OWASP
Open Web Application
Security Project

# Agil, aber sicher?

## Security im agilen Entwicklungsprozess

15.3.2016 OWASP Stammtisch München

# Über mich

Security
XP
Agile
Java
Kanban
Applications
Architecture
Scrum
ThreatModeling
Web
JavaEE
ContinuousIntegration
Microservices
StaticAnalysis
BigData
TDD
Software
SpecByExample
Testing
Development
Spring
BDD
CleanCode
Cloud
CodeReviews

**Andreas Falk**
**NovaTec Consulting GmbH**
andreas.falk@novatec-gmbh.de

**Mitglied der** OWASP

@andifalk
@agile_security

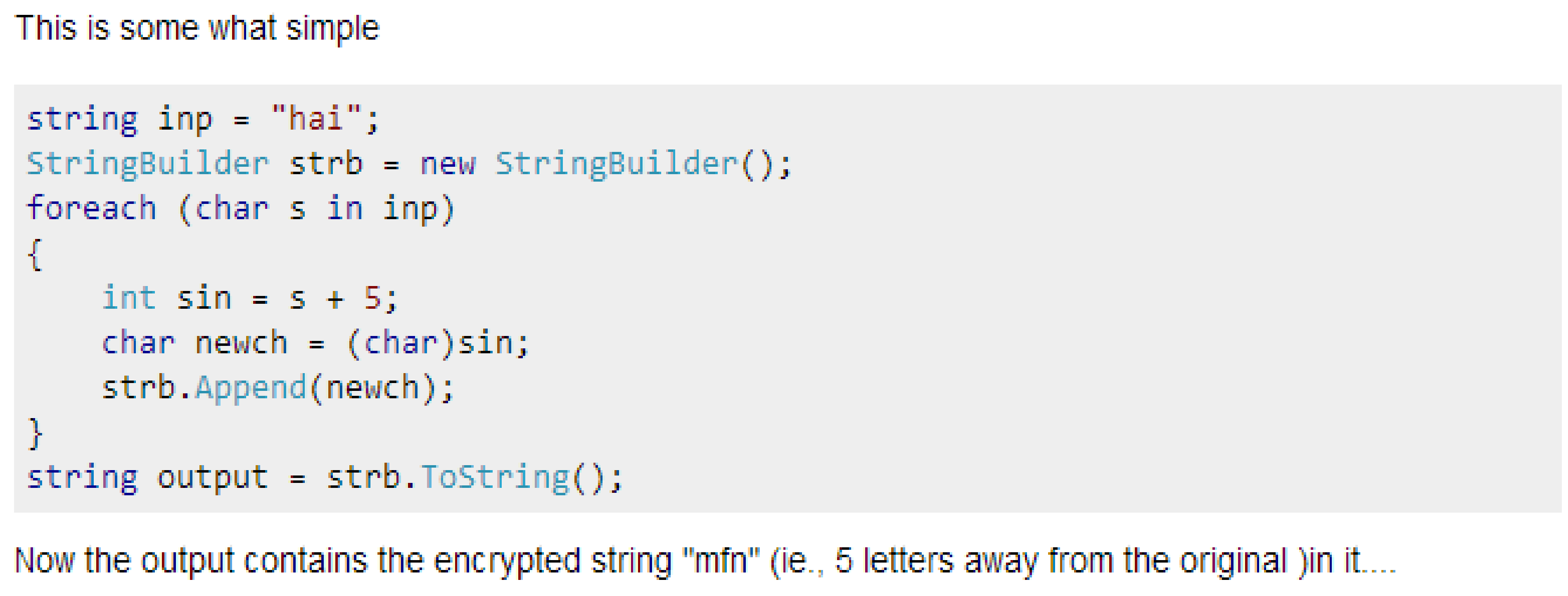
OWASP
Open Web Application
Security Project

Agile Security

# UNSERE SOFTWARE IST DOCH SICHER! SECURITY IST NICHT MEIN JOB!

OWASP
Open Web Application
Security Project

# Verschlüsselung „a la“ stackoverflow.com



This is some what simple

```
string inp = "hai";
StringBuilder strb = new StringBuilder();
foreach (char s in inp)
{
    int sin = s + 5;
    char newch = (char)sin;
    strb.Append(newch);
}
string output = strb.ToString();
```

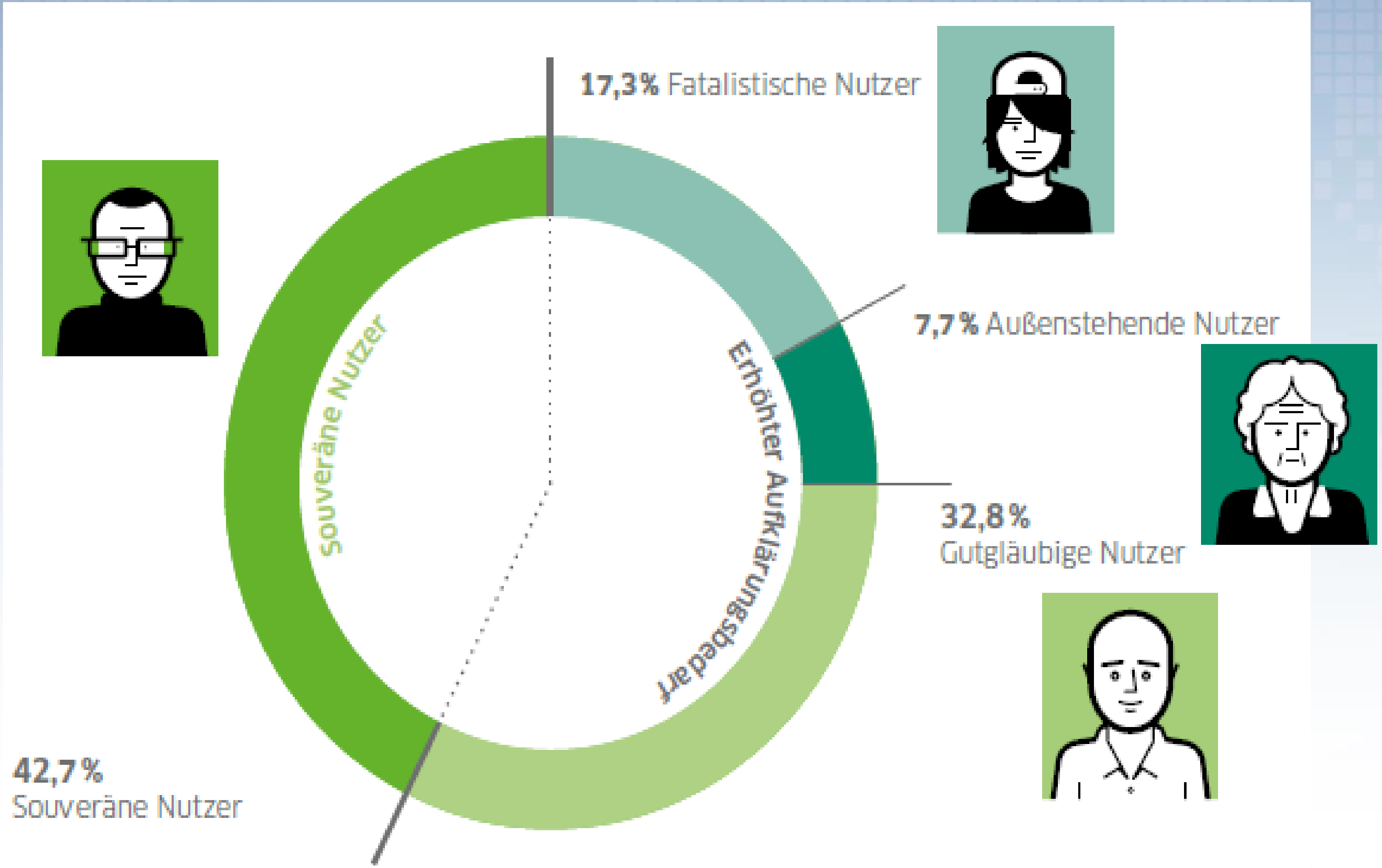
Now the output contains the encrypted string "mfn" (ie., 5 letters away from the original )in it....

Verschiebechiffre:

https://de.wikipedia.org/wiki/ROT13

OWASP
Open Web Application
Security Project

# Nutzerverhalten?



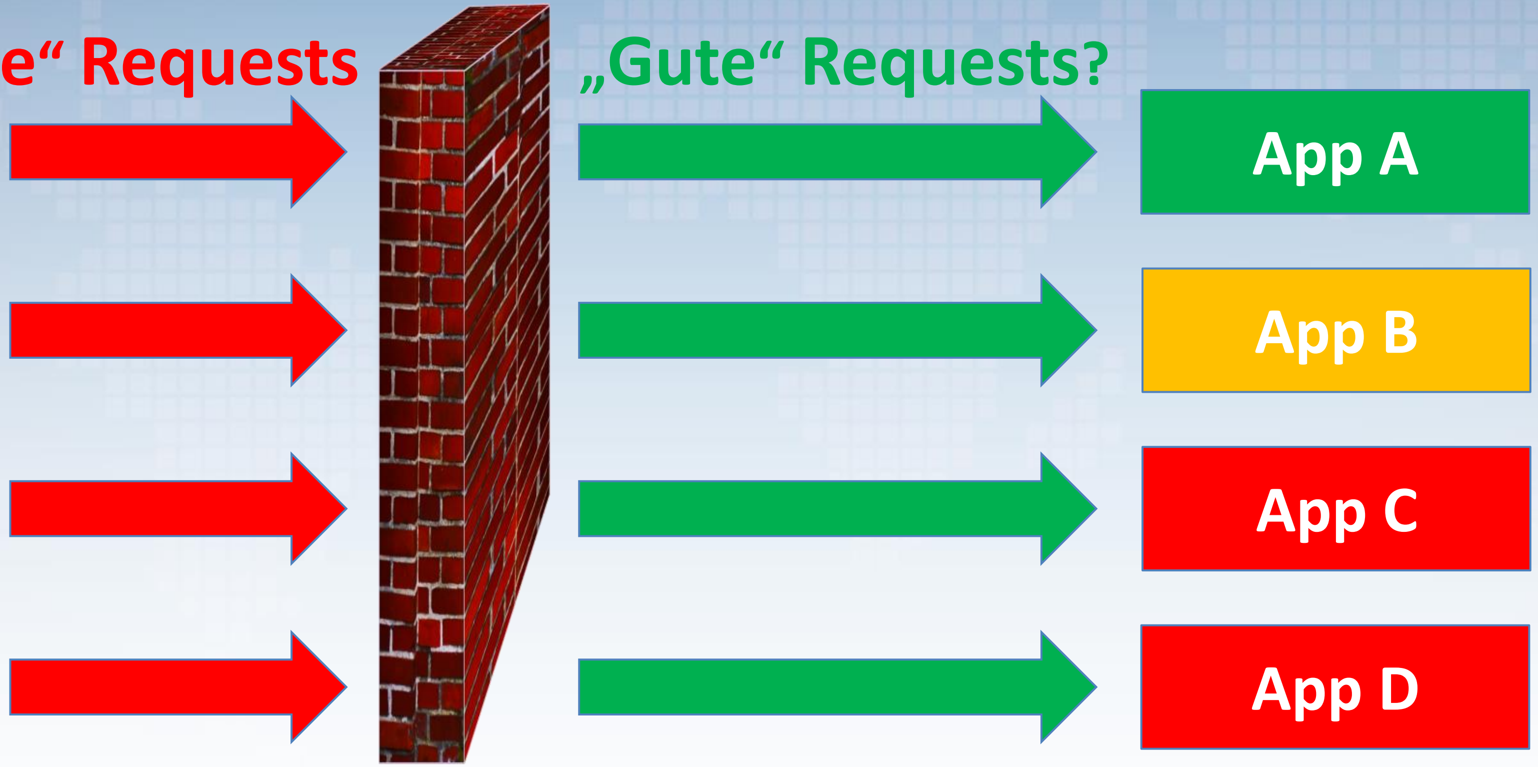
https://www.sicher-im-netz.de/downloads/dsin-sicherheitsindex-2015

OWASP
Open Web Application Security Project

# Wir haben doch eine „Security“-Firewall !?

„Böse“ Requests

„Gute“ Requests?



App A

App B

App C

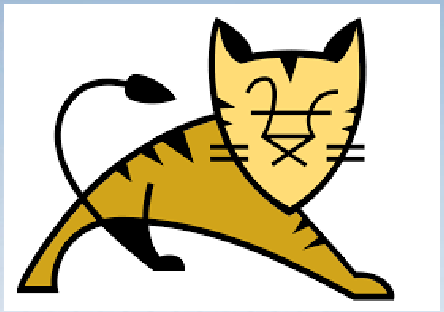
App D

„The Great Firewall“

Potentiell
unsichere Systeme

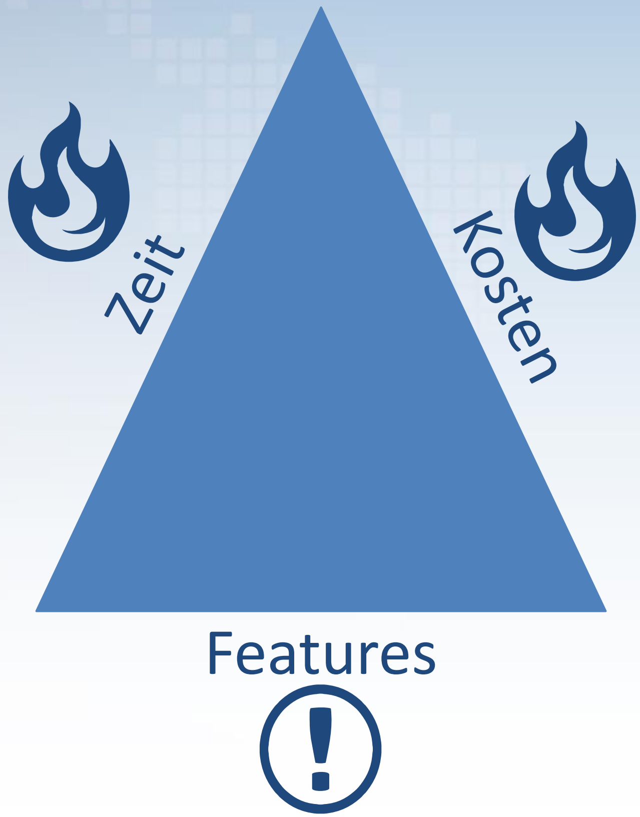
OWASP
Open Web Application
Security Project

# Wir setzen doch „sichere“ Frameworks und Plattformen ein!?



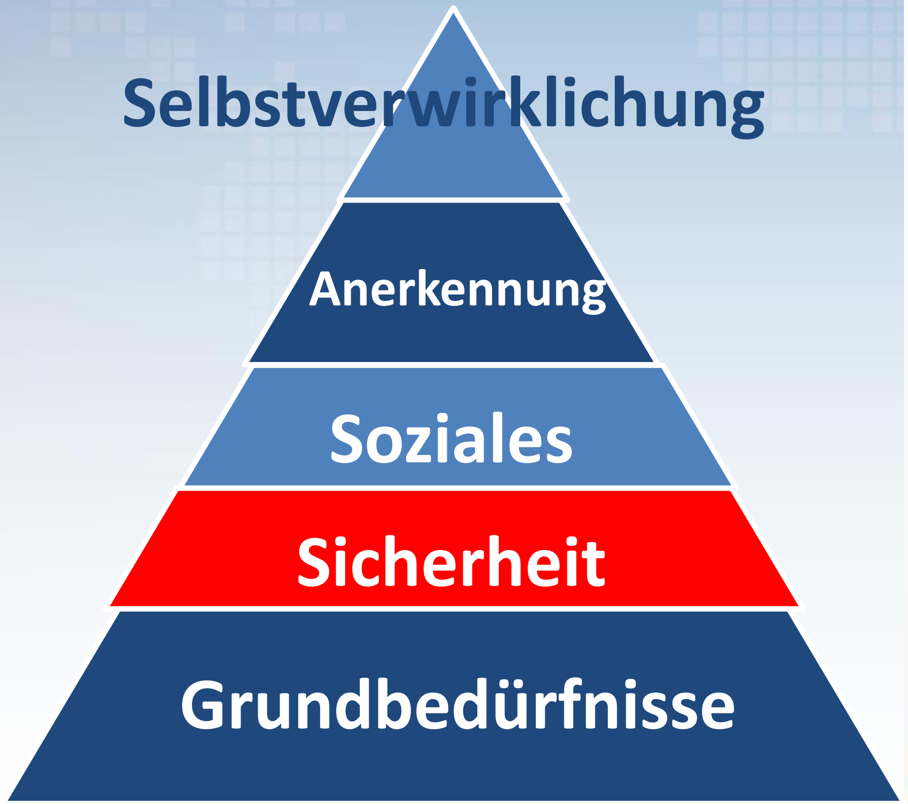
**und viele andere…**

# Dokumentation, Tests und Security fallen zuerst weg!



- ✗ ~~Dokumentation~~
- ✗ ~~Security / Tests~~
- ✓ Features!

