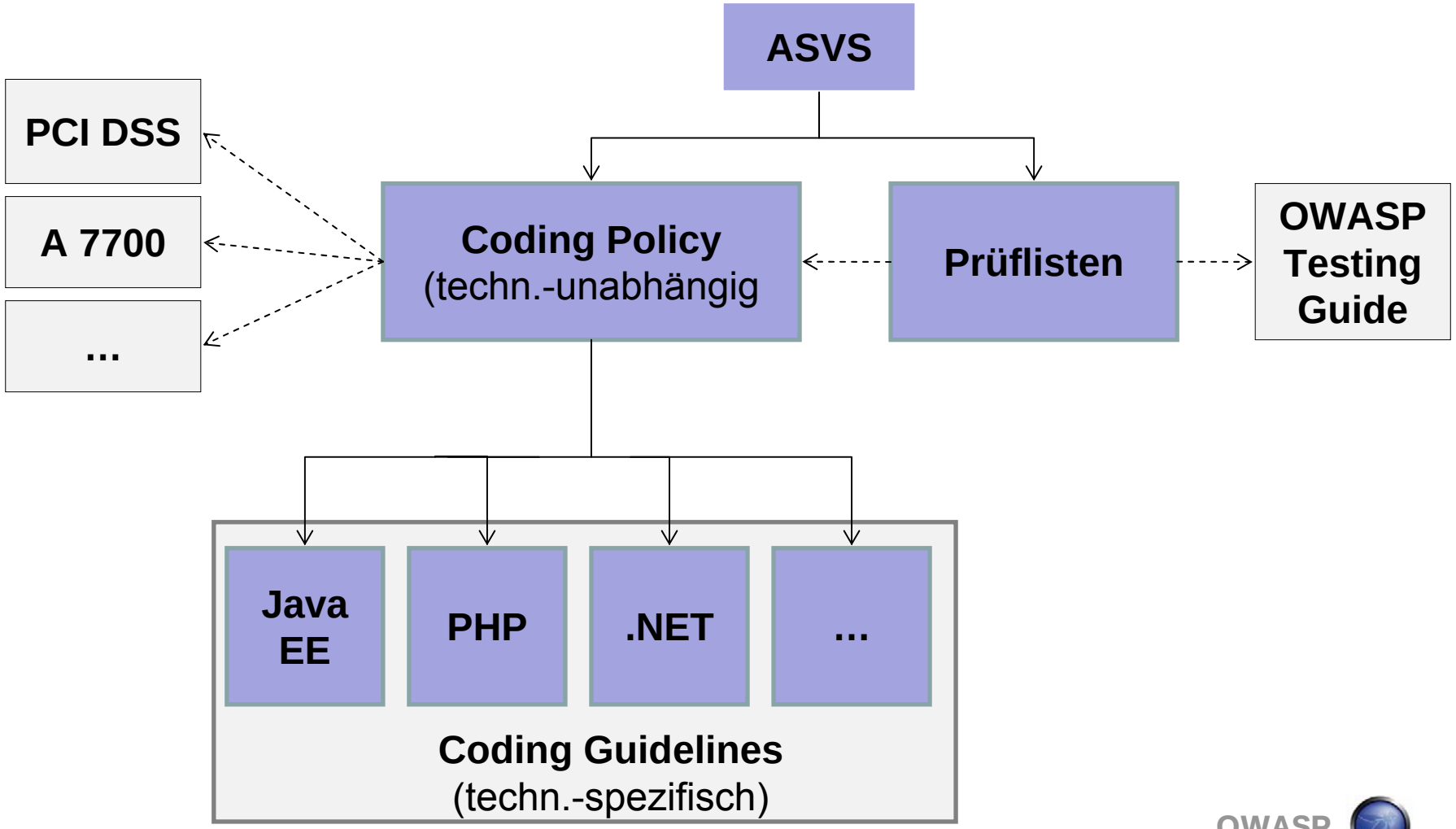


Sichere Implementierung ist meist eine handwerkliche Tätigkeit, keine Ingenieurs-Diszipliz, daher sind genaue Vorgaben hier essenziell!

