|  |  |  |
| --- | --- | --- |
| WHStore:watsonhall:groups:owasp:OWASP_Image_Toolbox:owasp_logo_122106.eps  **Cornucopia**  **${Common\_Title}**  ${Common\_T00010}  ${Common\_T00020}  Colin Watson  ${Common\_T00030}  Colin Watson and Darío De Filippis  ${Common\_T00040}  Tom Brennan, Johanna Curiel and Timo Goosen  ${Common\_T00100}  ${Common\_T00110}  ${Common\_T00120}  ${Common\_T00130}  ${Common\_T00140}  ${Common\_T00150} ${Common\_T00160} ${Common\_T00170}  ${Common\_T00180} | |  |
| ${Common\_T00200}  ${Common\_T00210} ${Common\_T00220}  ${Common\_T00230} ${Common\_T00240}  ${Common\_T00250} ${Common\_T00260}  ${Common\_T00270}  ${Common\_T00300}  ${Common\_T00310} ${Common\_T00320}   * ${Common\_T00330} * ${Common\_T00340} * ${Common\_T00350} * ${Common\_T00360} * ${Common\_T00370} * ${Common\_T00380}   ${Common\_T00390} ${Common\_T00400}  ${Common\_T00500}  ${Common\_T00510} ${Common\_T00520} ${Common\_T00530} |  | ${Common\_T00600}  ${Common\_T00610}  ${Common\_T00700}  ${Common\_T00710}  ${Common\_T00720} ${Common\_T00730} ${Common\_T00740} ${Common\_T00750} ${Common\_T00760} ${Common\_T00770}  ${Common\_T00780} ${Common\_T00790}  ${Common\_T00800} ${Common\_T00810} ${Common\_T00820} ${Common\_T00830} ${Common\_T00840} ${Common\_T00850}  ${Common\_T00900}  ${Common\_T00910} ${Common\_T00920}  ${Common\_T01000}  ${Common\_T01010} ${Common\_T01020}  ${Common\_T01030}   * ${Common\_T01040} <https://lists.owasp.org/mailman/listinfo/owasp_cornucopia> * ${Common\_T01050} <https://www.owasp.org/index.php/OWASP_Cornucopia>   ${Common\_T01060} ${Common\_T01070} |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ${Common\_T01100}  ${Common\_T01110} ${Common\_T01120} ${Common\_T01130} ${Common\_T01140} ${Common\_T01150}  *${Common\_T01160}*  ${Common\_T01170} ${Common\_T01180}  ${Common\_T01190}  <https://www.owasp.org/index.php/Cornucopia_-_Ecommerce_Website_Edition_-_Wiki_Deck>  ${Common\_T01200}   * ${Common\_T01210} <https://www.owasp.org/index.php/File:OWASP_SCP_Quick_Reference_Guide_v2.pdf> * ${Common\_T01220} <https://www.owasp.org/images/3/33/OWASP_Application_Security_Verification_Standard_3.0.1.pdf> * ${Common\_T01230} <https://www.owasp.org/index.php/AppSensor_DetectionPoints> * ${Common\_T01240}   <http://capec.mitre.org/data/archive/capec_v2.8.zip>   * ${Common\_T01250}   <http://www.safecode.org/publications/SAFECode_Agile_Dev_Security0712.pdf>  ${Common\_T01260} ${Common\_T01270} ${Common\_T01280} ${Common\_T01290}  ${Common\_T01300} ${Common\_T01310}  <https://youtu.be/i5Y0akWj31k><https://www.owasp.org/index.php/File:Cornucopia-scoresheet.pdf>  ${Common\_T01900}  ${Common\_T01910} ${Common\_T01920} ${Common\_T01930}  ${Common\_T01940}  ${Common\_T01950} ${Common\_T01960} ${Common\_T01970}  ${Common\_T01980}  ${Common\_T01990} ${Common\_T02000}  ${Common\_T02010} ${Common\_T02020} ${Common\_T02030}  ${Common\_T02040}  ${Common\_T02100}  ${Common\_T02110} ${Common\_T02120}  ${Common\_T02130} ${Common\_T02140}  ***${Common\_T02600}***  *${Common\_T02610}*  *${Common\_T02620} ${Common\_T02630} ${Common\_T02640}*  *${Common\_T02650}*  *${Common\_T02660}*  *${Common\_T02670}*  *${Common\_T02680} ${Common\_T02690} ${Common\_T02700} ${Common\_T02710} ${Common\_T02720} ${Common\_T02730} ${Common\_T02740}*  *${Common\_T02750}*  *${Common\_T02760} ${Common\_T02770} ${Common\_T02780}*  *${Common\_T02790}*  *${Common\_T02800} ${Common\_T02810}*  *${Common\_T02820}*  *${Common\_T02830} ${Common\_T02840}*  *${Common\_T02850}*  *${Common\_T02860} ${Common\_T02870} ${Common\_T02880}*  *${Common\_T02890}*  *${Common\_T02900} ${Common\_T02910} ${Common\_T02920}* |  | ${Common\_T01400}  ${Common\_T01410} ${Common\_T01420}  ${Common\_T01430} ${Common\_T01440} ${Common\_T01450}  ${Common\_T01500}  ${Common\_T01510} ${Common\_T01520} ${Common\_T01530}  ${Common\_T01540} ${Common\_T01550} ${Common\_T01560} ${Common\_T01570} ${Common\_T01580} ${Common\_T01590}  ${Common\_T01600} ${Common\_T01610}  ${Common\_T01700}  ${Common\_T01710}  ${Common\_T01720}  ${Common\_T01730} ${Common\_T01740}  ${Common\_T01800}  ${Common\_T01810} ${Common\_T01820}  ${Common\_T02200}  ${Common\_T02210}   |  |  |  | | --- | --- | --- | | ${Common\_T02220} | | | | ${Common\_T02230}  *${Common\_T02240}*  ${Common\_T02250}  *${Common\_T02260}* | ${Common\_T02270}  *${Common\_T02280}*  ${Common\_T02290}  *${Common\_T02300}* | ${Common\_T02310}  *${Common\_T02320}*  ${Common\_T02330}  *${Common\_T02340}* |   ${Common\_T02400}  ${Common\_T02410}   |  |  |  | | --- | --- | --- | | ${Common\_T02420} | | | | ${Common\_T02430}  *${Common\_T02440}*  ${Common\_T02450}  *${Common\_T02460}* | ${Common\_T02470}  *${Common\_T02480}*  ${Common\_T02490}  *${Common\_T02500}* | ${Common\_T02510}  *${Common\_T02520}*  ${Common\_T02530}  *${Common\_T02540}* |   *${Common\_T02930}*  *${Common\_T02940} ${Common\_T02950} ${Common\_T02960} ${Common\_T02970} ${Common\_T02980} ${Common\_T02990}*  *${Common\_T03000}*  *${Common\_T03010} ${Common\_T03020}*  *${Common\_T03030}*  *${Common\_T03040} ${Common\_T03050}*  <https://www.owasp.org/index.php/Cornucopia_-_Ecommerce_Website_Edition_-_Wiki_Deck>  *${Common\_T03060} ${Common\_T03070}*  [https://www.owasp.org/index.php/OWASP\_Cornucopia - tab=FAQs](https://www.owasp.org/index.php/OWASP_Cornucopia#tab=FAQs) |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Data validation & encoding** | **A** | **Data validation & encoding** |  | **Data validation & encoding** | **2** | **Data validation & encoding** | **3** |
| Você inventou um novo ataque contra a Validação de Dados de Entrada e Codificação de Dados de Saída | (${Common\_NoCard}) | 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  ${VE\_VE2\_owasp\_scp} | | OWASP ASVS  ${VE\_VE2\_owasp\_asvs} | | OWASP APPSENSOR  ${VE\_VE2\_owasp\_appsensor} | | CAPEC  ${VE\_VE2\_capec} | | SAFECODE  ${VE\_VE2\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${VE\_VE3\_owasp\_scp} | | OWASP ASVS  ${VE\_VE3\_owasp\_asvs} | | OWASP APPSENSOR  ${VE\_VE3\_owasp\_appsensor} | | CAPEC  ${VE\_VE3\_capec} | | SAFECODE  ${VE\_VE3\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Data validation & encoding** | **4** | **Data validation & encoding** | **5** | **Data validation & encoding** | **6** | **Data validation & encoding** | **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  ${VE\_VE4\_owasp\_scp} | | OWASP ASVS  ${VE\_VE4\_owasp\_asvs} | | OWASP APPSENSOR  ${VE\_VE4\_owasp\_appsensor} | | CAPEC  ${VE\_VE4\_capec} | | SAFECODE  ${VE\_VE4\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${VE\_VE5\_owasp\_scp} | | OWASP ASVS  ${VE\_VE5\_owasp\_asvs} | | OWASP APPSENSOR  ${VE\_VE5\_owasp\_appsensor} | | CAPEC  ${VE\_VE5\_capec} | | SAFECODE  ${VE\_VE5\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${VE\_VE6\_owasp\_scp} | | OWASP ASVS  ${VE\_VE6\_owasp\_asvs} | | OWASP APPSENSOR  ${VE\_VE6\_owasp\_appsensor} | | CAPEC  ${VE\_VE6\_capec} | | SAFECODE  ${VE\_VE6\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${VE\_VE7\_owasp\_scp} | | OWASP ASVS  ${VE\_VE7\_owasp\_asvs} | | OWASP APPSENSOR  ${VE\_VE7\_owasp\_appsensor} | | CAPEC  ${VE\_VE7\_capec} | | SAFECODE  ${VE\_VE7\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Data validation & encoding** | **8** | **Data validation & encoding** | **9** | **Data validation & encoding** | **10** | **Data validation & encoding** | **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  ${VE\_VE8\_owasp\_scp} | | OWASP ASVS  ${VE\_VE8\_owasp\_asvs} | | OWASP APPSENSOR  ${VE\_VE8\_owasp\_appsensor} | | CAPEC  ${VE\_VE8\_capec} | | SAFECODE  ${VE\_VE8\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${VE\_VE9\_owasp\_scp} | | OWASP ASVS  ${VE\_VE9\_owasp\_asvs} | | OWASP APPSENSOR  ${VE\_VE9\_owasp\_appsensor} | | CAPEC  ${VE\_VE9\_capec} | | SAFECODE  ${VE\_VE9\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${VE\_VE10\_owasp\_scp} | | OWASP ASVS  ${VE\_VE10\_owasp\_asvs} | | OWASP APPSENSOR  ${VE\_VE10\_owasp\_appsensor} | | CAPEC  ${VE\_VE10\_capec} | | SAFECODE  ${VE\_VE10\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${VE\_VEJ\_owasp\_scp} | | OWASP ASVS  ${VE\_VEJ\_owasp\_asvs} | | OWASP APPSENSOR  ${VE\_VEJ\_owasp\_appsensor} | | CAPEC  ${VE\_VEJ\_capec} | | SAFECODE  ${VE\_VEJ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Data validation & encoding** | **Q** | **Data validation & encoding** | **K** |  |  |  |  |