# Qualität als Maslow‘sche Pyramide



Selbstverwirklichung

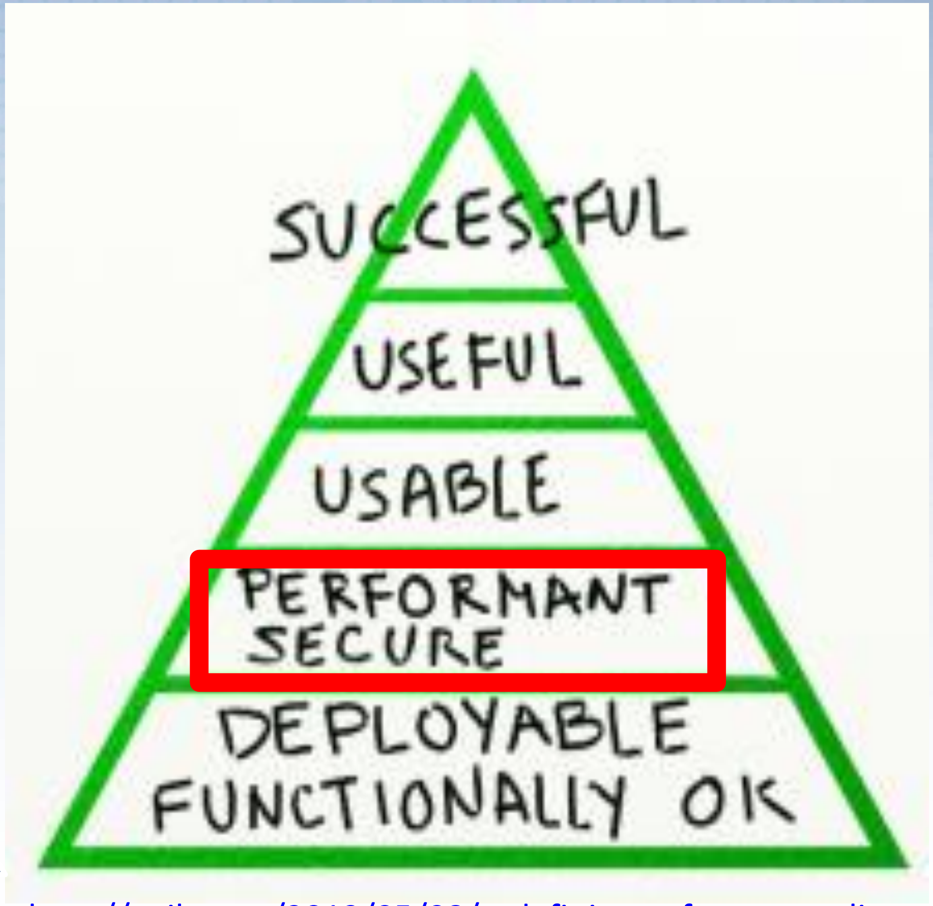
Anerkennung

Soziales

Sicherheit

Grundbedürfnisse

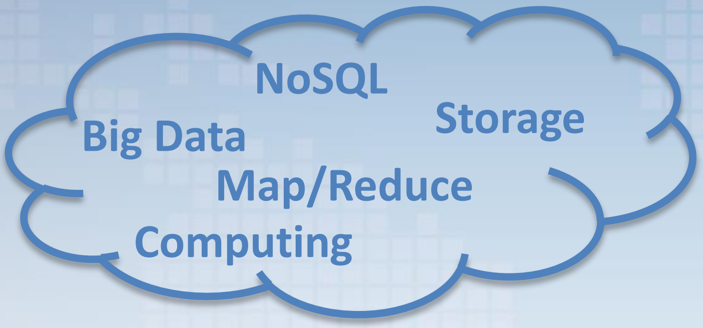
Maslow‘sche Pyramide



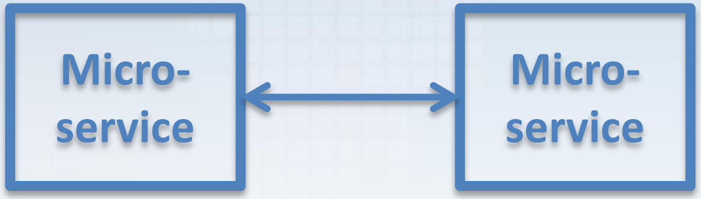
http://gojko.net/2012/05/08/redefining-software-quality

OWASP
Open Web Application
Security Project

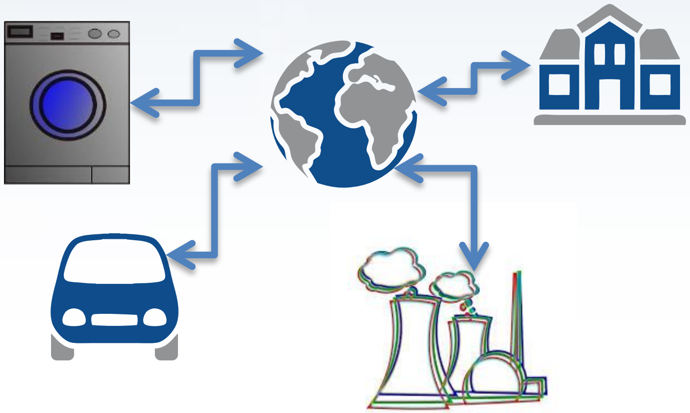
# Neue Herausforderungen für Security



Cloud Computing & Big Data



Microservices



Internet of Things (IoT)

OWASP
Open Web Application Security Project

Agile Security

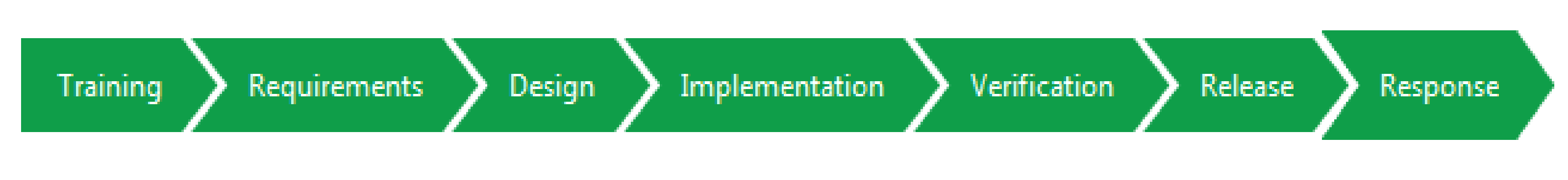
# „SICHERE“ AGILE ENTWICKLUNGSPROZESSE (SDLC)

OWASP
Open Web Application
Security Project

# Sichere Entwicklungsprozesse?

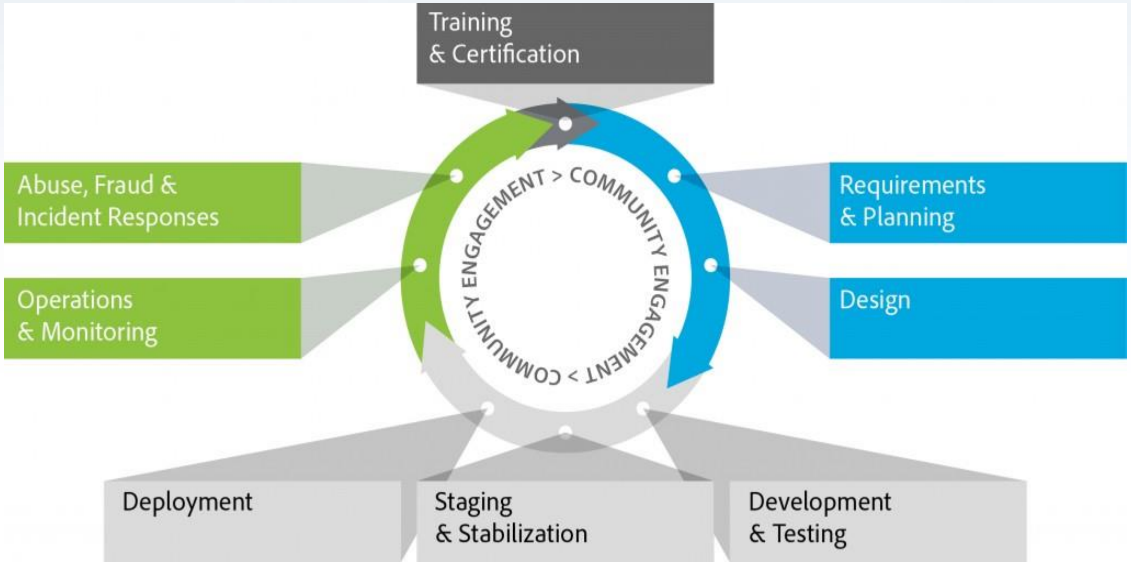
## Microsoft SDLC

https://www.microsoft.com/en-us/sdl



## Security @ Adobe

https://www.adobe.com/security/proactive-efforts.html



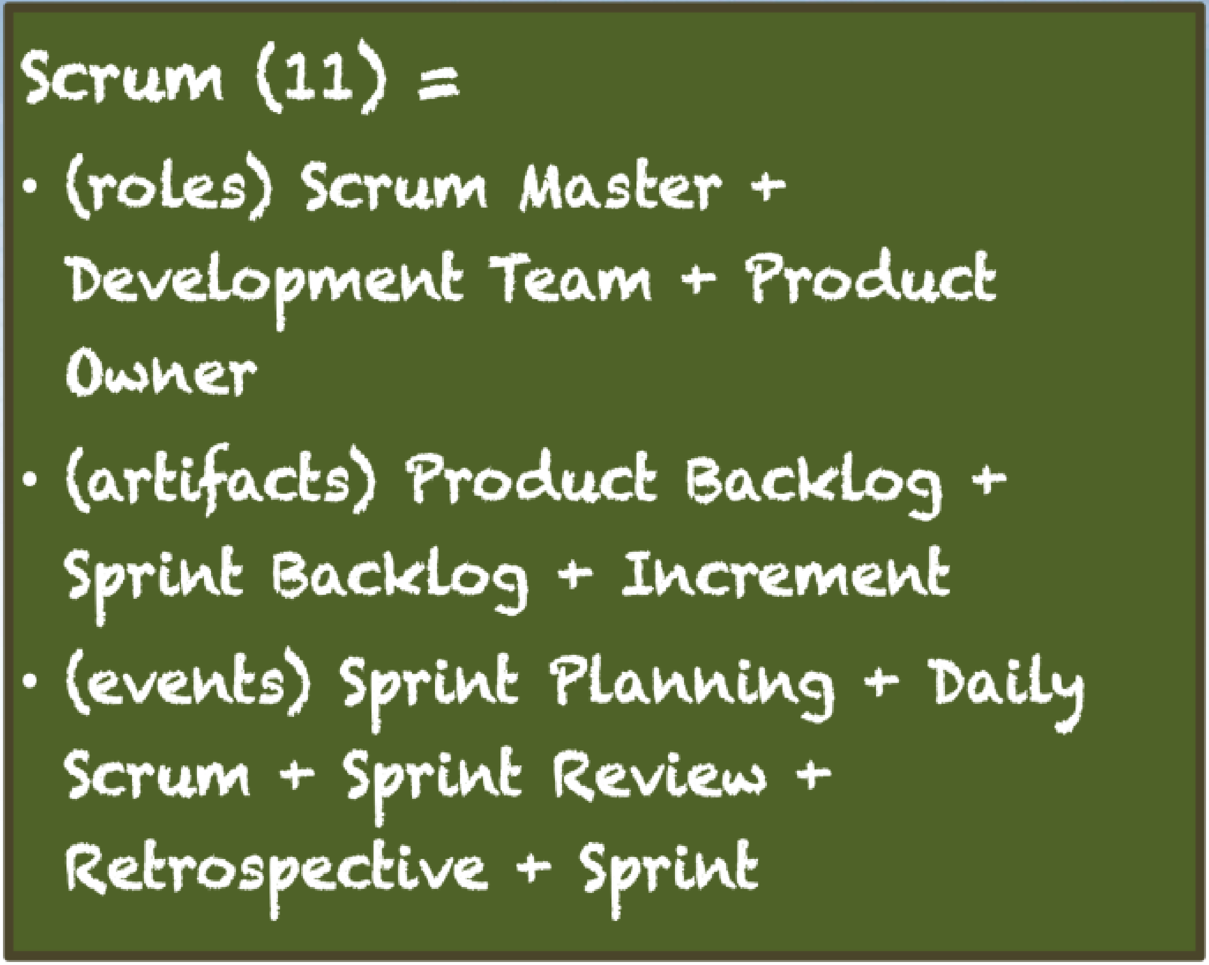
# Next Stop: **Sichere** Agile Entwicklung

# Sichere Agile Entwicklung

**+ Security?**

OWASP
Open Web Application
Security Project

# Sichere Agile Entwicklung – Scrum Framework Elemente

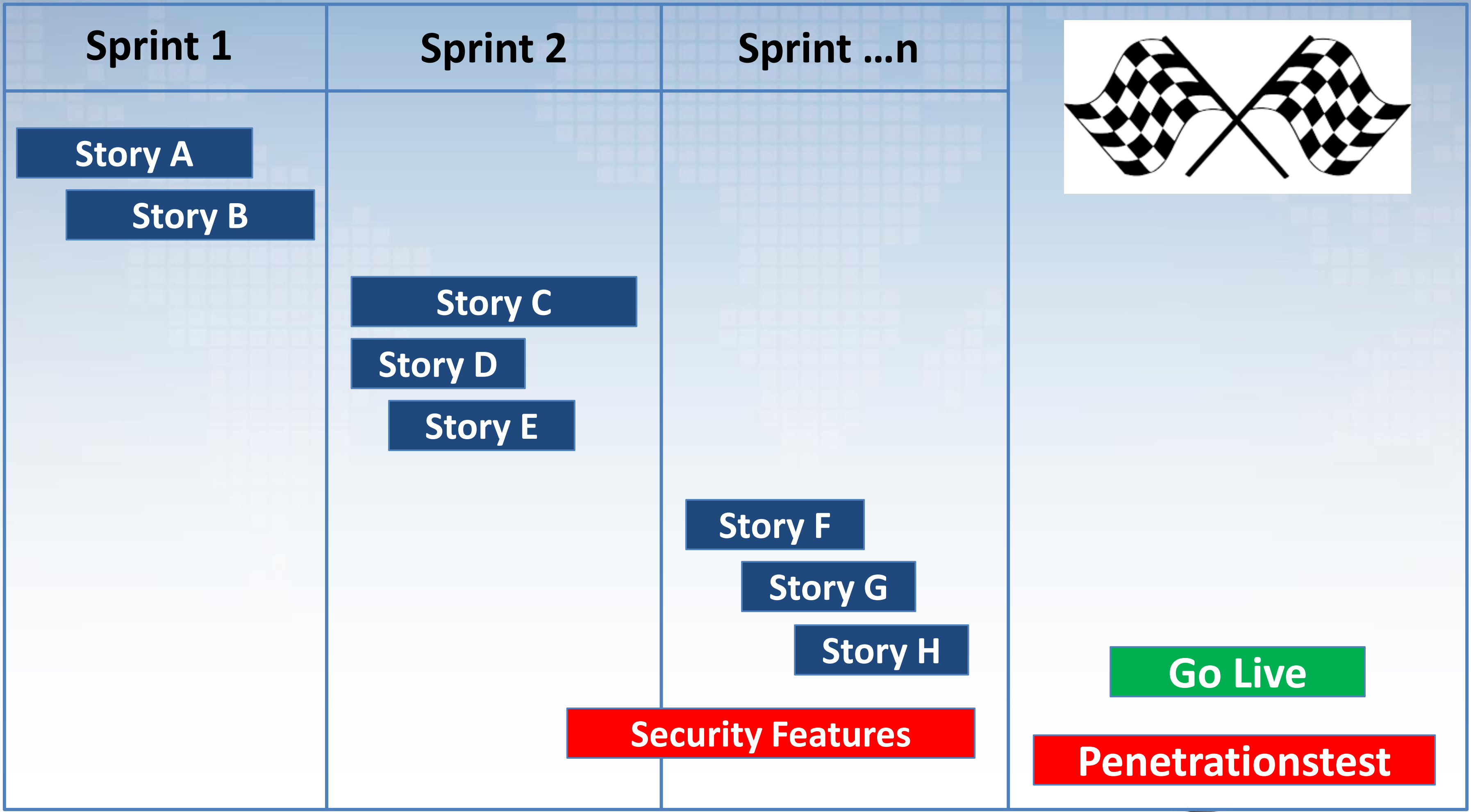


Scrum (11) =

- (roles) Scrum Master + Development Team + Product Owner
- (artifacts) Product Backlog + Sprint Backlog + Increment
- (events) Sprint Planning + Daily Scrum + Sprint Review + Retrospective + Sprint

