/bin/whoami

- DevSecOps Consultant/Trainer
- Lecturer for Security in Web Applications at different Universities
- Open Source / Open Knowledge Enthusiast
Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM

High Level

Doing

ISMS
High Level

ISMS

OWASP SAMM

Implementation

Governance

Verification

SAMM Practices

Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM

Doing
Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM

- **High Level**
  - ISMS

- **SAMM Practices**
  - Implementation
  - Governance
  - Verification

- **DSOMM Dimensions**
  - Build & Deployment
  - Culture and Org.
  - Test and Verification

Doing
Simplified view on ISO 27001 | OWASP SAMM | OWASP DSOMM

High Level
- ISMS
- OWASP SAMM
- ... 

SAMM Practices
- Implementation
- Governance
- Verification
- ... 

DSOMM Dimensions
- Build & Deployment
- Culture and Org.
- Test and Verification
- ... 

DSOMM Dynamic Depth Activities
- Simple Scan
- Usage of different roles
- JavaScript
- ... 

Doing
SAMM and DSOMM

**SAMM**

- “Standard”
  - -> High level overview
  - Management topics like compliance and governance
  - Planning of high level targets
  - Mapping to ISO in the future

**DSOMM**

- Emerging
  - -> Low level overview
  - Only DevSecOps topics
  - Planning of concrete targets
  - Mapping to ISO/SAMM
  - ISMS: documentation in DSOMM
DevSecOps Dimensions

- Build and Deployment
- Culture and Organisation
- Information Gathering
- Hardening
- Test and Verification
DevSecOps Dimensions

Build and Deployment

Culture and Organisation

Information Gathering

Hardening

Test and Verification
OWASP Juice Shop is probably the most modern and sophisticated insecure web application!
German OWASP Top Ten 2017
Great for an initial training plan
Possible Rewards / Motivations

- High-Fives

Timo Pagel
Possible Rewards / Motivations

- High-Fives 🙌
- Pins
Pro/Con Pins

- Reminder
- Fast achievements
- Gamification: “We want to collect all pins”
- Transforms non touchable security into touchable security

OWASP Pins Project: https://owasp.org/www-project-security-pins/
Pro/Con Pins

- Reminder
- Fast achievements
- Gamification: “We want to collect all pins”
- Transforms non touchable security into touchable security

- Needs to be designed and produced

OWASP Pins Project: https://owasp.org/www-project-security-pins/
Implementation

OWASP Pins Project: https://owasp.org/www-project-security-pins/
Implementation

OWASP Pins Project: https://owasp.org/www-project-security-pins/
Virtual COVID-19 way: Backstage at SDA SE
Training Rewards

OWASP JUICE SHOP
CHALLENGES

BROKEN AUTHENTICATION
BROKEN ACCESS CONTROL
INJECTION
CROSS-SITE SCRIPTING

github.com/juice-shop

OWASP Pins Project: https://owasp.org/www-project-security-pins/
Nud ging (Reminder)

- “Steer people in particular directions”
- E.g. road signs

-→ Security pins on a hat
- Reminder of topics

Nudging Advanced
Threat Modeling

- What are we building?
- What can go wrong?
- What are we going to do about that?
- Did we do a good enough job?
 Threat Modeling Playbook

- Get TM stakeholders buy-in
- Embed TM in your organization
- Train your people to TM
- Strengthen your TM processes
- Innovate with TM technology
Threat Modeling: What can go wrong?

- Card Games (e.g. OWASP Cornucopia)
- Remote:
  - Online Cue Cards
  - Hybrid
    -> Send out card games before
    -> Send out hand before
    -> Participants might look at it beforehand

Free Cards for German OWASP Members:
Request robert.seedorff@iteratec.com

DevSecOps Dimensions

- Build and Deployment
- Culture and Organisation
- Information Gathering
- Hardening
- Test and Verification
Dynamic depth for applications
Simple Scan

Coverage of client side dynamic components
Simple Scan
Coverage of client side dynamic components
Usage of different roles
Simple Scan

Coverage of client side dynamic components

Usage of different roles

Coverage of sequential operations
Simple Scan

- Coverage of client side dynamic components
- Usage of different roles
- Coverage of sequential operations
- Coverage of hidden paths
Simple Scan

Coverage of client side dynamic components

Usage of different roles

Coverage of sequential operations

Coverage of hidden paths

Usage of multiple scanners
Web Security Testing of (an unknown) Enterprise World

OWASP Amaas

y.pagel.pro
x.pagel.pro
z.a.pagel.pro

y.pagel.pro:8080
x.pagel.pro:443
z.a.pagel.pro:80

OWASP ZAP
OWASP secureCodeBox: New Way

Target Cluster (DEV)

1. Identifies Service via Kubernetes API
2. Create Scan for Service
3. Start Job for Scan
4. OpenAPI Endpoint Security Scan
5. Publish Scan Results
6. Send Notifications for new Vulnerabilities

namespace-a

auto-discovery.securecodebox.io/enabled: "true"

Kubernetes Service

OWASP ZAP Scanner

SCB AutoDiscovery

SCB Operator

slack
Vulnerability Management System: Deduplication

- Handle Findings
  
  Decision:
  
  - Accept (The risk is acknowledged, yet remains)
  - Avoid (Do not engage with whatever creates the risk)
  - Mitigate (The risk still exists, yet compensating controls make it less of a threat)
  - Fix (The risk is eradicated)
  - Transfer (The risk is transferred to a 3rd party)

- Deduplicate Findings to detect handled findings
SDA SE ClusterScanner in DSOMM

- Test of virtualized environments (e.g. root, distroless)
- Test for Malware
- Usage of a maximum lifetime for images (indirect)
- Nightly build of images (indirect)
- Automated PRs for patches (indirect)
- A patch policy is defined (indirect)
- Test of server side components with known vulnerabilities
- Usage of a maximum lifetime for images (indirect)
SDA SE ClusterScanner Overview

