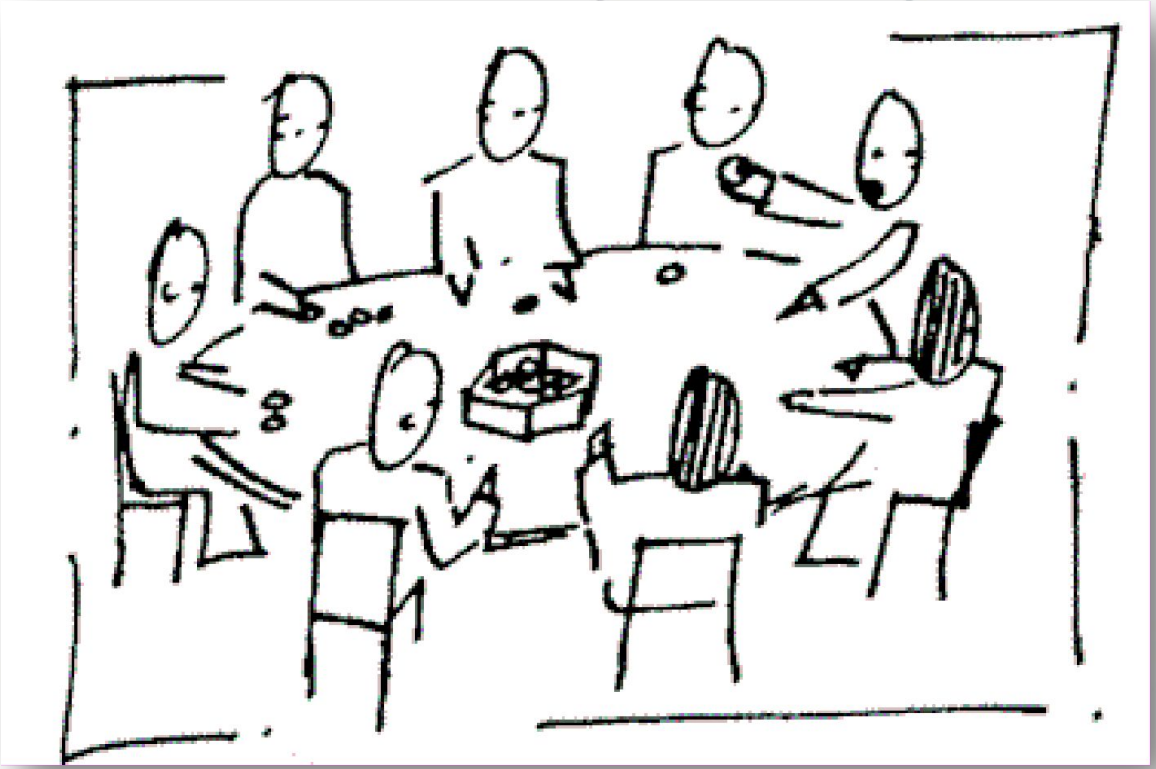
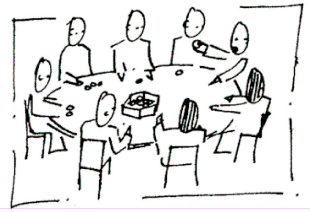
OWASP Stammtisch #43

Frankfurt am Main, 07.11.2018

Info

Intro





Intro

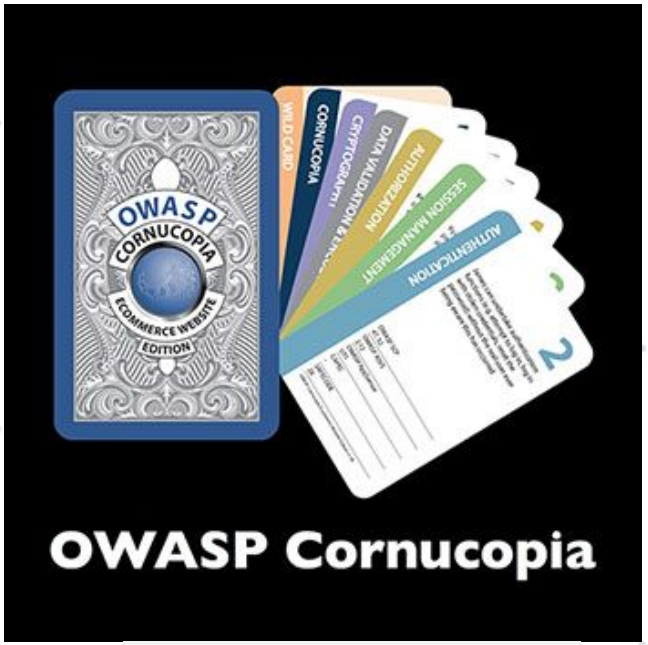
- My name is ...
- I work as ...
- I‘m here because ...

Agenda

Agenda

What's new ?
OWASP Projects Overview

Jim Manico



Mentoring

What‘s new?

What‘s new?

GERMAN OWASP DAY 2018

When?
Tuesday, 20th November 2018

Where?
Münster, Germany (Factory Hotel)

Who?
The conference is primarily aimed at a German-speaking audience

The target groups are developers, IT security managers, IT managers and the classic "security crowd".