http://guntherverheyen.com/2016/01/29/worrying-interpretations-of-scrum

# Ausgangslage: Sicherheit == Agil?



Sprint 1

Sprint 2

Sprint …n

Story A

Story B

Story C

Story D

Story E

Story F

Story G

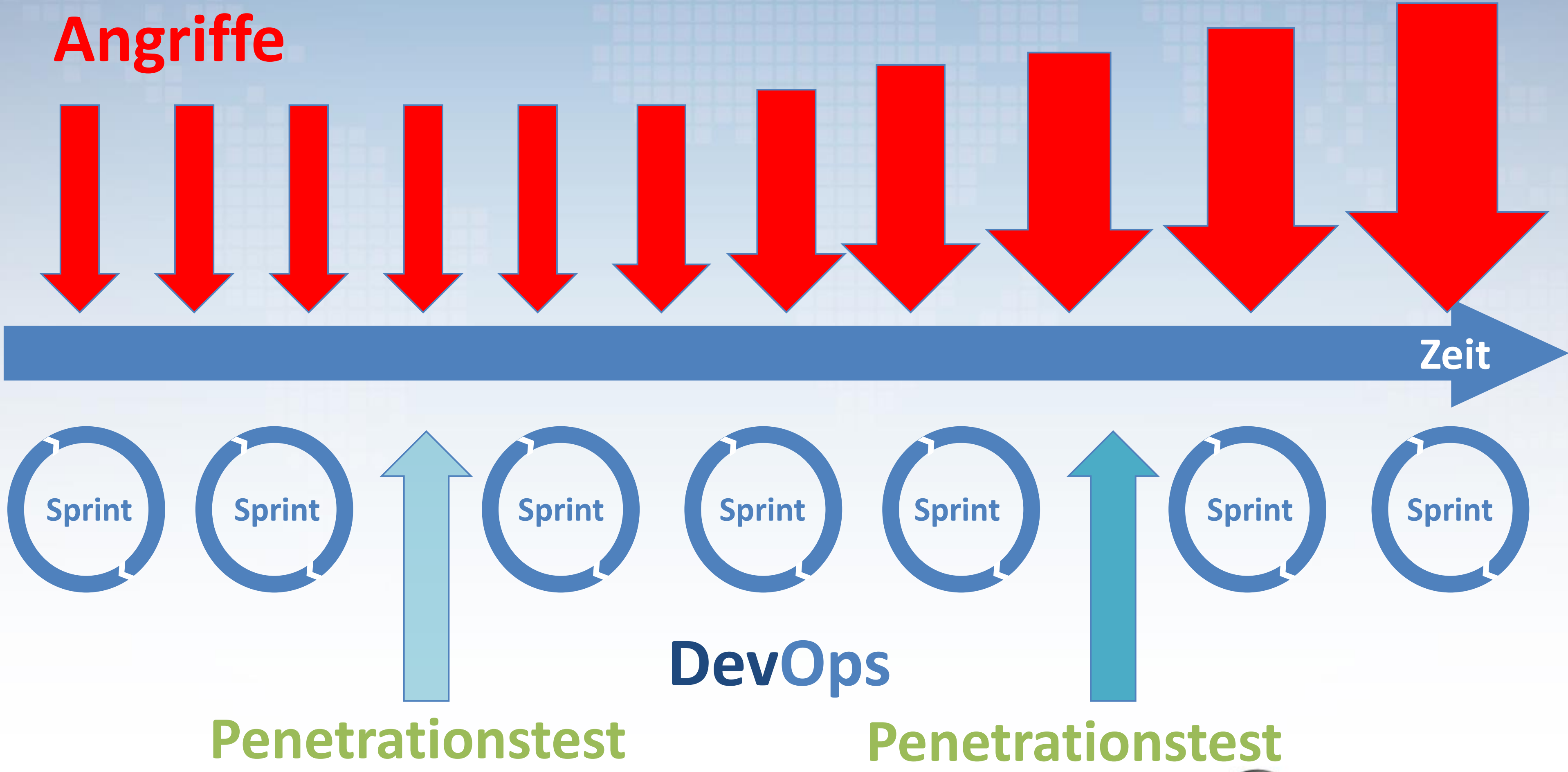
Story H

Security Features

Go Live

Penetrationstest

# Zeitplanung der Angreifer: 24h x 7d



Open Web Application Security Project

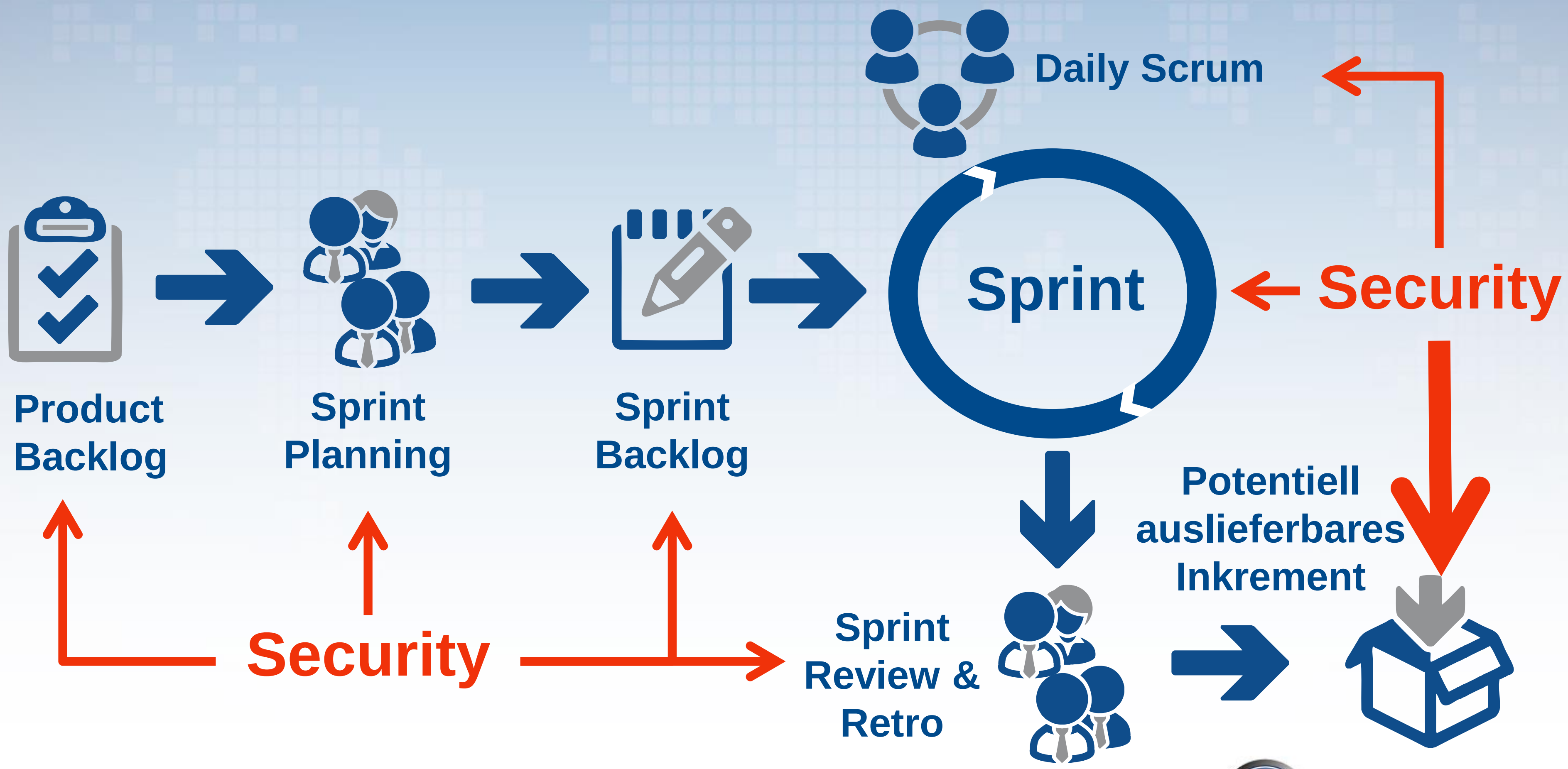
# Auslieferbare Inkremente in Scrum

“ Das Entwicklungsteam besteht aus Profis, die am Ende eines jeden Sprints ein fertiges Inkrement übergeben, welches **potentiell auslieferbar** ist. “

http://www.scrumguides.org

⇒ Potentiell **unsicher** ausliefern?

# Sichere
# Agile Entwicklung mit Scrum



Daily Scrum

Product Backlog

Sprint Planning

Sprint Backlog

Sprint

Security

Potentiell auslieferbares Inkrement

Security

Sprint Review & Retro

OWASP
Open Web Application Security Project

# Security Modelle, Vorschriften und Richtlinien

BSIMM

MS SDL

Cobit

ASVS

SAMM

TOGAF

PCI DSS

SABSA

ITIL

BSI Grundschutz

CLASP

SAFECode

BDSG

**Sichere**

**Agile**
**Entwicklung**

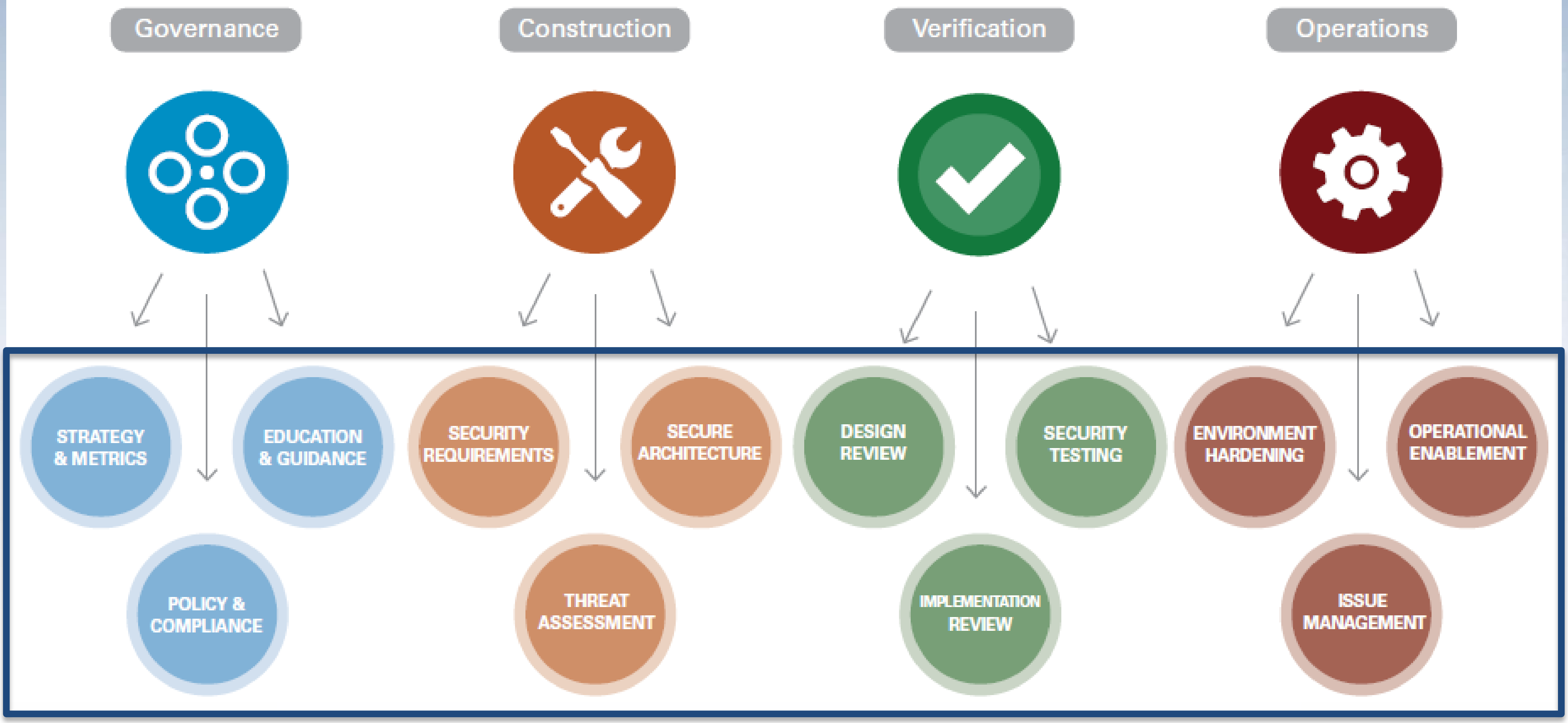
OWASP
Open Web Application
Security Project

# OWASP OpenSAMM

Software Assurance Maturity Model

A guide to building security into software development

Version 1.1



https://www.owasp.org/index.php/Category:Software_Assurance_Maturity_Model

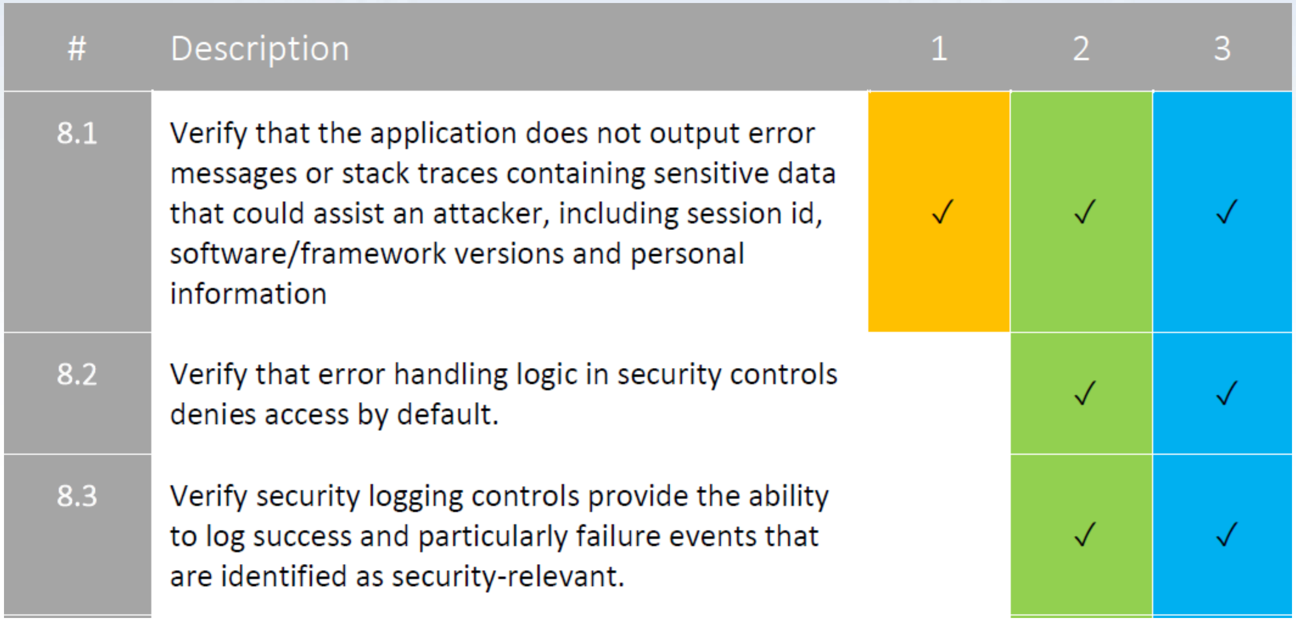
OWASP Open Web Application Security Project

# OWASP Application Security Verification Standard (ASVS)

Framework für Sicherheitsanforderungen und -verifikation

Design, Entwicklung und Test

"…reduce the risk from waterfall methodology penetration testing at the end…"



| # | Description | 1 | 2 | 3 |
|---|---|---|---|---|
| 8.1 | Verify that the application does not output error messages or stack traces containing sensitive data that could assist an attacker, including session id, software/framework versions and personal information | ✓ | ✓ | ✓ |
| 8.2 | Verify that error handling logic in security controls denies access by default. |  | ✓ | ✓ |
| 8.3 | Verify security logging controls provide the ability to log success and particularly failure events that are identified as security-relevant. |  | ✓ | ✓ |

OWASP
Open Web Application
Security Project

https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

# Rollenspezifische Security Trainings

**Product Owner**

- Sicherheits- und Datenschutz-Risiken
- Threat Modeling
- Spezifikation von Security Features
- **Ab**User Stories („Evil“ Stories)

