|  |  |  |
| --- | --- | --- |
| 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** |
| Vous avez inventé une nouvelle attaque contre la Validation des Données et l'Encodage | (${Common\_NoCard}) | Brian peut recueillir des informations sur les configurations sous-jacentes, les schémas, la logique, le code, le logiciel, les services et l'infrastructure, de par le contenu des messages d'erreur, ou une mauvaise configuration, ou la présence de fichiers d'installation par défaut, ou des ressources de test, de sauvegarde, de copie, ou l'exposition de code source | Robert peut saisir des données malveillantes, car le format attendu n'est pas vérifié, ou des duplicatas sont acceptés, ou la structure n'est pas vérifiée, ou les éléments individuels des données ne sont pas validées : type, plage, longueur, liste blanche de caractères ou de formats autorisés |
| *Apprenez-en plus à ce sujet dans les antisèches gratuites OWASP sur la Validation des Entrées, la Prévention des XSS, DOM-XSS, et des Injections SQL, ainsi que sur les Requêtes Paramétrées* |  | |  | | --- | | 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 peut saisir des noms de champs ou des données malveillantes, car ils ne sont pas vérifiés dans le contexte de l'utilisateur ou du processus en cours | Jee peut contourner les routines d'encodage centralisées, car celles-ci ne sont pas utilisées partout, ou bien de mauvais encodages sont utilisés | Jason peut contourner les routines d'encodage centralisées, car celles-ci ne sont pas utilisées à chaque saisie | Jan peut générer des messages de sorte à tromper la validation des données, car le jeu de caractères n'est pas spécifié/imposé, ou les données sont encodées plusieurs fois, ou les données ne sont pas pleinement converties dans le format que l'application utilise (par exemple canonicalisation) avant leur validation, ou les variables sont insuffisamment typées |
| |  | | --- | | 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 peut contourner les routines de sanitisation centralisées, car celles-ci ne sont pas pleinement utilisées | Shamun peut contourner la validation des saisies ou la validation des sorties, car les échecs de validation ne sont pas rejetés et/ou sanitisés | Darío peut exploiter la confiance que l'application place dans une source de données (par exemple données définies par l'utilisateur, manipulation de données stockées localement, changement de déclaration des données sur un système client, manque de vérification de l'identité pendant la validation de données de telle manière que Darío peut se faire passer pour Colin) | Dennis a le contrôle sur la validation des saisies, la validation des sorties, ou le code d'encodage des sorties, ou les routines, de telle manière que celles-ci peuvent être contournées |
| |  | | --- | | 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  ${VE\_VEJ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Data validation & encoding** | **Q** | **Data validation & encoding** | **K** |  |  |  |  |
| Geoff peut injecter des données dans un client ou un système interpréteur, car une interface paramétrée n'est pas utilisée, ou n'a pas été implémentée correctement, ou les données n'ont pas été encodées correctement dans ce contexte, ou il n'y a pas de politique restrictive sur le code ou les ajouts de données | Gabe peut injecter des données dans un interpréteur côté serveur (ex : SQL, commandes OS, Xpath, Server JavaScript, SMTP), car une interface paramétrée fortement typée n'est pas utilisée ou n'a pas été implémentée correctement | (${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** |
| Vous avez inventé une nouvelle attaque contre l'Authentification | (${Common\_NoCard}) | James peut entreprendre des fonctions d'authentification sans que l'utilisateur légitime ne s'en aperçoive (par exemple tentative d'authentification, authentification avec des identifiants volés, mise à jour du mot de passe) | Muhammad peut obtenir le mot de passe d'un utilisateur ou d'autres secrets comme des questions de sécurité, de par l'observation pendant la saisie, ou à partir d'un cache local, de la mémoire, en transit, par lecture d'une ressource non protégée, parce qu'ils sont communément répandus, qu'ils n'expirent jamais, que l'utilisateur ne peut pas changer son propre mot de passe |
