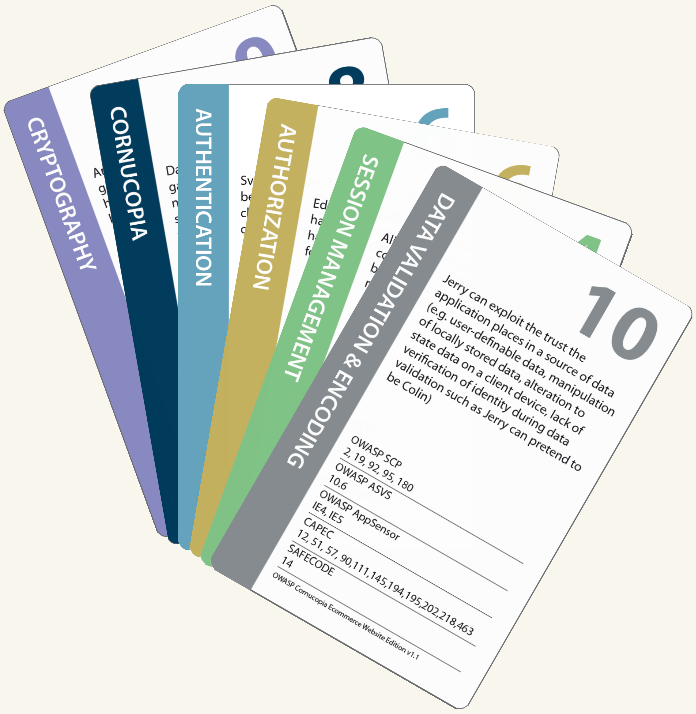
OWASP
Open Web Application
Security Project

CORNUCOPIA
Ecommerce website edition

OWASP Cornucopia is a card game used to help derive application security requirements during the software development life cycle.

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.



Jerry can exploit the trust the application places in a source of data (e.g. user-definable data, manipulation of locally stored data, alteration to state data on a client device, lack of verification of identity during data validation such as Jerry can pretend to be Colin)

OWASP SCP
2, 19, 92, 95, 180
OWASP ASVS
10.6
OWASP AppSensor
IE4, IE5
CAPEC
12, 51, 57, 90,111,145,194,195,202,218,463
SAFECODE
14

OWASP Cornucopia Ecommerce Website Edition v1.1

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 other threat modelling techniques.

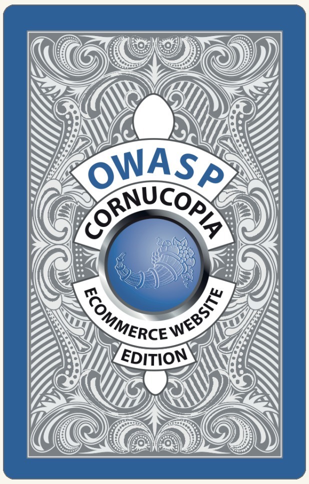
Created by Colin Watson. Ideas have been submitted, updates suggested, and the game used and promoted by volunteers areound the world. OWASP Cornucopia is free to use. It is licensed under the Creative Commons Attribution-ShareAlike 3.0 license.

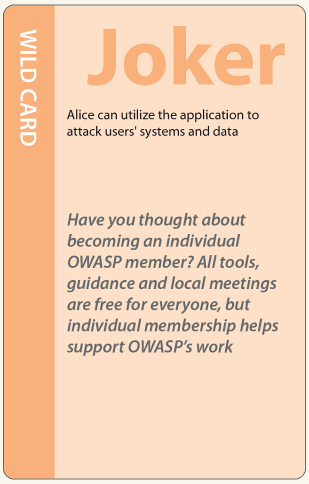
Cornucopia suits are based on the structure of the OWASP Secure Coding Practices - Quick Reference Guide (SCP), but with additional consideration of sections in the OWASP Application Security Verification Standard (ASVS), the OWASP Testing Guide and David Rook’s Principles of Secure Development. These 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 patterns, 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 maintained in Word format, but the data also exists as XML. Print-ready files have also been generously donated, and ready-printed decks can be obtained. See the Cornucopia Project website for details.





Alice can utilize the application to attack users' systems and data

Have you thought about becoming an individual OWASP member? All tools, guidance and local meetings are free for everyone, but individual membership helps support OWASP’s work

https://www.owasp.org/index.php/OWASP_Cornucopia @OWASPCornucopia

OWASP
Open Web Application
Security Project

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.

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.

The 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.

Play 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.

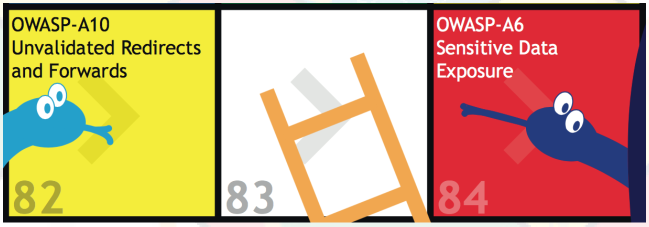
Use the game for an office party, celebration, festival, seasonal event, application security awareness, or training exercise. Or just to help spread the word about controls and risks at work, at college or at school.

For training related to the OWASP Top Ten, OWASP Proactive Controls, or the OWASP Mobile projects, consider giving each attendee a printed copy of the game as a take away.

Created by Colin Watson. Translated by other volunteers around the world. 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 the OWASP Proactive Controls Project 2014, and the vices (snakes) are application security risks from the OWASP Top Ten Project 2013.

Mobile Apps

40
OWASP-C4
ユーザー認証、認可
および
セッション管理の
正しい実装
OWASP-M4
意図しない
データ漏えい
39
38

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 available to download as print-ready PDFs and also in the source Illustrator format. Print them as large as you can - they are designed for the international A2 size. For individual sheets and small quantities, digital printing is most economic, but for quantities of a few hundred or more, lithographic printing can be better value.

https://www.owasp.org/index.php/OWASP_Snakes_and_Ladders @OWASPSnakesWeb / @OWASPSnakesMob