



OWASP

Open Web Application
Security Project

Frankfurt

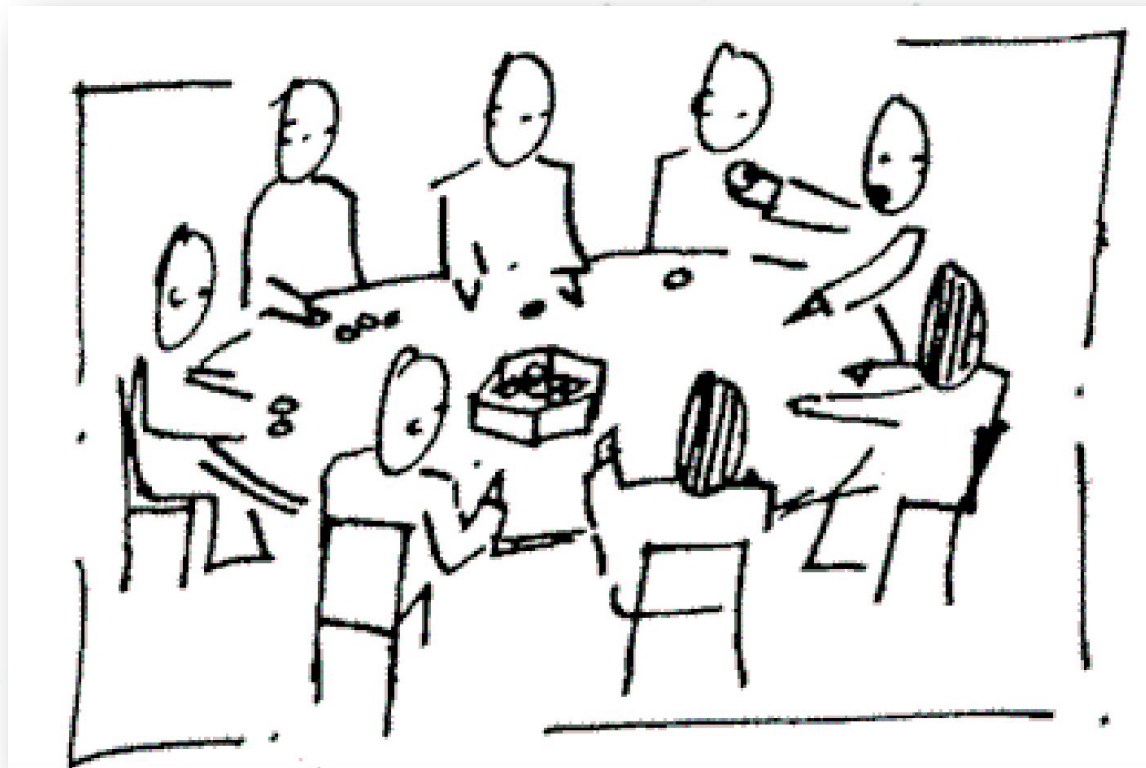
OWASP Stammtisch #43

Frankfurt am Main, 07.11.2018

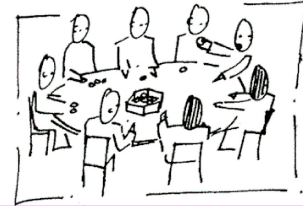
Info



Intro



Intro



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



Agenda

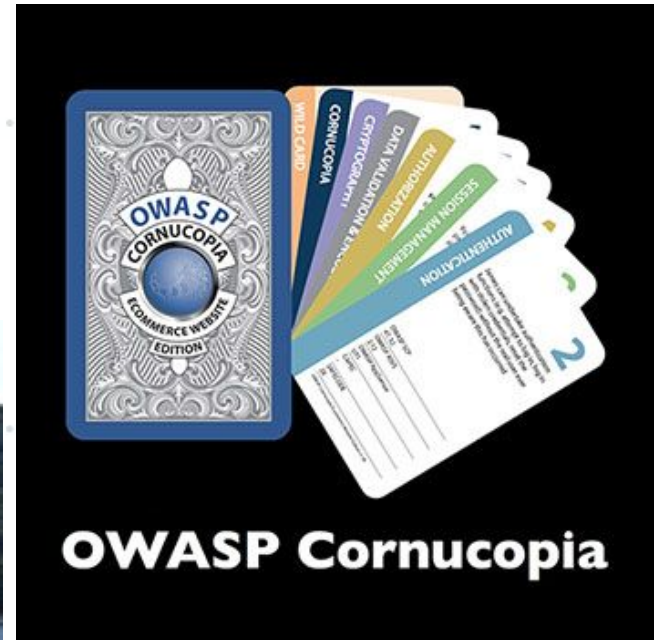


Agenda

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/



OWASP

Open Web Application
Security Project

WWW.OWASP.ORG

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	<i>Keynote</i> 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	<i>Invited Talk</i> Entwicklung von APT-Vorfällen in den letzten 5 Jahren Christoph Fischer
13:40 - 14:05	Der Feind in meiner Anlage - Risiken im Umfeld des industriellen IoT am Beispiel verteilte Ingo Hanke
14:05 - 14:50	<i>Lightning Talks</i> <ul style="list-style-type: none"> • IT-security weaknesses of emergency-alert apps - Marc Schoenefeld, Malte Schoenefeld • 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	<i>Invited Talk</i> 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]

- 1 Global AppSec Events
- 2 Regional and Local Events
- 3 Training Events
- 4 Project Summits
- 5 Developer Summits
- 6 Partner and Promotional Events

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]

- 1 General Information
 - 1.1 When
 - 1.2 Where
 - 1.3 What
 - 1.4 Etiquette
 - 1.5 Organization
 - 1.6 Further Information
- 2 Coming Up
- 3 Previous Stammtische / Meetups
