AGILE TESTING DAYS ONLINE EDITION

OWASP Cornucopia

BACKGROUND

Cornucopia: Heavily based on EoP

FOCUS

Primarily for Webapplication-Analysis

RECAP: GAMEPLAY

Choose first player by chance

Different topics

Different colors

Turn based

Proposals

Valid for all players?

Proposals

Valid for all players?

If not discard card

A winner every round

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

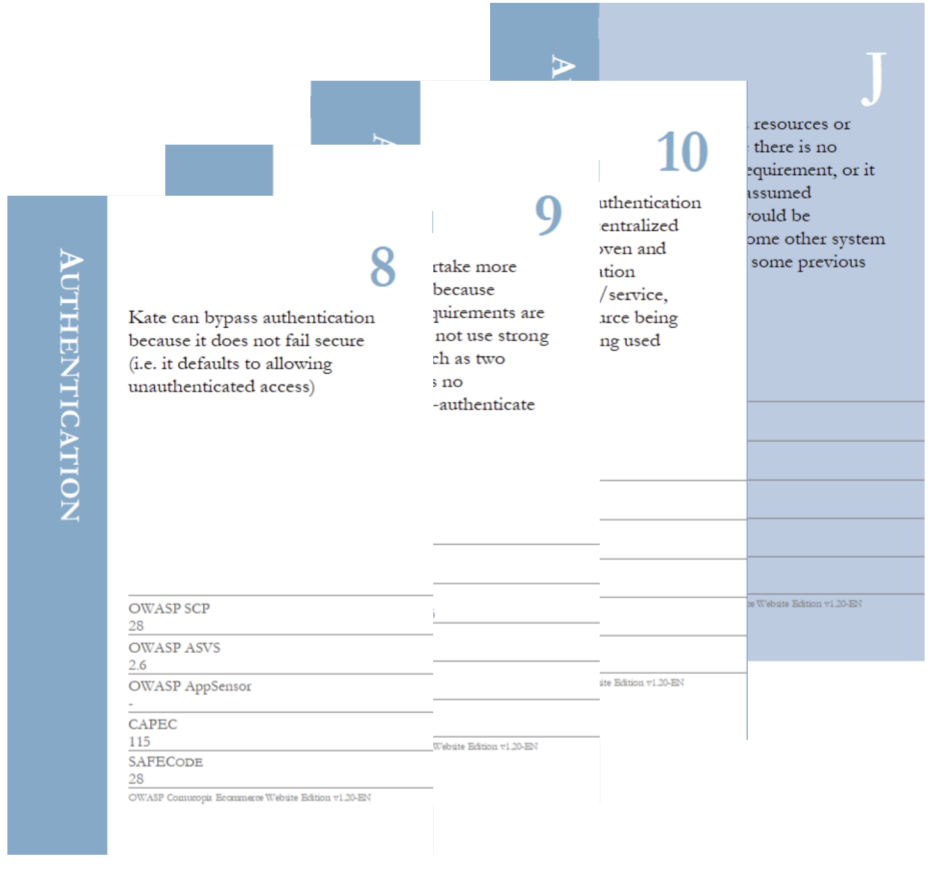
Round over

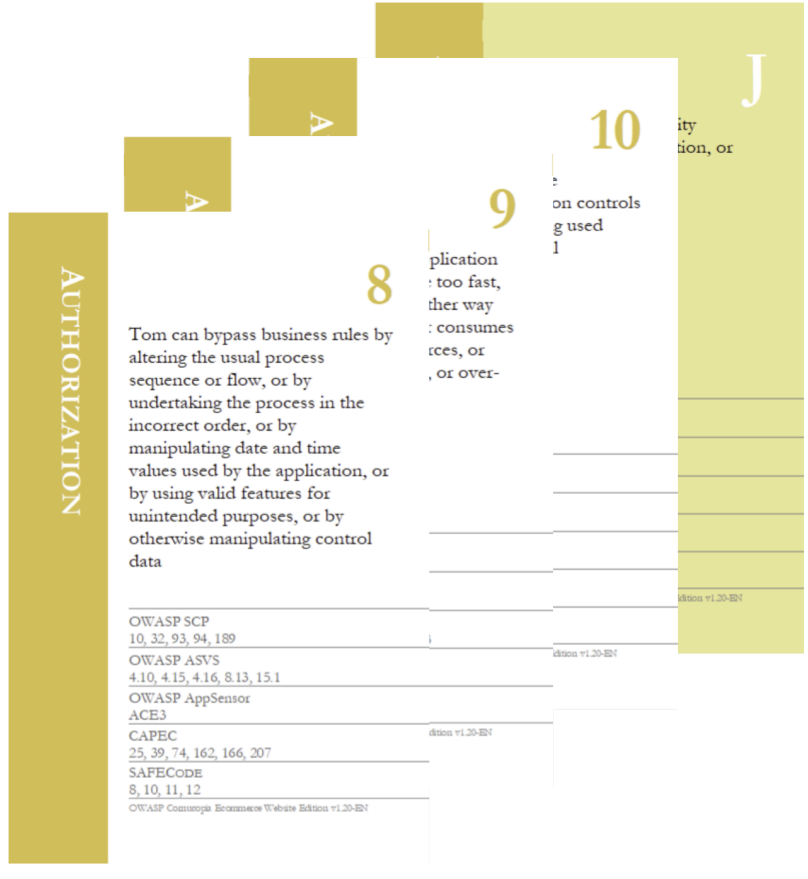