OWASP German Chapter

owasp.github.io/german-owasp-day/

GERMAN OWASP DAY 2018

Dienstag, 20. November 2018

Uhrzeit	Beschreibung
08:15 - 08:55	Einlass
08:55 - 09:00	**Begrüßung** Christian Dresen und Sebastian Schinzel
09:00 - 09:45	*Keynote* **Sicherheitslücken in der künstlichen Intelligenz** Konrad Rieck
09:45 - 09:55	**OWASP Top 10 – 2017: Die 10 größten Risiken für Webanwendungen** Torsten Gigler
09:55 - 10:20	**Introduction to Mobile Security Testing: Approaches and Examples using OWASP MSTG** Carlos Holguera
10:20 - 10:50	Kaffeepause / Coffee Break
10:50 - 11:15	**Don't Trust The Locals: Exploiting Persistent Client-Side Cross-Site Scripting in the Wild** Marius Steffens, Ben Stock
11:15 - 11:40	**Docker Threat Modelling und Top 10** Dirk Wetter
11:40 - 12:05	**How API design impacts security: An empirical study of the PostMessage API** Sebastian Lekies
13:00 - 13:40	*Invited Talk* **Entwicklung von APT-Vorfällen in den letzen 5 Jahren** Christoph Fischer
13:40 - 14:05	**Der Feind in meiner Anlage - Risiken im Umfeld des industriellen IoT am Beispiel vertei** Ingo Hanke
14:05 - 14:50	*Lightning Talks* • **IT-security weaknesses of emergency-alert apps** - Marc Schoenefeld, Malte Schoe • **Mapping technischer Schwachstellen aus der OWASP Top 10 auf ISO/IEC 27001 C** • **Fun with Apache and MIME types** - Hanno Böck
14:50 - 15:20	Kaffeepause / Coffee Break
15:20 - 16:00	*Invited Talk* **Daniel Gruss** Transient Execution Attacks: Meltdown, Spectre, and how to mitigate them
16:00 - 16:25	**Efail: Angriffe gegen Ende-zu-Ende-Verschlüsselung von Email Kommunikation mit S/M** Christian Dresen
16:25 - 16:50	**PostScript Undead: Pwning the Web with a 35 Years Old Language** Jens Müller
16:50 - 17:00	**The traditional/inevitable OWASP Juice Shop update** Björn Kimminich
17:00	Ende der Veranstaltung

What‘s new?

OWASP Events/upcoming events

[hide]

Global AppSec Events

Global AppSec Events	Date	Location	Registration
TBA			

Regional and Local Events

Event	Type	Date	Location
AppSec Morocco 2018	Regional Event	November 15-16, 2018	Morocco
German OWASP Day	Regional Event	November 19-20, 2018	Münster, Germany
OWASP Norway Day 2018	Regional Event	November 29, 2018	Norway
OWASP BeNeLux-Day 2018	Regional Event	November 30, 2018	Mechelen, Belgium
AppSec California 2019	Regional Event	January 22-25, 2019	Santa Monica, CA
Mansoura Chapter and Besides Cairo Security Day	Local Event	February 1-2, 2019	Cairo, Egypt
SnowFROC 2019	Regional	March 14, 2019	Cable Center Denver, CO

owasp.org/index.php/OWASP_Events/upcoming_events

What‘s new?

Page | Discussion

OWASP German Chapter Stammtisch Initiative/Frankfurt

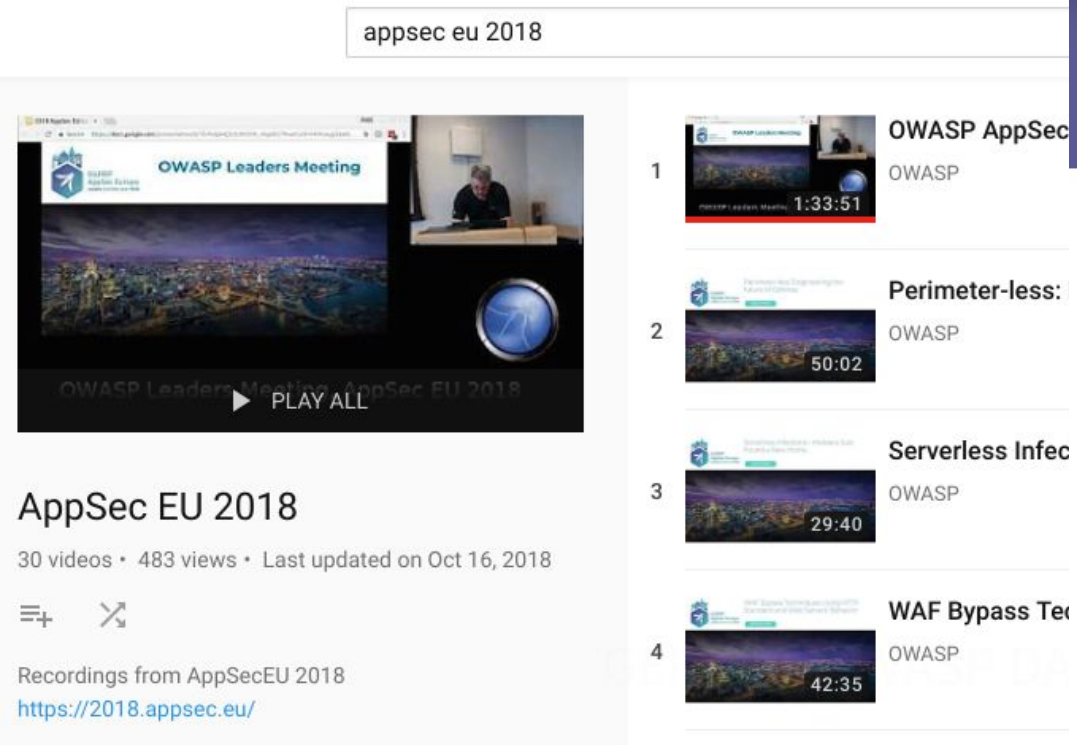
- Home
- About OWASP
- Acknowledgements
- Advertising
- AppSec Events
- Supporting Partners
- Books
- Brand Resources
- Chapters
- Donate to OWASP
- Downloads
- Funding
- Governance
- Initiatives
- Mailing Lists
- Membership
- Merchandise
- Presentations

[hide]

owasp.org/index.php/OWASP_German_Chapter_Stammtisch_Initiative/Frankfurt

What‘s new?