 - 3.1 #42 | OWASP Stammtisch Frankfurt | 05.09.2018, 19:30h
 - 3.2 #41 | OWASP Stammtisch Frankfurt | 30.05.2018, 19:30h
 - 3.3 #40 | OWASP Stammtisch Frankfurt | 28.03.2018, 19:30h
 - 3.4 #39 | OWASP Stammtisch Frankfurt | 30.01.2018, 19:30h
 - 3.5 #38 | OWASP Stammtisch Frankfurt | 29.11.2017, 19:30h

owasp.org/index.php/OWASP_German_Chapter_Stammtisch_Initiative/Frankfurt



OWASP

Open Web Application
Security Project

WWW.OWASP.ORG

What's new?

APPSEC EU 2018 VIDEO AND SLIDES NOW ONLINE

appsec eu 2018



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



- 1 OWASP AppSec OWASP 1:33:51
- 2 Perimeter-less: OWASP 50:02
- 3 Serverless Infec OWASP 29:40
- 4 WAF Bypass Te OWASP 42:35

AppSec EU 2018

30 videos • 483 views • Last updated on Oct 16, 2018



Recordings from AppSecEU 2018

<https://2018.appsec.eu/>

2018.appsec.eu/slides-and-videos



OWASP

Open Web Application
Security Project

WWW.OWASP.ORG

Introduction to OWASP with Jim Manico



OWASP Project Overview



OWASP Project Classification



Incubator Projects



Lab Projects



Flagship

Builders

Defenders

Breakers



OWASP

Open Web Application
Security Project

WWW.OWASP.ORG

OWASP Projects

Tools

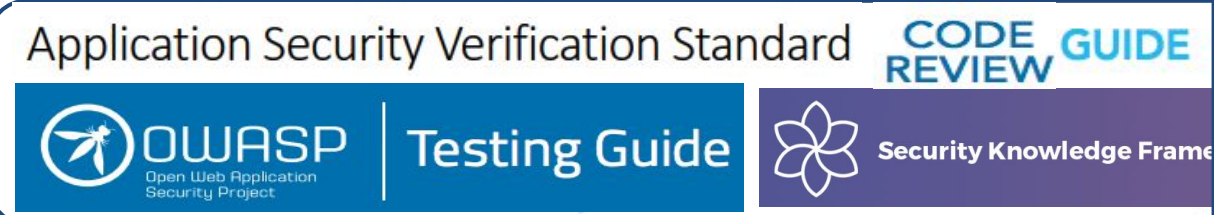


DEPENDENCY-CHECK
DEFECTDOJO
OWASP ModSecurity Core Rule Set
THE 1ST LINE OF DEFENSE



Security
Community

Documentation



Application Security Verification Standard
OWASP Testing Guide
CODE REVIEW GUIDE
Security Knowledge Framework