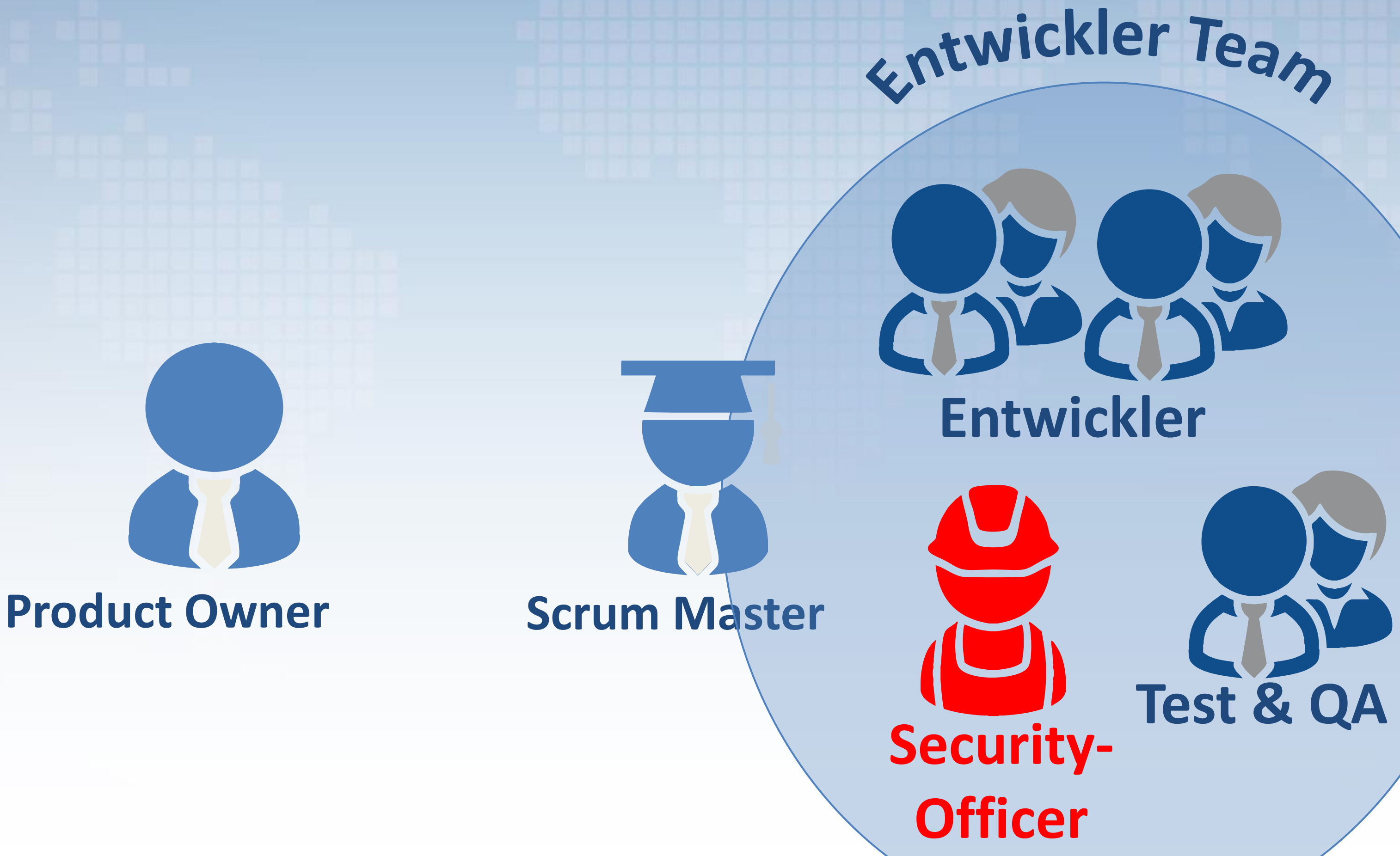
**Security-Officer**

**Development Team**

- Threat Modeling
- Secure Design und Coding
- Security Code Reviews
- Security Testing

OWASP
Open Web Application
Security Project

# Sichere Agile Entwicklung mit Scrum



Entwickler Team

Entwickler

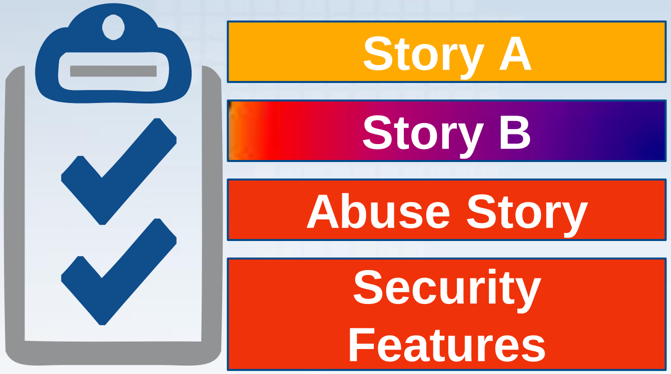
Product Owner

Scrum Master

Security-Officer

Test & QA

# Sichere Agile Entwicklung mit Scrum



**Product Backlog**

Threat Modell pflegen

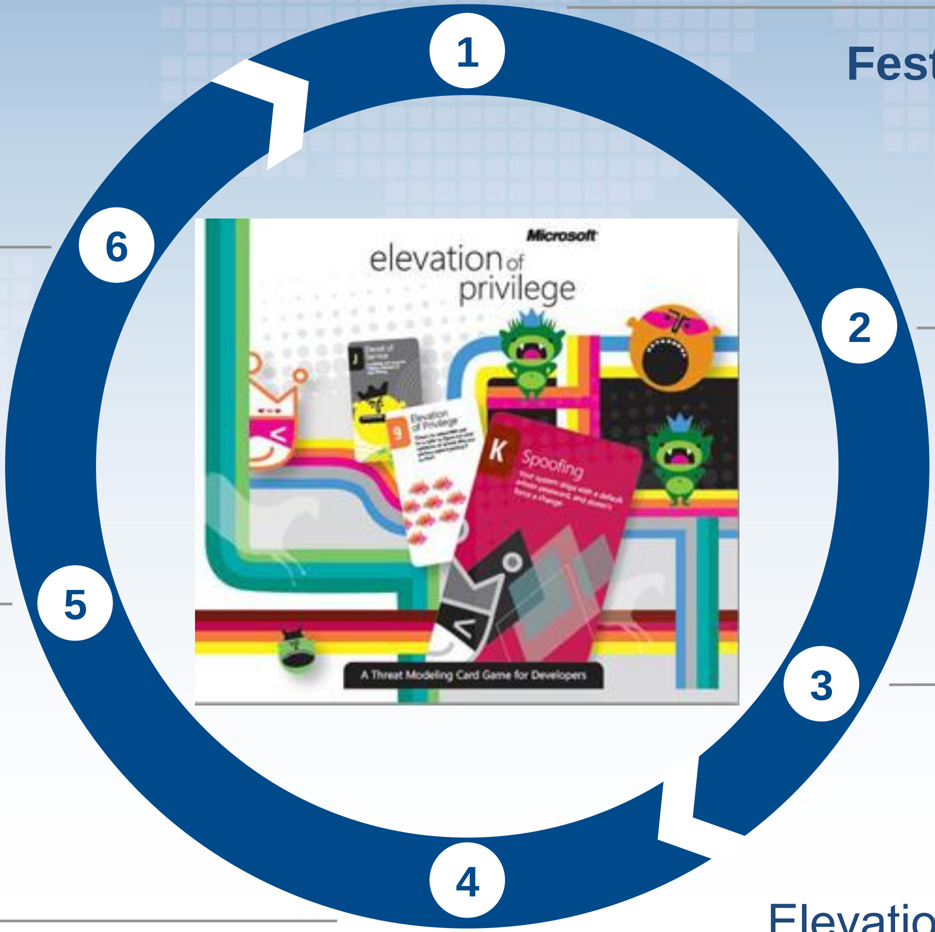
AbUser Stories erstellen

Security-Features mit hoher Prio

Akzeptanzkriterien für Security

Secure „Definition of Ready“

# Threat Modeling ist auch „Agil“



**Festlegung Software-Architektur**

User Stories, UML Diagramme

**Threat Model**

Als Diskussions-Basis

**Identifikation und Vermeidung**

**von Bedrohungen**

„Elevation of privilege“ Spiel

**Security Testfälle und AbUser Stories**

Absicherung gegen Bedrohungen

**Test Driven Development (TDD)**

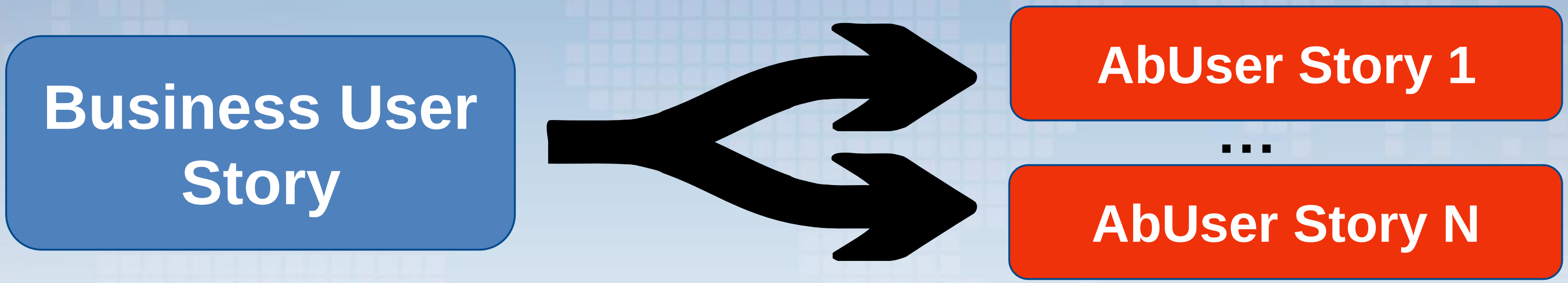
Zuerst die Security Tests

**Produktiv Code erstellen**

Security-Tests → **Grün**!

OWASP
Open Web Application Security Project

# AbUser Stories



Business User Story

AbUser Story 1

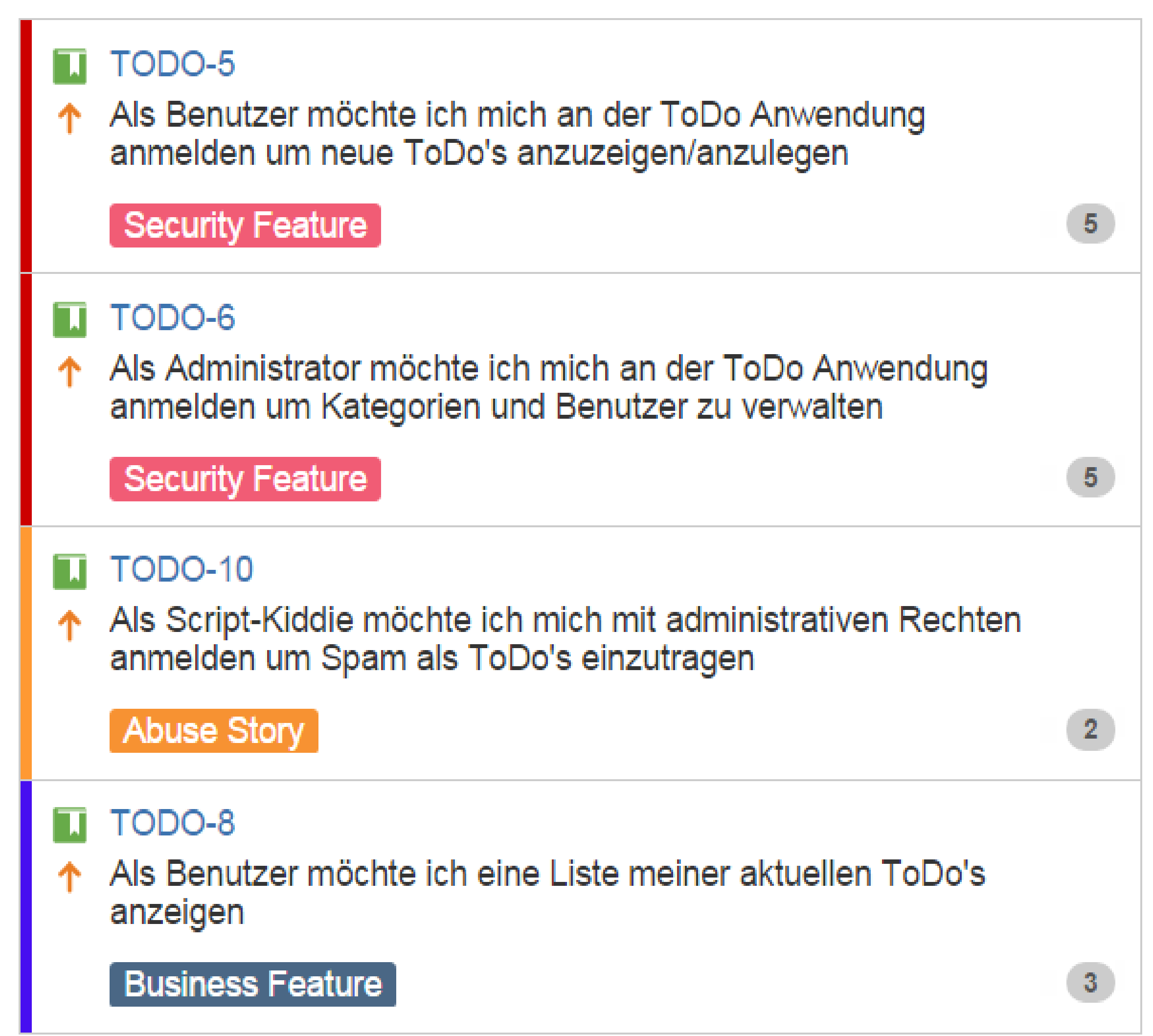
...

AbUser Story N

Als Kunde möchte ich Produkte auswählen und zum Warenkorb hinzufügen um diese zu kaufen.

Als Angreifer möchte ich Anfragen so manipulieren um Preise der Produkte im Warenkorb zu ändern.

# Beispiel: **AbUser** und **Security** User Stories



TODO-5

Als Benutzer möchte ich mich an der ToDo Anwendung anmelden um neue ToDo's anzuzeigen/anzulegen

Security Feature 5

TODO-6

Als Administrator möchte ich mich an der ToDo Anwendung anmelden um Kategorien und Benutzer zu verwalten

Security Feature 5

TODO-10

Als Script-Kiddie möchte ich mich mit administrativen Rechten anmelden um Spam als ToDo's einzutragen

Abuse Story 2

TODO-8

Als Benutzer möchte ich eine Liste meiner aktuellen ToDo's anzeigen

Business Feature 3

OWASP
Open Web Application Security Project

# Sichere Agile Entwicklung mit Scrum

**Sprint Planning**

Detaillierung Threat Modell

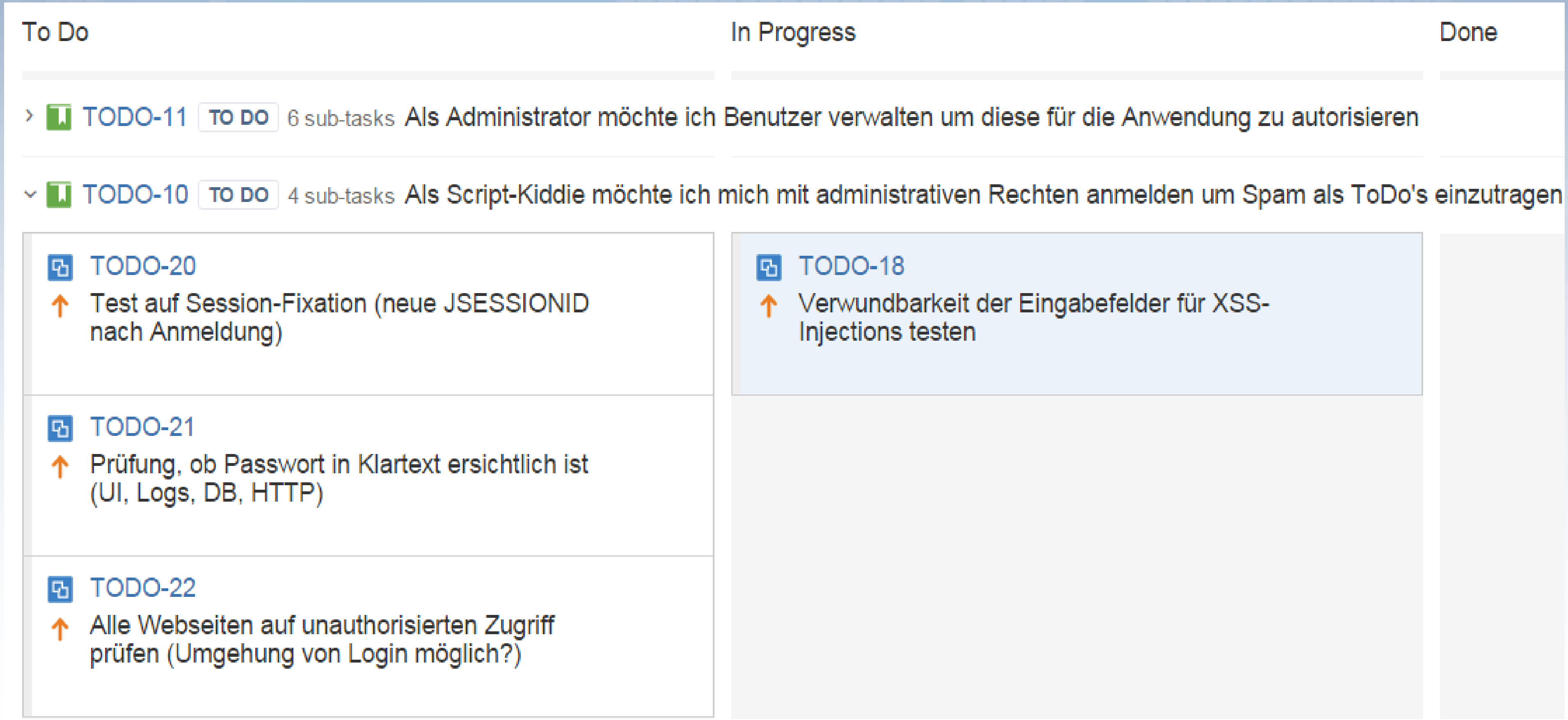
**Ab**User Story Tasks

Security-Feature Tasks

Security Akzeptanzkriterien

Security-Testfälle

# Beispiel: Tasks für **Ab**User Stories



To Do | In Progress | Done

› TODO-11 TO DO 6 sub-tasks Als Administrator möchte ich Benutzer verwalten um diese für die Anwendung zu autorisieren

