OWASP

OWASP

> The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

Core Values

- **Open**: Everything at OWASP is radically transparent from our finances to our code.
- **Innovative**: We encourage and support innovation and experiments for solutions to software security challenges.
- **Global**: Anyone around the world is encouraged to participate in the OWASP community.
- **Integrity**: Our community is respectful, supportive, truthful, and vendor neutral

OWASP Projects

OWASP Projects

An OWASP project is a collection of related tasks that have a defined roadmap and team members.

Project Type	Examples
Tool	ZAP, Dependency Check, DefectDojo, Juice Shop
Code	ModSecurity Core Rule Set
Documentation	OWASP Top 10, Application Security Verification Standard (ASVS), Cornucopia

Project Lifecycle

Level	Icon	Description
Incubator		OWASP Incubator projects represent the experimental playground where projects are still being fleshed out, ideas are still being proven, and development is still underway.
Labs		OWASP Labs projects represent projects that have produced an OWASP reviewed deliverable of value.
Flagship		The OWASP Flagship designation is given to projects that have demonstrated strategic value to OWASP and application security as a whole.

OWASP Chapters

OWASP Chapters

> OWASP Local Chapters build community for application security professionals around the world. Our Local Chapter Meetings are free and open to anyone to attend so both members and non-members are always welcomed. Local meetings include:
>
> - Training to improve your skills
> - Talks relevant to your work
> - Networking opportunities

OWASP German Chapter

There is one Chapter for Germany in total which is complemented by a so-called OWASP Stammtisch each in several metropolitan areas such as München, Frankfurt, Hamburg, Stuttgart, Köln, Hannover, Karlsruhe, Dresden, Ruhrpott, Heilbronn-Franken.

OWASP
German Chapter

Mandatory Chapter Rules

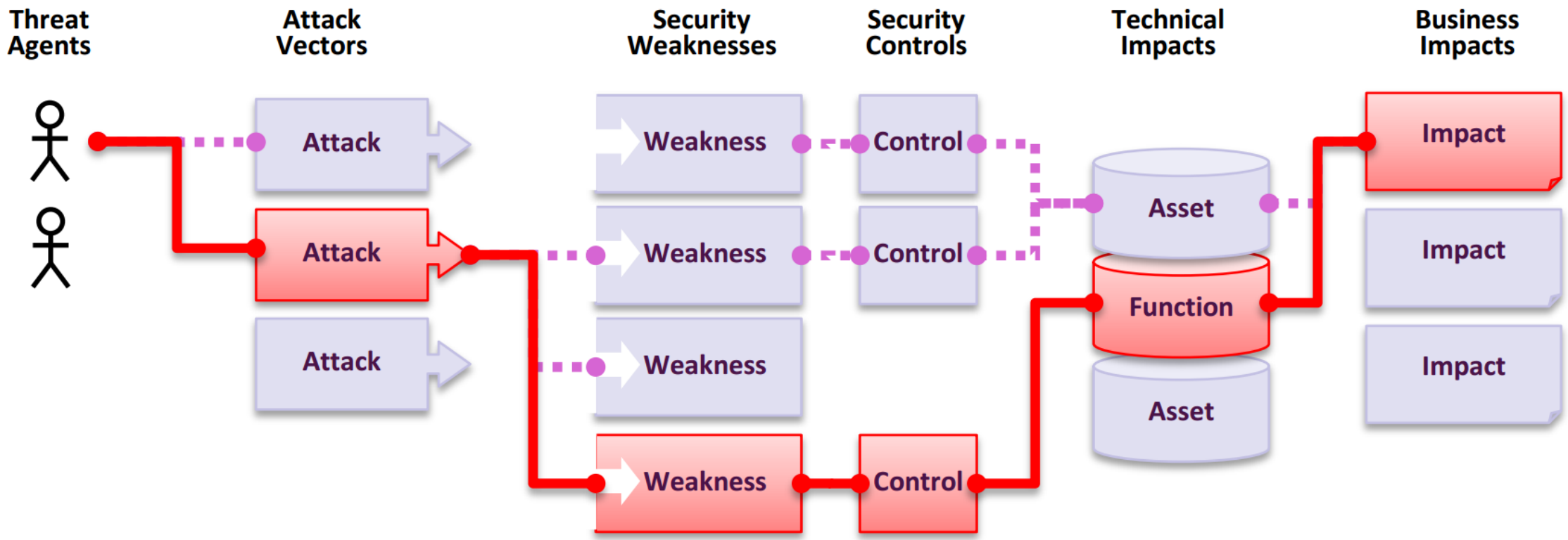
- Organize free and open meetings
- Hold a minimum of 4 chapter meetings or events each year
- Give official notice on the website and chapter mailing list
- Abide by OWASP principles and the code of ethics
- Protect the privacy of the chapter's local contacts
- Maintain vendor neutrality (act independently)
- Spend any chapter funds in accordance with the OWASP goals, code of ethics, and principles

