AUTENTICAÇÃO E GERENCIAMENTO DE CREDENCIAIS

A

Você inventou um novo ataque contra a Autenticação e Gerenciamento de Credenciais

Leia mais sobre este tópico em OWASP Authentication Cheat Sheet

AUTENTICAÇÃO E GERENCIAMENTO DE CREDENCIAIS

(vazio)

AUTENTICAÇÃO E GERENCIAMENTO DE CREDENCIAIS

2

James pode assumir as funções de autenticação sem que o usuário real esteja ciente do uso destas funções (ex: tente fazer login, logar com credenciais, redefinir a senha)

OWASP SCP 47, 52
OWASP ASVS 2.12, 8.4, 8.10
OWASP AppSensor UT1
CAPEC -
SAFECODE 28

AUTENTICAÇÃO E GERENCIAMENTO DE CREDENCIAIS

3

Muhammad consegue obter a senha de um usuário ou outros dados, pela observação durante a autenticação, ou cache local, ou pela memória, ou pelo tráfego de dados, ou pela leitura de algum local desprotegido, ou porque isto é amplamente conhecido, ou porque não há expiração de dados, ou por que o usuário não consegue trocar sua própria senha.

OWASP SCP 36-7, 40, 43, 48, 51, 119, 139-40, 146
OWASP ASVS 2.2, 2.17, 2.24, 8.7, 9.1, 9.4, 9.5, 9.9, 9.11
OWASP AppSensor -
CAPEC 37, 546
SAFECODE 28

AUTENTICAÇÃO E GERENCIAMENTO DE CREDENCIAIS

4

Sebastien pode identificar facilmente nomes de usuários ou consegue elencar quem eles são

OWASP SCP 33, 53
OWASP ASVS 2.18, 2.28
OWASP AppSensor AE1
CAPEC 383
SAFECODE 28

AUTENTICAÇÃO E GERENCIAMENTO DE CREDENCIAIS

5

Javier pode usar credenciais padrões (default), de teste ou facilmente adivinhadas para autenticação, ou consegue autenticar através de contas inativas ou autentica-se por contas não necessariamente da aplicação

OWASP SCP 54, 175, 178
OWASP ASVS 2.19
OWASP AppSensor AE12, HT3
CAPEC 70
SAFECODE 28

AUTENTICAÇÃO E GERENCIAMENTO DE CREDENCIAIS

6

Sven consegue reutilizar uma senha temporária porque o usuário não precisa troca-la no primeiro acesso, ou o tempo de expiração é muito longo, ou o tempo de expiração não existe, ou não é usado um método de entrega *out-of-band* (ex: aplicação mobile, SMS)

OWASP SCP 37, 45, 46, 178
OWASP ASVS 2.22
OWASP AppSensor -
CAPEC 50
SAFECODE 28

AUTENTICAÇÃO E GERENCIAMENTO DE CREDENCIAIS

7

Cecilia consegue usar força bruta e ataques de dicionário (*dictionary attacks*) contra uma ou muitas contas sem limitação, ou estes ataques são simplificados pois as senhas tem baixa complexidade, tamanho reduzido, inexistência de expiração e regras para reuso.

OWASP SCP 33, 38, 39, 41, 50, 53
OWASP ASVS 2.7, 2.20, 2.23, 2.25, 2.27
OWASP AppSensor AE2, AE3
CAPEC 2, 16
SAFECODE 27

Autenticação e Gerenciamento de Credenciais

8

Kate consegue ignorar a autenticação porque isto não é uma falha de segurança (ex: o acesso sem autenticação está assinalado como padrão)

OWASP SCP
28

OWASP ASVS
2.6

OWASP AppSensor
-

CAPEC
115

SAFECode
28

Autenticação e Gerenciamento de Credenciais

9

Claudia consegue assumir funções críticas porque os requisitos de autenticação são muito fracos (ex: não é usado autenticação com força de senha), ou não é um requisito revalidar a autenticação com frequência

OWASP SCP
55, 56

OWASP ASVS
2.1, 2.9, 2.26, 2.31, 4.15

OWASP AppSensor
-

CAPEC
21

SAFECode
14, 28

Autenticação e Gerenciamento de Credenciais

10

Pravin consegue ignorar controle de autenticação porque não está sendo usado um módulo/framework/serviço de autenticação que seja centralizado, testado, comprovado e aprovado para gerir requisições

OWASP SCP
25, 26, 27

OWASP ASVS
1.7, 2.30

OWASP AppSensor
-

CAPEC
90, 115

SAFECode
14, 28

Autenticação e Gerenciamento de Credenciais

J

Mark consegue acessar recursos ou serviços porque não há requisitos de autenticação, ou, por engano, um outro sistema ou outra ação realizou autenticação.

OWASP SCP
23, 32, 34

OWASP ASVS
2.1

OWASP AppSensor
-

CAPEC
115

SAFECode
14, 28

Autenticação e Gerenciamento de Credenciais

Q

Jaime consegue ignorar a autenticação porque não é aplicado o mesmo rigor para todas as funções de autenticação (ex: logar, troca de senha, recuperação de senha, *logout*, acesso administrador) ou não é aplicado o mesmo rigor nos diversos locais de acesso e versões do sistema(ex:*mobile website, mobile app, full website, API, call center*)

OWASP SCP
23, 29, 42, 49

OWASP ASVS
2.1, 2.8

OWASP AppSensor
-

CAPEC
36, 50, 115, 121, 179

SAFECode
14, 28

Autenticação e Gerenciamento de Credenciais

K

Olga consegue influenciar ou alterar o código ou a rotina de autenticação e com isto ignorar a autenticação

OWASP SCP
24

OWASP ASVS
2.4, 13.2

OWASP AppSensor
-

CAPEC
115, 207, 554

SAFECode
14, 28

(vazio)

(vazio)