| Geoff consegue injetar dados num dispositivo ou num interpretador no lado do cliente porque uma interface parametrizada não foi usada, ou não foi implementada corretamente, ou os dados não foram codificados corretamente para o contexto proposto, ou não há uma política restritiva para a codificação ou a inclusão de dados | Gabe consegue injetar dados num interpretador no lado do servidor (ex: SQL, comandos para o sistema operacional, Xpath, Server JavaScript, SMTP) porque uma interface parametrizada não foi usada ou não foi implementada corretamente | (${Common\_NoCard}) | (${Common\_NoCard}) |
| |  | | --- | | OWASP SCP  ${VE\_VEQ\_owasp\_scp} | | OWASP ASVS  ${VE\_VEQ\_owasp\_asvs} | | OWASP APPSENSOR  ${VE\_VEQ\_owasp\_appsensor} | | CAPEC  ${VE\_VEQ\_capec} | | SAFECODE  ${VE\_VEQ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${VE\_VEK\_owasp\_scp} | | OWASP ASVS  ${VE\_VEK\_owasp\_asvs} | | OWASP APPSENSOR  ${VE\_VEK\_owasp\_appsensor} | | CAPEC  ${VE\_VEK\_capec} | | SAFECODE  ${VE\_VEK\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Authentication** | **A** | **Authentication** |  | **Authentication** | **2** | **Authentication** | **3** |
| Você inventou um novo ataque contra a Autenticação e Gerenciamento de Credenciais | (${Common\_NoCard}) | 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  ${AT\_AT2\_owasp\_scp} | | OWASP ASVS  ${AT\_AT2\_owasp\_asvs} | | OWASP APPSENSOR  ${AT\_AT2\_owasp\_appsensor} | | CAPEC  ${AT\_AT2\_capec} | | SAFECODE  ${AT\_AT2\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${AT\_AT3\_owasp\_scp} | | OWASP ASVS  ${AT\_AT3\_owasp\_asvs} | | OWASP APPSENSOR  ${AT\_AT3\_owasp\_appsensor} | | CAPEC  ${AT\_AT3\_capec} | | SAFECODE  ${AT\_AT3\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Authentication** | **4** | **Authentication** | **5** | **Authentication** | **6** | **Authentication** | **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  ${AT\_AT4\_owasp\_scp} | | OWASP ASVS  ${AT\_AT4\_owasp\_asvs} | | OWASP APPSENSOR  ${AT\_AT4\_owasp\_appsensor} | | CAPEC  ${AT\_AT4\_capec} | | SAFECODE  ${AT\_AT4\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${AT\_AT5\_owasp\_scp} | | OWASP ASVS  ${AT\_AT5\_owasp\_asvs} | | OWASP APPSENSOR  ${AT\_AT5\_owasp\_appsensor} | | CAPEC  ${AT\_AT5\_capec} | | SAFECODE  ${AT\_AT5\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${AT\_AT6\_owasp\_scp} | | OWASP ASVS  ${AT\_AT6\_owasp\_asvs} | | OWASP APPSENSOR  ${AT\_AT6\_owasp\_appsensor} | | CAPEC  ${AT\_AT6\_capec} | | SAFECODE  ${AT\_AT6\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${AT\_AT7\_owasp\_scp} | | OWASP ASVS  ${AT\_AT7\_owasp\_asvs} | | OWASP APPSENSOR  ${AT\_AT7\_owasp\_appsensor} | | CAPEC  ${AT\_AT7\_capec} | | SAFECODE  ${AT\_AT7\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Authentication** | **8** | **Authentication** | **9** | **Authentication** | **10** | **Authentication** | **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  ${AT\_AT8\_owasp\_scp} | | OWASP ASVS  ${AT\_AT8\_owasp\_asvs} | | OWASP APPSENSOR  ${AT\_AT8\_owasp\_appsensor} | | CAPEC  ${AT\_AT8\_capec} | | SAFECODE  ${AT\_AT8\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${AT\_AT9\_owasp\_scp} | | OWASP ASVS  ${AT\_AT9\_owasp\_asvs} | | OWASP APPSENSOR  ${AT\_AT9\_owasp\_appsensor} | | CAPEC  ${AT\_AT9\_capec} | | SAFECODE  ${AT\_AT9\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${AT\_AT10\_owasp\_scp} | | OWASP ASVS  ${AT\_AT10\_owasp\_asvs} | | OWASP APPSENSOR  ${AT\_AT10\_owasp\_appsensor} | | CAPEC  ${AT\_AT10\_capec} | | SAFECODE  ${AT\_AT10\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${AT\_ATJ\_owasp\_scp} | | OWASP ASVS  ${AT\_ATJ\_owasp\_asvs} | | OWASP APPSENSOR  ${AT\_ATJ\_owasp\_appsensor} | | CAPEC  ${AT\_ATJ\_capec} | | SAFECODE  ${AT\_ATJ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Authentication** | **Q** | **Authentication** | **K** |  |  |  |  |
| Jaime consegue ignorar a autenticação porque não é aplicado o mesmo rigor para todas as funções de autenticação (ex: logar, troca de senha, recuperação de senha, logout, acesso administrador) ou não é aplicado o mesmo rigor nos diversos locais de acesso e versões do sistema(ex:mobile website, mobile app, full website, API, call center) | Olga consegue influenciar ou alterar o código ou a rotina de autenticação e com isto ignorar a autenticação | (${Common\_NoCard}) | (${Common\_NoCard}) |