Kubernetes Cluster 1
Image Collector
Container A, Image B

Kubernetes Cluster 2
Image Collector
Container X, Image Y
SDA SE ClusterScanner Overview

Kubernetes Cluster 1
- Image Collector
  - Container A, Image B
- Orchestrator
  - Scan A

Kubernetes Cluster n
- Image Collector
  - Container X, Image Y
- Image Registry
  - Scan B

Kubernetes Cluster 2
Cluster Scanner
+
DefectDojo
SDA SE ClusterScanner Overview

Image Collector
Container A, Image B
Kubernetes Cluster 1

Image Collector
Container X, Image Y
Kubernetes Cluster 2

Orchestrator
Scan A
DefectDojo

Scan B e.g. Image Lifetime
Image Registry

EMail/Messenger
Dev/Ops
DevSecOps Dimensions

- Build and Deployment
- Culture and Organisation
- Information Gathering
- Hardening
- Test and Verification
## OWASP AppSensor: What/When

<table>
<thead>
<tr>
<th>Logged information</th>
<th>Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>When</td>
<td>Event date/time</td>
</tr>
<tr>
<td></td>
<td>Log date/time</td>
</tr>
<tr>
<td>Security event</td>
<td>Type</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
</tr>
<tr>
<td></td>
<td>Confidence</td>
</tr>
<tr>
<td></td>
<td>Custom classification(s)</td>
</tr>
<tr>
<td></td>
<td>Owner</td>
</tr>
<tr>
<td>Location</td>
<td>Host</td>
</tr>
<tr>
<td></td>
<td>Service/application name</td>
</tr>
<tr>
<td></td>
<td>Port</td>
</tr>
<tr>
<td></td>
<td>Protocol</td>
</tr>
<tr>
<td></td>
<td>HTTP method</td>
</tr>
<tr>
<td></td>
<td>Entry point</td>
</tr>
<tr>
<td>Request</td>
<td>Purpose</td>
</tr>
<tr>
<td></td>
<td>Target</td>
</tr>
<tr>
<td>User</td>
<td>Source</td>
</tr>
<tr>
<td></td>
<td>Identity</td>
</tr>
<tr>
<td></td>
<td>HTTP user agent</td>
</tr>
<tr>
<td></td>
<td>Client fingerprint</td>
</tr>
<tr>
<td>AppSensor detection</td>
<td>Sensor ID</td>
</tr>
<tr>
<td></td>
<td>Sensor location</td>
</tr>
<tr>
<td></td>
<td>AppSensor Detection Point ID(s)</td>
</tr>
<tr>
<td></td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td>Message</td>
</tr>
<tr>
<td>Optional supporting details</td>
<td>Request headers</td>
</tr>
<tr>
<td></td>
<td>Request body</td>
</tr>
<tr>
<td></td>
<td>Response headers</td>
</tr>
<tr>
<td></td>
<td>Response body</td>
</tr>
<tr>
<td></td>
<td>Error stack trace</td>
</tr>
<tr>
<td>Result (including AppSensor response)</td>
<td>Error message</td>
</tr>
<tr>
<td>Response ID(s)</td>
<td>Other system response</td>
</tr>
<tr>
<td>Status</td>
<td>Reason for status</td>
</tr>
<tr>
<td>HTTP status code</td>
<td>AppSensor Result Response ID(s)</td>
</tr>
<tr>
<td>Description</td>
<td>Message</td>
</tr>
<tr>
<td>Message</td>
<td>Hash</td>
</tr>
</tbody>
</table>
## OWASP AppSensor: Detection Points

<table>
<thead>
<tr>
<th>Category</th>
<th>Detection Point Category</th>
<th>Detection Point ID</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control Exception</td>
<td>ACE1</td>
<td>Modifying URL Argument Within a GET for Direct Object Access Attempt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ACE2</td>
<td>Modifying Parameter Within A POST for Direct Object Access Attempt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ACE3</td>
<td>Force Browsing Attempt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ACE4</td>
<td>Evading Presentation Access Control Through Custom POST</td>
<td></td>
</tr>
<tr>
<td>Input Exception</td>
<td>IE1</td>
<td>Cross Site Scripting Attempt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IE2</td>
<td>Violation Of Implemented White Lists</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IE3</td>
<td>Violation Of Implemented Black Lists</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IE4</td>
<td>Violation of Input Data Integrity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IE5</td>
<td>Violation of Stored Business Data Integrity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IE6</td>
<td>Violation of Security Log Integrity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IE7</td>
<td>Detect Abnormal Content Output Structure</td>
<td></td>
</tr>
<tr>
<td>Encoding Exception</td>
<td>EE1</td>
<td>Double Encoded Character</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EE2</td>
<td>Unexpected Encoding Used</td>
<td></td>
</tr>
<tr>
<td>Command Injection Exception</td>
<td>CIE1</td>
<td>Blacklist Inspection for Common SQL Injection Values</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CIE2</td>
<td>Detect Abnormal Quantity of Returned Records</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CIE3</td>
<td>Null Byte Character in File Request</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CIE4</td>
<td>Carriage Return or Line Feed Character in File Request</td>
<td></td>
</tr>
<tr>
<td>File IO Exception</td>
<td>FIO1</td>
<td>Detect Large Individual File</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FIO2</td>
<td>Detect Large Number of File Uploads</td>
<td></td>
</tr>
</tbody>
</table>
Conclusion

- Open Source/Knowledge is startup and enterprise ready
  - Even for security
- OWASP® provides a lot of useful projects
Questions?

OWASP: timo.pagel@owasp.org
Business: owasp21@pagel.pro