APPSEC EU 2018 VIDEO AND SLIDES NOW ONLINE



Slides and videos

CISO

- *"Adding Privacy by Design "*, by Sebastien Deleersnyder - [Slides]
- *"A View from Above "*, by Chris Horn - [Slides]
- *"Current Research and Standards "*, by Charles M Schmidt - [Slides]
- *"Deconstructing Threat Modeling "*, by Ciaran Conliffe - [Slides]
- *"Development to Risk Management "*, by Johanna Curiel.key - [Slides]
- *"Regular to Enterprise Ready "*, by Ovidiu Cical - [Slides]
- *"Seconds out "*, by Etienne Greeff - [Slides]
- *"Security is Everyone's Job "*, by Tanya Janca - [Slides]
- *"Threat Modeling for IOT "*, by Dan Cornell - [Slides]
- *"Threat Perspectives "*, by Jacky Fox and Gina Dollard - [Slides]

Developer

2018.appsec.eu/slides-and-videos

Introduction to OWASP with Jim Manico

OWASP Project Overview

OWASP Project Classification

Incubator Projects

Lab Projects

Flagship

Builders | Defenders | Breakers

OWASP Projects

Tools

Documentation

Awareness and education

Security Community

Flagship Projects

Tools [Health Check January 2017]

- OWASP Zed Attack Proxy
- OWASP Web Testing Environment Project
- OWASP OWTF
- OWASP Dependency Check
- OWASP Security Shepherd
- OWASP DefectDojo Project
- OWASP Juice Shop Project
- OWASP Security Knowledge Framework
- OWASP Dependency Track Project

Code [Health Check January 2017]

- OWASP ModSecurity Core Rule Set Project
- OWASP CSRFGuard Project
- OWASP AppSensor Project

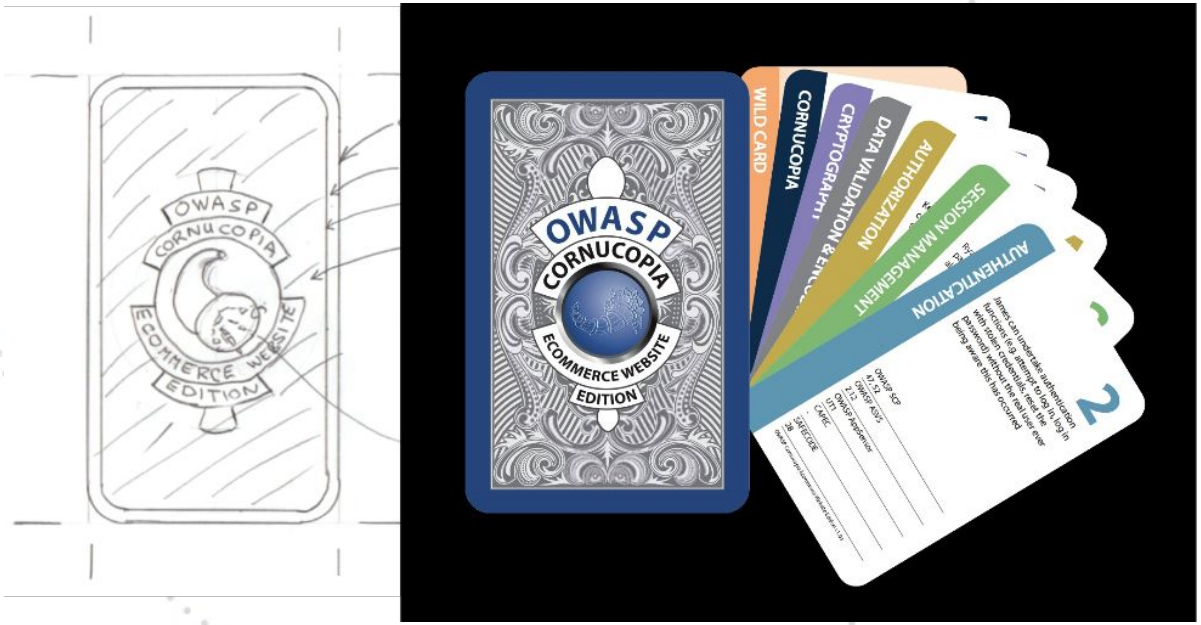
Documentation[Health Check January 2017]

- OWASP Application Security Verification Standard Project
- OWASP Software Assurance Maturity Model (SAMM)
- OWASP AppSensor Project
- OWASP Top Ten Project
- OWASP Testing Project