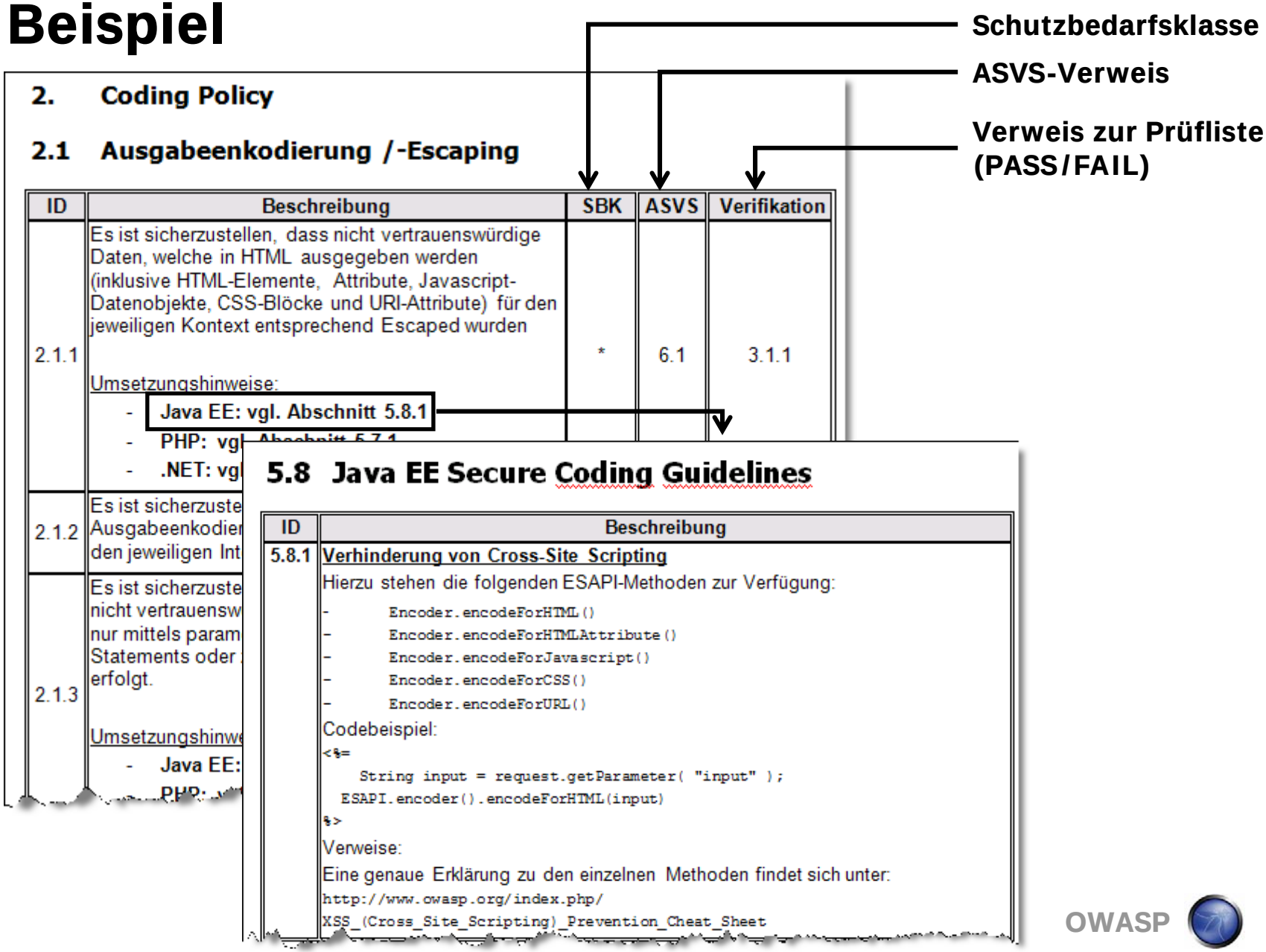
Test Driven Security Development

- Anforderungen sind nur dann sinnvoll, wenn auch deren Einhaltung geprüft oder zumindestens zugesichert werden kann!
- Ansatz: Ableitung von Coding Guidelines aus ASVS-Prüfanweisung

Security Framework auf Basis des ASVS



Beispiel


Schutzbedarfsklasse
ASVS-Verweis
Verweis zur Prüfliste (PASS/FAIL)
2. Coding Policy
2.1 Ausgabeenkodierung /-Escaping
ID
Beschreibung
SBK
ASVS
Verifikation
2.1.1
Es ist sicherzustellen, dass nicht vertrauenswürdige Daten, welche in HTML ausgegeben werden (inklusive HTML-Elemente, Attribute, Javascript-Datenobjekte, CSS-Blöcke und URI-Attribute) für den jeweiligen Kontext entsprechend Escaped wurden
*
6.1
3.1.1
Umsetzungshinweise:
- Java EE: vgl. Abschnitt 5.8.1
- PHP: vgl
- .NET: vgl
2.1.2
Es ist sicherzuste
Ausgabeenkodier
den jeweiligen Int
2.1.3
Es ist sicherzuste
nicht vertrauensw
nur mittels param
Statements oder
erfolgt.
Umsetzungshinwe
- Java EE:
- PHP:
5.8 Java EE Secure Coding Guidelines
ID
Beschreibung
5.8.1
Verhinderung von Cross-Site Scripting
Hierzu stehen die folgenden ESAPI-Methoden zur Verfügung:
- Encoder.encodeForHTML()
- Encoder.encodeForHTMLAttribute()
- Encoder.encodeForJavascript()
- Encoder.encodeForCSS()
- Encoder.encodeForURL()
Codebeispiel:
<%=
String input = request.getParameter("input");
ESAPI.encoder().encodeForHTML(input)
%>
Verweise:
Eine genaue Erklärung zu den einzelnen Methoden findet sich unter:
http://www.owasp.org/index.php/
XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

Wo fange ich an?

- ASVS als interner Prüfkatalog:
  - Verifikationsbedarf (VB)= SBK + Confidence Index
  - ASVS-Level leitet sich aus dem festgelegten VB ab
  - Min.: Durchführung von ASVS-Level-1-Prüfungen
- Käufer und Lieferant:
  - Vertragl. Festlegung des ASVS-Levels zu dem die gelieferte Anwendung compliant sein muss (Level >=2)
  - min. Stichprobentests!
- ASVS als Vorgabe für interne SW-Entwicklung (Secure Coding Guidelines)

Informationen & Download

- Kopie beziehbar von ASVS-Projektseite:
  - http://www.owasp.org/index.php/ASVS
- Vorschläge zur Verbesserung und Fragen über ASVS-Mailingliste:
  - Siehe “Mailing List/Subscribe”-Link auf der Projektseite

Fragen?