| |  | | --- | | OWASP SCP  ${AT\_ATQ\_owasp\_scp} | | OWASP ASVS  ${AT\_ATQ\_owasp\_asvs} | | OWASP APPSENSOR  ${AT\_ATQ\_owasp\_appsensor} | | CAPEC  ${AT\_ATQ\_capec} | | SAFECODE  ${AT\_ATQ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${AT\_ATK\_owasp\_scp} | | OWASP ASVS  ${AT\_ATK\_owasp\_asvs} | | OWASP APPSENSOR  ${AT\_ATK\_owasp\_appsensor} | | CAPEC  ${AT\_ATK\_capec} | | SAFECODE  ${AT\_ATK\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Session management** | **A** | **Session management** |  | **Session management** | **2** | **Session management** | **3** |
| Você inventou um novo ataque contra o Gerenciamento de Sessões | (${Common\_NoCard}) | 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  ${SM\_SM2\_owasp\_scp} | | OWASP ASVS  ${SM\_SM2\_owasp\_asvs} | | OWASP APPSENSOR  ${SM\_SM2\_owasp\_appsensor} | | CAPEC  ${SM\_SM2\_capec} | | SAFECODE  ${SM\_SM2\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${SM\_SM3\_owasp\_scp} | | OWASP ASVS  ${SM\_SM3\_owasp\_asvs} | | OWASP APPSENSOR  ${SM\_SM3\_owasp\_appsensor} | | CAPEC  ${SM\_SM3\_capec} | | SAFECODE  ${SM\_SM3\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Session management** | **4** | **Session management** | **5** | **Session management** | **6** | **Session management** | **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  ${SM\_SM4\_owasp\_scp} | | OWASP ASVS  ${SM\_SM4\_owasp\_asvs} | | OWASP APPSENSOR  ${SM\_SM4\_owasp\_appsensor} | | CAPEC  ${SM\_SM4\_capec} | | SAFECODE  ${SM\_SM4\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${SM\_SM5\_owasp\_scp} | | OWASP ASVS  ${SM\_SM5\_owasp\_asvs} | | OWASP APPSENSOR  ${SM\_SM5\_owasp\_appsensor} | | CAPEC  ${SM\_SM5\_capec} | | SAFECODE  ${SM\_SM5\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${SM\_SM6\_owasp\_scp} | | OWASP ASVS  ${SM\_SM6\_owasp\_asvs} | | OWASP APPSENSOR  ${SM\_SM6\_owasp\_appsensor} | | CAPEC  ${SM\_SM6\_capec} | | SAFECODE  ${SM\_SM6\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${SM\_SM7\_owasp\_scp} | | OWASP ASVS  ${SM\_SM7\_owasp\_asvs} | | OWASP APPSENSOR  ${SM\_SM7\_owasp\_appsensor} | | CAPEC  ${SM\_SM7\_capec} | | SAFECODE  ${SM\_SM7\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Session management** | **8** | **Session management** | **9** | **Session management** | **10** | **Session management** | **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  ${SM\_SM8\_owasp\_scp} | | OWASP ASVS  ${SM\_SM8\_owasp\_asvs} | | OWASP APPSENSOR  ${SM\_SM8\_owasp\_appsensor} | | CAPEC  ${SM\_SM8\_capec} | | SAFECODE  ${SM\_SM8\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${SM\_SM9\_owasp\_scp} | | OWASP ASVS  ${SM\_SM9\_owasp\_asvs} | | OWASP APPSENSOR  ${SM\_SM9\_owasp\_appsensor} | | CAPEC  ${SM\_SM9\_capec} | | SAFECODE  ${SM\_SM9\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${SM\_SM10\_owasp\_scp} | | OWASP ASVS  ${SM\_SM10\_owasp\_asvs} | | OWASP APPSENSOR  ${SM\_SM10\_owasp\_appsensor} | | CAPEC  ${SM\_SM10\_capec} | | SAFECODE  ${SM\_SM10\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${SM\_SMJ\_owasp\_scp} | | OWASP ASVS  ${SM\_SMJ\_owasp\_asvs} | | OWASP APPSENSOR  ${SM\_SMJ\_owasp\_appsensor} | | CAPEC  ${SM\_SMJ\_capec} | | SAFECODE  ${SM\_SMJ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Session management** | **Q** | **Session management** | **K** |  |  |  |  |
| Salim consegue ignorar o gerenciamento de sessão porque este não é aplicado de forma abrangente e consistente por toda a aplicação | Peter consegue ignorar o controle de gerenciamento de sessão porque este foi autoconstruído e/ou é fraco, ao invés de ter sido usado a estrutura padrão de um framework ou um modulo testado e aprovado | (${Common\_NoCard}) | (${Common\_NoCard}) |