⌄ TODO-10 TO DO 4 sub-tasks Als Script-Kiddie möchte ich mich mit administrativen Rechten anmelden um Spam als ToDo's einzutragen

| To Do | In Progress | Done |
|---|---|---|
| TODO-20<br>↑ Test auf Session-Fixation (neue JSESSIONID nach Anmeldung) | TODO-18<br>↑ Verwundbarkeit der Eingabefelder für XSS-Injections testen | |
| TODO-21<br>↑ Prüfung, ob Passwort in Klartext ersichtlich ist (UI, Logs, DB, HTTP) | | |
| TODO-22<br>↑ Alle Webseiten auf unauthorisierten Zugriff prüfen (Umgehung von Login möglich?) | | |

OWASP
Open Web Application
Security Project

# Sichere Agile Entwicklung mit Scrum

**Daily Scrum**

Neue Security-Risiken diskutieren

Security Tasks ggf. neu planen

**Sprint**

Secure Design / Coding

Pairing mit Security-Officer

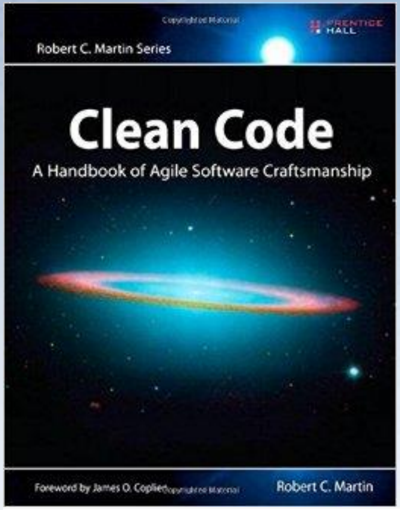
„Security-Aware“ Definition of Done

Security Regressions-Testing (CI)

Security Code Reviews

OWASP
Open Web Application
Security Project

# Secure Design / Coding – Security Patterns


Robert C. Martin Series
PRENTICE HALL
Clean Code
A Handbook of Agile Software Craftsmanship
Foreword by James O. Coplien
Robert C. Martin

OWASP ProActive CONTROLS

OWASP Cheat Sheets

Clean Code

Input Validierung

Output Escaping

Prepared SQL Statements

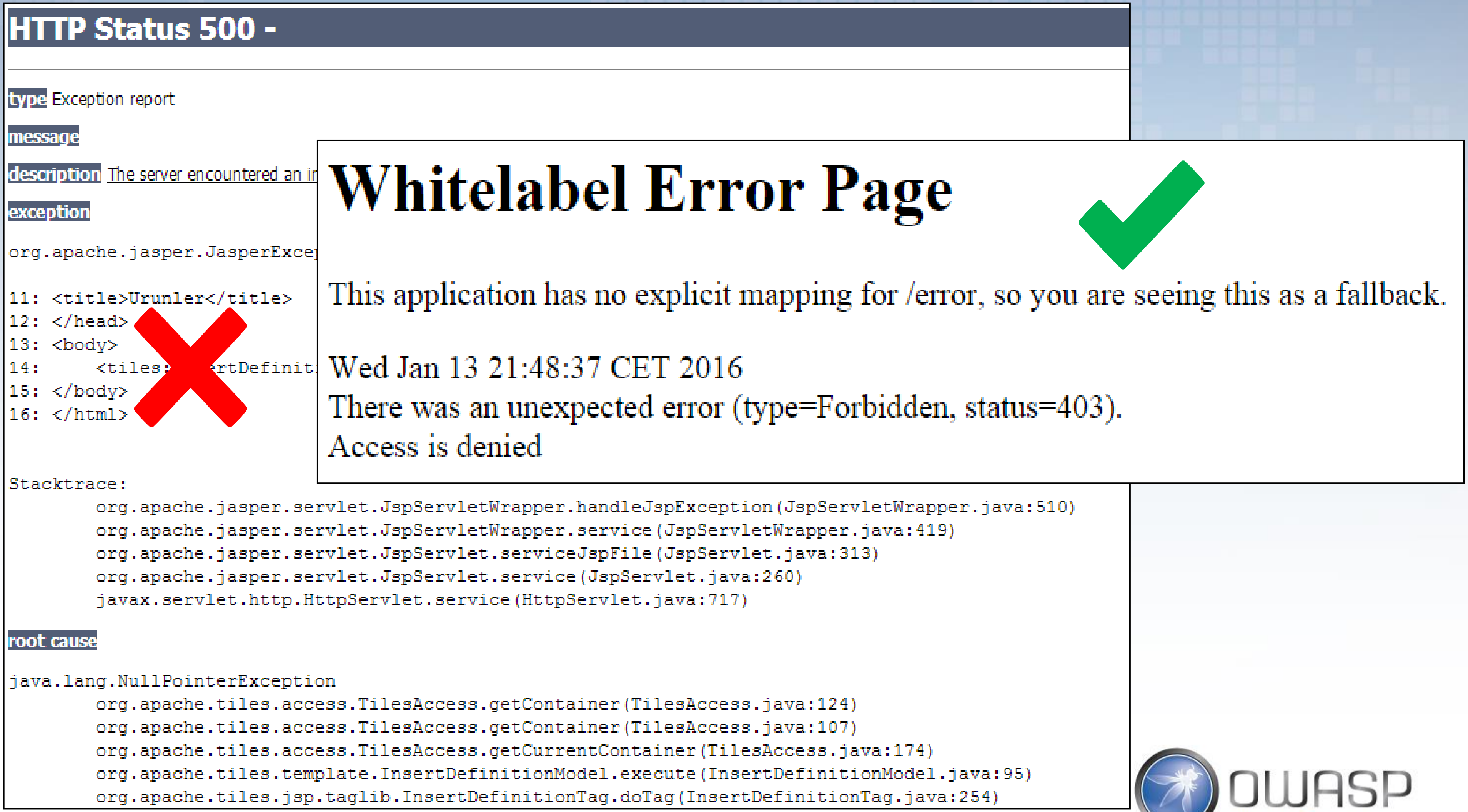
Keine Fehlerdetails in UI

Session Management

Access Controls

OWASP Open Web Application Security Project

# Secure Design / Coding – Sichere Fehlermeldungen



## HTTP Status 500 -

**type** Exception report

**message**

**description** The server encountered an i

**exception**

```
org.apache.jasper.JasperExce

11: <title>Urunler</title>
12: </head>
13: <body>
14:     <tiles:      rtDefinit
15: </body>
16: </html>


Stacktrace:
        org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:510)
        org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:419)
        org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:313)
        org.apache.jasper.servlet.JspServlet.service(JspServlet.java:260)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
```

**root cause**

```
java.lang.NullPointerException
        org.apache.tiles.access.TilesAccess.getContainer(TilesAccess.java:124)
        org.apache.tiles.access.TilesAccess.getContainer(TilesAccess.java:107)
        org.apache.tiles.access.TilesAccess.getCurrentContainer(TilesAccess.java:174)
        org.apache.tiles.template.InsertDefinitionModel.execute(InsertDefinitionModel.java:95)
        org.apache.tiles.jsp.taglib.InsertDefinitionTag.doTag(InsertDefinitionTag.java:254)
```

## Whitelabel Error Page

This application has no explicit mapping for /error, so you are seeing this as a fallback.

Wed Jan 13 21:48:37 CET 2016
There was an unexpected error (type=Forbidden, status=403).
Access is denied

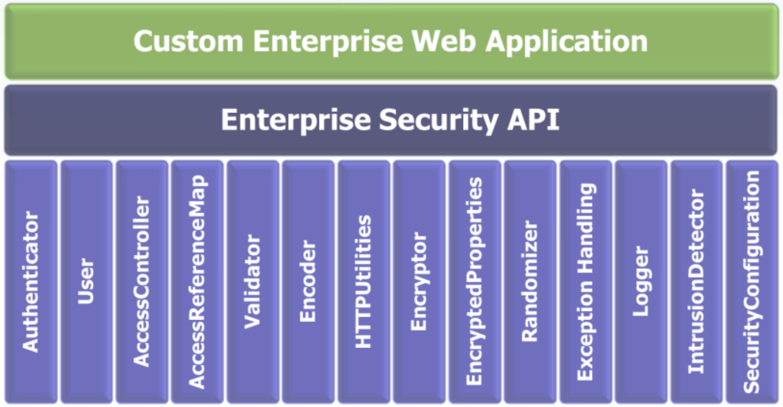
OWASP
Open Web Application Security Project

# Secure Design / Coding – Standard Frameworks

jasypt. JAVA SIMPLIFIED ENCRYPTION

spring

APACHE SHIRO



**Standard Kryptographie**

→ Keyczar, Bouncy Castle, Jasypt

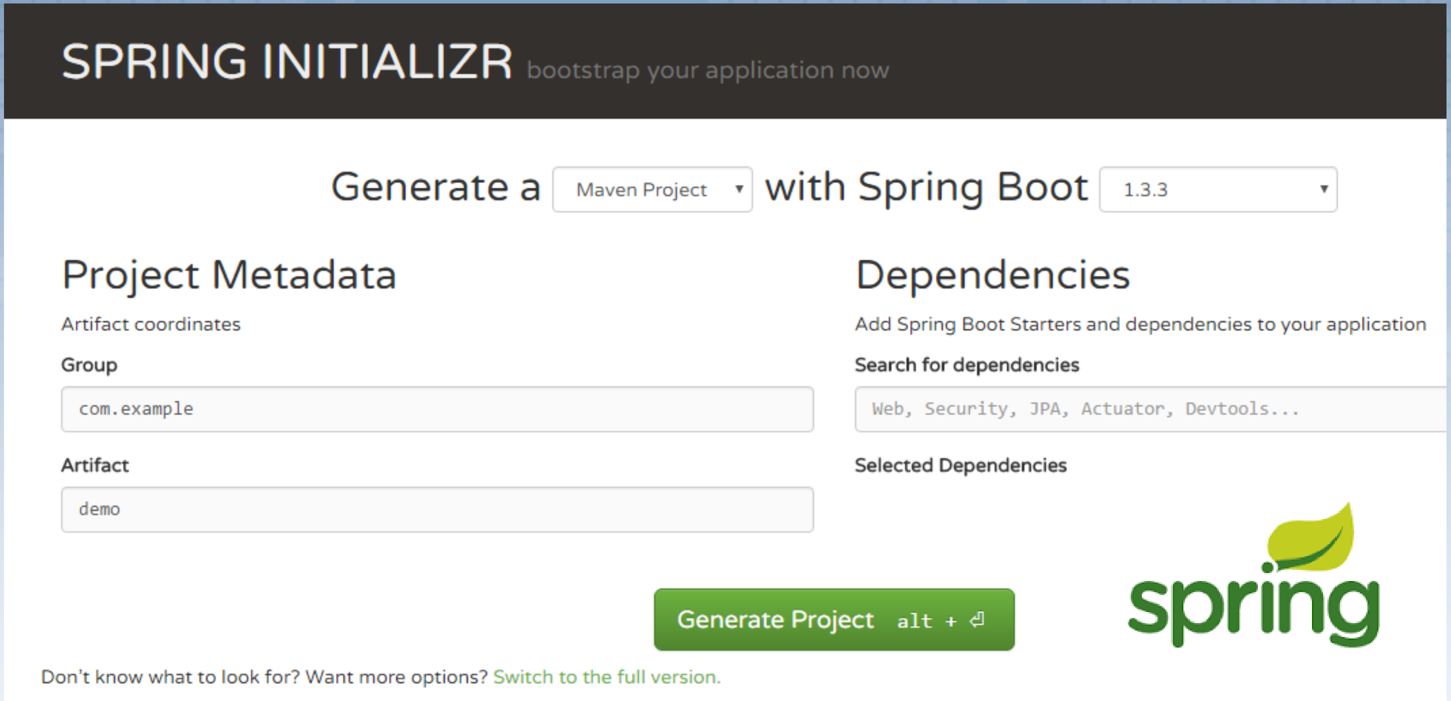
**Frameworks mit Validierung / Escaping**

→ JavaServer Faces
→ Spring MVC + Thymeleaf
→ Vaadin (GWT)

**Robuste Security Frameworks**

→ Java EE Security
→ Spring Security
→ Apache Shiro
→ OWASP ESAPI

OWASP Open Web Application Security Project



SPRING INITIALIZR bootstrap your application now

Generate a Maven Project with Spring Boot 1.3.3

Project Metadata

Artifact coordinates

Group: com.example

Artifact: demo

Dependencies

Add Spring Boot Starters and dependencies to your application

Search for dependencies: Web, Security, JPA, Actuator, Devtools...

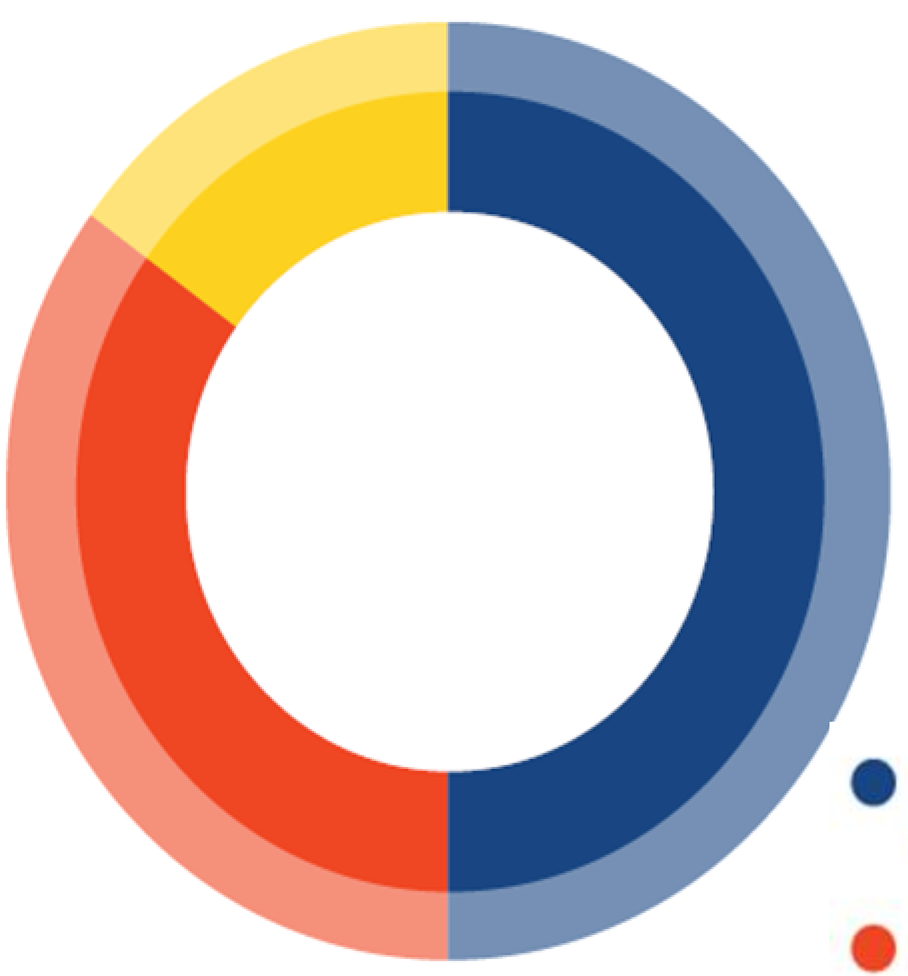
Selected Dependencies

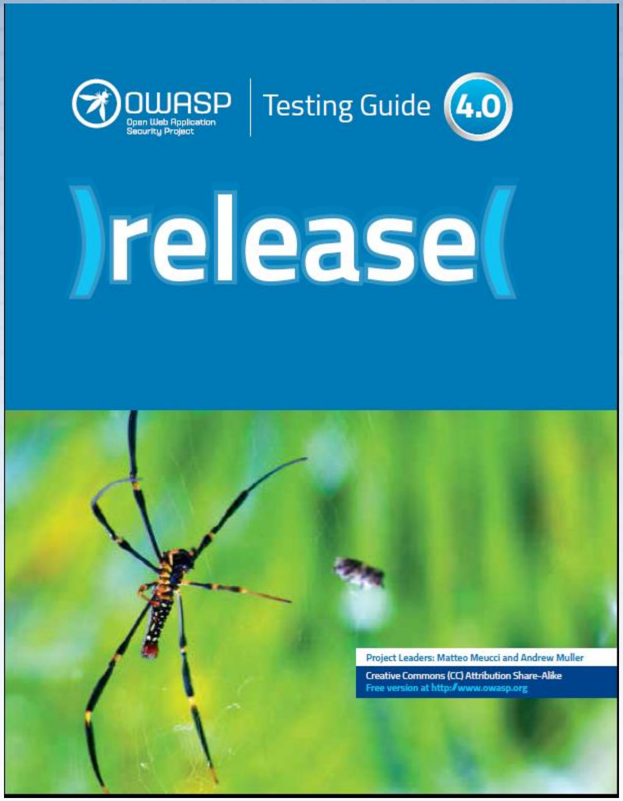
Don't know what to look for? Want more options? Switch to the full version.