Awareness
and education



OWASP Pro Active CONTROLS
Security Shepherd
DevSLOp
WEBGOAT
OWASP Cheat Sheets

Flagship Projects

OWASP

FLAGSHIP

mature 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



OWASP

Open Web Application
Security Project

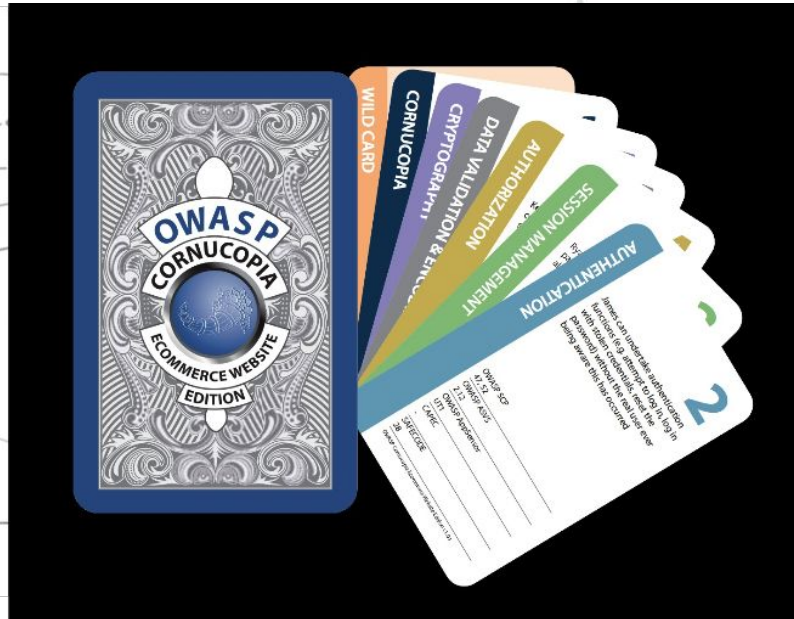
OWASP Frankfurt Stammtisch #43

WWW.OWASP.ORG

Introduction to OWASP