OWASP Top 10

OWASP Top 10

1	Injection	6	Security Misconfiguration
2	Broken Authentication	7	Cross-Site-Scripting (XSS)
3	Sensitive Data Exposure	8	Insecure Deserialization
4	XML External Entities	9	Using Components with Known Vulnerabilities
5	Broken Access Control	10	Insufficient Logging & Monitoring

Application Security Risks

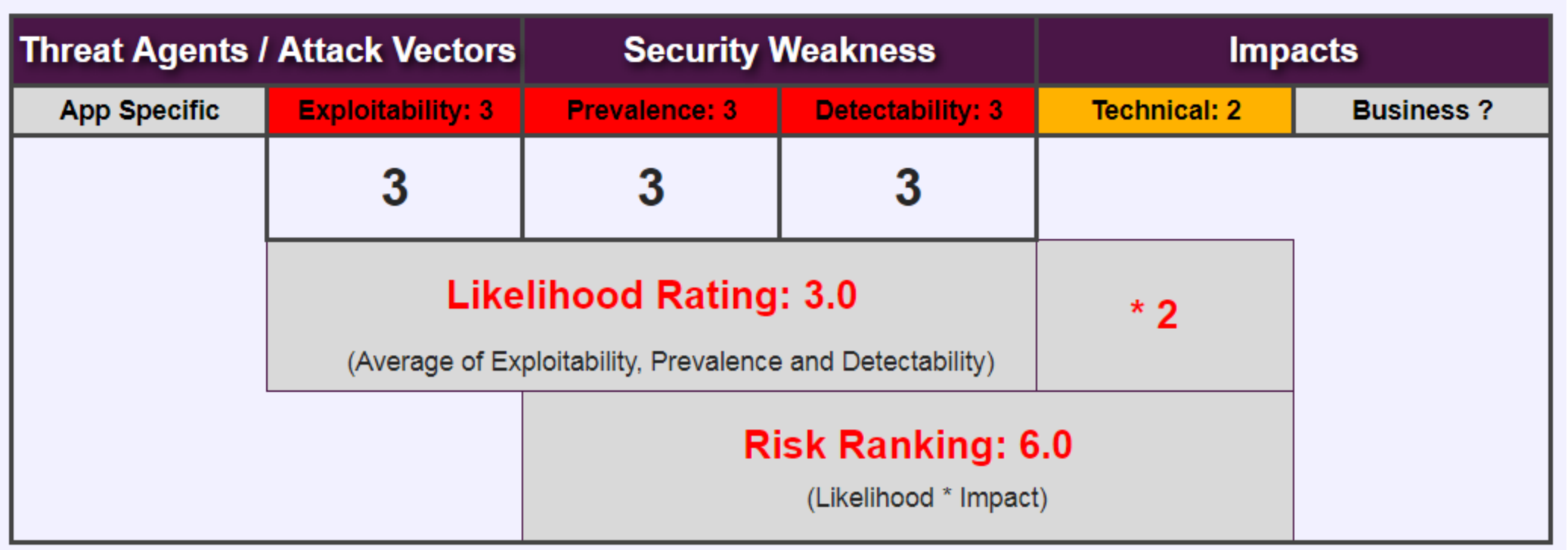


Risk Rating Table

Threat Agents	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	SEVERE: 3	App / Business Specific
	AVERAGE: 2	COMMON: 2	AVERAGE: 2	MODERATE: 2	
	DIFFICULT: 1	UNCOMMON: 1	DIFFICULT: 1	MINOR: 1	

ℹ *Based on the OWASP Risk Rating Methodology*

Risk Calculation Example



Top 10 Risk Factor Summary

Risk	Threat Agents	Attack Vectors (Exploitability)	Security Weakness (Prevalence)	Security Weakness (Detectability)	Impacts (Technical)	Impacts (Business)	Score
A1:2017-Injection	App Specific	EASY: 3	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	8.0
A2:2017-Broken Authentication	App Specific	EASY: 3	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A3:2017-Sensitive Data Exposure	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A4:2017-XML External Entities (XXE)	App Specific	AVERAGE: 2	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	7.0
A5:2017-Broken Access Control	App Specific	AVERAGE: 2	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	6.0
A6:2017-Security Misconfiguration	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A7:2017-Cross-Site Scripting (XSS)	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A8:2017-Insecure Deserialization	App Specific	DIFFICULT: 1	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	5.0
A9:2017-Vulnerable Components	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	MODERATE: 2	App Specific	4.7
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE: 2	WIDESPREAD: 3	DIFFICULT: 1	MODERATE: 2	App Specific	4.0

Some(!) Additional Risks to Consider

Cross-Site Request Forgery (CSRF)	Unvalidated Forward and Redirects
Uncontrolled Resource Consumption ('Resource Exhaustion', 'AppDoS')	Improper Control of Interaction Frequency (Anti-Automation)
Unrestricted Upload of File with Dangerous Type	Inclusion of Functionality from Untrusted Control Sphere (3rd Party Content)
User Interface (UI) Misrepresentation of Critical Information (Clickjacking etc.)	Server-Side Request Forgery (SSRF)