| |  | | --- | | OWASP SCP  ${SM\_SMQ\_owasp\_scp} | | OWASP ASVS  ${SM\_SMQ\_owasp\_asvs} | | OWASP APPSENSOR  ${SM\_SMQ\_owasp\_appsensor} | | CAPEC  ${SM\_SMQ\_capec} | | SAFECODE  ${SM\_SMQ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${SM\_SMK\_owasp\_scp} | | OWASP ASVS  ${SM\_SMK\_owasp\_asvs} | | OWASP APPSENSOR  ${SM\_SMK\_owasp\_appsensor} | | CAPEC  ${SM\_SMK\_capec} | | SAFECODE  ${SM\_SMK\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Authorization** | **A** | **Authorization** |  | **Authorization** | **2** | **Authorization** | **3** |
| Você inventou um novo ataque contra Controle de Acessos | (${Common\_NoCard}) | 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 outra vazamento de informação |
| *Leia mais sobre este tópico em OWASP Development Guide e OWAPS Testing Guide* |  | |  | | --- | | OWASP SCP  ${AZ\_AZ2\_owasp\_scp} | | OWASP ASVS  ${AZ\_AZ2\_owasp\_asvs} | | OWASP APPSENSOR  ${AZ\_AZ2\_owasp\_appsensor} | | CAPEC  ${AZ\_AZ2\_capec} | | SAFECODE  ${AZ\_AZ2\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${AZ\_AZ3\_owasp\_scp} | | OWASP ASVS  ${AZ\_AZ3\_owasp\_asvs} | | OWASP APPSENSOR  ${AZ\_AZ3\_owasp\_appsensor} | | CAPEC  ${AZ\_AZ3\_capec} | | SAFECODE  ${AZ\_AZ3\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Authorization** | **4** | **Authorization** | **5** | **Authorization** | **6** | **Authorization** | **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  ${AZ\_AZ4\_owasp\_scp} | | OWASP ASVS  ${AZ\_AZ4\_owasp\_asvs} | | OWASP APPSENSOR  ${AZ\_AZ4\_owasp\_appsensor} | | CAPEC  ${AZ\_AZ4\_capec} | | SAFECODE  ${AZ\_AZ4\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${AZ\_AZ5\_owasp\_scp} | | OWASP ASVS  ${AZ\_AZ5\_owasp\_asvs} | | OWASP APPSENSOR  ${AZ\_AZ5\_owasp\_appsensor} | | CAPEC  ${AZ\_AZ5\_capec} | | SAFECODE  ${AZ\_AZ5\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${AZ\_AZ6\_owasp\_scp} | | OWASP ASVS  ${AZ\_AZ6\_owasp\_asvs} | | OWASP APPSENSOR  ${AZ\_AZ6\_owasp\_appsensor} | | CAPEC  ${AZ\_AZ6\_capec} | | SAFECODE  ${AZ\_AZ6\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${AZ\_AZ7\_owasp\_scp} | | OWASP ASVS  ${AZ\_AZ7\_owasp\_asvs} | | OWASP APPSENSOR  ${AZ\_AZ7\_owasp\_appsensor} | | CAPEC  ${AZ\_AZ7\_capec} | | SAFECODE  ${AZ\_AZ7\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Authorization** | **8** | **Authorization** | **9** | **Authorization** | **10** | **Authorization** | **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  ${AZ\_AZ8\_owasp\_scp} | | OWASP ASVS  ${AZ\_AZ8\_owasp\_asvs} | | OWASP APPSENSOR  ${AZ\_AZ8\_owasp\_appsensor} | | CAPEC  ${AZ\_AZ8\_capec} | | SAFECODE  ${AZ\_AZ8\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${AZ\_AZ9\_owasp\_scp} | | OWASP ASVS  ${AZ\_AZ9\_owasp\_asvs} | | OWASP APPSENSOR  ${AZ\_AZ9\_owasp\_appsensor} | | CAPEC  ${AZ\_AZ9\_capec} | | SAFECODE  ${AZ\_AZ9\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${AZ\_AZ10\_owasp\_scp} | | OWASP ASVS  ${AZ\_AZ10\_owasp\_asvs} | | OWASP APPSENSOR  ${AZ\_AZ10\_owasp\_appsensor} | | CAPEC  ${AZ\_AZ10\_capec} | | SAFECODE  ${AZ\_AZ10\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${AZ\_AZJ\_owasp\_scp} | | OWASP ASVS  ${AZ\_AZJ\_owasp\_asvs} | | OWASP APPSENSOR  ${AZ\_AZJ\_owasp\_appsensor} | | CAPEC  ${AZ\_AZJ\_capec} | | SAFECODE  ${AZ\_AZJ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Authorization** | **Q** | **Authorization** | **K** |  |  |  |  |
| Christopher consegue injetar um comando que a aplicação vai executar no mais alto nível de privilégio | Ryan consegue influenciar ou alterar controles de acesso e permissões e consegue ignora-los | (${Common\_NoCard}) | (${Common\_NoCard}) |
| |  | | --- | | OWASP SCP  ${AZ\_AZQ\_owasp\_scp} | | OWASP ASVS  ${AZ\_AZQ\_owasp\_asvs} | | OWASP APPSENSOR  ${AZ\_AZQ\_owasp\_appsensor} | | CAPEC  ${AZ\_AZQ\_capec} | | SAFECODE  ${AZ\_AZQ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${AZ\_AZK\_owasp\_scp} | | OWASP ASVS  ${AZ\_AZK\_owasp\_asvs} | | OWASP APPSENSOR  ${AZ\_AZK\_owasp\_appsensor} | | CAPEC  ${AZ\_AZK\_capec} | | SAFECODE  ${AZ\_AZK\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Cryptography** | **A** | **Cryptography** |  | **Cryptography** | **2** | **Cryptography** | **3** |
