|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Validação de Dados de Entrada e Codificação de Dados de Saída** | **A** | **Validação de Dados de Entrada e Codificação de Dados de Saída** |  | **Validação de Dados de Entrada e Codificação de Dados de Saída** | **2** | **Validação de Dados de Entrada e Codificação de Dados de Saída** | **3** |
| Você inventou um novo ataque contra a Validação de Dados de Entrada e Codificação de Dados de Saída | (vazio) | 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. | 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 |
| *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* |  | |  | | --- | | 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 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | 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 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | |
| **Validação de Dados de Entrada e Codificação de Dados de Saída** | **4** | **Validação de Dados de Entrada e Codificação de Dados de Saída** | **5** | **Validação de Dados de Entrada e Codificação de Dados de Saída** | **6** | **Validação de Dados de Entrada e Codificação de Dados de Saída** | **7** |
| Dave consegue inserir nomes ou dados de campos mal-intencionados porque isto não está sendo verificado no contexto de cada usuário e processo. | 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 | 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 | 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  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 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | 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 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  3, 168 | | OWASP ASVS  1.7, 5.6, 5.19 | | OWASP AppSensor  IE2-3 | | CAPEC  28 | | SAFECode  3, 16, 24 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | 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 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Validação de Dados de Entrada e Codificação de Dados de Saída** | **8** | **Validação de Dados de Entrada e Codificação de Dados de Saída** | **9** | **Validação de Dados de Entrada e Codificação de Dados de Saída** | **10** | **Validação de Dados de Entrada e Codificação de Dados de Saída** | **J** |
| Sarah consegue ignorar as rotinas centralizadas de tratamento (sanitização) pois elas não estão sendo usadas de forma abrangente | Shamun consegue ignorar as verificações de validação de entrada ou de saída porque as falhas de validação não são rejeitadas e/ou tratadas (sanitização) | 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) | 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  15, 169 | | OWASP ASVS  1.7, 5.21, 5.23 | | OWASP AppSensor  - | | CAPEC  28, 31, 152, 160, 468 | | SAFECode  2, 17 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  6, 21, 22, 168 | | OWASP ASVS  5.3 | | OWASP AppSensor  IE2-3 | | CAPEC  28 | | SAFECode  3, 16, 24 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | 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 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  1, 17 | | OWASP ASVS  5.5, 5.18 | | OWASP AppSensor  RE3, RE4 | | CAPEC  87, 207, 554 | | SAFECode  2, 17 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | |
| **Validação de Dados de Entrada e Codificação de Dados de Saída** | **Q** | **Validação de Dados de Entrada e Codificação de Dados de Saída** | **K** |  |  |  |  |
| 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/inclusão de dados | 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  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 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | 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 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Autenticação e Gerenciamento de Credenciais** | **A** | **Autenticação e Gerenciamento de Credenciais** |  | **Autenticação e Gerenciamento de Credenciais** | **2** | **Autenticação e Gerenciamento de Credenciais** | **3** |
| Você inventou um novo ataque contra a Autenticação e Gerenciamento de Credenciais |  | 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) | 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. |
| *Leia mais sobre este tópico em OWASP Authentication Cheat Sheet* |  | |  | | --- | | OWASP SCP  47, 52 | | OWASP ASVS  2.12, 8.4, 8.10 | | OWASP AppSensor  UT1 | | CAPEC  - | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | 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 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | |
| **Autenticação e Gerenciamento de Credenciais** | **4** | **Autenticação e Gerenciamento de Credenciais** | **5** | **Autenticação e Gerenciamento de Credenciais** | **6** | **Autenticação e Gerenciamento de Credenciais** | **7** |