| *Apprenez-en plus à ce sujet dans les antisèches gratuites OWASP sur l'Authentification* |  | |  | | --- | | 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 peut facilement identifier les noms des utilisateurs ou peut les énumérer | Javier peut utiliser les identifiants par défaut, de test, ou facilement devinables, ou peut utiliser un ancien compte ou un compte dont l'application n'a pas besoin | Sven peut réutiliser un mot de passe temporaire car l'utilisateur n'a pas besoin de le changer à la première connexion, ou sa durée de vie est trop longue ou n'expire pas, ou sa communication ne nécessite pas de deuxième canal distinct (par exemple voie postale, application mobile, SMS) | Cecilia peut réaliser des attaques de type brute force ou de dictionnaire contre un ou plusieurs comptes sans limitation, ou ses attaques sont simplifiées du fait d'une faible politique de mots de passe (faible complexité, longueur, historique, ou durée de vie insuffisante) |
| |  | | --- | | 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 peut contourner l'authentification car son échec n'est pas contrôlé (passage en accès non authentifié) | Claudia peut effectuer davantage de fonctions critiques car l'authentification est trop faible (ex : pas d'authentification forte à deux facteurs), ou la réauthentification n'est pas requise pour ces fonctions | Pravin peut contourner les contrôles d'authentification car un module/framework/service d'authentification, qui est centralisé, standardisé, testé, autorisé, et séparé de la ressource requêtée, n'est pas utilisé | Mark peut accéder à des ressources ou des services parce qu'il n'y a pas d'authentification, ou il a été pensé à tort que l'authentification était prise en compte par un autre système ou réalisée dans une action précédente |
| |  | | --- | | 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  ${AT\_ATJ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Authentication** | **Q** | **Authentication** | **K** |  |  |  |  |
| Jaime peut contourner l'authentification car celle-ci n'est pas implémentée avec la même rigueur dans toutes les fonctionnalités (ex : inscription, changement de mot de passe, recouvrement de mot de passe, déconnexion, administration) ou dans toutes les versions/canaux (ex : site web mobile, appli mobile, site web, API, centre d'appel) | Olga peut influencer ou modifier du code/routines d'authentification de telle manière que celle-ci soit contournée | (${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** |
| Vous avez inventé une nouvelle attaque contre la Gestion des Sessions | (${Common\_NoCard}) | William a le contrôle sur la génération des identifiants de session | Ryan peut utiliser le même compte en parallèle, puisque les sessions concurrentes sont autorisées |
| *Apprenez-en plus à ce sujet dans les antisèches gratuites OWASP sur la Gestion des Sessions, et sur la prévention des 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 peut régler les cookies d'identification de session vers une autre application web, car le chemin et le domaine sont insuffisamment restreints | John peut prédire ou deviner les identifiants de session car ceux-ci ne sont pas modifiés lorsque le rôle de l'utilisateur change (par exemple pré et post authentification) et lors de la bascule entre communications chiffrées et non chiffrées, ou ne sont pas suffisamment longs et aléatoires, ou ne sont pas changés périodiquement | Gary peut prendre la main sur une session d'un utilisateur car le délai d'attente sur l'inactivité est trop long ou inexistant, ou la même session peut être utilisée depuis plus d'un équipement/site | Casey peut utiliser la session d'Adam après qu'il ait terminé, car il n'existe pas de fonction de déconnexion, ou il ne peut pas se déconnecter facilement, ou la déconnexion ne clôt pas proprement la session |
| |  | | --- | | 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 peut profiter abusivement de sessions longues car l'application ne réauthentifie pas régulièrement pour vérifier si les privilèges ont changé | Ivan peut voler des identifiants de session car ceux-ci sont transmis via des canaux non sécurisés, ou sont journalisés, ou sont révélés dans les messages d'erreur, ou sont inutilement accessibles par du code que l'attaquant peut influencer ou modifier | Marce peut contrefaire des requêtes car des tokens per-session, ou per-request pour des actions plus critiques (ex : tokens anti-CSRF ou similaires), ne sont pas utilisés lors des actions qui changent l'état d'une session | Jeff peut rejouer une interaction identique (ex : requête HTTP, signal, click sur bouton), celle-ci est acceptée et non rejetée |