| Você inventou um novo ataque contra Práticas de Criptografia | (${Common\_NoCard}) | 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  ${CR\_CR2\_owasp\_scp} | | OWASP ASVS  ${CR\_CR2\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CR2\_owasp\_appsensor} | | CAPEC  ${CR\_CR2\_capec} | | SAFECODE  ${CR\_CR2\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${CR\_CR3\_owasp\_scp} | | OWASP ASVS  ${CR\_CR3\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CR3\_owasp\_appsensor} | | CAPEC  ${CR\_CR3\_capec} | | SAFECODE  ${CR\_CR3\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Cryptography** | **4** | **Cryptography** | **5** | **Cryptography** | **6** | **Cryptography** | **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  ${CR\_CR4\_owasp\_scp} | | OWASP ASVS  ${CR\_CR4\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CR4\_owasp\_appsensor} | | CAPEC  ${CR\_CR4\_capec} | | SAFECODE  ${CR\_CR4\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${CR\_CR5\_owasp\_scp} | | OWASP ASVS  ${CR\_CR5\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CR5\_owasp\_appsensor} | | CAPEC  ${CR\_CR5\_capec} | | SAFECODE  ${CR\_CR5\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${CR\_CR6\_owasp\_scp} | | OWASP ASVS  ${CR\_CR6\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CR6\_owasp\_appsensor} | | CAPEC  ${CR\_CR6\_capec} | | SAFECODE  ${CR\_CR6\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${CR\_CR7\_owasp\_scp} | | OWASP ASVS  ${CR\_CR7\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CR7\_owasp\_appsensor} | | CAPEC  ${CR\_CR7\_capec} | | SAFECODE  ${CR\_CR7\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Cryptography** | **8** | **Cryptography** | **9** | **Cryptography** | **10** | **Cryptography** | **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  ${CR\_CR8\_owasp\_scp} | | OWASP ASVS  ${CR\_CR8\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CR8\_owasp\_appsensor} | | CAPEC  ${CR\_CR8\_capec} | | SAFECODE  ${CR\_CR8\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${CR\_CR9\_owasp\_scp} | | OWASP ASVS  ${CR\_CR9\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CR9\_owasp\_appsensor} | | CAPEC  ${CR\_CR9\_capec} | | SAFECODE  ${CR\_CR9\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${CR\_CR10\_owasp\_scp} | | OWASP ASVS  ${CR\_CR10\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CR10\_owasp\_appsensor} | | CAPEC  ${CR\_CR10\_capec} | | SAFECODE  ${CR\_CR10\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${CR\_CRJ\_owasp\_scp} | | OWASP ASVS  ${CR\_CRJ\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CRJ\_owasp\_appsensor} | | CAPEC  ${CR\_CRJ\_capec} | | SAFECODE  ${CR\_CRJ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Cryptography** | **Q** | **Cryptography** | **K** |  |  |  |  |
| Randolph consegue acessar ou prever os dados mestres de criptografia | Dan consegue influenciar ou alternar as rotinas/codificações de criptografia (encriptação, hashing, assinaturas digitais, números aleatórios e geração de GUID) e consegue ignorá-los também | (${Common\_NoCard}) | (${Common\_NoCard}) |
| |  | | --- | | OWASP SCP  ${CR\_CRQ\_owasp\_scp} | | OWASP ASVS  ${CR\_CRQ\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CRQ\_owasp\_appsensor} | | CAPEC  ${CR\_CRQ\_capec} | | SAFECODE  ${CR\_CRQ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${CR\_CRK\_owasp\_scp} | | OWASP ASVS  ${CR\_CRK\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CRK\_owasp\_appsensor} | | CAPEC  ${CR\_CRK\_capec} | | SAFECODE  ${CR\_CRK\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Cornucopia** | **A** | **Cornucopia** |  | **Cornucopia** | **2** | **Cornucopia** | **3** |
| Você inventou um novo ataque de qualquer tipo | (${Common\_NoCard}) | Lee consegue ignorar os controles do aplicativo pois foram usadas funções arriscadas da linguagem de programação ao invés de opções seguras, ou há erros de conversão, ou porque o aplicativo está inseguro quando um recurso externo está indisponível, ou há race condition, ou há problemas na inicialização ou alocação de recursos, ou quando há sobrecarga | Andrew consegue acessar o código fonte, ou descompilar o aplicativo, ou consegue acessar a lógica do negócio para entender como a aplicação funciona e quais segredos ela contêm |