Security Gamification with OWASP Cornucopia



Daniel Gora

OWASP Volunteer

Senior Cyber Security Consultant

danielgora@owasp.org

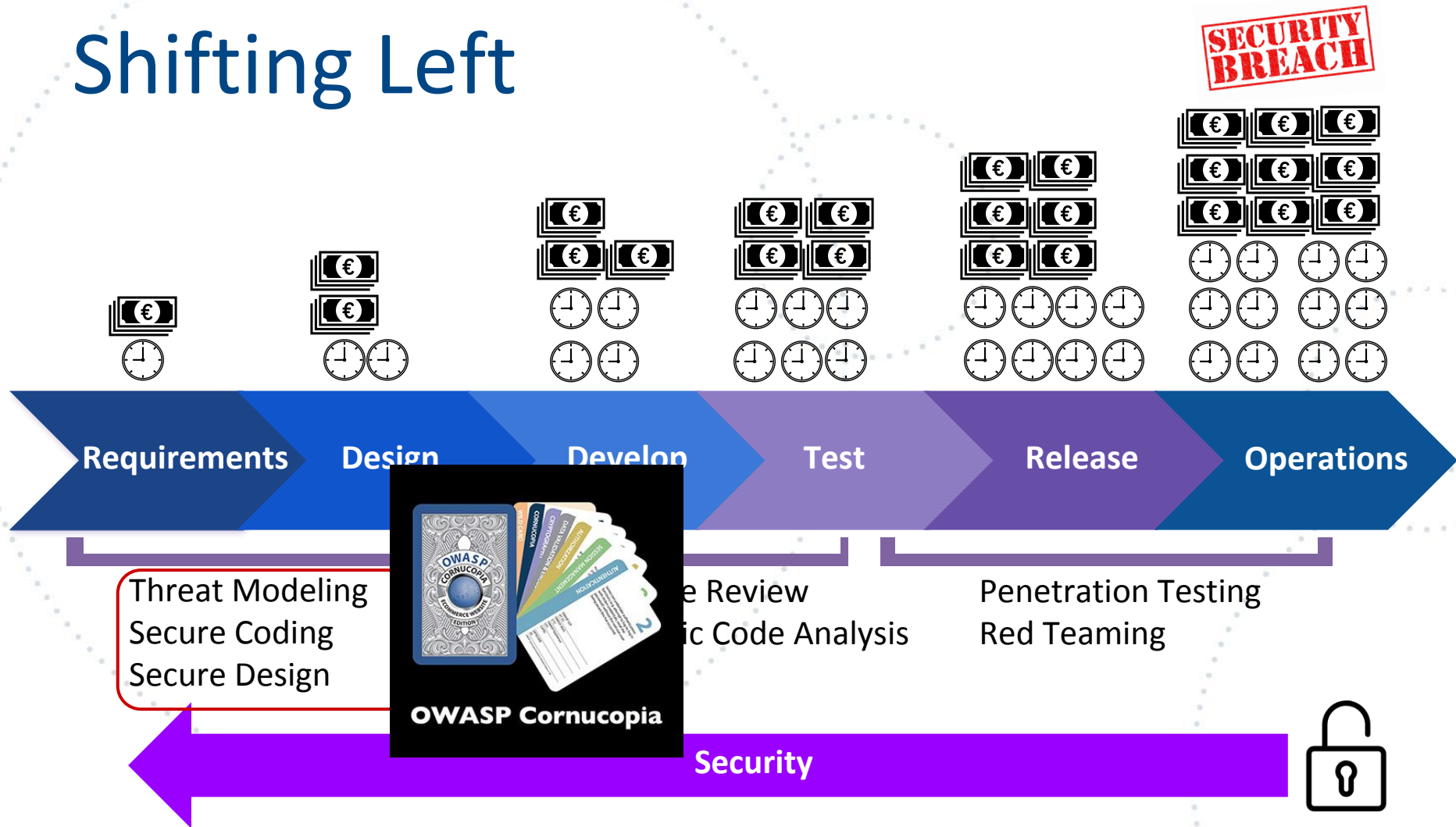


Agenda

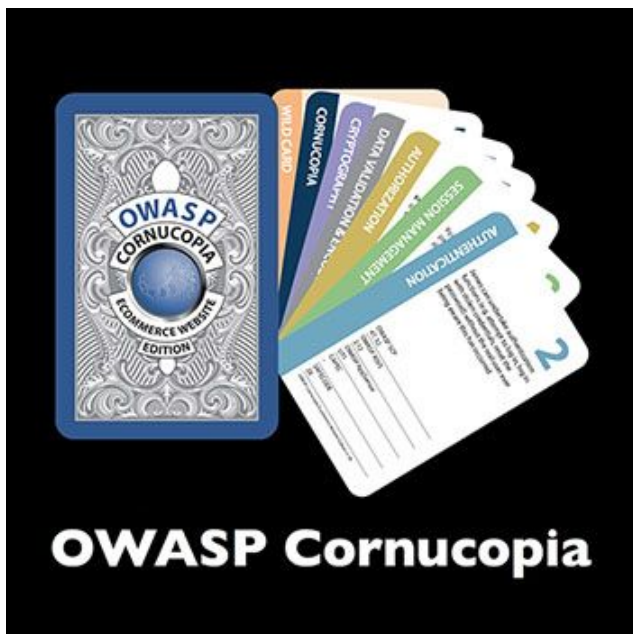
1. Shift security in SDLC
2. Cornucopia Card Game Introduction
3. How to play Cornucopia
4. Let's Play Online Dating
5. Benefits
6. Play Cornucopia at bar afterwards