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

Introduction to OWASP

Security Gamification with OWASP Cornucopia



Daniel Gora

OWASP Volunteer

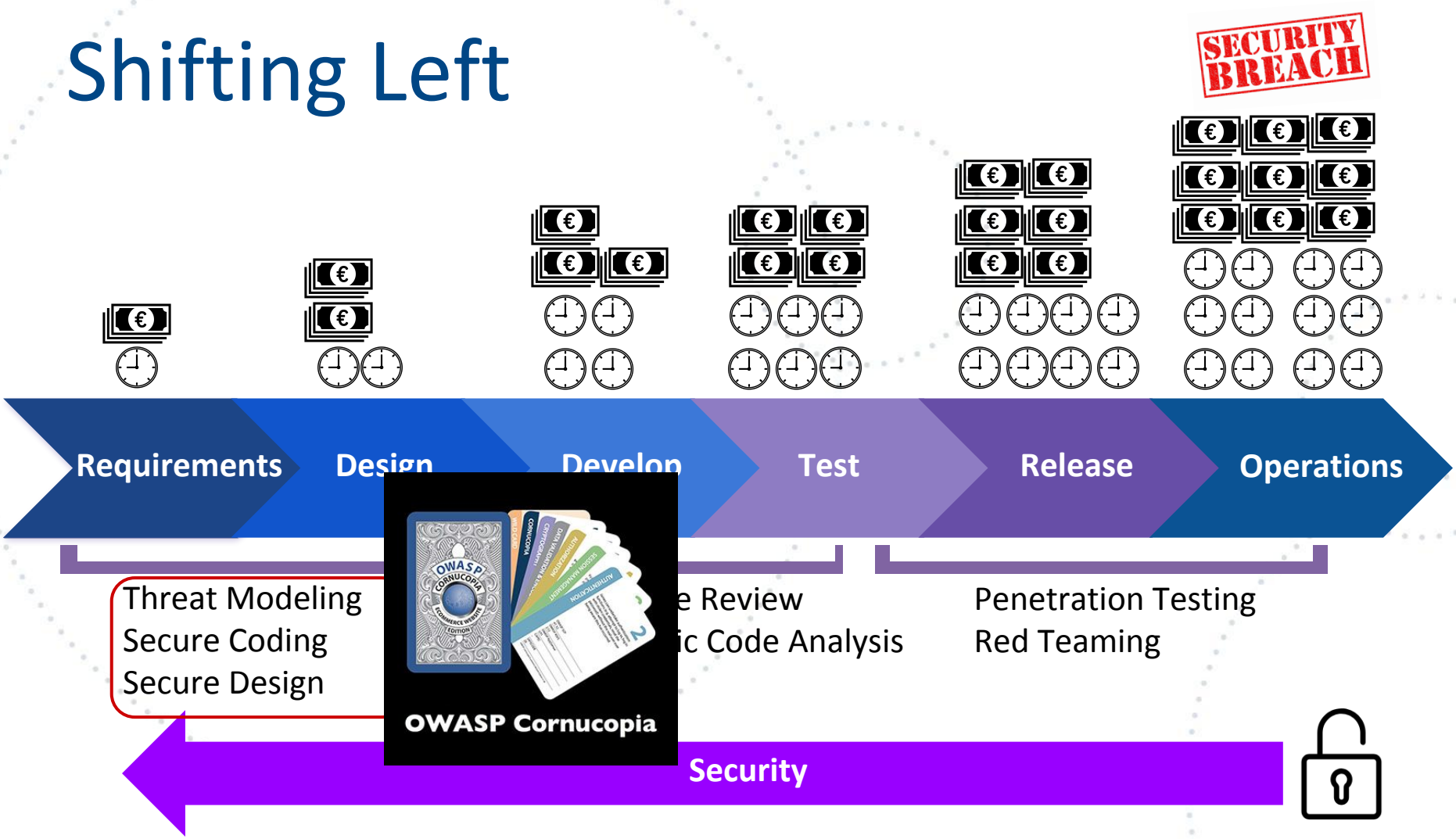
Senior Cyber Security Consultant

danielgora@owasp.org

Agenda

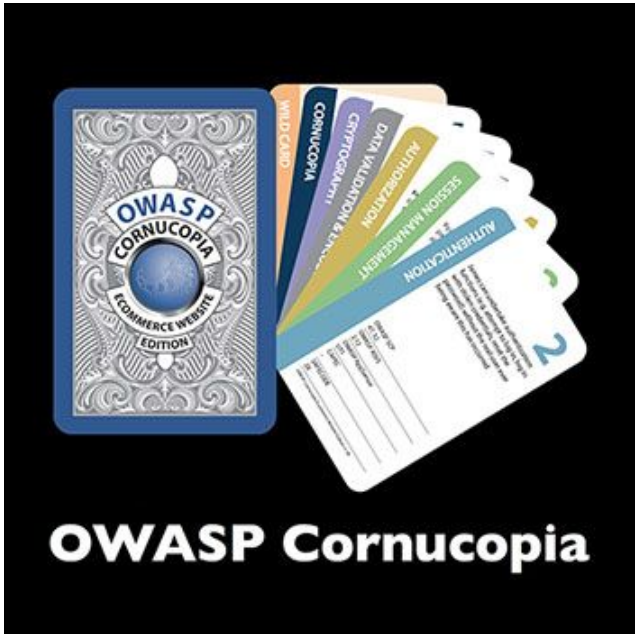
1. Shift security in SDLC
2. Cornucopia Card Game Introduction
3. How to play Cornucopia
4. Let's Play Online Dating
5. Benefits
6. Play Cornucopia at bar afterwards