Other Resources on AppSec

- **SANS** Software Security Community
  - CWE/SANS TOP 25 Most Dangerous Software Errors
  - Securing Web Application Technologies [SWAT] Checklist
- **CWE** Common Weakness Enumeration
  - Community-developed list of common software security weaknesses

OWASP Juice Shop

OWASP Juice Shop

> OWASP Juice Shop is probably the most modern and sophisticated insecure web application! It can be used in security trainings, awareness demos, CTFs and as a guinea pig for security tools! Juice Shop encompasses vulnerabilities from the entire OWASP Top Ten along with many other security flaws found in real-world applications!

Main Selling Points

- **Free and Open source**: Licensed under the MIT license with no hidden costs or caveats
- **Easy-to-install**: Choose between node.js, Docker and Vagrant to run on Windows/Mac/Linux
- **Self-contained**: Additional dependencies are pre-packaged or will be resolved and downloaded automatically
- **Beginner-friendly**: Hacking Instructor tutorial scripts guide users through several of the easier challenges while explaining the underlying vulnerabilities
- **Gamification**: The application notifies you on solved challenges and keeps track of successfully exploited vulnerabilities on a Score Board

- **Self-healing**: The simple SQLite and MarsDB databases are wiped and repopulated from scratch on every server startup
- **Re-branding**: Fully customizable in business context and look & feel to your own corporate or customer requirements
- **CTF-support**: Challenge notifications optionally contain a flag code for your own Capture-The-Flag events

Installation

- Individual local instance per student
- Runs on node.js, Docker, Vagrant and in the ☁️

⚠️ Hacking Rules

- Do **not** look at the source code on GitHub
- Do **not** look at GitHub issues, PRs etc.
- Do **not** cheat (with online tutorials or walkthroughs) before trying
- Report problems during exercises immediately

Official Companion Guide

> Pwning OWASP Juice Shop [...] will give you a complete overview of the vulnerabilities found in the application including hints how to spot and exploit them. In the appendix you will even find complete step-by-step solutions to every challenge. The ebook is published under CC BY-NC-ND 4.0 and is available **for free** online-readable. The latest officially released edition is available **for free** on LeanPub in PDF, Kindle and ePub format.

THIS IS THE OFFICIAL COMPANION GUIDE TO THE OWASP JUICE SHOP APPLICATION. BEING A WEB APPLICATION WITH A VAST NUMBER OF INTENDED SECURITY VULNERABILITIES, THE OWASP JUICE SHOP IS SUPPOSED TO BE THE OPPOSITE OF A BEST PRACTICE OR TEMPLATE APPLICATION FOR WEB DEVELOPERS: IT IS AN AWARENESS, TRAINING, DEMONSTRATION AND EXERCISE TOOL FOR SECURITY RISKS IN MODERN WEB APPLICATIONS. THE OWASP JUICE SHOP IS AN OPEN-SOURCE PROJECT HOSTED BY THE NON-PROFIT OPEN WEB APPLICATION SECURITY PROJECT (OWASP) AND IS DEVELOPED AND MAINTAINED BY VOLUNTEERS.

BJÖRN KIMMINICH HAS OVER TWO DECADES OF PROGRAMMING EXPERIENCE WITH EXPERTISE ON SOFTWARE SUSTAINABILITY, CLEAN CODE AND TEST AUTOMATION AS WELL AS APPLICATION SECURITY. HE IS THE PROJECT LEADER OF THE OWASP JUICE SHOP AND MEMBER OF THE GERMAN OWASP CHAPTER BOARD.

Exercise 1.1

Install the OWASP Juice Shop `v11.x`

1. Install the latest Node.js 12.x (or 14.x) release on your computer
2. On https://github.com/bkimminich/juice-shop#setup follow the instructions for either
   - From Sources or
   - Packaged Distributions

🐳 *If you want to use Docker you need to run the container with* `docker run -d -e "NODE_ENV=unsafe" -p 3000:3000 bkimminich/juice-shop` *or you won't be able to solve several of the exercises.*

Exercise 1.2

Happy path shopping tour

1. Register a user account at your local Juice Shop
2. Browse the inventory and purchase some products
3. Try out all other functionality you find in the application

Exercise 1.3

Score Board

1. Find the hidden Score Board in the Juice Shop (⭐)

ℹ️ *You can let the application's friendly Hacking Instructor guide you through this exercise by clicking "Help getting started" on the welcome banner or in the side bar.*

Exercise 1.4 *(optional)*

Transfer your hacking progress

1. Open your browser's developer tools (`F12` in Chrome/Firefox)
2. Find the cookie `continueCode` and copy its value to your other computer
3. Install OWASP Juice Shop on your other computer and launch it
4. `F12` into the developer tools and create the cookie `continueCode` with the value from your first computer
5. Restart the Juice Shop server