Shifting Left



Introduction



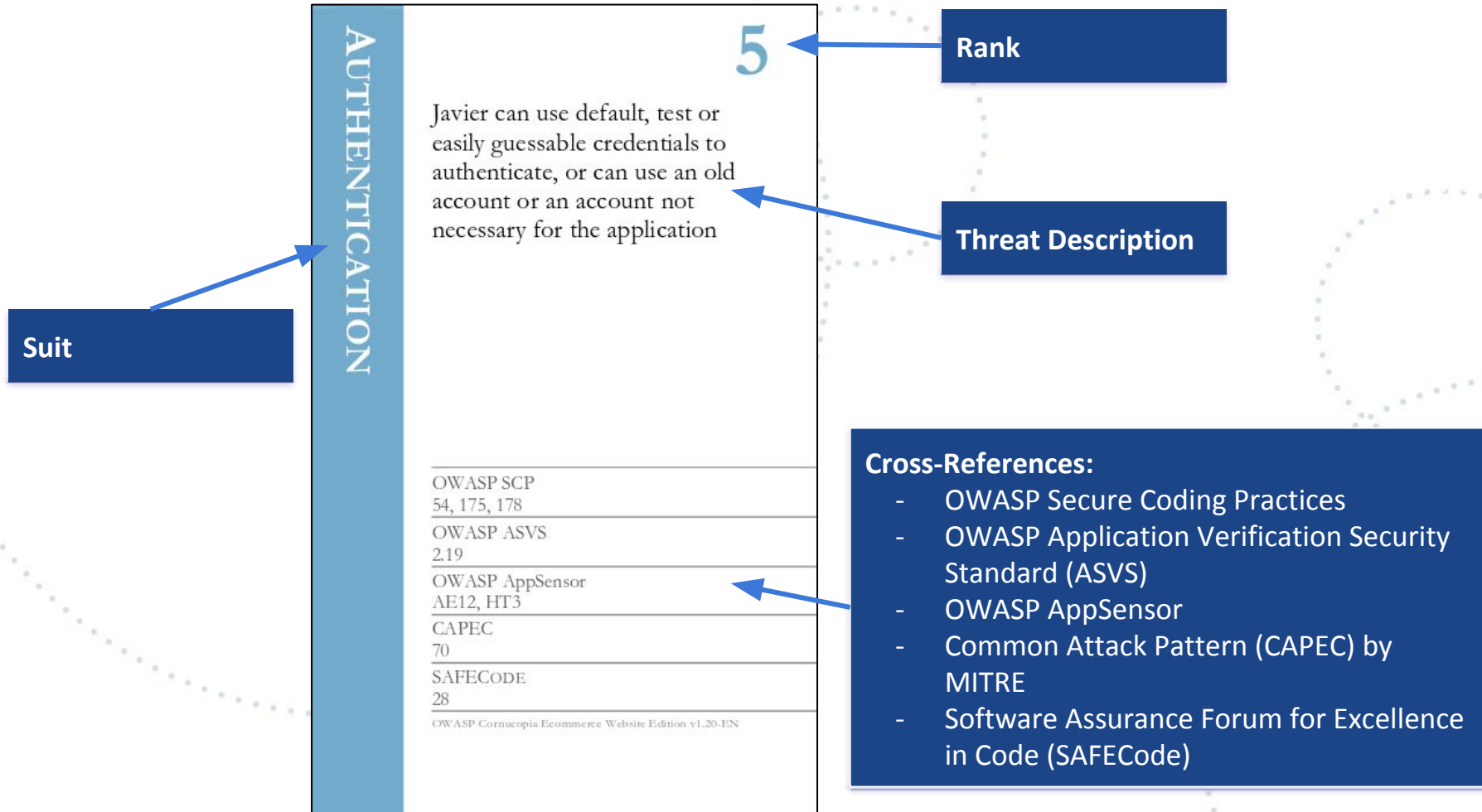
**OWASP Secure Coding Practices
Quick