https://start.spring.io

# DEMO: EINE SICHERE WEBANWENDUNG IN 5 MINUTEN

# Agile **Security** Testing





OWASP Open Web Application Security Project | Testing Guide 4.0

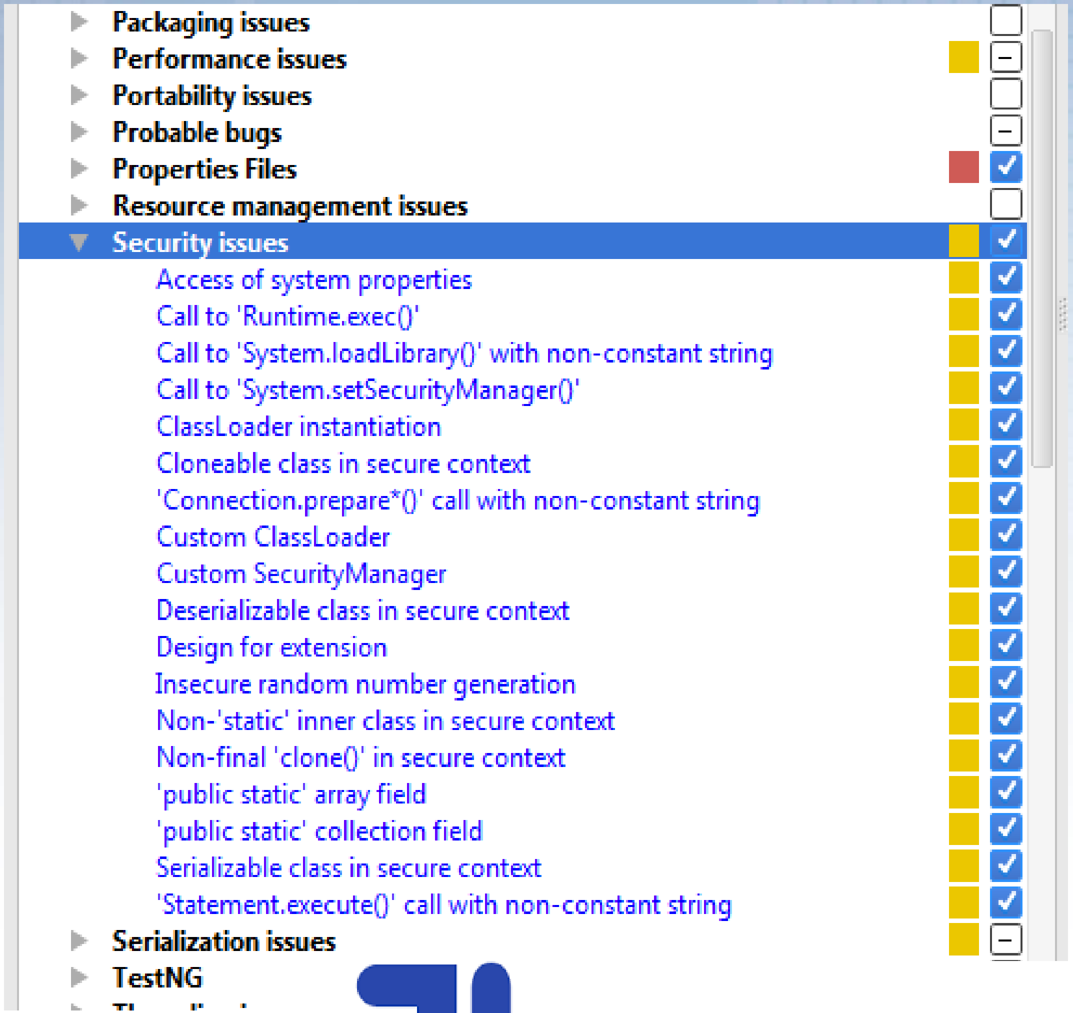
)release(

Project Leaders: Matteo Meucci and Andrew Muller

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

OWASP
Open Web Application
Security Project

# Agile **Security** Testing – Statische Code Analyse



- ▶ Packaging issues □
- ▶ Performance issues 🟨 ⊟
- ▶ Portability issues □
- ▶ Probable bugs ⊟
- ▶ Properties Files 🟥 ☑
- ▶ Resource management issues □
- ▼ Security issues 🟨 ☑
  - Access of system properties 🟨 ☑
  - Call to 'Runtime.exec()' 🟨 ☑
  - Call to 'System.loadLibrary()' with non-constant string 🟨 ☑
  - Call to 'System.setSecurityManager()' 🟨 ☑
  - ClassLoader instantiation 🟨 ☑
  - Cloneable class in secure context 🟨 ☑
  - 'Connection.prepare*()' call with non-constant string 🟨 ☑
  - Custom ClassLoader 🟨 ☑
  - Custom SecurityManager 🟨 ☑
  - Deserializable class in secure context 🟨 ☑
  - Design for extension 🟨 ☑
  - Insecure random number generation 🟨 ☑
  - Non-'static' inner class in secure context 🟨 ☑
  - Non-final 'clone()' in secure context 🟨 ☑
  - 'public static' array field 🟨 ☑
  - 'public static' collection field 🟨 ☑
  - Serializable class in secure context 🟨 ☑
  - 'Statement.execute()' call with non-constant string 🟨 ☑
- ▶ Serialization issues 🟨 ⊟
- ▶ TestNG

FindBugs™ because it's easy

+

Find Security Bugs

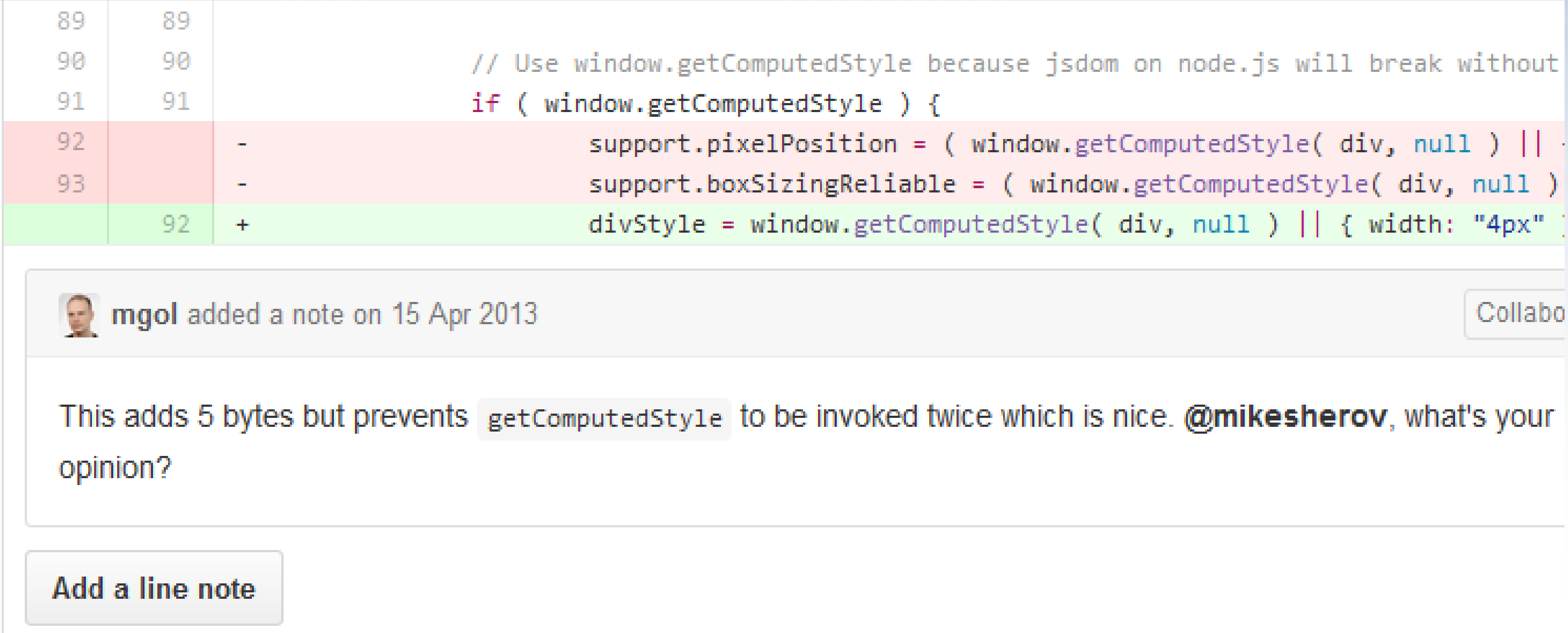
The FindBugs plugin for security audits of Java web applications.

IntelliJ IDEA

OWASP Open Web Application Security Project

# Agile **Security** Testing – Code Review

## Code-Reviews (GitHub, GitLab, Gerrit, BitBucket, …)



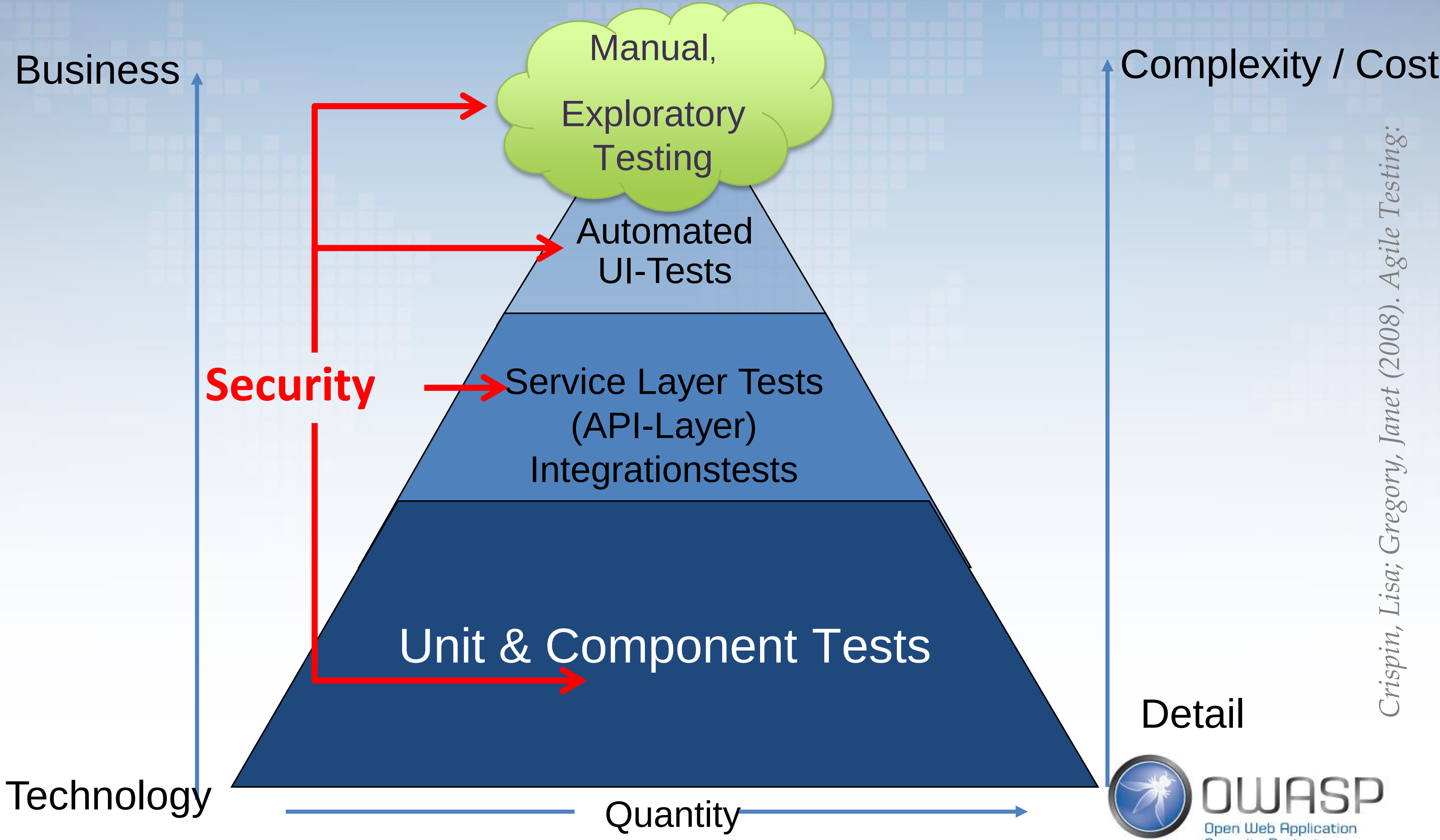
```
        // Use window.getComputedStyle because jsdom on node.js will break without
        if ( window.getComputedStyle ) {
-               support.pixelPosition = ( window.getComputedStyle( div, null ) ||
-               support.boxSizingReliable = ( window.getComputedStyle( div, null )
+               divStyle = window.getComputedStyle( div, null ) || { width: "4px"
```

**mgol** added a note on 15 Apr 2013

This adds 5 bytes but prevents `getComputedStyle` to be invoked twice which is nice. **@mikesherov**, what's your opinion?

OWASP
Open Web Application
Security Project

# Agile **Security** Testing - Test-Pyramide



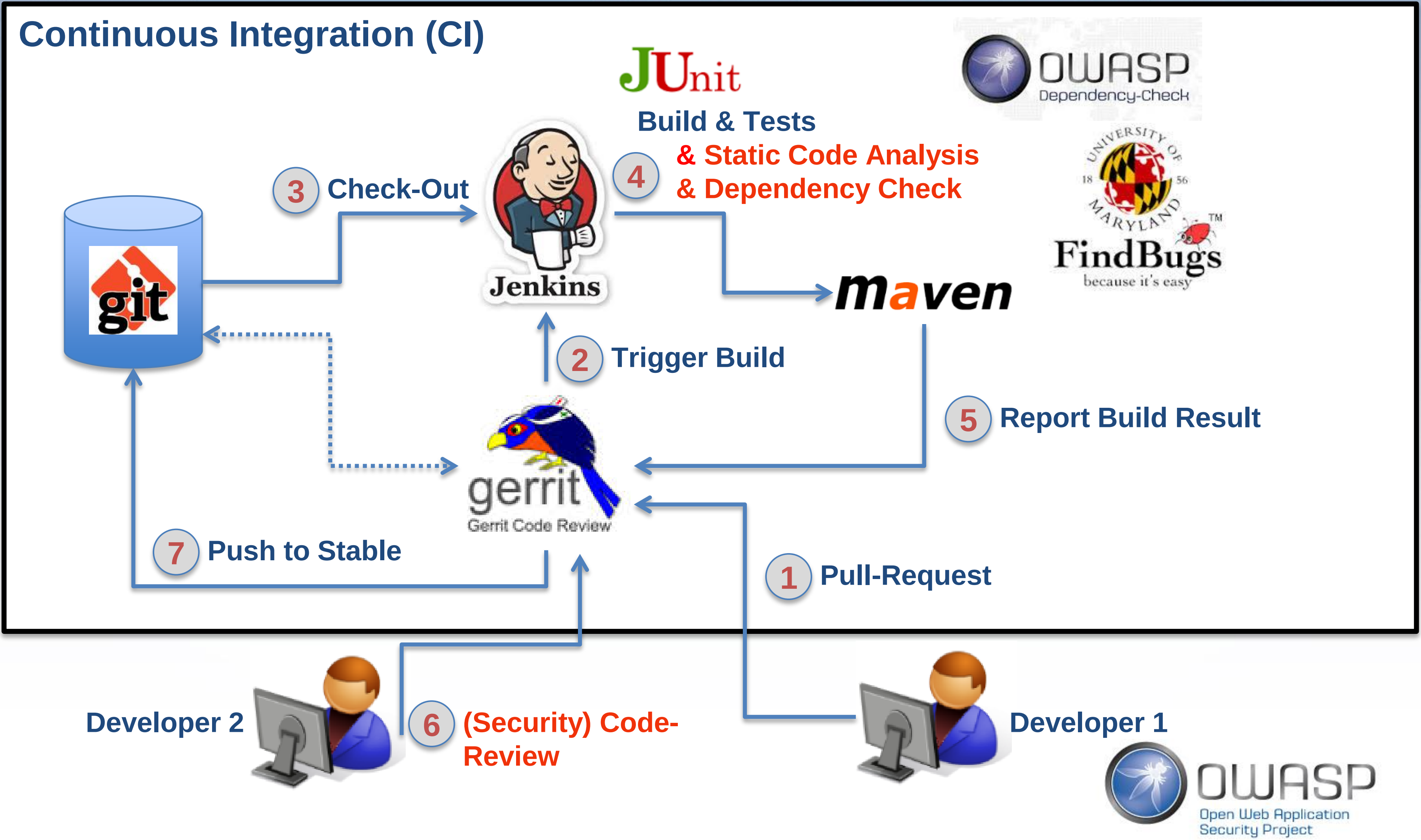
*Crispin, Lisa; Gregory, Janet (2008). Agile Testing:*

