Validação de Dados de Entrada e Codificação de Dados de Saída

A

Você inventou um novo ataque contra a Validação de Dados de Entrada e Codificação de Dados de Saída

Leia mais sobre este tópico em OWASP Cheat Sheets. Pesquise sobre validação dos dados de entrada, Prevenção de XSS(Cross-site Scripting), Prevenção do DOM baseado em XSS, Prevenção de SQL Injection e Parametrização de Consultas

Validação de Dados de Entrada e Codificação de Dados de Saída

(vazio)

Validação de Dados de Entrada e Codificação de Dados de Saída

2

Brian consegue reunir o básico de informações sobre a utilização e configuração de base de dados, lógica, codificação, além da utilização de softwares, serviços e infraestrutura nas mensagens de erro ou em mensagens de configuração, ou na presença de arquivos de instalação (padrões ou antigos), ou em evidências de testes, ou em backups ou em exposição de código fonte.

OWASP SCP 69, 107-109, 136, 137, 153, 156, 158, 162
OWASP ASVS 1.10, 4.5, 8.1, 11.5, 19.1, 19.5
OWASP AppSensor HT1-3
CAPEC 54, 541
SAFECODE 4, 23

Validação de Dados de Entrada e Codificação de Dados de Saída

3

Robert consegue inserir dados maliciosos pois o formato de protocolo não foi checado, ou duplicações são aceitas, ou a estrutura não está sendo verificada, ou os dados individuais não foram validados por formato, tipo, intervalo, tamanho e por uma lista de caracteres ou formatos possíveis

OWASP SCP 8, 9, 11-14, 16, 159, 190, 191
OWASP ASVS 5.1, 5.16, 5.17, 5.18, 5.19, 5.20, 11.1, 11.2
OWASP AppSensor RE7-8, AE4-7, IE2-3,CIE1,CIE3-4,HT1-3
CAPEC 28,48,126,165,213,220,221,261,262,271,272
SAFECODE 3, 16, 24, 35

Validação de Dados de Entrada e Codificação de Dados de Saída

4

Dave consegue inserir nomes ou dados de campos mal intencionados porque isto não está sendo verificado no contexto de cada usuário e processo.

OWASP SCP 8, 10, 183
OWASP ASVS 4.16, 5.16, 5.17, 15.1
OWASP AppSensor RE3-6,AE8-11,SE1,3-6,IE2-4,HT1-3
CAPEC 28, 31, 48, 126, 162, 165, 213, 220, 221,261
SAFECODE 24, 35

Validação de Dados de Entrada e Codificação de Dados de Saída

5

Jee consegue ignorar as rotinas centralizadas de codificação de saída pois elas não estão sendo usadas em todos os lugares, ou a codificação errada está sendo usada

OWASP SCP 3, 15, 18-22 168
OWASP ASVS 1.7, 5.15, 5.21, 5.22, 5.23
OWASP AppSensor -
CAPEC 28, 31, 152, 160, 468
SAFECODE 2, 17

Validação de Dados de Entrada e Codificação de Dados de Saída

6

Jason consegue ignorar as rotinas centralizadas de validação de dados de entrada pois elas não estão sendo usadas em todos os campos de entrada de dados

OWASP SCP 3, 168
OWASP ASVS 1.7, 5.6, 5.19
OWASP AppSensor IE2-3
CAPEC 28
SAFECODE 3, 16, 24

Validação de Dados de Entrada e Codificação de Dados de Saída

7

Jan consegue carregar/enviar informações especiais visando evitar validações de campos porque o conjunto de caracteres não é especificado e aplicado, ou o dado de entrada é codificado diversas vezes, ou o dado não é totalmente convertido no mesmo formado que a aplicação usa (ex: *canonicalização*) antes da validação, ou as variáveis não são fortemente tipadas.

OWASP SCP 4, 5, 7, 150
OWASP ASVS 5.6, 11.8
OWASP AppSensor IE2-3, EE1-2
CAPEC 28, 153, 165
SAFECODE 3, 16, 24

Validação de Dados de Entrada e Codificação de Dados de Saída

8

Sarah consegue ignorar as rotinas centralizadas de tratamento (sanitização) pois elas não estão sendo usadas de forma abrangente

OWASP SCP
15, 169
OWASP ASVS
1.7, 5.21, 5.23
OWASP AppSensor
-
CAPEC
28, 31, 152, 160, 468
SAFECODE
2, 17

Validação de Dados de Entrada e Codificação de Dados de Saída

9

Shamun consegue ignorar as verificações de validação de entrada ou de saída porque as falhas de validação não são rejeitadas e/ou tratadas (sanitização)

OWASP SCP
6, 21, 22, 168
OWASP ASVS
5.3
OWASP AppSensor
IE2-3
CAPEC
28
SAFECODE
3, 16, 24

Validação de Dados de Entrada e Codificação de Dados de Saída

10

Dario consegue explorar a confiabilidade da aplicação em fonte de dados (ex: dados definidos pelo usuário, manipulação de dados armazenados localmente, mudança do estado dos dados em dispositivos clientes, falta de verificação da identidade durante uma validação de dados, como Dario pode fingir ser Colin)

OWASP SCP
2, 19, 92, 95, 180
OWASP ASVS
5.19, 10.6, 16.2, 16.3, 16.4, 16.5, 16.8
OWASP AppSensor
IE4, IE5
CAPEC
12, 51, 57, 90,111,145,194,195,202,218,463
SAFECODE
14

Validação de Dados de Entrada e Codificação de Dados de Saída

J

Dennis tem o controle sobre validações de entrada de dados, validações de saída de dados ou codificação de saída ou rotinas que ele consegue ignorar/burlar

OWASP SCP
1, 17
OWASP ASVS
5.5, 5.18
OWASP AppSensor
RE3, RE4
CAPEC
87, 207, 554
SAFECODE
2, 17

Validação de Dados de Entrada e Codificação de Dados de Saída

Q

Geoff consegue injetar dados num dispositivo ou num interpretador no lado do cliente porque uma interface parametrizada não foi usada, ou não foi implementada corretamente, ou os dados não foram codificados corretamente para o contexto proposto, ou não há uma política restritiva para a codificação ou a inclusão de dados.

OWASP SCP
10, 15, 16, 19, 20
OWASP ASVS
5.15, 5.22, 5.23, 5.24, 5.25
OWASP AppSensor
IE1, RP3
CAPEC
28, 31, 152, 160, 468
SAFECODE
2, 17

Validação de Dados de Entrada e Codificação de Dados de Saída

K

Gabe consegue injetar dados num interpretador no lado do servidor (ex: SQL, comandos para o sistema operacional, Xpath, Server JavaScript, SMTP) porque uma interface parametrizada não foi usada ou não foi implementada corretamente

OWASP SCP
15, 19-22, 167, 180, 204, 211, 212
OWASP ASVS
5.10, 5.11, 5.12, 5.13, 5.14, 5.16, 5.21
OWASP AppSensor
CIE1-2
CAPEC
23, 28, 76, 152, 160, 261
SAFECODE
2, 19, 20

(vazio)

(vazio)