Reference Guide**



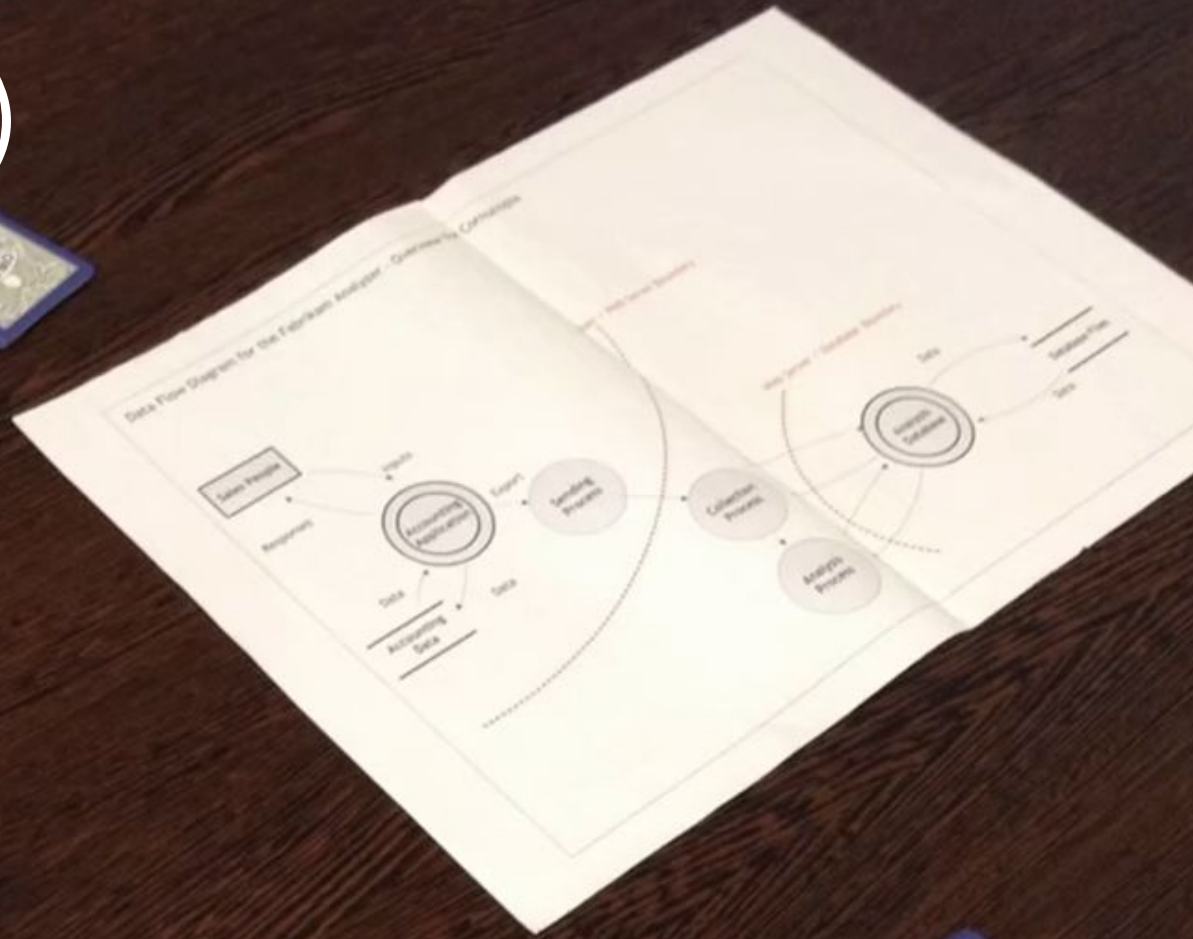
Application Security Verification Standard 3.0.1