| *Leia mais sobre segurança da aplicação nos guias da OWASP (Requirements, Development, Code Review and Testing) e na série OWASP Cheat Sheet, e no modelo de maturidade Open SAMM (Software Assurance Maturity Model)* |  | |  | | --- | | OWASP SCP  ${CO\_CO2\_owasp\_scp} | | OWASP ASVS  ${CR\_CO2\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CO2\_owasp\_appsensor} | | CAPEC  ${CR\_CO2\_capec} | | SAFECODE  ${CR\_CO2\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${CO\_CO3\_owasp\_scp} | | OWASP ASVS  ${CR\_CO3\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CO3\_owasp\_appsensor} | | CAPEC  ${CR\_CO3\_capec} | | SAFECODE  ${CR\_CO3\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Cornucopia** | **4** | **Cornucopia** | **5** | **Cornucopia** | **6** | **Cornucopia** | **7** |
| Keith consegue realizar uma ação e isto não é atribuído a ele | Larry consegue induzir a confiança de outras partes, incluindo usuários autenticados, ou violar esta confiança em outro lugar (ex: em outro aplicativo) | Aaron consegue ignorar os controles porque a manipulação de erros/exceções é perdida/ignorada, ou é implementada de forma inconsistente ou parcial, ou não há negação de acesso por padrão (ex: erros devem terminar o acesso/execução da funcionalidade), ou depende do tratamento por algum outro serviço ou sistema | As ações de Mwengu não podem ser investigadas porque não há um registro correto de eventos de segurança com precisão, ou não há uma trilha de auditoria completa, ou estas podem ser alteradas ou excluídas pelo Mwengu, ou não existe um serviço de registro centralizado |
| |  | | --- | | OWASP SCP  ${CO\_CO4\_owasp\_scp} | | OWASP ASVS  ${CR\_CO4\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CO4\_owasp\_appsensor} | | CAPEC  ${CR\_CO4\_capec} | | SAFECODE  ${CR\_CO4\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${CO\_CO5\_owasp\_scp} | | OWASP ASVS  ${CR\_CO5\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CO5\_owasp\_appsensor} | | CAPEC  ${CR\_CO5\_capec} | | SAFECODE  ${CR\_CO5\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${CO\_CO6\_owasp\_scp} | | OWASP ASVS  ${CR\_CO6\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CO6\_owasp\_appsensor} | | CAPEC  ${CR\_CO6\_capec} | | SAFECODE  ${CR\_CO6\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${CO\_CO7\_owasp\_scp} | | OWASP ASVS  ${CR\_CO7\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CO7\_owasp\_appsensor} | | CAPEC  ${CR\_CO7\_capec} | | SAFECODE  ${CR\_CO7\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Cornucopia** | **8** | **Cornucopia** | **9** | **Cornucopia** | **10** | **Cornucopia** | **J** |
| David consegue ignorar o aplicativo para obter acesso aos dados porque a infraestrutura de rede e servidores e os serviços suportados não foram configurados de forma segura, as configurações não são verificadas periodicamente e os patches de segurança não são aplicados, ou os dados armazenados localmente não são fisicamente protegidos | Michael consegue ignorar o aplicativo para obter acesso aos dados porque ferramentas ou interfaces administrativas não estão adequadamente seguras | Xavier consegue contornar os controles do aplicativo porque os códigos fontes tanto dos frameworks, como de bibliotecas e componentes utilizados contêm código malicioso ou vulnerabilidades | Roman consegue explorar o aplicativo pois este foi compilado usando ferramentas desatualizadas ou configurações não seguras como padrão ou informações de segurança não foram documentadas e passadas para o time operacional |
| |  | | --- | | OWASP SCP  ${CO\_CO8\_owasp\_scp} | | OWASP ASVS  ${CR\_CO8\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CO8\_owasp\_appsensor} | | CAPEC  ${CR\_CO8\_capec} | | SAFECODE  ${CR\_CO8\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${CO\_CO9\_owasp\_scp} | | OWASP ASVS  ${CR\_CO9\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CO9\_owasp\_appsensor} | | CAPEC  ${CR\_CO9\_capec} | | SAFECODE  ${CR\_CO9\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${CO\_CO10\_owasp\_scp} | | OWASP ASVS  ${CR\_CO10\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_CO10\_owasp\_appsensor} | | CAPEC  ${CR\_CO10\_capec} | | SAFECODE  ${CR\_CO10\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${CO\_COJ\_owasp\_scp} | | OWASP ASVS  ${CR\_COJ\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_COJ\_owasp\_appsensor} | | CAPEC  ${CR\_COJ\_capec} | | SAFECODE  ${CR\_COJ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Cornucopia** | **Q** | **Cornucopia** | **K** | **Joker** | **Joker** | **Joker** | **Joker** |