| Sebastien pode identificar facilmente nomes de usuários ou consegue elencar quem eles são | 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 | 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) | 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, 53 | | OWASP ASVS  2.18, 2.28 | | OWASP AppSensor  AE1 | | CAPEC  383 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  54, 175, 178 | | OWASP ASVS  2.19 | | OWASP AppSensor  AE12, HT3 | | CAPEC  70 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  37, 45, 46, 178 | | OWASP ASVS  2.22 | | OWASP AppSensor  - | | CAPEC  50 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | 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 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Autenticação e Gerenciamento de Credenciais** | **8** | **Autenticação e Gerenciamento de Credenciais** | **9** | **Autenticação e Gerenciamento de Credenciais** | **10** | **Autenticação e Gerenciamento de Credenciais** | **J** |
| Kate consegue ignorar a autenticação porque isto não é uma falha de segurança (ex: o acesso sem autenticação está assinalado como padrão) | 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 | 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 | 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  28 | | OWASP ASVS  2.6 | | OWASP AppSensor  - | | CAPEC  115 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  55, 56 | | OWASP ASVS  2.1, 2.9, 2.26, 2.31, 4.15 | | OWASP AppSensor  - | | CAPEC  21 | | SAFECode  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  25, 26, 27 | | OWASP ASVS  1.7, 2.30 | | OWASP AppSensor  - | | CAPEC  90, 115 | | SAFECode  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  23, 32, 34 | | OWASP ASVS  2.1 | | OWASP AppSensor  - | | CAPEC  115 | | SAFECode  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | |
| **Autenticação e Gerenciamento de Credenciais** | **Q** | **Autenticação e Gerenciamento de Credenciais** | **K** |  |  |  |  |
| 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*) | Olga consegue influenciar ou alterar o código ou a rotina de autenticação e com isto ignorar a autenticação |  |  |
| |  | | --- | | OWASP SCP  23, 29, 42, 49 | | OWASP ASVS  2.1, 2.8 | | OWASP AppSensor  - | | CAPEC  36, 50, 115, 121, 179 | | SAFECode  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  24 | | OWASP ASVS  2.4, 13.2 | | OWASP AppSensor  - | | CAPEC  115, 207, 554 | | SAFECode  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Gerenciamento de Sessões** | **A** | **Gerenciamento de Sessões** |  | **Gerenciamento de Sessões** | **2** | **Gerenciamento de Sessões** | **3** |
| Você inventou um novo ataque contra o Gerenciamento de Sessões |  | William tem o controle sobre a geração de identificadores de sessão | Ryan consegue usar uma única conta em paralelo, pois as sessões simultâneas são permitidas |
| *Leia mais sobre este tópico em OWASP Session Management Cheat Sheet e prevenção de ataques do tipo Cross Site Request Forgery (CSRF)* |  | |  | | --- | | OWASP SCP  58, 59 | | OWASP ASVS  3.10 | | OWASP AppSensor  SE2 | | CAPEC  31, 60, 61 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  68 | | OWASP ASVS  3.16, 3.17, 3.18 | | OWASP AppSensor  - | | CAPEC  - | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | |
| **Gerenciamento de Sessões** | **4** | **Gerenciamento de Sessões** | **5** | **Gerenciamento de Sessões** | **6** | **Gerenciamento de Sessões** | **7** |
| Alison consegue configurar identificadores de *cookies* em outras aplicações web porque o domínio ou o caminho não são suficientemente limitados | 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 | 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 | 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  59, 61 | | OWASP ASVS  3.12 | | OWASP AppSensor  SE2 | | CAPEC  31, 61 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  60, 62, 66, 67, 71, 72 | | OWASP ASVS  3.2, 3.7, 3.11 | | OWASP AppSensor  SE4-6 | | CAPEC  31 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  64, 65 | | OWASP ASVS  3.3, 3.4, 3.16, 3.17, 3.18 | | OWASP AppSensor  SE5, SE6 | | CAPEC  21 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  62, 63 | | OWASP ASVS  3.2, 3.5 | | OWASP AppSensor  - | | CAPEC  21 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Gerenciamento de Sessões** | **8** | **Gerenciamento de Sessões** | **9** | **Gerenciamento de Sessões** | **10** | **Gerenciamento de Sessões** | **J** |
| 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 | 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 | 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 | Jeff consegue reenviar uma interação de repetição idêntica (ex: requisição HTTP, sinal, botão pressionado) e ela é aceita, sem rejeição |