Cornucopia Card



How to play (1)



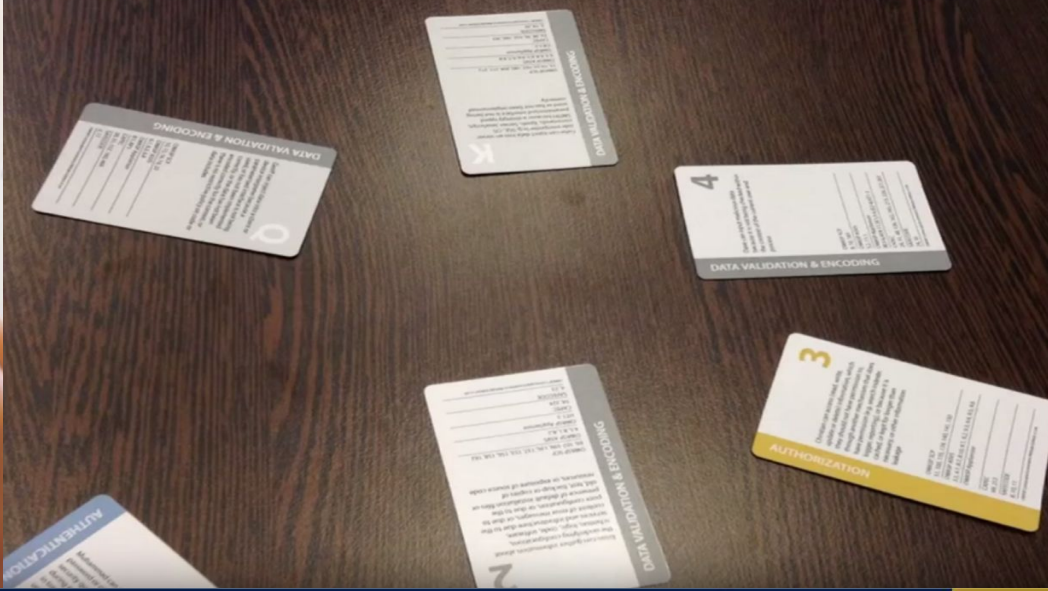
Preparations and Play



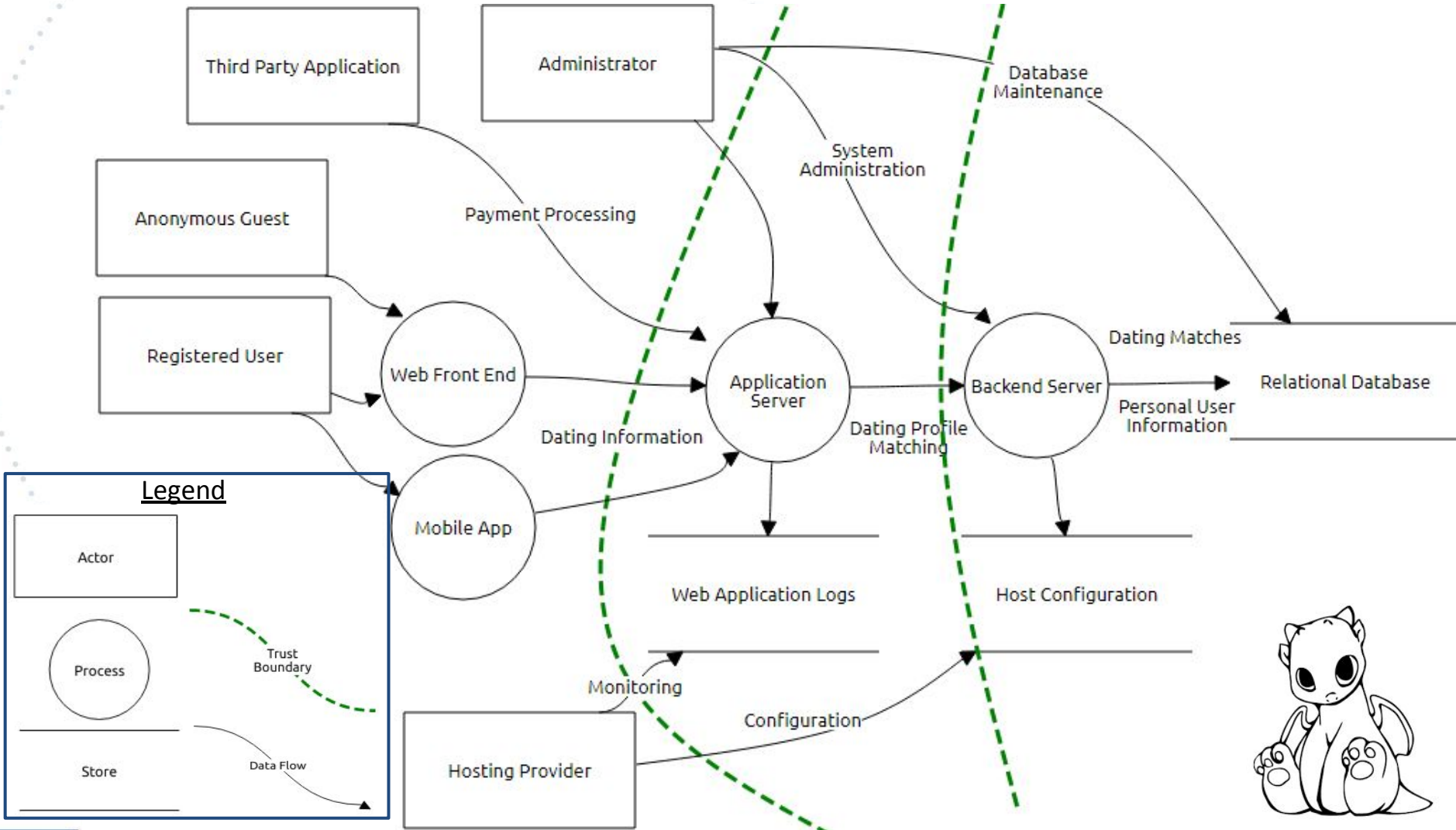
How to play (2)

