OWASP Cornucopia

BACKGROUND

OWASP = Open Web Application Security Project

https://owasp.org/#

OWASP

PROJECTS CHAPTERS EVENTS ABOUT

Search OWASP.org

Donate

Join

Who is the OWASP® Foundation?

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.

- Tools and Resources
- Community and Networking
- Education & Training

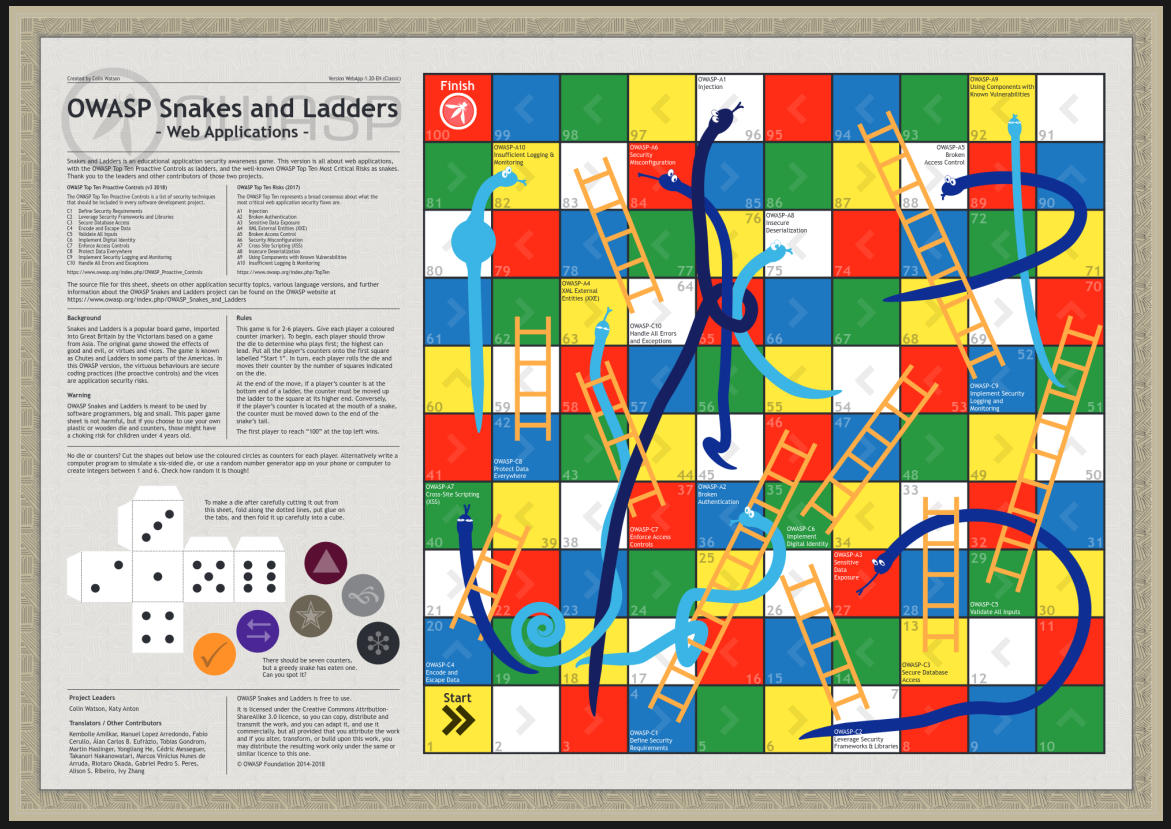
For nearly two decades corporations, foundations, developers, and volunteers have supported the OWASP Foundation and its work. Donate, Join, or become a Corporate Member today.