Shifting Left



Builders | Defenders

Introduction

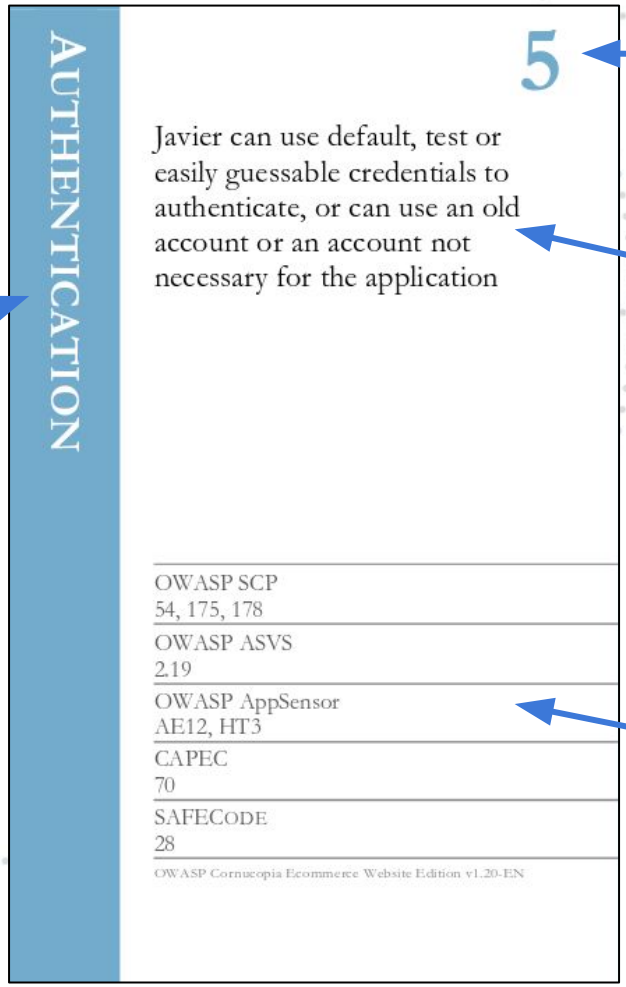


OWASP Secure Coding Practices Quick Reference Guide

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

Application Security Verification Standard 3.0.1

Cornucopia Card



Rank

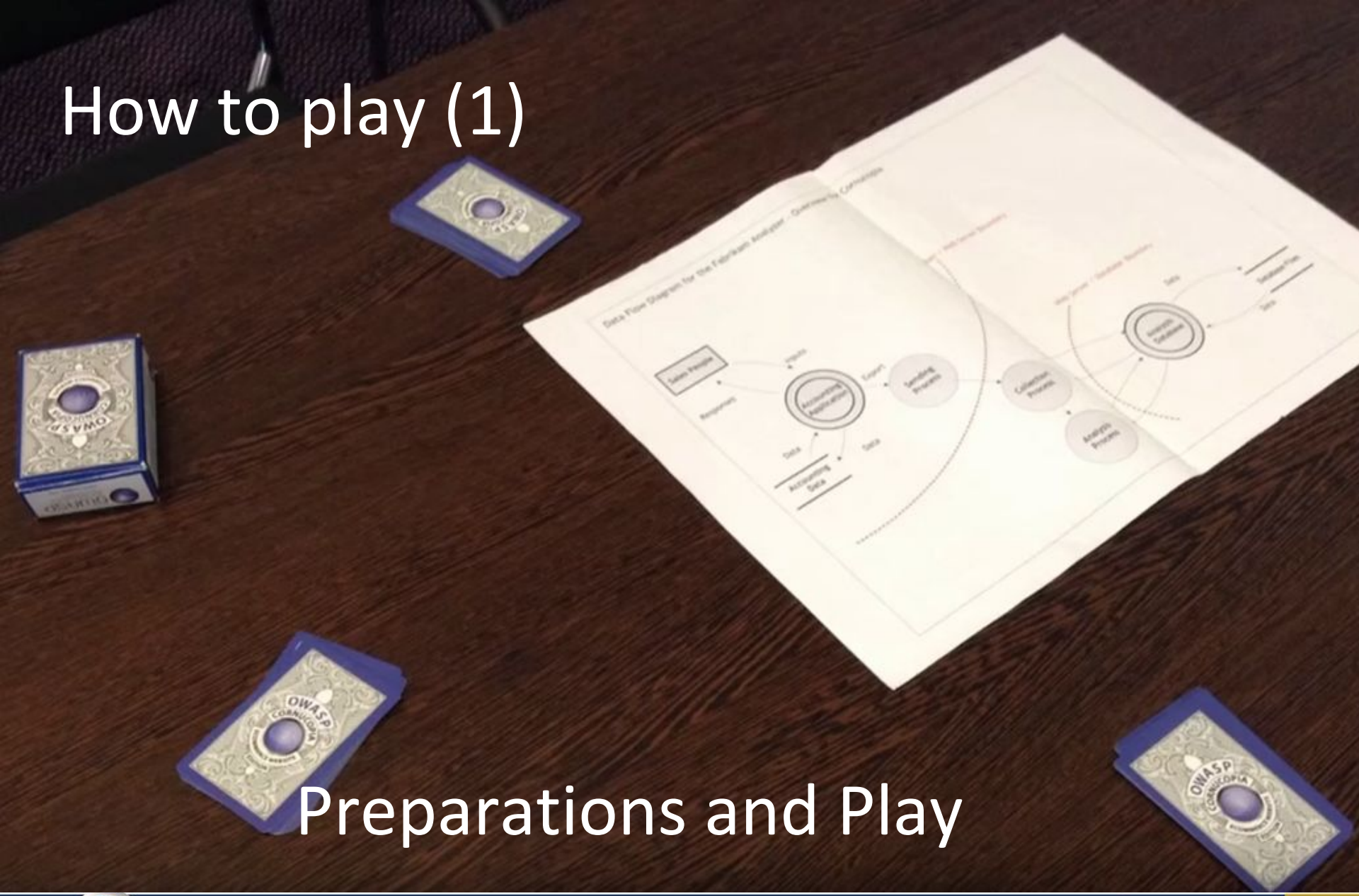
Threat Description

Suit

Cross-References:

