

Created by Colin Watson

Version WebApp-1.01-EN (Classic)

OWASP Snakes and Ladders - Web Applications -

Snakes and Ladders is an educational application security awareness game. This version is all about web applications, with the OWASP Top Ten Proactive Controls as ladders, and the well-known OWASP Top Ten Most Critical Risks as snakes. Thank you to the leaders and other contributors of those two projects.

OWASP Top Ten Proactive Web Application Controls (2014)

The OWASP Top Ten Proactive Controls is a list of security techniques that should be included in every software development project.

- C1 Parameterize Queries
- C2 Encode Data
- C3 Validate All Inputs
- C4 Implement Appropriate Access Controls
- C5 Establish Identity and Authentication Controls
- C6 Protect Data and Privacy
- C7 Implement Logging, Error Handling and Intrusion Detection
- C8 Leverage Security Features of Frameworks and Security Libraries
- C9 Include Security-Specific Requirements
- C10 Design and Architect Security In

https://www.owasp.org/index.php/OWASP_Proactive_Controls

OWASP Top Ten Most Critical Web Application Risks (2013)

The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are.

- A1 Injection
- A2 Broken Authentication and Session Management
- A3 Cross-Site Scripting (XSS)
- A4 Insecure Direct Object References
- A5 Security Misconfiguration
- A6 Sensitive Data Exposure
- A7 Missing Function Level Access Control
- A8 Cross-Site Request Forgery (CSRF)
- A9 Using Components with Known Vulnerabilities
- A10 Unvalidated Redirects and Forwards

<https://www.owasp.org/index.php/TopTen>

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

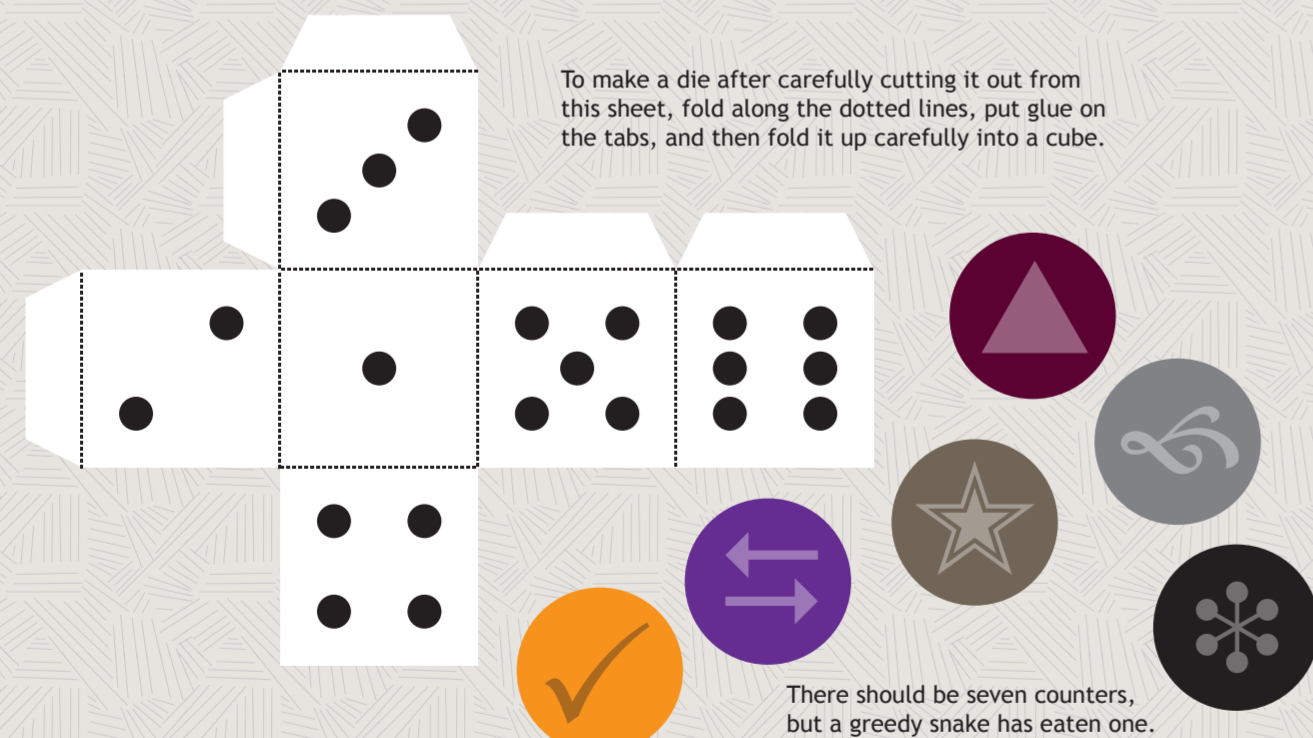
Background

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 (the proactive controls) and the vices are application 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.

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!



Project Leader

Colin Watson

Translators / Other Contributors

Manuel Lopez Arredondo, Fabio Cerullo, Tobias Gondrom, Martin Haslinger, Riatora Okada, Ferdinand Vroom, Ivy Zhang

OWASP Snakes and Ladders is free to use. It is licensed under the Creative Commons Attribution-ShareAlike 3.0 licence, so you can copy, distribute and transmit the work, and you can adapt it, and use it commercially, but all provided that you attribute the work and if you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar licence to this one. © OWASP Foundation 2014.

Finish (100)

Start (1)

OWASP-A1 Injection (96)

OWASP-A9 Using Components with Known Vulnerabilities (92)

OWASP-A10 Unvalidated Redirects and Forwards (82)

OWASP-A6 Sensitive Data Exposure (84)

OWASP-A5 Security Misconfiguration (89)

OWASP-A8 Cross-Site Request Forgery (CSRF) (76)

OWASP-A4 Insecure Direct Object References (78)

OWASP-A7 Missing Function Level Access Control (37)

OWASP-A2 Broken Authentication and Session Management (35)

OWASP-C10 Design and Architect Security In (64)

OWASP-C7 Implement Logging, Error Handling and Intrusion Detection (36)

OWASP-C6 Protect Data and Privacy (34)

OWASP-C9 Include Security-Specific Requirements (52)

OWASP-C8 Leverage Security Features of Frameworks and Security Libraries (42)

OWASP-A3 Cross-Site Scripting (XSS) (27)

OWASP-C5 Establish Identity and Authentication Controls (29)

OWASP-C4 Implement Appropriate Access Controls (19)

OWASP-C3 Validate All Inputs (12)

OWASP-C2 Encode Data (8)

OWASP-C1 Parameterize Queries (5)