| |  | | --- | | OWASP SCP  96 | | OWASP ASVS  - | | OWASP AppSensor  - | | CAPEC  21 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  69, 75, 76, 119, 138 | | OWASP ASVS  3.6, 8.7, 10.3 | | OWASP AppSensor  SE4-6 | | CAPEC  31, 60 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  73, 74 | | OWASP ASVS  4.13 | | OWASP AppSensor  IE4 | | CAPEC  62, 111 | | SAFECode  18 | |  | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  - | | OWASP ASVS  15.1, 15.2 | | OWASP AppSensor  IE5 | | CAPEC  60 | | SAFECode  12, 14 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | |
| **Gerenciamento de Sessões** | **Q** | **Gerenciamento de Sessões** | **K** |  |  |  |  |
| Salim consegue ignorar o gerenciamento de sessão porque este não é aplicado de forma abrangente e consistente por toda a aplicação | 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 | | OWASP ASVS  3.1 | | OWASP AppSensor  - | | CAPEC  21 | | SAFECode  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  58, 60 | | OWASP ASVS  1.7 | | OWASP AppSensor  - | | CAPEC  21 | | SAFECode  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Controle de Acessos** | **A** | **Controle de Acessos** |  | **Controle de Acessos** | **2** | **Controle de Acessos** | **3** |
| Você inventou um novo ataque contra Controle de Acessos |  | Tim consegue alterar nomes/endereços (*paths*) onde os dados são enviados ou encaminhados para alguém | Christian consegue acessar informações, que ele não deveria ter permissão, por meio de outro mecanismo que tenha permissão (ex: indexador de pesquisa, log, relatórios) ou porque a informação está armazenada em cache, ou mantida por mais tempo do que o necessário, ou outro vazamento de informação |
| *Leia mais sobre este tópico em OWASP Development Guide e OWAPS Testing Guide* |  | |  | | --- | | OWASP SCP  44 | | OWASP ASVS  4.1, 4.16, 16.1 | | OWASP AppSensor  - | | CAPEC  153 | | SAFECode  8, 10, 11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  51, 100, 135, 139, 140, 141, 150 | | OWASP ASVS  4.1, 8.2, 9.1-9.6, 9.11, 16.6, 16.7 | | OWASP AppSensor  - | | CAPEC  69, 213 | | SAFECode  8, 10, 11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | |
| **Controle de Acessos** | **4** | **Controle de Acessos** | **5** | **Controle de Acessos** | **6** | **Controle de Acessos** | **7** |
| Kelly consegue ignorar controles de acesso porque estes não falham seguramente (ex: a permissão de acesso está assinalada como padrão) | Chad consegue acessar recursos que não deveria ter acesso devido a inexistência de uma autorização ou por concessão de privilégios excessivos (ex: não usar o princípio de menor privilégio possível). Os recursos podem ser serviços, processos, AJAX, Flash, vídeo, imagens, documentos, arquivos temporários, dados de sessão, propriedades do sistema, dados de configuração, logs | Eduardo consegue acessar dados que ele não tem permissão embora ele tem permissão em formulários, páginas, URL ou pontos de entrada | Yuanjing consegue acessar funções, telas e propriedades do aplicativo, a qual ele não está autorizado a ter acesso |
| |  | | --- | | OWASP SCP  79, 80 | | OWASP ASVS  4.8 | | OWASP AppSensor  - | | CAPEC  122 | | SAFECode  8, 10, 11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP 70,81,83-4,87-9, 99,117,131-2,142,154,170,179 | | OWASP ASVS  4.1, 4.4, 4.9,, 19.3 | | OWASP AppSensor  ACE1-4, HT2 | | CAPEC  75, 87, 95, 126, 149, 155, 203, 213, 264-5 | | SAFECode  8, 10, 11, 13 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  81, 88, 131 | | OWASP ASVS  4.1, 4.4 | | OWASP AppSensor  ACE1-4 | | CAPEC  122 | | SAFECode  8, 10, 11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  81, 85, 86, 131 | | OWASP ASVS  4.1, 4.4 | | OWASP AppSensor  ACE1-4 | | CAPEC  122 | | SAFECode  8, 10, 11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Controle de Acessos** | **8** | **Controle de Acessos** | **9** | **Controle de Acessos** | **10** | **Controle de Acessos** | **J** |
| Tom consegue ignorar regras de negócios alterando o fluxo/sequência usual do processo, ou realizando o processo na forma incorreta, ou manipulando valores de data e hora usados pela aplicação, ou usando recursos válidos para fins não intencionais, ou pela manipulação incorreta do controle de dados | Mike consegue usar indevidamente uma aplicação quando uma funcionalidade é usada de forma muito rápida, ou com muita frequência, ou de outra maneira a qual a funcionalidade não se destina, ou pelo consumo de recursos da aplicação ou pela condição de corrida (*race conditions*) ou utilização excessiva da funcionalidade | Richard consegue ignorar os controles de acesso centralizados pois estes não estão sendo utilizados de forma abrangente em todas as interações | Dinis consegue acessar informações referente a configurações de segurança ou consegue acessar a lista de controle de acesso |