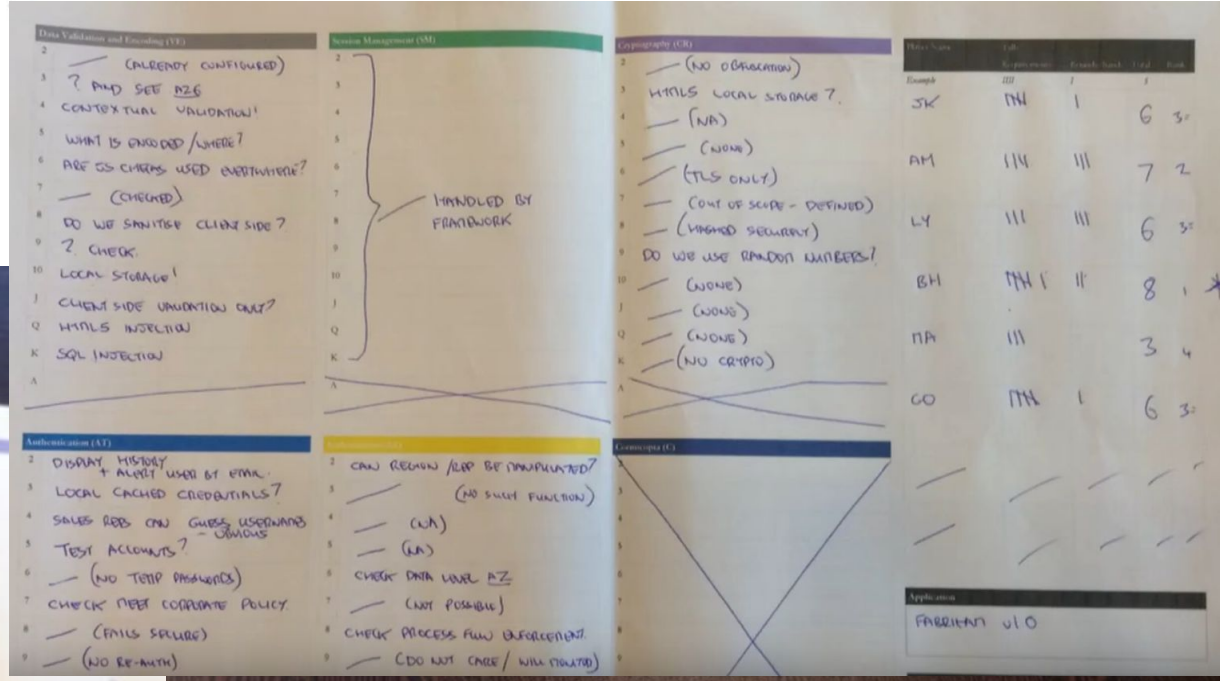
- OWASP Secure Coding Practices
- OWASP Application Verification Security Standard (ASVS)
- OWASP AppSensor
- Common Attack Pattern (CAPEC) by MITRE
- Software Assurance Forum for Excellence in Code (SAFECode)

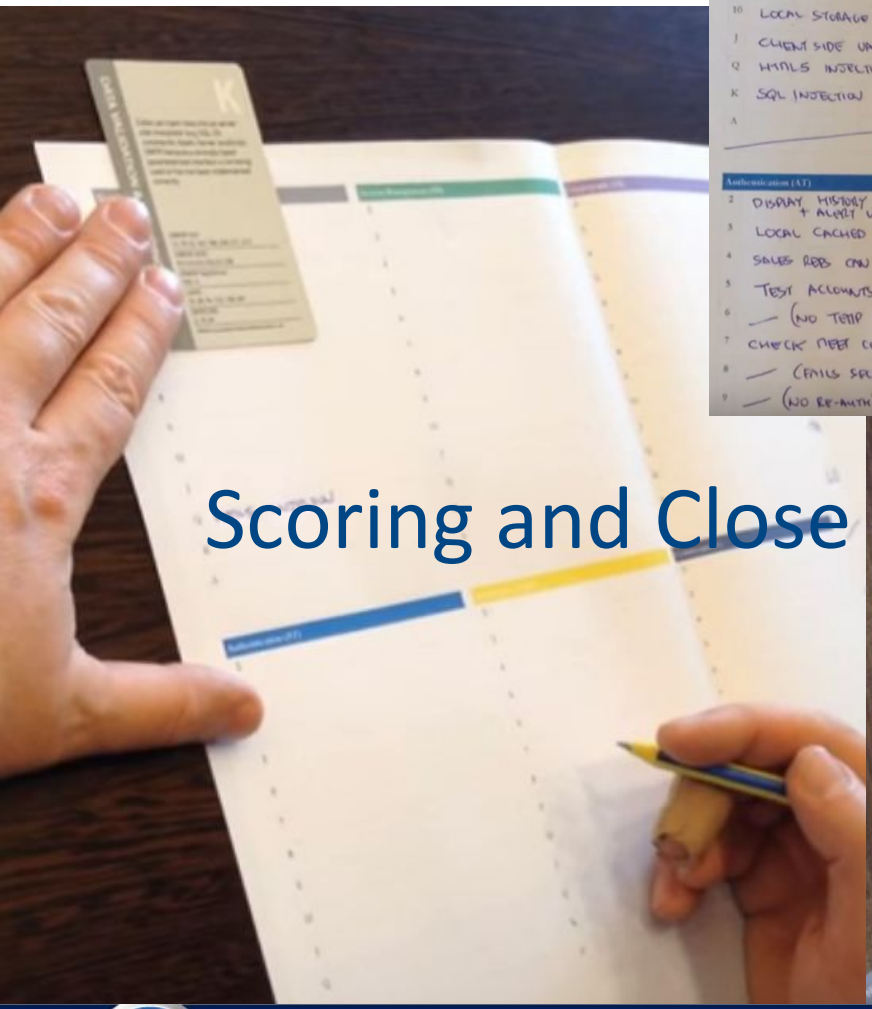
How to play (1)



