CORNUCOPIA

A

Você inventou um novo ataque contra de qualquer tipo.

Leia mais sobre segurança da aplicação nos guias da OWASP (Requirements, Development, Code Review and Testing) e na série OWASP Cheat Sheet, e no modelo de maturidade Open SAMM (Software Assurance Maturity Model)

CORNUCOPIA

(vazio)

CORNUCOPIA

2

Lee consegue ignorar os controles do aplicativo pois foram usadas funções arriscadas da linguagem de programação ao invés de opções seguras, ou há erros de conversão, ou porque o aplicativo está inseguro quando um recurso externo está indisponível, ou há *race condition*, ou há problemas na inicialização ou alocação de recursos, ou quando há sobrecarga

OWASP SCP
194-202, 205-209

OWASP ASVS
5.1

OWASP AppSensor
-

CAPEC
25, 26, 29, 96, 123-4, 128-9, 264-5

SAFECODE
3, 5-7, 9, 22, 25-26, 34

CORNUCOPIA

3

Andrew consegue acessar o código fonte, ou descompilar o aplicativo, ou consegue acessar a lógica do negócio para entender como a aplicação funciona e quais segredos ela contêm

OWASP SCP
134

OWASP ASVS
19.5

OWASP AppSensor
-

CAPEC
189, 207

SAFECODE
-

CORNUCOPIA

4

Keith consegue realizar uma ação e isto não é atribuído a ele.

OWASP SCP
23, 32, 34, 42, 51, 181

OWASP ASVS
8.10

OWASP AppSensor
-

CAPEC
-

SAFECODE
-

CORNUCOPIA

5

Larry consegue induzir a confiança de outras partes, incluindo usuários autenticados, ou violar esta confiança em outro lugar (ex: em outro aplicativo)

OWASP SCP
-

OWASP ASVS
-

OWASP AppSensor
-

CAPEC
89, 103, 181, 459

SAFECODE
-

CORNUCOPIA

6

Aaron consegue ignorar os controles porque a manipulação de erros/exceções é perdida/ignorada, ou é implementada de forma inconsistente ou parcial, ou não há negação de acesso por padrão (ex: erros devem terminar o acesso/execução do da funcionalidade), ou depende do tratamento por algum outro serviço ou sistema

OWASP SCP
109, 110, 111, 112, 155

OWASP ASVS
8.2, 8.4

OWASP AppSensor
-

CAPEC
54, 98, 164

SAFECODE
4, 11, 23

CORNUCOPIA

7

As ações de Mwengu não podem ser investigadas porque não há um registro correto de eventos de segurança com precisão, ou não há uma trilha de auditoria completa, ou estas podem ser alteradas ou excluídas pelo Mwengu, ou não existe um serviço de registro centralizado

OWASP SCP
113-115, 117, 118, 121-130

OWASP ASVS
2.12, 8.3-8.12, 9.10, 10.4

OWASP AppSensor
-

CAPEC
93

SAFECODE
4

CORNUCOPIA

8

David consegue ignorar o aplicativo para obter acesso aos dados porque a infraestrutura de rede e servidores e os serviços suportados não foram configurados de forma segura, as configurações não são verificadas periodicamente e os patches de segurança não são aplicados, ou os dados armazenados localmente não são fisicamente protegidos

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
-

CORNUCOPIA

9

Michael consegue ignorar o aplicativo para obter acesso aos dados porque ferramentas ou interfaces administrativas não estão adequadamente seguras

OWASP SCP
23, 29, 56, 81, 82, 84-90

OWASP ASVS
2.1, 2.32

OWASP AppSensor
-

CAPEC
122, 233

SAFECODE
-

CORNUCOPIA

10

Xavier consegue contornar os controles do aplicativo porque os códigos fontes tanto dos frameworks, como de bibliotecas e componentes utilizados contêm código malicioso ou vulnerabilidades

OWASP SCP
57, 151, 152, 204, 205, 213, 214

OWASP ASVS
1.11-

OWASP AppSensor
-

CAPEC
68, 438, 439, 442, 524, 538

SAFECODE
15

CORNUCOPIA

J

Roman consegue explorar o aplicativo pois este foi compilado usando ferramentas desatualizadas ou configurações não seguras como padrão ou informações de segurança não foram documentadas e passadas para o time operacional

OWASP SCP
90, 137, 148, 151-154, 175-179, 186, 192

OWASP ASVS
19.5, 19.9

OWASP AppSensor
-

CAPEC
-

SAFECODE
4

CORNUCOPIA

Q

Jim pode realizar ações mal-intencionadas, não normais, sem detecção e resposta em tempo real pela aplicação

OWASP SCP
-

OWASP ASVS
4.14, 9.8, 15.1, 15.2

OWASP AppSensor
(All)

CAPEC
-

SAFECODE
1, 27

CORNUCOPIA

K

Gareth pode utilizar o aplicativo para negar o serviço a alguns ou a todos os usuários

OWASP SCP
41, 55

OWASP ASVS
-

OWASP AppSensor
UT1-4, STE3

CAPEC
2, 25, 119, 125

SAFECODE
1

CURINGA

Curinga

Alice consegue utilizar a aplicação para realizar ataques a dados e usuários do sistema

Você pensou em se tornar membro individual da OWASP? Todas as ferramentas, guias e reuniões locais são gratuitas para todos, mas ser um membro individual apoia o trabalho da OWASP

CURINGA

Curinga

Bob pode influenciar, alterar ou mudar a aplicação para que ela não cumpra os propósitos legais, regulamentadores, contratuais ou outras diretrizes organizacionais

Examine as vulnerabilidades e descubra como elas podem ser solucionadas através do aplicativo de treinamento OWASP Broken Web Applications VM, ou usando o desafio online Hacking Lab. Ambos são gratuitos.