| Jim pode realizar ações mal-intencionadas, não normais, sem detecção e resposta em tempo real pela aplicação | Gareth pode utilizar o aplicativo para negar o serviço a alguns ou a todos os usuários | Alice consegue utilizar a aplicação para realizar ataques a dados e usuários do sistema | Bob pode influenciar, alterar ou mudar a aplicação para que ela não cumpra os propósitos legais, regulamentadores, contratuais ou outras diretrizes organizacionais |
| |  | | --- | | OWASP SCP  ${CO\_COQ\_owasp\_scp} | | OWASP ASVS  ${CR\_COQ\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_COQ\_owasp\_appsensor} | | CAPEC  ${CR\_COQ\_capec} | | SAFECODE  ${CR\_COQ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  ${CO\_COK\_owasp\_scp} | | OWASP ASVS  ${CR\_COK\_owasp\_asvs} | | OWASP APPSENSOR  ${CR\_COK\_owasp\_appsensor} | | CAPEC  ${CR\_COK\_capec} | | SAFECODE  ${CR\_COK\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | *Você pensou em se tornar membro individual da OWASP? Todas as ferramentas, guias e reuniões locais são gratuitas para todos, mas ser um membro individual apoia o trabalho da OWASP* | *Examine as vulnerabilidades e descubra como elas podem ser solucionadas através do aplicativo de treinamento OWASP Broken Web Applications VM, ou usando o desafio online Hacking Lab. Ambos são gratuitos* |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Cut here |  |  |  |  |  |  |  |  |
|  | **${ }** |  |  |  |  |  | **J** |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |



${Common\_T03100}

| ${Common\_T03110} | | ${Common\_T03120} |
| --- | --- | --- |
| ${Common\_T03130} | 30 Jul 2012 | ${Common\_T03140} |
| ${Common\_T03150} | 10 Aug 2012 | ${Common\_T03160} |
| ${Common\_T03170} | 15 Aug 2012 | ${Common\_T03180} |
| ${Common\_T03190} | 25 Feb 2013 | ${Common\_T03200} ${Common\_T03210} ${Common\_T03220} ${Common\_T03230} |
| ${Common\_T03240} | 25 Feb 2013 | ${Common\_T03250} |
| ${Common\_T03260} | 03 Jun 2013 | ${Common\_T03270} ${Common\_T03280} ${Common\_T03290} ${Common\_T03300} ${Common\_T03310} ${Common\_T03320} ${Common\_T03330} ${Common\_T03340} |
| ${Common\_T03350} | 14 Aug 2013 | ${Common\_T03360} ${Common\_T03370} ${Common\_T03380} ${Common\_T03390} ${Common\_T03400} ${Common\_T03410} |
| ${Common\_T03420} | 18 Sep 2013 | ${Common\_T03430} ${Common\_T03440} ${Common\_T03450} ${Common\_T03460} |
| ${Common\_T03470} | 01 Feb 2014 | ${Common\_T03480} |
| ${Common\_T03490} | 21 Mar 2014 | ${Common\_T03500} ${Common\_T03510} ${Common\_T03520} ${Common\_T03530} |
| ${Common\_T03540} | 04 Mar 2015 | ${Common\_T03550} ${Common\_T03560} ${Common\_T03570} |
| ${Common\_T03580} | 29 Jun 2016 | ${Common\_T03590} ${Common\_T03600} ${Common\_T03610} ${Common\_T03620} ${Common\_T03630} ${Common\_T03640} ${Common\_T03650} ${Common\_T03660} ${Common\_T03670} ${Common\_T03680} ${Common\_T03690} ${Common\_T03700} |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ${Common\_T03800}  ${Common\_T03810}  ${Common\_T03820}  ${Common\_T03830}  ${Common\_T03840}   |  |  |  | | --- | --- | --- | | * Simon Bennetts * Tom Brennan * Fabio Cerullo * Oana Cornea * Johanna Curiel * Todd Dahl * Luis Enriquez * Ken Ferris * Darío De Filippis | * Sebastien Gioria * Tobias Gondrom * Timo Goosen * Anthony Harrison * John Herrlin * Jerry Hoff * Marios Kourtesis * Antonis Manaras * Jim Manico | * Mark Miller * Cam Morris * Susana Romaniz * Ravishankar Sahadevan * Tao Sauvage * Stephen de Vries * Colin Watson |  * ${Common\_T03850} * ${Common\_T03860} * ${Common\_T03870} * ${Common\_T03880}   ${Common\_T03900}  ${Common\_T03910}   * ${Common\_T03920} <https://www.youtube.com/watch?v=i5Y0akWj31k> * ${Common\_T03930} <http://trustedsoftwarealliance.com/2014/03/21/the-owasp-cornucopia-project-with-colin-watson/> * ${Common\_T03940} <https://www.youtube.com/watch?v=Q_LE-8xNXVk>   ${Common\_T03950} |  |