Winner chooses new topic

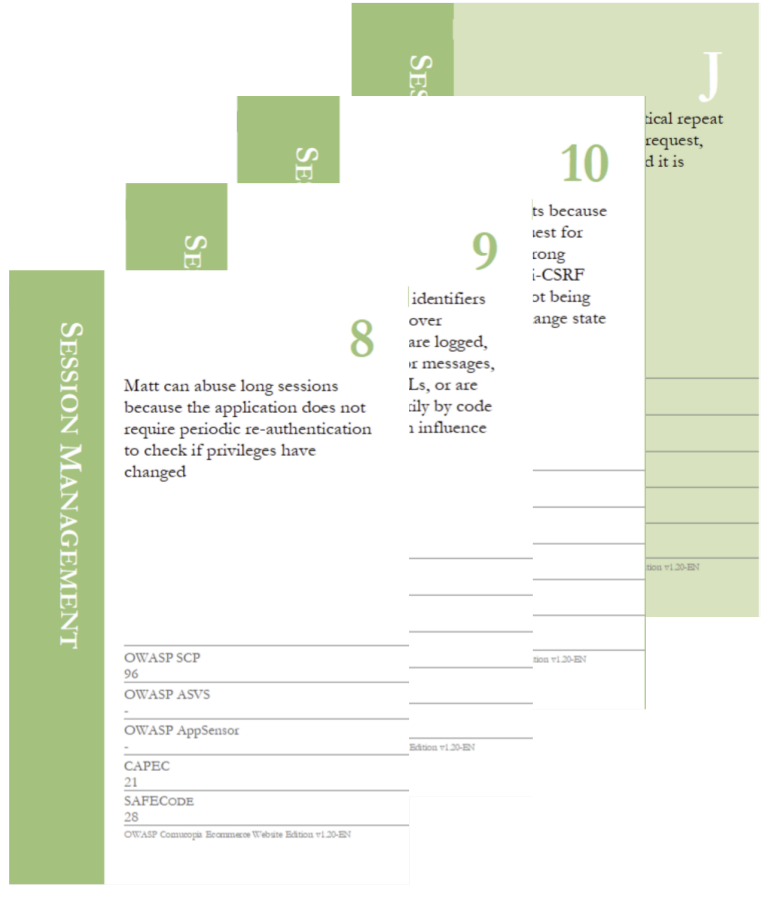
TOPICS

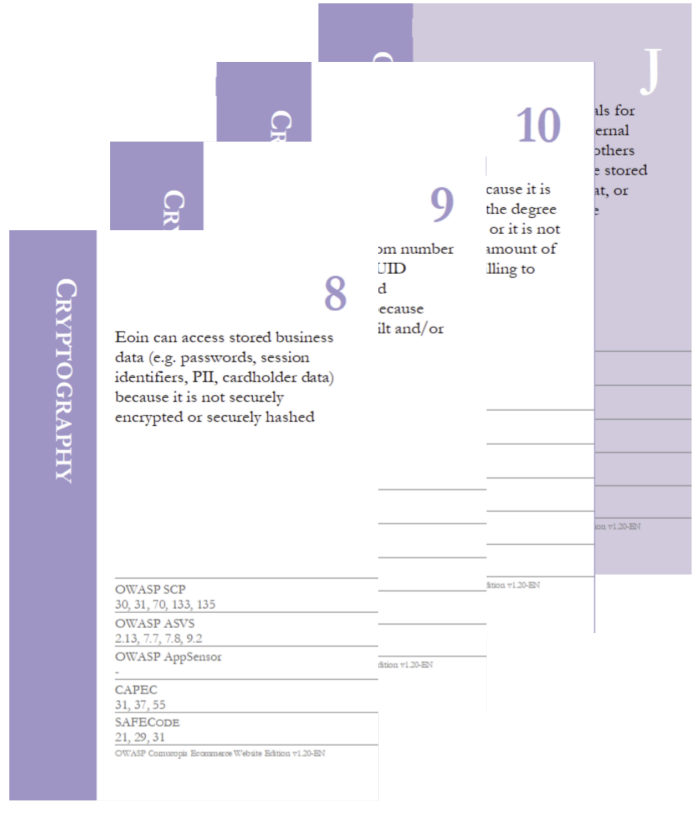
Data Validation & Encoding

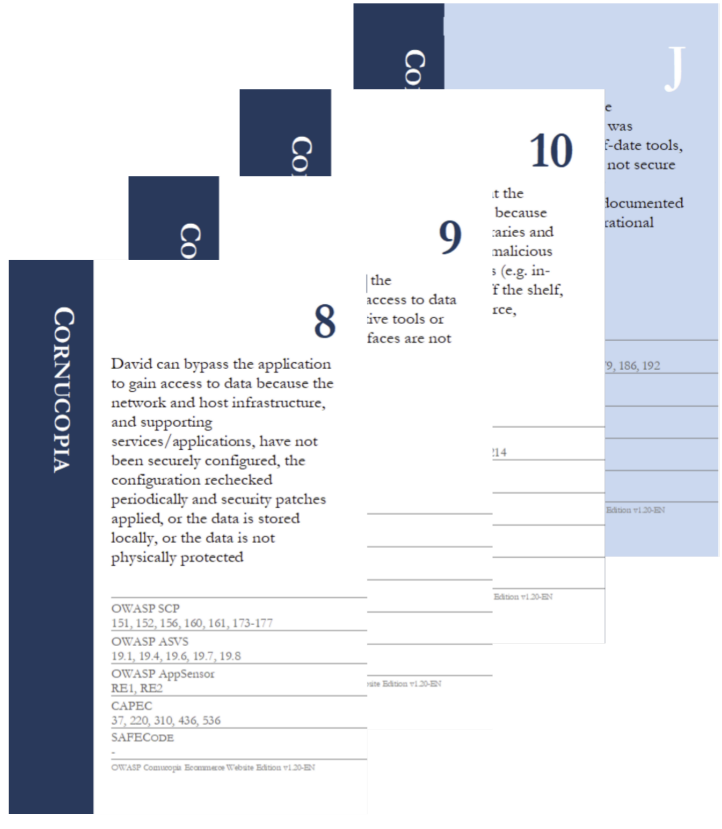
8	9	10	J
Sarah can bypass the centralized sanitization routines since they are not being used comprehensively	put alidation ion failures r sanitized	trust the source of le data, y stored e data on a erification validation end to be	over input alidation or de or routines ssed
OWASP SCP 15, 169			
OWASP 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 Comunopia Ecommerce Website Edition v1.20-EN
9
10
J


AUTHORIZATION
A
A
J
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 Comunopia Ecommerce Website Edition v1.20-EN
9
10


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
i-CSRF
ot being
ange state
ion v1.20-EN
J
ical 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

NOTES

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/

AGILE TESTING DAYS ONLINE EDITION

AGILE TESTING DAYS ONLINE EDITION

ANY QUESTIONS?