Category	Item	Example	Exp. Score	Fract. Score	1st	2nd
Data Validation and Encoding (VE)	2	ALREADY CONFIGURED				
	3	? AND SET A2G				
	4	CONTEXTUAL VALIDATION!				
	5	WHAT IS ENCODED / WHERE?				
	6	ARE CS CHECKS USED EVERYWHERE?				
	7	(CHECKED)				
	8	DO WE SANITIZE CLIENT SIDE?				
	9	? CHECK				
	10	LOCAL STORAGE!				
	11	CLIENT SIDE VALIDATION ONLY?				
	12	HTMLS INJECTION				
Session Management (SM)	2					
	3					
	4					
	5					
	6					
	7					
	8					
	9					
	10					
	11					
	12					
Cryptography (CS)	2	(NO OBJECTION)				
	3	HTMLS LOCAL STORAGE?				
	4	(N/A)				
	5	(NONE)				
	6	(TLS ONLY)				
	7	(OUT OF SCOPE - DEFINED)				
	8	(VARIABLE SECURITY)				
	9	DO WE USE RANDOM NUMBERS?				
	10	(NONE)				
	11	(NONE)				
	12	(NONE)				
Authentication (AT)	2	DISPLAY HISTORY + ALERT USER BY EMAIL				
	3	LOCAL CACHED CREDENTIALS?				
	4	SAMESite COOKIES GUESSES USERNAMES - OBTAIN				
	5	TEST ACCOUNTS?				
	6	(NO TOTP PASSWORDS)				
	7	CHECK MFA CORPORATE POLICY				
	8	(FAILS SECURE)				
	9	(NO RE-AUTH)				
	10					
	11					
	Authorization (A)	2	CAN ADMIN / REP BE IMPLEMENTED?			
3		(NO SPLIT FUNCTION)				
4		(N/A)				
5		(N/A)				
6		CHECK DATA LEVEL A-Z				
7		(NOT POSSIBLE)				
8		CHECK PROCESS ALLOW ENFORCEMENT				
9		(DO NOT CHECK / WITH ROUTING)				
10						
11						
Cryptography (C)		2				
	3					
	4					
	5					
	6					
	7					
	8					
	9					
	10					
	11					

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)

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

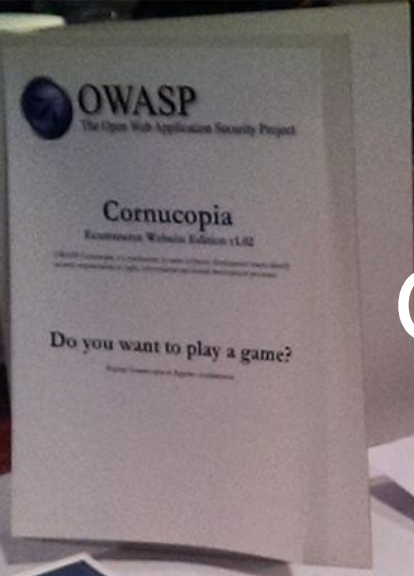
Agile User Stories

Requirements
Engineering

Security Championship

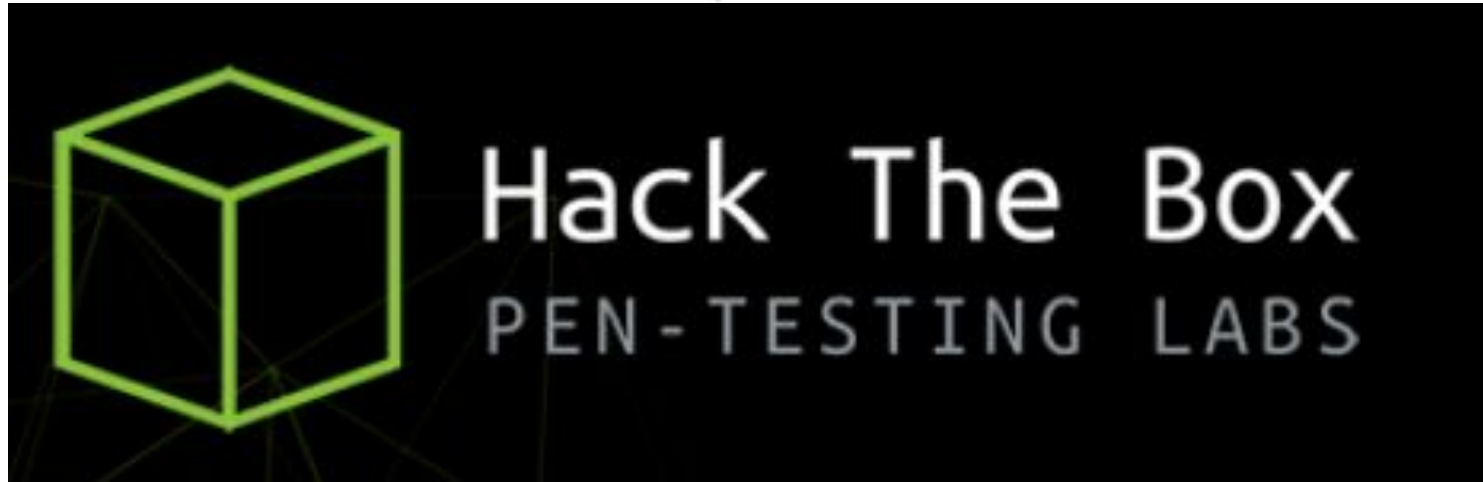


Game Time!



OWASP 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

