© 2012-2016 OWASP Foundation

Práticas de Criptografia

A

Você inventou um novo ataque contra Práticas de Criptografia

Leia mais sobre este tópico em OWASP Cryptographic Storage Cheat Sheet e OWASP Transport Layer Protection Cheat Sheet

Práticas de Criptografia

(vazio)

Práticas de Criptografia

2

Kyun consegue acesso a dados porque isto foi ocultado/ofuscado/escondido ao invés de ser usada uma função de criptografia aprovada.

OWASP SCP 105, 133, 135
OWASP ASVS -
OWASP AppSensor -
CAPEC -
SAFECODE 21, 29

Práticas de Criptografia

3

Axel consegue modificar dados que estão armazenados ou que são temporários ou transitórios, ou consegue modificar código fonte, ou consegue modificar patches/atualizações, ou alterar dados de configuração, pois a integridade não foi checada.

OWASP SCP 92, 205, 212
OWASP ASVS 8.11, 11.7, 13.2, 19.5, 19.6, 19.7, 19.8
OWASP AppSensor SE1, IE4
CAPEC 31, 39, 68, 75, 133, 145, 162, 203,438-9,442
SAFECODE 12, 14

Práticas de Criptografia

4

Paulo consegue acesso a dados transitórios não criptografados, embora o canal de comunicação esteja criptografado

OWASP SCP 37, 88, 143, 214
OWASP ASVS 7.12, 9.2
OWASP AppSensor -
CAPEC 185, 186, 187
SAFECODE 14, 29, 30

Práticas de Criptografia

5

Kyle consegue ignorar controles criptográficos porque eles não falham de forma segura (ex: eles são desprotegidos por padrão)

OWASP SCP 103, 145
OWASP ASVS 7.2, 10.3
OWASP AppSensor -
CAPEC -
SAFECODE 21, 29

Práticas de Criptografia

6

Romain consegue ler e modificar dados descriptografados que estão na memória ou são transitórios (ex: credenciais, identificadores de sessão, dados pessoais e comercialmente relevantes), em uso ou em comunicação dentro da aplicação, ou entre aplicação e usuário, ou entre a aplicação e sistemas externos

OWASP SCP 36, 37, 143, 146, 147
OWASP ASVS 2.16, 9.2, 9.11, 10.3, 19.2
OWASP AppSensor -
CAPEC 31, 57, 102, 157, 158, 384, 466, 546
SAFECODE 29

Práticas de Criptografia

7

Gunter consegue interceptar ou modificar dados criptografados em trânsito porque o protocolo está mal implantado, ou configurado de forma fraca, ou os certificados estão inválidos, ou os certificados não são confiáveis, ou a conexão pode ser deteriorada para uma comunicação mais fraca ou descriptografado

OWASP SCP 75, 144, 145, 148
OWASP ASVS 10.1, 10.5, 10.10, 10.11, 10.12, 10.13, 10.14
OWASP AppSensor IE4
CAPEC 31, 216
SAFECODE 14, 29, 30

© 2012-2016 OWASP Foundation

Práticas de Criptografia

8

Eoin consegue acesso a dados de negócios armazenados (ex: senhas, identificadores de sessão, informações de identificação pessoal - PII, dados de titular de cartão) pois estes dados não estão criptografados de forma segura ou com segurança

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

Práticas de Criptografia

9

Andy consegue ignorar a geração de números aleatórios/randômicos, ou ignorar a geração aleatória de GUID, ou ignorar as funções de criptografia e *hashing* porque eles são fracos ou foram autoconstruídos

OWASP SCP
60, 104, 105

OWASP ASVS
7.6, 7.7, 7.8, 7.15

OWASP AppSensor
-

CAPEC
97

SAFECode
14, 21, 29, 32, 33

Práticas de Criptografia

10

Susanna consegue quebrar a criptografia em uso pois a criptografia não é forte o suficiente para oferecer a proteção exigida, ou esta não é forte o suficiente para tratar a quantidade de esforço que o atacante está disposto a fazer

OWASP SCP
104, 105

OWASP ASVS
-

OWASP AppSensor
-

CAPEC
97, 463

SAFECode
14, 21, 29, 31, 32, 33

Práticas de Criptografia

J

Justin consegue ler credenciais para acessar recursos internos e externos, serviços e outros sistemas porque estas credenciais estão armazenadas num formato descriptografado ou salvos no código fonte

OWASP SCP
35, 90, 171, 172

OWASP ASVS
2.29

OWASP AppSensor
-

CAPEC
116

SAFECode
21, 29

Práticas de Criptografia

Q

Randolph consegue acessar ou prever os dados mestres de criptografia

OWASP SCP
35, 102

OWASP ASVS
7.8, 7.9, 7.11, 7.13, 7.14

OWASP AppSensor
-

CAPEC
116, 117

SAFECode
21, 29

Práticas de Criptografia

K

Dan consegue influenciar ou alternar as rotinas/codificações de criptografia (encriptação, *hashing*, assinaturas digitais, números aleatórios e geração de GUID) e consegue ignorá-los também

OWASP SCP
31, 101

OWASP ASVS
7.11

OWASP AppSensor
-

CAPEC
207, 554

SAFECode
14, 21, 29

(vazio)

(vazio)