# Agile **Security** Testing – Security-Integrationstests

```
@Test
public void verifyAdminPathAuthorizeOK() throws Exception {
   this.mvc.perform( get( "/admin" )
         .with(user("admin").password("admin").roles("ADMIN") ) )
         .andExpect ( status ().isOk () );
}

@Test
public void verifyAdminPathAuthorizeNOK() throws Exception {
   this.mvc.perform ( get( "/admin")
     .with(user("user").password("secure").roles("USER") ) )
         .andExpect ( status ().isForbidden () );
}
```

# Stage 1: Statisches Security Testing



Continuous Integration (CI)

1 Pull-Request

2 Trigger Build

3 Check-Out

4 Build & Tests
& Static Code Analysis
& Dependency Check

5 Report Build Result

6 (Security) Code-Review

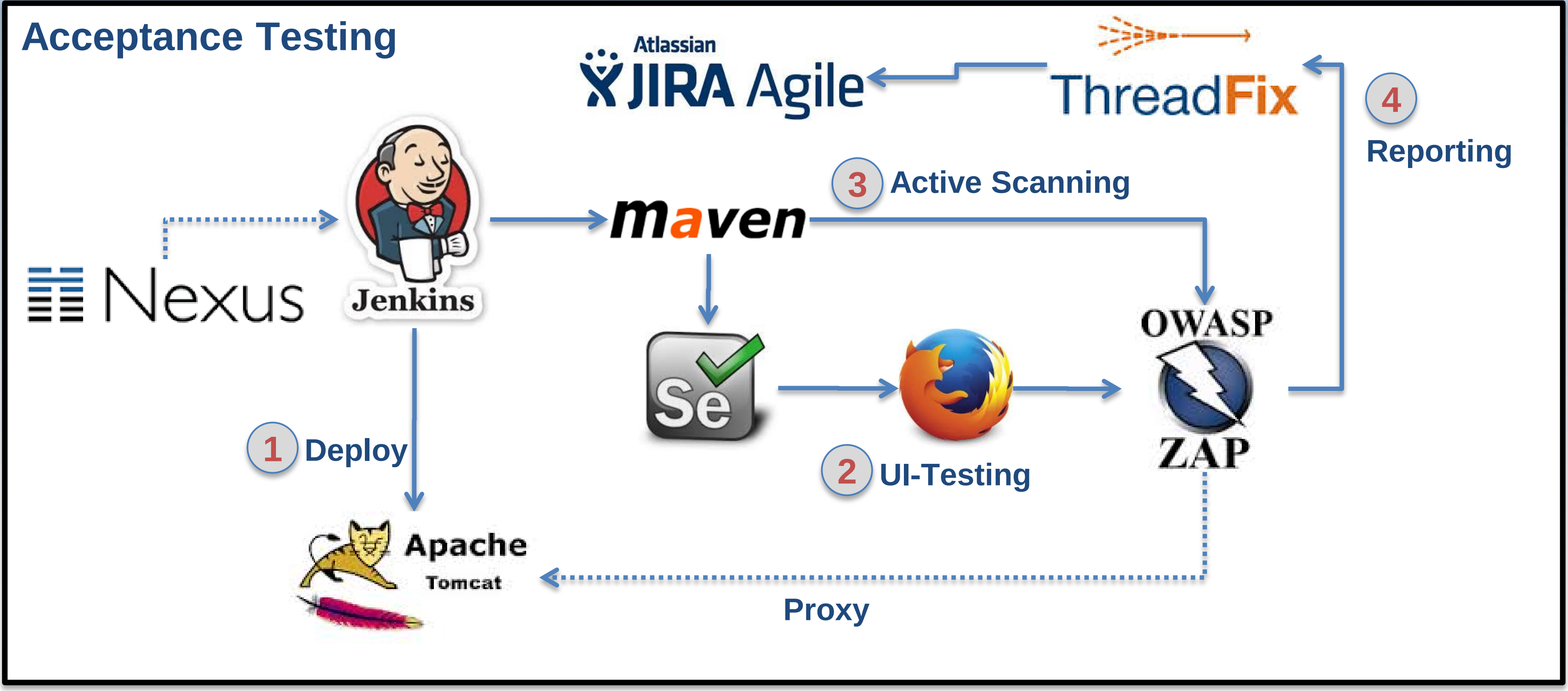
7 Push to Stable

Developer 1

Developer 2

JUnit
OWASP Dependency-Check
University of Maryland 18 56
FindBugs™ because it's easy
Jenkins
maven
git
gerrit Gerrit Code Review
OWASP Open Web Application Security Project