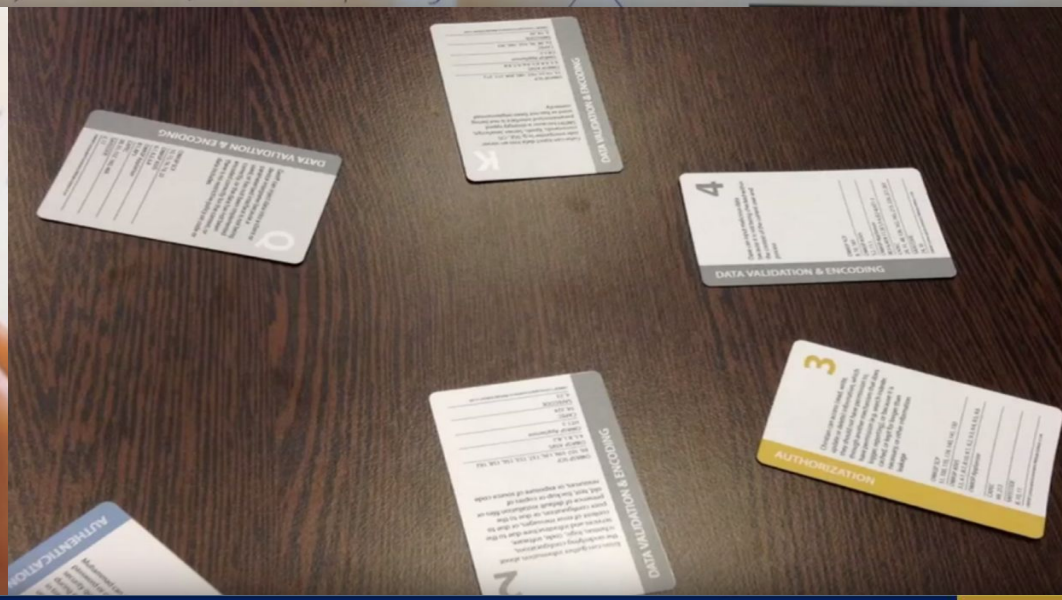
Preparations and Play

How to play (2)

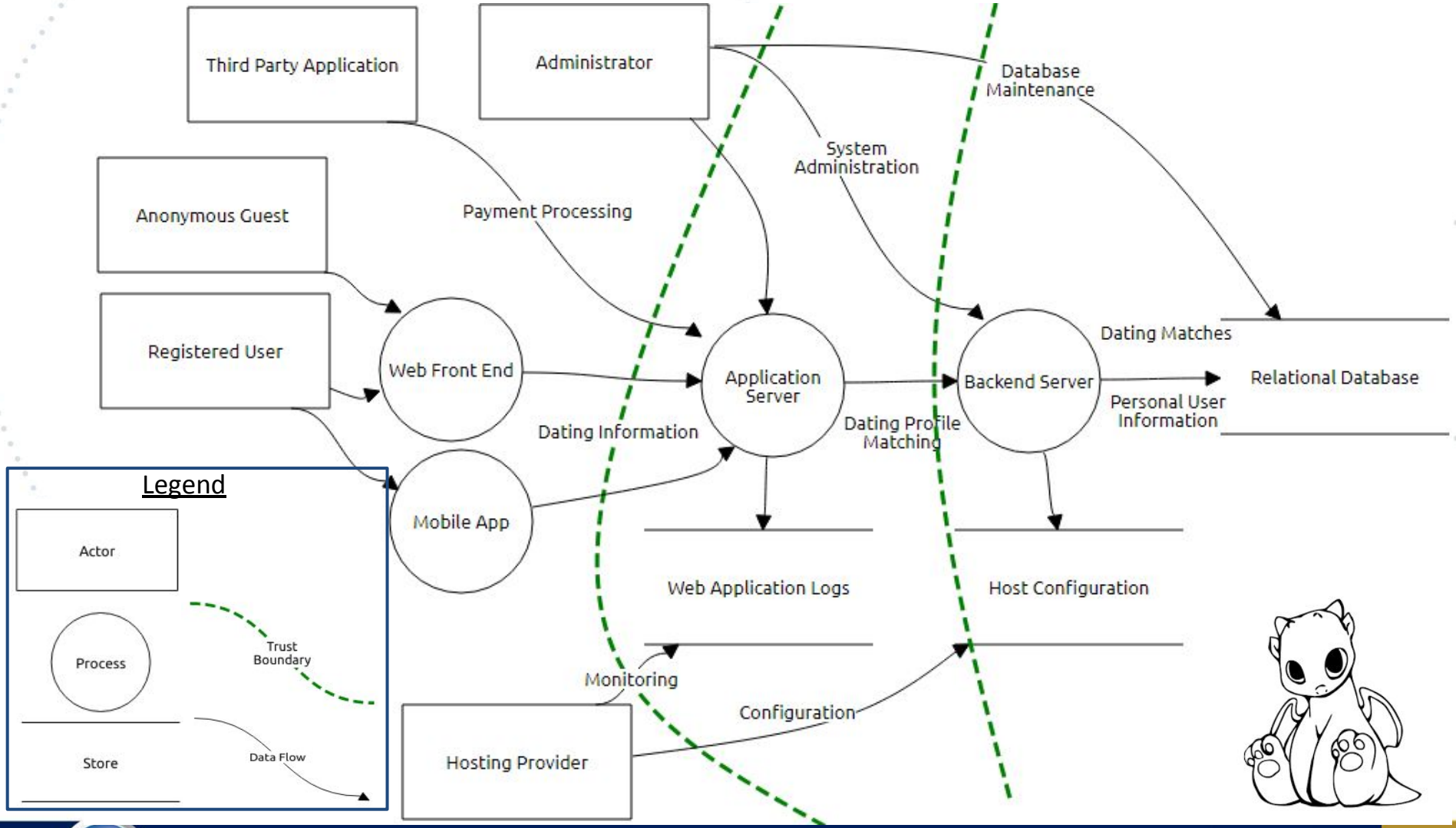




Scoring and Close



Damn Defenseless Dating App



Let's play! (1)