PEN-AND-PAPER GAMES OWASP

Snakes and Ladders

Cornucopia

Side note: Snakes and Ladders



Created by Colin Watson Version WebApp-1.30-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 Controls (v3 2018)

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

C1 Define Security Requirements
C2 Leverage Security Frameworks and Libraries
C3 Secure Database Access
C4 Encode and Escape Data
C5 Validate All Inputs
C6 Implement Digital Identity
C7 Enforce Access Controls
C8 Protect Data Everywhere
C9 Implement Security Logging and Monitoring
C10 Handle All Errors and Exceptions

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

OWASP Top Ten Risks (2017)

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

A1 Injection
A2 Broken Authentication
A3 Sensitive Data Exposure
A4 XML External Entities (XXE)
A5 Broken Access Control
A6 Security Misconfiguration
A7 Cross-Site Scripting (XSS)
A8 Insecure Deserialization
A9 Using Components with Known Vulnerabilities
A10 Insufficient Logging & Monitoring

https://www.owasp.org/index.php/Top10

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.

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.

There should be seven counters, but a greedy snake has eaten one. Can you spot it?

Project Leaders

Colin Watson, Katy Anton

Translators / Other Contributors

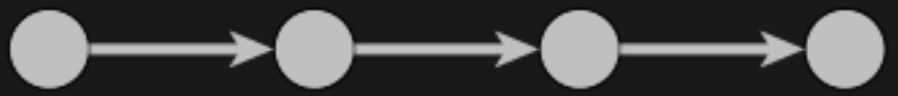
Kembolle Amilkar, Manuel Lopez Arredondo, Fabio Cerullo, Alan Carlos B. Eufrásio, Tobias Gondrom, Martin Haslinger, Yonglang He, Cédric Messeguer, Takanori Nakanowatari, Marcos Vinicius Nunes de Arruda, Rintaro Okada, Gabriel Pedro S. Peres, Alison S. Ribeiro, Ivy Zhang

Cornucopia: Heavily based on EoP

FOCUS

Primarily for Webapplication-Analysis

GAMEPLAY



Choose first player by chance

Different topics

Different colors

Turn based

Proposals

Valid for all players?

Proposals

Valid for all players?

Current player gets

+1

Proposals

Valid for all players?

