



CORNUCOPIA

Ecommerce website edition

OWASP Cornucopia is a card game used to help derive application security requirements during the software development life cycle. See the project website about how to get hold of a copy and ready-printed decks.

Cornucopia “Ecommerce Website Edition” is based the concepts and game ideas in Microsoft’s open source Elevation of Privilege: The Threat Modeling Game (EoP), but those have been modified to be more relevant to the types of issues ecommerce website developers encounter.

Cornucopia suits are based on the structure of the OWASP Secure Coding Practices - Quick Reference Guide (SCP), but with additional consideration of sections in the OWASP Application Security Verification Standard (ASVS), the OWASP Testing Guide and David Rook’s Principles of Secure Development. These provide five suits, and a sixth called “Cornucopia” contains everything else:

- Data validation and encoding
- Authentication
- Session management
- Authorization
- Cryptography
- Cornucopia.

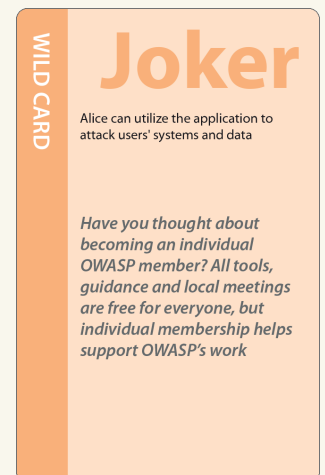
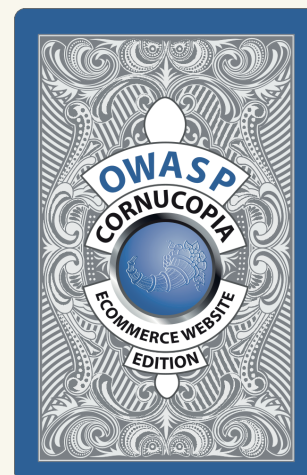
Each card is mapped to Mitre’s CAPEC software attack pattern IDs, 36 SAFECODE’s Agile security stories, OWASP ASVS v2 2014 and OWASP AppSensor attack detection points, as well as to the OWASP SCP v2.

Cornucopia is developed, maintained, updated and promoted by volunteers. The contributors to date are Simon Bennetts, Tom Brennan, Fabio Cerullo, Tobias Gondrom, Anthony Harrison, Ken Ferris, Jerry Hoff, Jim Manico, Mark Miller, Cam Morris, Stephen de Vries, and project leader Colin Watson.



Cornucopia introduces threat-modelling ideas into development teams that use Agile methodologies, or are more focused on web application weaknesses than other types of software vulnerabilities, or are not familiar with STRIDE and DREAD.

Created by Colin Watson. OWASP Cornucopia is free to use. It is licensed under the Creative Commons Attribution-ShareAlike 3.0 license.





SNAKES and LADDERS

For web applications / For mobile apps

OWASP Snakes and Ladders is an educational board game. It uses gamification to promote awareness of application security controls and risks, and in particular knowledge of other OWASP documents and tools. Download and print the game yourself.

Snakes and Ladders is a popular board game with ancient provenance, imported into Great Britain from Asia in the 19th century. The original game showed the effects of good and evil, or virtues and vices. This OWASP game is a poster-sized print-your-own paper sheet with the game board on it. Just get some players together with a die and counters. The virtues are application security controls, and the vices are risks.

This board game was created to use as an ice-breaker in application security training, but it potentially has wider appeal simply as a promotional hand-out, and maybe also more usefully as learning materials for younger coders. To cover all of that, we use the phrase:

"OWASP Snakes and Ladders is meant to be used by software programmers, big and small"

The game is quite lightweight, and does not have the same rigour or depth as the card game Cornucopia (see overleaf), but it is meant to be just some fun with some associated learning.

Print-ready PDFs have been published. We recommend playing using a real die and counters (markers), but you can cut out and make these from the paper sheet itself if you have scissor and glue skills.

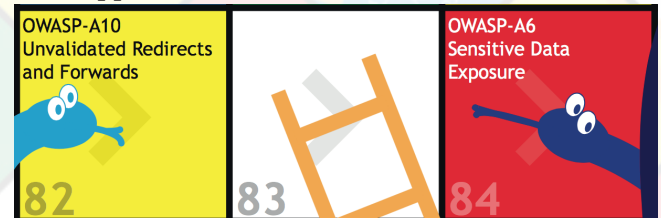
We hope it may be of use in any upcoming office party, celebration, festival, seasonal event, application security awareness or training exercise. Or just to help spread the word about controls and risks at work, at college or at school.

If you are training anyone about the OWASP Top Ten, OWASP Proactive Controls or the OWASP Mobile projects, please consider giving each attendee a printed copy of the game as a take away.

Created by Colin Watson. OWASP Snakes and Ladders is free to use. It is licensed under the Creative Commons Attribution- ShareAlike 3.0 license.

There are two editions of the board game:

Web Applications



DE: Deutsch EN: English ES: Español
FR: Français JA: 日本語 ZH: 中文

In the board game for web applications, the virtuous behaviours (ladders) are secure coding practices from OWASP Proactive Controls project 2014, and the vices (snakes) are application security risks from OWASP Top Ten Project 2013.

Mobile Apps



EN: English JA: 日本語

The identical board game for mobile apps uses mobile controls from the Mobile Security Project Top Ten Controls 2013 as the virtuous behaviours, and mobile risks from the Top Ten Mobile Risks 2014 from the same project as the vices.

Snakes and Ladders is developed, maintained, updated and promoted by volunteers. The contributors to date are Katy Anton, Manuel Lopez Arredondo, Fabio Cerullo, Tobias Gondrom, Martin Haslinger, Yongliang He, Cédric Messeguer, Takanori Nakanowatari, Riotaro Okada, Alison Ribeiro, Ivy Zhang, and project leader Colin Watson.