AUTHENTICATION

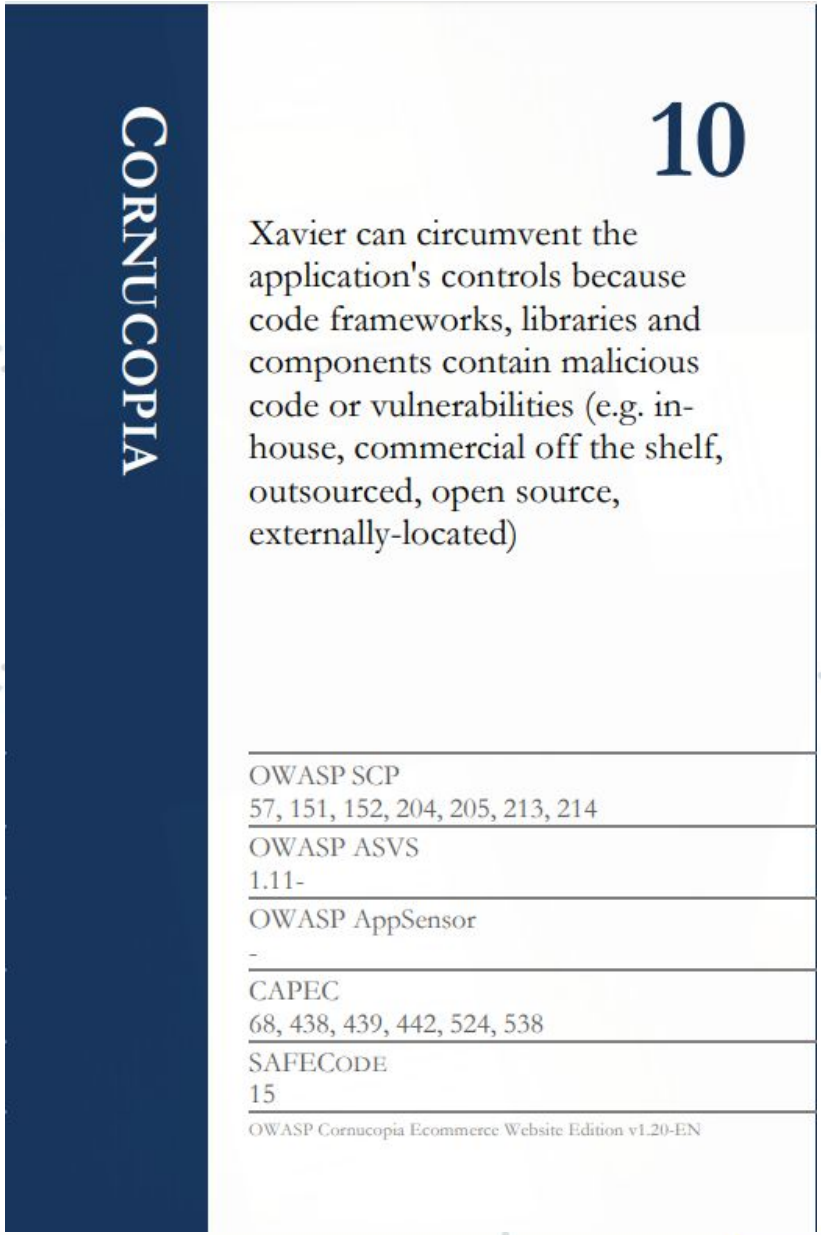
4

Sebastien can easily identify user names or can enumerate them

OWASP SCP 33, 53
OWASP ASVS 2.18, 2.28
OWASP AppSensor AE1
CAPEC 383
SAFECODE 28

OWASP Cornucopia Ecommerce Website Edition v1.20-EN

Let’s play! (2)


CORNUCOPIA
10
Xavier can circumvent the application's controls because code frameworks, libraries and components contain malicious code or vulnerabilities (e.g. in-house, commercial off the shelf, outsourced, open source, externally-located)
OWASP SCP
57, 151, 152, 204, 205, 213, 214
OWASP ASVS
1.11-
OWASP AppSensor
-
CAPEC
68, 438, 439, 442, 524, 538
SAFECODE
15
OWASP Cornucopia Ecommerce Website Edition v1.20-EN

Benefits Cornucopia

Gamification

Security Education

Training Sessions

Agile User Stories

Requirements Engineering

Security Championship

Game Time!


OWASP
Cornucopia
Do you want to play a game?
CORNUCOPIA
Joker
OWASP
Cornucopia

OWASP Ethical Hacking Mentoring

Hacking with Cedric Klosa

Next OWASP Meetup

My Favourite BBQ: Kerberoasting

by Jan Fischbach and Kevin Ott

Save the date: 06.02.2019

Spread the word

- Mailinglisten
  - OWASP Deutschland
    - https://lists.owasp.org/pipermail/owasp-germany/
  - Stammtisch Frankfurt
    - https://lists.owasp.org/mailman/listinfo/owasp-frankfurt

- **Meetup**
  - **Stammtisch Frankfurt**
    http://www.meetup.com/de/IT-Security-Stammtisch-Frankfurt-OWASP-u-w/

- OWASP Germany
  - https://www.owasp.org/index.php/Germany
  - https://www.owasp.org/index.php/OWASP_German_Chapter_Stammtisch_Initiative
  - https://www.owasp.org/index.php/Germany/Projekte
  - https://twitter.com/#!/search/OWASP_de

Outro