© 2012-2016 OWASP Foundation

GERENCIAMENTO DE SESSÕES

A

Você inventou um novo ataque contra o Gerenciamento de Sessões

Leia mais sobre este tópico em OWASP Session Management Cheat Sheet e prevenção de ataques do tipo Cross Site Request Forgery (CSRF)

GERENCIAMENTO DE SESSÕES

(vazio)

GERENCIAMENTO DE SESSÕES

2

William tem o controle sobre a geração de identificadores de sessão

OWASP SCP 58, 59
OWASP ASVS 3.10
OWASP AppSensor SE2
CAPEC 31, 60, 61
SAFECODE 28

GERENCIAMENTO DE SESSÕES

3

Ryan consegue usar uma única conta em paralelo, pois as sessões simultâneas são permitidas

OWASP SCP 68
OWASP ASVS 3.16, 3.17, 3.18
OWASP AppSensor -
CAPEC -
SAFECODE 28

GERENCIAMENTO DE SESSÕES

4

Alison consegue configurar identificadores de *cookies* em outras aplicações web porque o domínio ou o caminho não são suficientemente limitados

OWASP SCP 59, 61
OWASP ASVS 3.12
OWASP AppSensor SE2
CAPEC 31, 61
SAFECODE 28

GERENCIAMENTO DE SESSÕES

5

John consegue prever ou adivinhar identificadores de sessão porque estes não são alterados quando uma regra de usuário é alterada (ex: antes e depois da autenticação) e quando uma troca entre meios de comunicação criptografados e não criptografados acontece, ou os identificadores são curtos e não randômicos, ou não são modificados periodicamente

OWASP SCP 60, 62, 66, 67, 71, 72
OWASP ASVS 3.2, 3.7, 3.11
OWASP AppSensor SE4-6
CAPEC 31
SAFECODE 28

GERENCIAMENTO DE SESSÕES

6

Gary consegue ter o controle da sessão de um usuário porque o tempo de encerramento(*timeout*) da sessão é longo ou inexiste, ou o tempo limite da sessão é longo ou inexiste, ou a mesma sessão pode ser usada para mais de um dispositivo/local

OWASP SCP 64, 65
OWASP ASVS 3.3, 3.4, 3.16, 3.17, 3.18
OWASP AppSensor SE5, SE6
CAPEC 21
SAFECODE 28

GERENCIAMENTO DE SESSÕES

7

Casey consegue utilizar a sessão de Adam depois dele ter finalizado o uso da aplicação, porque a função de logout inexiste, ou Adam não fez logout, ou a função de logout não termina a sessão de forma adequada

OWASP SCP 62, 63
OWASP ASVS 3.2, 3.5
OWASP AppSensor -
CAPEC 21
SAFECODE 28

© 2012-2016 OWASP Foundation

GERENCIAMENTO DE SESSÕES

8

Matt consegue utilizar longas sessões porque a aplicação não solicita uma nova autenticação de forma periódica para validar se os privilégios do usuário foram alterados

OWASP SCP 96
OWASP ASVS -
OWASP AppSensor -
CAPEC 21
SAFECODE 28

GERENCIAMENTO DE SESSÕES

9

Ivan consegue roubar identificadores de sessão porque estes são transmitidos em canais inseguros, ou estão logados, ou são exibidos em mensagens de erros, ou estão em URLs, ou são acessíveis pelo código que o atacante consegue alterar ou influenciar

OWASP SCP 69, 75, 76, 119, 138
OWASP ASVS 3.6, 8.7, 10.3
OWASP AppSensor SE4-6
CAPEC 31, 60
SAFECODE 28

GERENCIAMENTO DE SESSÕES

10

Marce consegue inventar requisições porque *tokens* randômicos e fortes (ou seja, *tokens* anti-CSRF) ou similares não estão sendo usados para ações que mudam estado. Estas requisições podem ser por sessão ou por requisição (*request*) em ações mais críticas

OWASP SCP 73, 74
OWASP ASVS 4.13
OWASP AppSensor IE4
CAPEC 62, 111
SAFECODE 18

GERENCIAMENTO DE SESSÕES

J

Jeff consegue reenviar uma interação de repetição idêntica (ex: requisição HTTP, sinal, botão pressionado) e ela é aceita, sem rejeição

OWASP SCP -
OWASP ASVS 15.1, 15.2
OWASP AppSensor IE5
CAPEC 60
SAFECODE 12, 14

GERENCIAMENTO DE SESSÕES

Q

Salim consegue ignorar o gerenciamento de sessão porque este não é aplicado de forma abrangente e consistente por toda a aplicação

OWASP SCP 58
OWASP ASVS 3.1
OWASP AppSensor -
CAPEC 21
SAFECODE 14, 28

GERENCIAMENTO DE SESSÕES

K

Peter consegue ignorar o controle de gerenciamento de sessão porque este foi autoconstruído e/ou é fraco, ao invés de ter sido usado a estrutura padrão de um framework ou um modulo testado e aprovado

OWASP SCP 58, 60
OWASP ASVS 1.7
OWASP AppSensor -
CAPEC 21
SAFECODE 14, 28

(vazio)

(vazio)