Created by Colin Watson Version MobApp-1.02-EN (Farringdon)

OWASP Snakes and Ladders
- Mobile Apps -

Snakes and Ladders is an educational application security awareness game. This version is all about mobile applications, with the OWASP Top Ten Mobile Controls as ladders, and the OWASP Top Ten Mobile Risks as snakes. Thank you to the leaders and other contributors to these.

OWASP Top Ten Mobile Controls (2013)

The OWASP Top Ten Mobile Controls is a list of development controls that should be used to reduce the impact or likelihood of exploitation.

- C1 Identify and Protect Sensitive Data on the Mobile Device
- C2 Handle Password Credentials Securely on the Device
- C3 Ensure Sensitive Data is Protected in Transit
- C4 Implement User Authentication, Authorization and Session Management Correctly
- C5 Keep the Backend APIs (Services) and the Platform (Server) Secure
- C6 Secure Data Integration with Third Party Services and Applications
- C7 Pay Specific Attention to the Collection and Storage of Consent for the Collection and Use of the User's Data
- C8 Implement Controls to Prevent Unauthorized Access to Paid-for Resources (wallet, SMS, phone calls, etc)
- C9 Ensure Secure Distribution/Provisioning of Mobile Apps
- C10 Carefully Check Any Runtime Interpretation of Code for Errors

OWASP Top Ten Mobile Risks (2014)

The OWASP Top Ten Mobile Risks represents a broad consensus about what the most critical mobile app risks at the application layer are.

- M1 Weak Server Side Controls
- M2 Insecure Data Storage
- M3 Insufficient Transport Layer Protection
- M4 Unintended Data Leakage
- M5 Poor Authorization and Authentication
- M6 Broken Cryptography
- M7 Client Side Injection
- M8 Security Decisions Via Untrusted Inputs
- M9 Improper Session Handling
- M10 Lack of Binary Protections

Both the controls and risks are detailed in one OWASP project https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

The source file for this sheet, sheets on other application security topics, various language versions, and further information about the project can be found at https://www.owasp.org/index.php/OWASP_Snakes_and_Ladders

Background

Snakes and Ladders is a popular board game, imported into Great Britain by the Victorians based on a game from Asia. The original game showed the effects of good and evil, or virtues and vices. The game is known as Chutes and Ladders in some parts of the Americas. In this OWASP version, the virtuous behaviours are secure coding practices and the vices are mobile app security risks.

Warning

OWASP Snakes and Ladders is meant to be used by software programmers, big and small. This paper game sheet is not harmful, but if you choose to use your own plastic or wooden die and counters, those might have a choking risk for children under 4 years old.

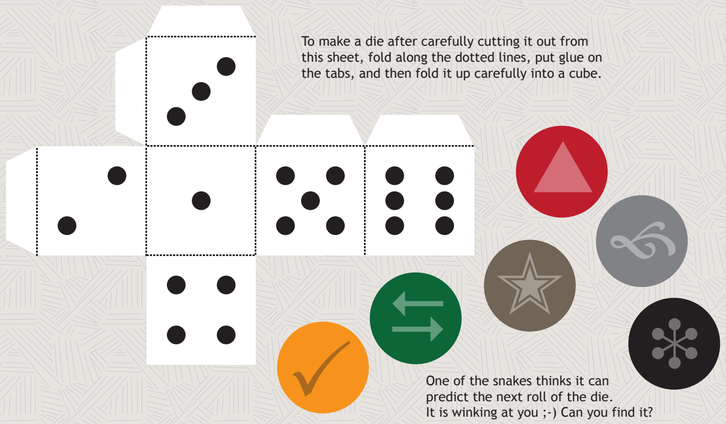
Rules

This game is for 2-6 players. Give each player a coloured counter (marker). To begin, each player should throw the die to determine who plays first; the highest can lead. Put all the player's counters onto the first square labelled "Start 1". In turn, each player rolls the die and moves their counter by the number of squares indicated on the die.

At the end of the move, if a player's counter is at the bottom end of a ladder, the counter must be moved up the ladder to the square at its higher end. Conversely, if the player's counter is located at the mouth of a snake, the counter must be moved down to the end of the snake's tail.

The first player to reach "100" at the top left wins.

No die or counters? Cut the shapes out below use the coloured circles as counters for each player. Alternatively write a computer program to simulate a six-sided die, or use a random number generator app on your phone or computer to create integers between 1 and 6. Check how random it is though!



To make a die after carefully cutting it out from this sheet, fold along the dotted lines, put glue on the tabs, and then fold it up carefully into a cube.

One of the snakes thinks it can predict the next roll of the die. It is winking at you ;-) Can you find it?

Project Leader

Colin Watson

Translators / Other Contributors

Manuel Lopez Arredondo, Fabio Cerullo, Tobias Gondrom, Martin Haslinger, Yongliang He, Cédric Messeguer, Takanori Nakanowatari, Riotaro Okada, Ferdinand Vroom, Ivy Zhang