Current player gets

+1

A winner every round

Order A, K, Q, 10 ... 2

A winner every round

Order A, K, Q, 10 ... 2

Winner scores

+1

A winner every round

Order A, K, Q, 10 ... 2

Winner scores

+1

Round over

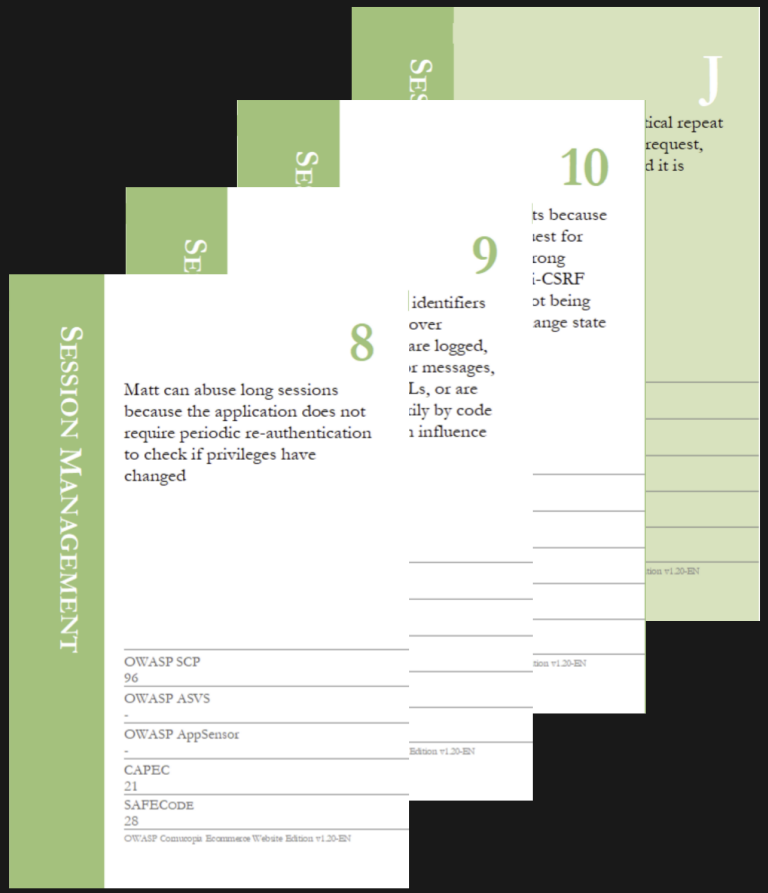
Winner chooses new topic

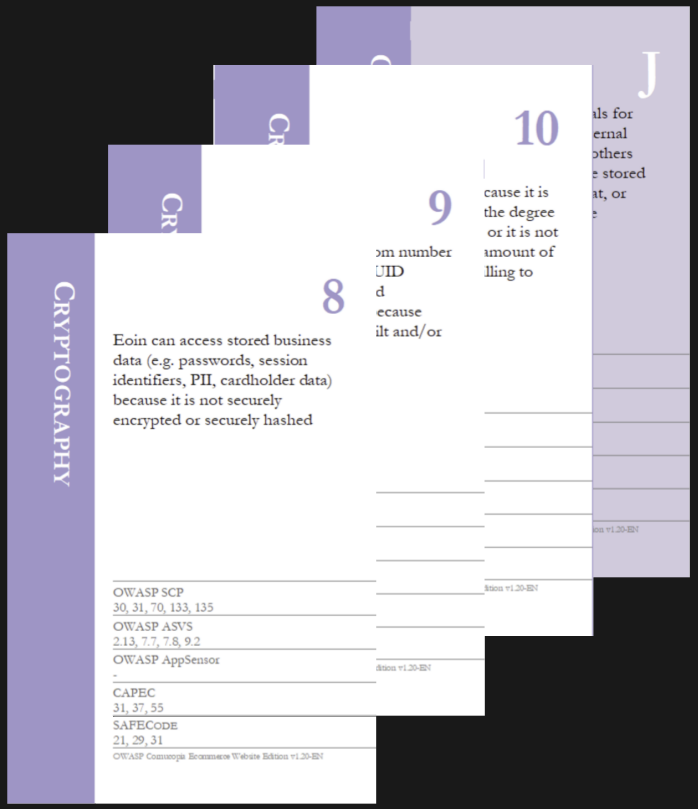
TOPICS

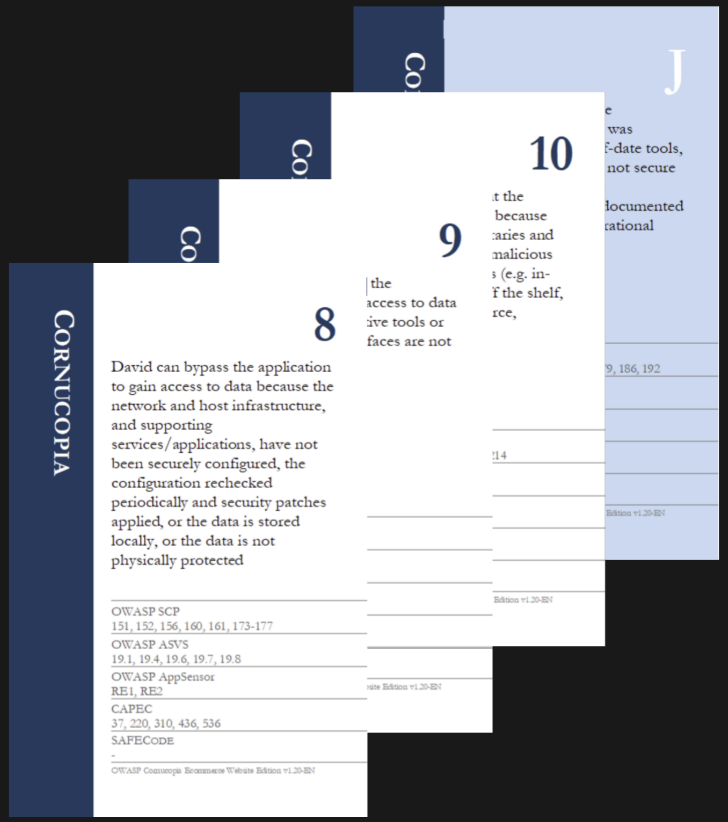
8	9	10	J
Sarah can bypass the centralized sanitization routines since they are not being used comprehensively	put alidation ion failures r sanitized	trust the source of le data, y stored e data on a erification validation end to be	over input alidation or de or routines ssed
OWASP SCP 15, 169			
OWASP ASVS 1.7, 5.21, 5.23		.5, 16.8	
OWASP AppSensor -			
CAPEC 28, 31, 152, 160, 468		5,202,218,463	
SAFECode 2, 17			


