



OWASP Cornucopia

BACKGROUND

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

DATA VALIDATION & ENCODING

	8	9	10	J
Sarah can bypass the centralized sanitization routines since they are not being used comprehensively	put validation failures or sanitized	trust the source of the data, only stored data on a verification validation tend to be	over input validation or code or routines passed	
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				
OWASP Compendium Ecommerce Website Edition v1.20-EN	Edition v1.20-EN	Edition v1.20-EN	Edition v1.20-EN	Edition v1.20-EN

AUTHENTICATION

8

Kate can bypass authentication because it does not fail secure (i.e. it defaults to allowing unauthenticated access)

9

Take more because requirements are not use strong such as two ; no -authenticate

10

Authentication centralized even and tion /service, once being used

J

resources or there is no requirement, or it assumed would be some other system some previous

OWASP SCP
28
OWASP ASVS
2.6
OWASP AppSensor
1
CAPEC
115
SAFECODE
28
OWASP Commerce Ecommerce Website Edition v1.20-EN

i
Website Edition v1.20-EN
ite Edition v1.20-EN
Website Edition v1.20-EN



SESSION MANAGEMENT

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 Commerce Ecommerce Website Edition v1.2-EN

8

entifiers
er
e logged,
essages,
, or are
y by code
nfluence

SES

SE

S

SES

10

ts because
iest for
rong
i-CSRF
ot being
ange state

tical repeat
request,
d it is

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
2.1.3, 7.7, 7.8, 9.2
OWASP AppSensor
CAPEC
31, 37, 55
SAFECode
21, 29, 31
OWASP Commerce Ecommerce Website Edition v1.20-EN

CORNUCOPIA

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

1

OWASP Confluence Ecommerce Website Edition v1.20-EN

8

the
access to data
ive tools or
faces are not

10

it the
because
aries and
malicious
s (e.g. in-
f the shelf,
ice,

J

documented
national

2, 186, 192

114

Edition v1.20-EN

SCORESHEET

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

Set a proper
session
timeout

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/>



A large, dark, textured question mark is centered on a light-colored, horizontally-grained wall. The question mark has a thick, dark outline and a lighter, textured interior. It is positioned vertically, with its top curve pointing upwards and its bottom curve pointing downwards.

ANY QUESTIONS?