| |  | | --- | | OWASP SCP  10, 32, 93, 94, 189 | | OWASP ASVS  4.10, 4.15, 4.16, 8.13, 15.1 | | OWASP AppSensor  ACE3 | | CAPEC  25, 39, 74, 162, 166, 207 | | SAFECode  8, 10, 11, 12 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  94 | | OWASP ASVS  4.14, 15.2 | | OWASP AppSensor  AE3, FIO1-2, UT2-4, STE1-3 | | CAPEC  26, 29, 119, 261 | | SAFECode  1, 35 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  78, 91 | | OWASP ASVS  1.7, 4.11 | | OWASP AppSensor  ACE1-4 | | CAPEC  36, 95, 121, 179 | | SAFECode  8, 10, 11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  89, 90 | | OWASP ASVS  4.10, 13.2 | | OWASP AppSensor  - | | CAPEC  75, 133, 203 | | SAFECode  8, 10, 11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | |
| **Controle de Acessos** | **Q** | **Controle de Acessos** | **K** |  |  |  |  |
| Christopher consegue injetar um comando que a aplicação vai executar no mais alto nível de privilégio | Ryan consegue influenciar ou alterar controles de acesso e permissões e consegue ignora-los |  |  |
| |  | | --- | | OWASP SCP  209 | | OWASP ASVS  5.12 | | OWASP AppSensor  - | | CAPEC  17, 30, 69, 234 | | SAFECode  8, 10, 11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  77, 89, 91 | | OWASP ASVS  4.9, 4.10, 13.2 | | OWASP AppSensor  - | | CAPEC  207, 554 | | SAFECode  8, 10, 11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Práticas de Criptografia** | **A** | **Práticas de Criptografia** |  | **Práticas de Criptografia** | **2** | **Práticas de Criptografia** | **3** |
| Você inventou um novo ataque contra Práticas de Criptografia |  | Kyun consegue acesso a dados porque isto foi ocultado/ofuscado/escondido ao invés de ser usada uma função de criptografia aprovada. | 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. |
| *Leia mais sobre este tópico em OWASP Cryptographic Storage Cheat Sheet e OWASP Transport Layer Protection Cheat Sheet* |  | |  | | --- | | OWASP SCP  105, 133, 135 | | OWASP ASVS  - | | OWASP AppSensor  - | | CAPEC  - | | SAFECode  21, 29 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | 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 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | |
| **Práticas de Criptografia** | **4** | **Práticas de Criptografia** | **5** | **Práticas de Criptografia** | **6** | **Práticas de Criptografia** | **7** |
| Paulo consegue acesso a dados transitórios não criptografados, embora o canal de comunicação esteja criptografado | Kyle consegue ignorar controles criptográficos porque eles não falham de forma segura (ex: eles são desprotegidos por padrão) | 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 | 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 descriptografada |
| |  | | --- | | OWASP SCP  37, 88, 143, 214 | | OWASP ASVS  7.12, 9.2 | | OWASP AppSensor  - | | CAPEC  185, 186, 187 | | SAFECode  14, 29, 30 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  103, 145 | | OWASP ASVS  7.2, 10.3 | | OWASP AppSensor  - | | CAPEC  - | | SAFECode  21, 29 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | 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 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | 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 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Práticas de Criptografia** | **8** | **Práticas de Criptografia** | **9** | **Práticas de Criptografia** | **10** | **Práticas de Criptografia** | **J** |
| 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 | 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 | 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 | 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  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 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | 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 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  104, 105 | | OWASP ASVS  - | | OWASP AppSensor  - | | CAPEC  97, 463 | | SAFECode  14, 21, 29, 31, 32, 33 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  35, 90, 171, 172 | | OWASP ASVS  2.29 | | OWASP AppSensor  - | | CAPEC  116 | | SAFECode  21, 29 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | |
| **Práticas de Criptografia** | **Q** | **Práticas de Criptografia** | **K** |  |  |  |  |
| Randolph consegue acessar ou prever os dados mestres de criptografia | 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  35, 102 | | OWASP ASVS  7.8, 7.9, 7.11, 7.13, 7.14 | | OWASP AppSensor  - | | CAPEC  116, 117 | | SAFECode  21, 29 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | | |  | | --- | | OWASP SCP  31, 101 | | OWASP ASVS  7.11 | | OWASP AppSensor  - | | CAPEC  207, 554 | | SAFECode  14, 21, 29 | | OWASP Cornucopia Ecommerce Website Edition v1.20-PT-BR | |  |  |