AUTHENTICATION
8
Kate can bypass authentication because it does not fail secure (i.e. it defaults to allowing unauthenticated access)
OWASP SCP
28
OWASP ASVS
2.6
OWASP AppSensor
-
CAPEC
115
SAFECODE
28
OWASP Cornucopia Ecommerce Website Edition v1.20-EN
9
10
J
resources or
there is no
equirement, or it
assumed
would be
ome other system
some previous


AUTHORIZATION
8
Tom can bypass business rules by altering the usual process sequence or flow, or by undertaking the process in the incorrect order, or by manipulating date and time values used by the application, or by using valid features for unintended purposes, or by otherwise manipulating control data
OWASP SCP
10, 32, 93, 94, 189
OWASP ASVS
4.10, 4.15, 4.16, 8.13, 15.1
OWASP AppSensor
ACE3
CAPEC
25, 39, 74, 162, 166, 207
SAFECODE
8, 10, 11, 12
OWASP Cornucopia Ecommerce Website Edition v1.20-EN
9
10
J


SESSION MANAGEMENT
8
Matt can abuse long sessions because the application does not require periodic re-authentication to check if privileges have changed
OWASP SCP
96
OWASP ASVS
-
OWASP AppSensor
-
CAPEC
21
SAFECODE
28
OWASP Cornucopia Ecommerce Website Edition v1.20-EN
9
identifiers
over
are logged,
r messages,
Ls, or are
ily by code
influence
Edition v1.20-EN
10
ts because
iest for
rong
-CSRF
ot being
ange state
ion v1.20-EN
J
tical repeat
request,
d it is
ion v1.20-EN


J
10
9
8
Cryptography
Eoin can access stored business data (e.g. passwords, session identifiers, PII, cardholder data) because it is not securely encrypted or securely hashed
OWASP SCP
30, 31, 70, 133, 135
OWASP ASVS
2.13, 7.7, 7.8, 9.2
OWASP AppSensor
-
CAPEC
31, 37, 55
SAFECode
21, 29, 31
OWASP Cornucopia Ecommerce Website Edition v1.20-EN


CORNUCOPIA
8
David can bypass the application to gain access to data because the network and host infrastructure, and supporting services/applications, have not been securely configured, the configuration rechecked periodically and security patches applied, or the data is stored locally, or the data is not physically protected
OWASP SCP
151, 152, 156, 160, 161, 173-177
OWASP ASVS
19.1, 19.4, 19.6, 19.7, 19.8
OWASP AppSensor
RE1, RE2
CAPEC
37, 220, 310, 436, 536
SAFECODE
-
OWASP Cornucopia Ecommerce Website Edition v1.20-EN
9
10
J

SCORESHEET

Data Validation and Encoding
8 -
9 -
10 -
J -

Session Management
8 -
9 -
10 -
J -

Cryptography
8 -
9 -
10 -
J -

Authentication
8 -
9 -
10 -
J -

Authorization
8 -
9 -
10 -
J -

Cornucopia
8 -
9 -
10 -
J -

SESSION MANAGEMENT

8

Matt can abuse long sessions because the application does not require periodic re-authentication to check if privileges have changed

OWASP SCP 96
OWASP ASVS -
OWASP AppSensor -
CAPEC 21
SAFECODE 28

Session Management

8 - Set a proper session timeout

9 -

10 -

J -

FURTHER INFORMATION

https://www.youtube.com/watch?v=BZVoQurTEMc

https://www.youtube.com/watch?v=i5Y0akWj31k

https://owasp.org/www-project-cornucopia/

https://owasp.org/www-project-snakes-and-ladders/


ANY QUESTIONS?