# Stage 2: Dynamisches Security-Testing



# Sichere Agile Entwicklung mit Scrum

**Sprint Review & Retro**

Review Threat Model Abdeckung

Review von…

…**Ab**User Stories

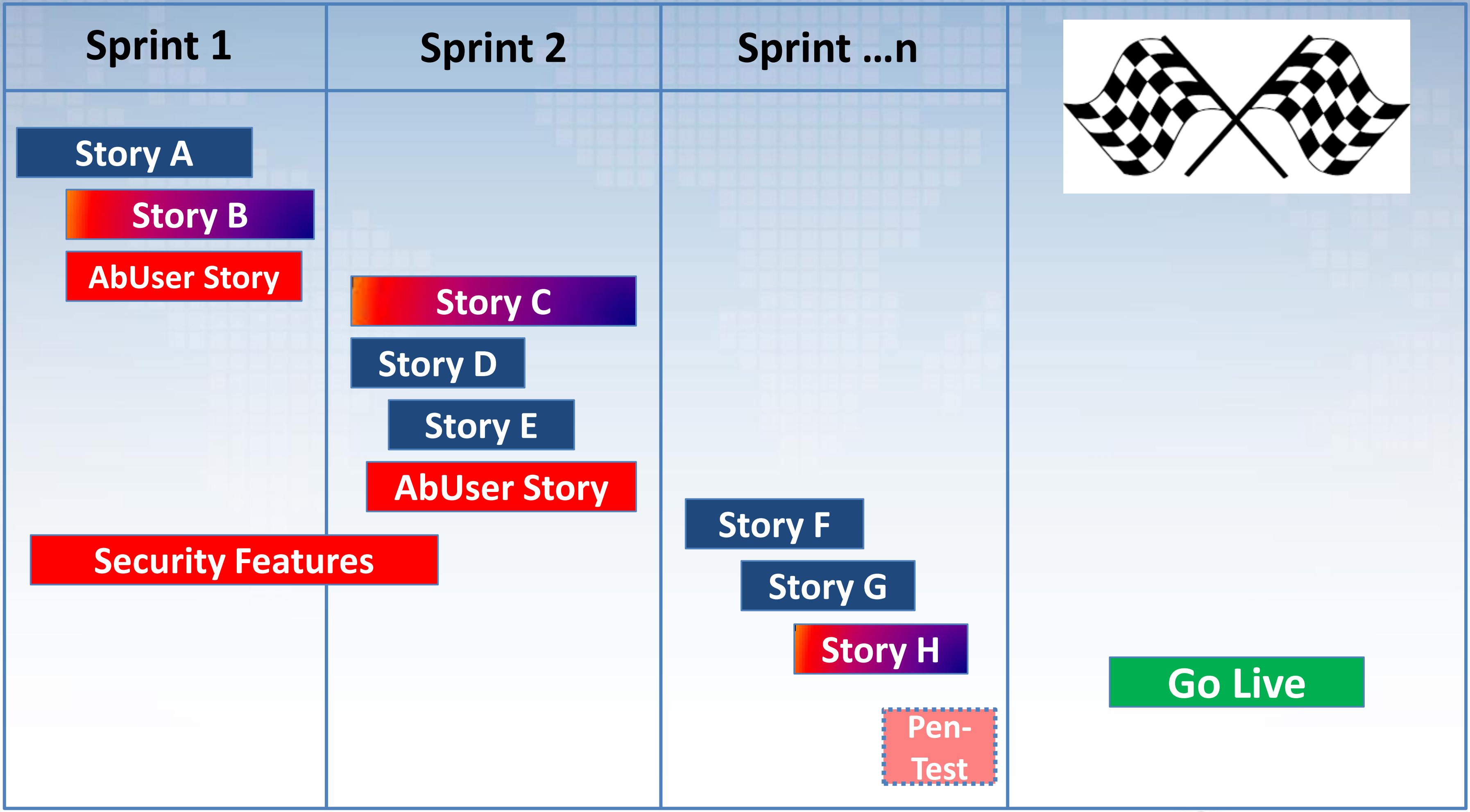
…Security Akzeptanzkriterien

Transparenz der Security gegenüber Kunde

„Inspect And Adapt“ aller Security- Aktivitäten

OWASP
Open Web Application
Security Project

# Idealzustand: Security == Agile!



Sprint 1

Sprint 2

Sprint …n

Story A

Story B

AbUser Story

Security Features

Story C

Story D

Story E

AbUser Story

Story F

Story G

Story H

Pen-Test

Go Live

OWASP

Open Web Application Security Project

Agile Security

# SECURE DEVOPS

# SecDevOps = Security + DevOps

Kommunikation

Zusammenarbeit

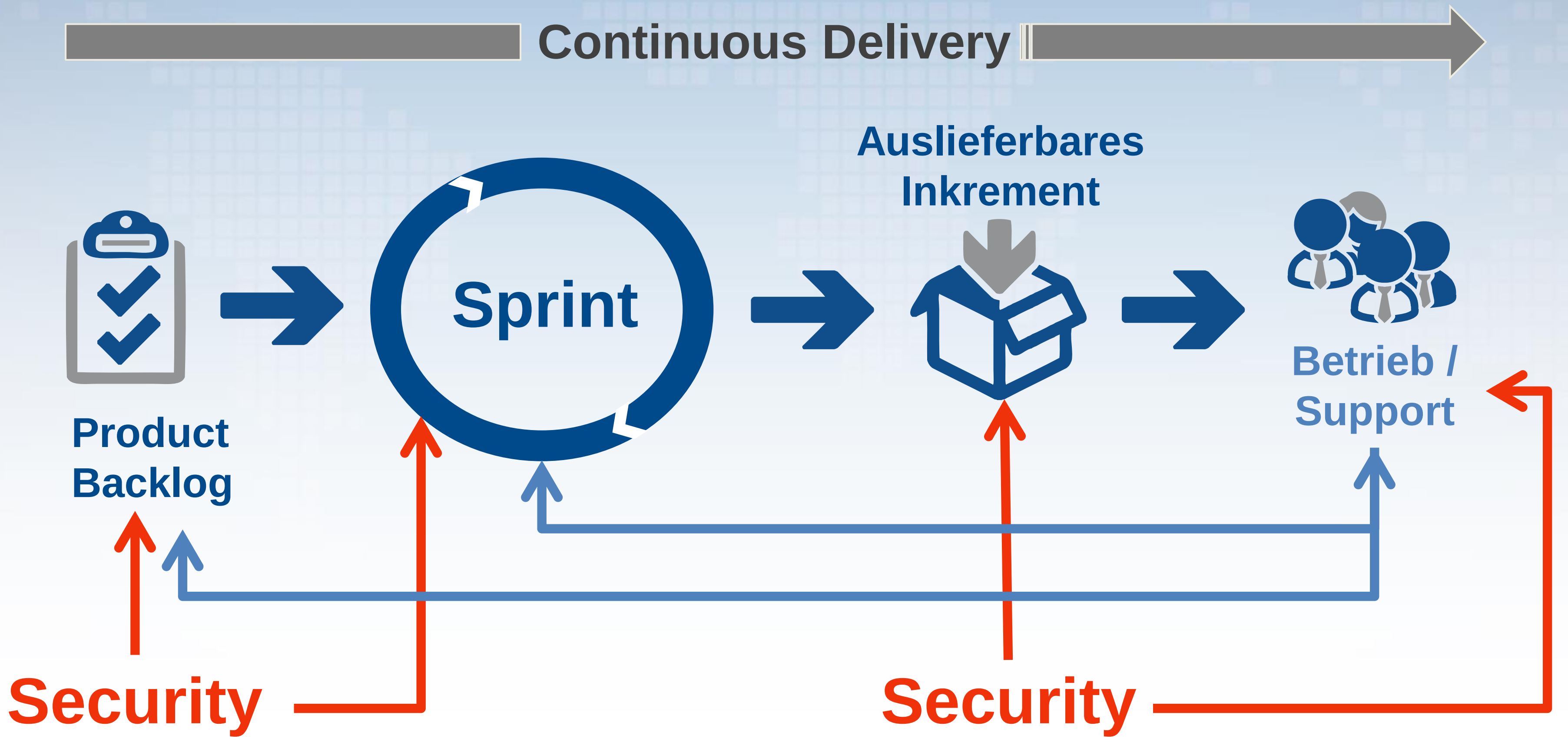
Security

Werkzeuge

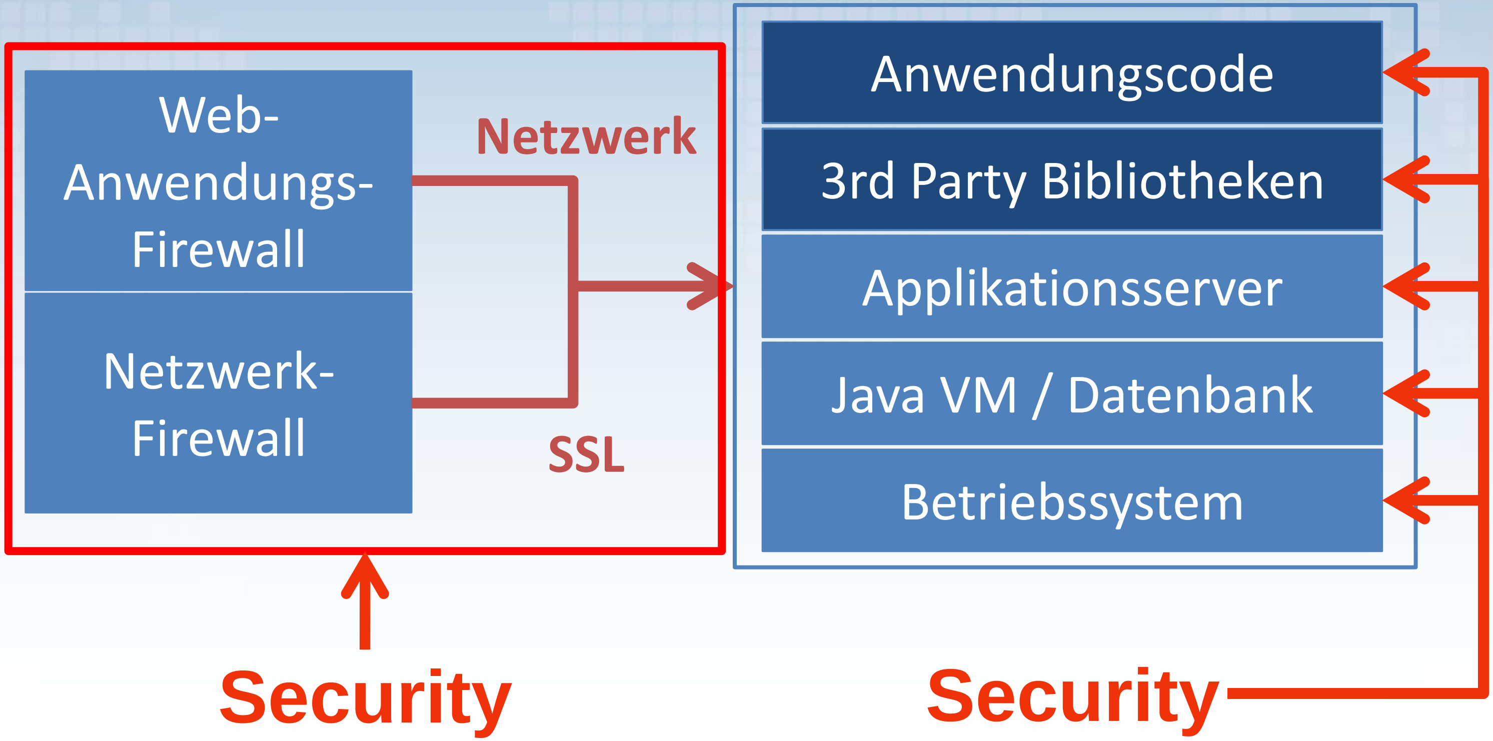
Continuous Delivery

OWASP
Open Web Application
Security Project

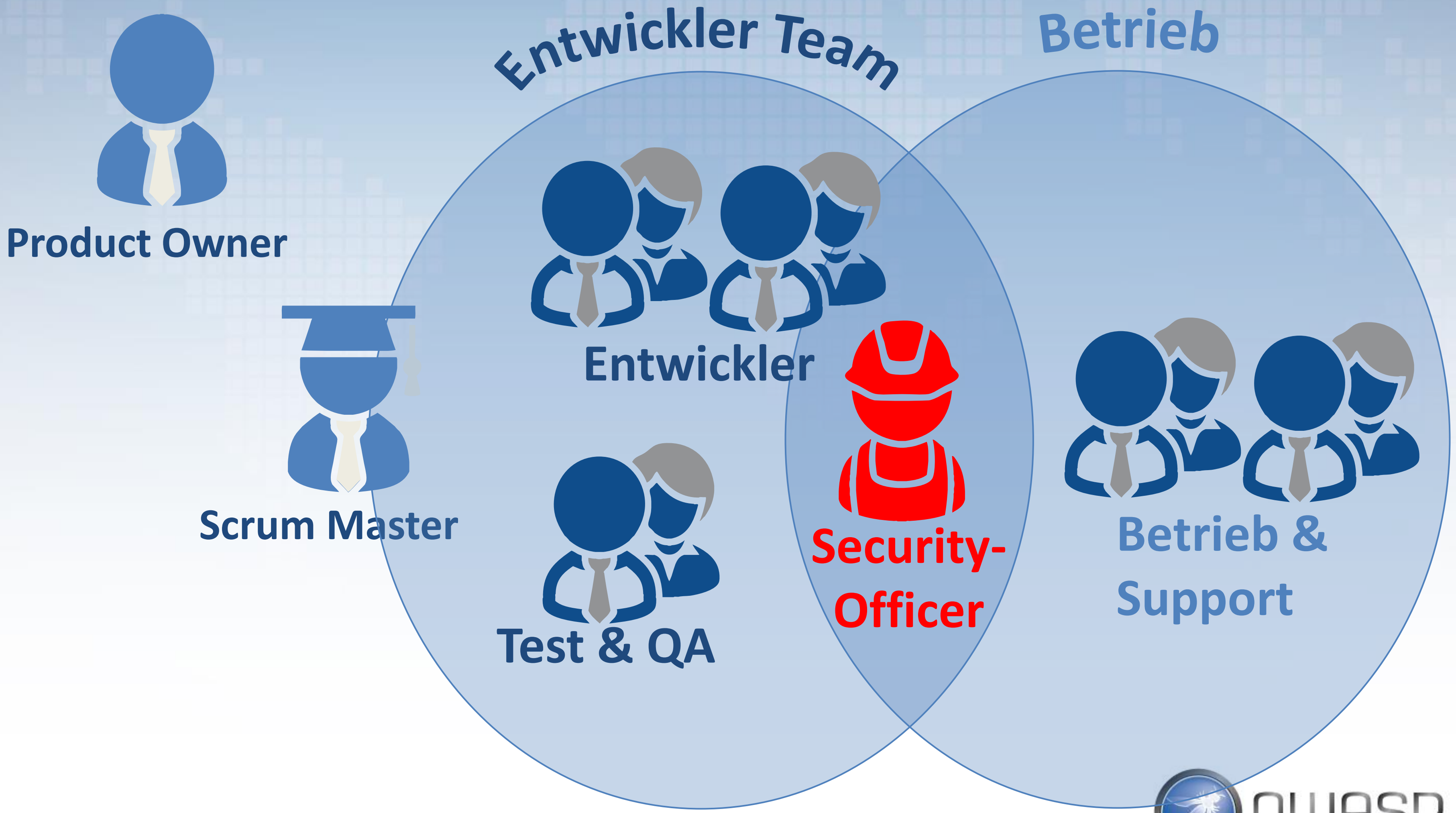
# SecDevOps = Security + DevOps



# SecDevOps = Security + DevOps



# SecDevOps = Security + DevOps



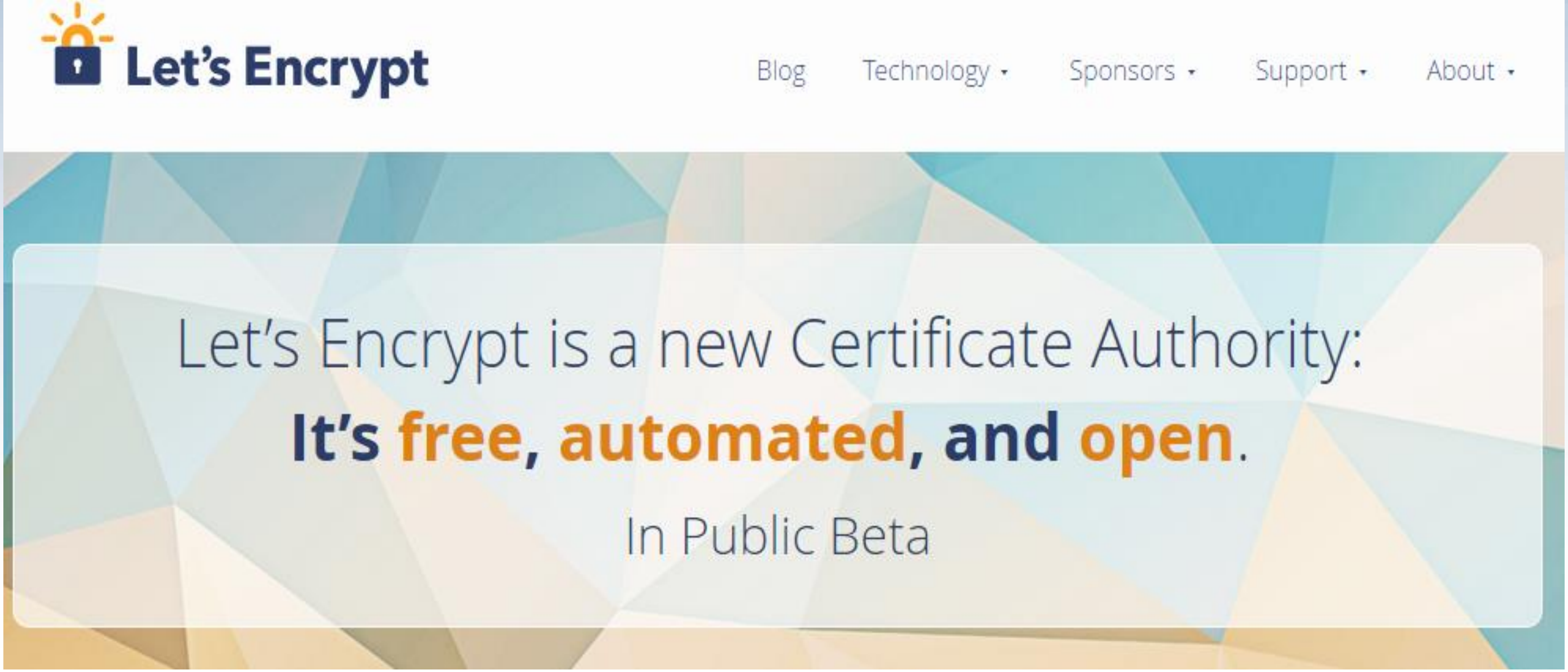
# SecDevOps – Testing „Infrastructure As Code“

http://serverspec.org

```
/usr/bin/ruby -S rspec spec/www.example.jp/sample_spec.rb
Package "httpd"  should be installed
Service "httpd"
  should be enabled
  should be running
Port "8443"
  should be listening
Finished in 0.21091 seconds (files took 6.37 seconds to load)
4 examples, 0 failures
```

# SecDevOps – Kostenlose SSL-Zertifikate

## HTTPS für alle Websites !!



Let's Encrypt is a new Certificate Authority:

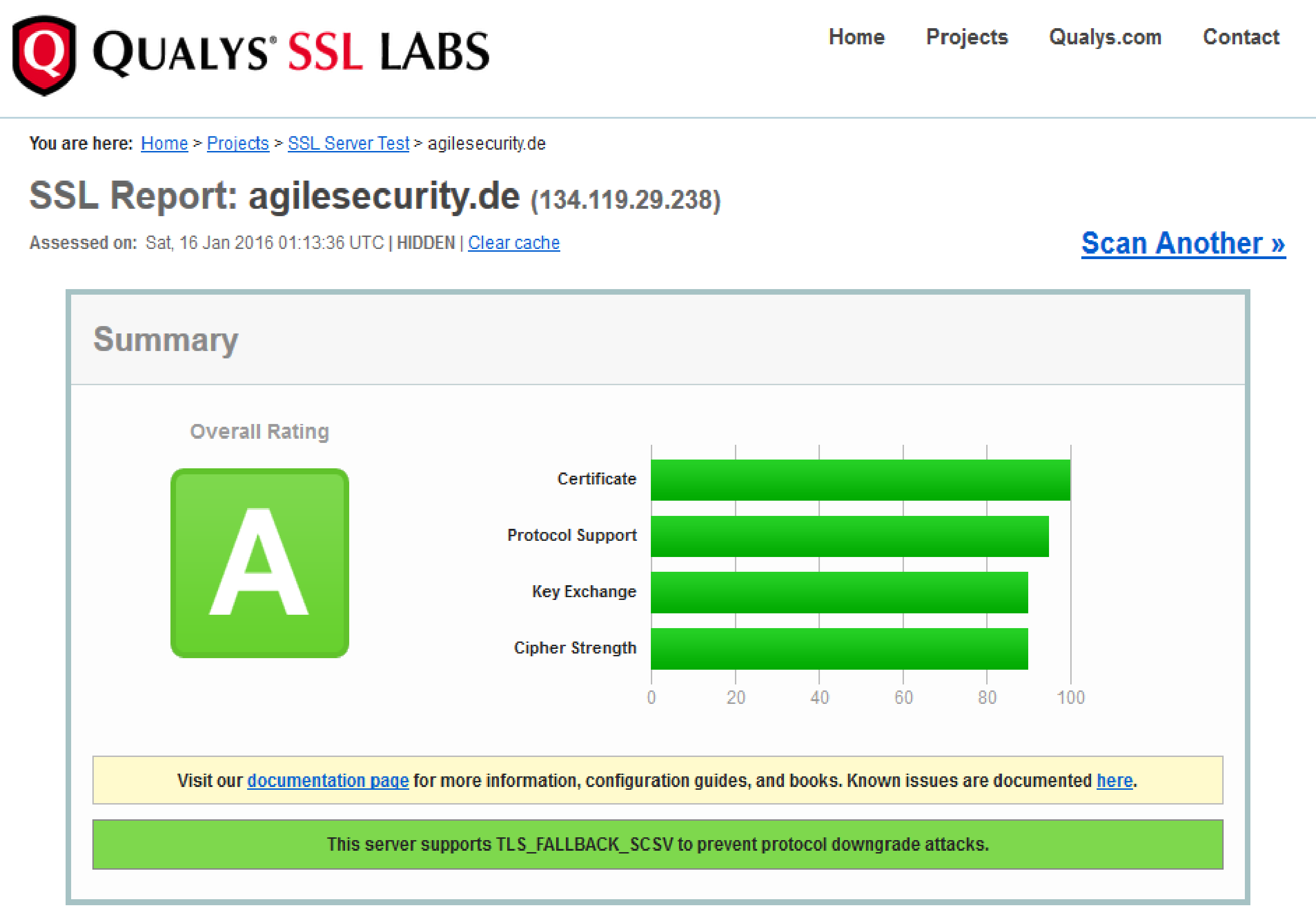
**It's free, automated, and open.**

In Public Beta

https://letsencrypt.org

OWASP
Open Web Application
Security Project

# SecDevOps – Sichere TLS (SSL) Konfiguration



You are here: Home > Projects > SSL Server Test > agilesecurity.de

SSL Report: agilesecurity.de (134.119.29.238)

Assessed on: Sat, 16 Jan 2016 01:13:36 UTC | HIDDEN | Clear cache

Scan Another »

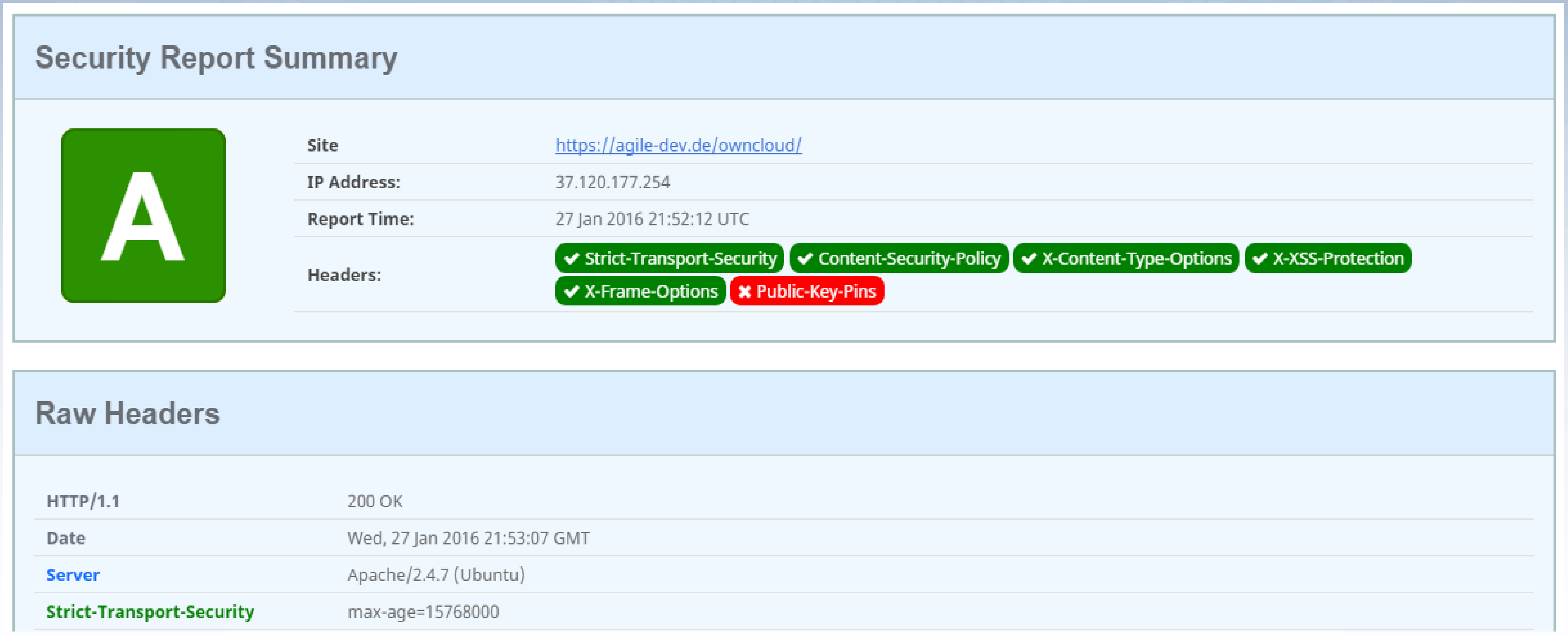
Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

https://www.ssllabs.com/ssltest/index.html

# SecDevOps – HTTP Response-Header



## Security Report Summary

A

| | |
|---|---|
| Site | https://agile-dev.de/owncloud/ |
| IP Address: | 37.120.177.254 |
| Report Time: | 27 Jan 2016 21:52:12 UTC |
| Headers: | ✓ Strict-Transport-Security ✓ Content-Security-Policy ✓ X-Content-Type-Options ✓ X-XSS-Protection ✓ X-Frame-Options ✗ Public-Key-Pins |

## Raw Headers

| | |
|---|---|
| HTTP/1.1 | 200 OK |
| Date | Wed, 27 Jan 2016 21:53:07 GMT |
| Server | Apache/2.4.7 (Ubuntu) |
| Strict-Transport-Security | max-age=15768000 |

https://securityheaders.io

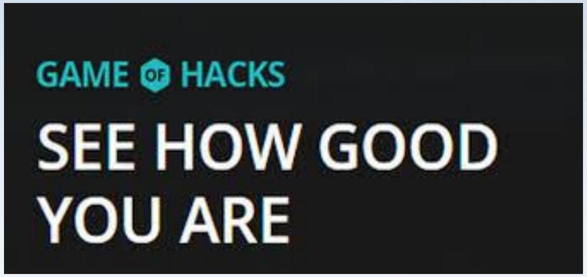
OWASP
Open Web Application
Security Project

# Fazit

Ausbildung für Security

http://www.itsecgames.com

Security transparent machen



http://www.gameofhacks.com

Security-Aktivitäten
im gesamten Entwicklungsprozess

OWASP
Open Web Application
Security Project

ROMA
MMXVI

APPSEC
EUROPE

# Building secure cloud-native applications with spring boot and spring security

***30.06.2016 / 01.07.2016***

***https://2016.appsec.eu***