| |  | | --- | | 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  ${SM\_SMJ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Session management** | **Q** | **Session management** | **K** |  |  |  |  |
| Salim peut contourner la gestion de session car celle-ci n'est pas globalement et régulièrement appliquée à travers l'application | Peter peut contourner les contrôles de gestion de session car ceux-ci ont été développés en interne, au lieu d'utiliser un framework standard ou un module approuvé et testé | (${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** |
| Vous avez inventé une nouvelle attaque contre les Habilitations | (${Common\_NoCard}) | Tim peut modifier l'emplacement où la donnée est envoyée ou renvoyée | Christian peut accéder à des informations auxquelles il n'est pas habilité via un autre canal pour lequel il l'est (ex : résultats de recherche, journaux, reporting) ou parce que celles-ci sont en cache, ou l'information est conservée plus longtemps que nécessaire, ou toute autre fuite de données |
| *Apprenez-en plus à ce sujet dans les guides gratuits OWASP sur le Développement et les Tests* |  | |  | | --- | | 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 peut contourner les contrôles d'habilitation car ils n'échouent pas de façon sécurisée (c'est-à-dire qu'en cas d'échec, retour au comportement par défaut qui est un accès autorisé) | Chad peut accéder à des ressources (services, processus, AJAX, Flash, vidéo, images, documents, fichiers temporaires, données de session, de configuration, propriétés système, registre, journaux) auxquelles il ne devrait pas à cause d'habilitations défaillantes ou de privilèges excessifs (par exemple en n'appliquant pas le principe de moindre privilège) | Eduardo peut avoir accès à des données auxquelles il n'est pas habilité, même s'il a un accès légitime au formulaire/page/ URL/point d'entrée | Yuanjing peut accéder à des fonctions de l'application, des objets ou des propriétés auxquels elle n'est pas habilitée |
| |  | | --- | | 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 peut contourner les règles métier en altérant la séquence normale du processus ou du flux, ou en réalisant celui-ci dans un ordre incorrect, ou en manipulant la date et l'heure utilisée par l'application, ou en détournant l'usage d'outils légitimes, ou encore en manipulant les données de contrôle. | Mike peut altérer le fonctionnement d'une application en utilisant une fonctionnalité légitime trop rapidement ou trop fréquemment, ou d'une façon différente de celle qui est prévue, ou consomme les ressources de l'application, ou cause des situations de compétition (accès concurrent), ou surutilise une fonctionnalité | Richard peut contourner les contrôles d'habilitation centralisés puisqu'ils ne sont pas utilisés de façon exhaustive pour toutes les interactions. | Dinis peut accéder à des informations sur la configuration de sécurité, ou des listes des contrôles d'accès |
| |  | | --- | | 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  ${AZ\_AZJ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Authorization** | **Q** | **Authorization** | **K** |  |  |  |  |
| Christopher peut injecter une commande que l'application exécutera avec un niveau de privilège plus élevé | Ryan peut influencer ou altérer les contrôles d'habilitations et les permissions, et peut ainsi les contourner | (${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** |
| Vous avez inventé une nouvelle attaque contre la Cryptographie | (${Common\_NoCard}) | Kyun peut accéder aux données parce qu'elles ont été obfusquées au lieu d'être protégées par une fonction de cryptographie approuvée | Axel peut modifier des données temporaires ou permanentes (stockées ou en transit), ou du code source, ou des mises à jour/patchs, ou des données de configuration, parce qu'elles ne sont protégées par aucun contrôle d'intégrité |
| *Apprenez-en plus à ce sujet dans les antisèches gratuites OWASP sur le Stockage Cryptographique et la Protection de la Couche de Transport* |  | |  | | --- | | 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 peut accéder aux données en transit qui ne sont pas chiffrées, même si le canal de communication est chiffré | Kyle peut contourner les contrôles cryptographiques car ils n'échouent pas de façon sécurisée (c'est-à-dire qu'ils reviennent à leur état non protégé par défaut) | Romain peut lire et modifier des données non chiffrées en mémoire ou en transit (ex. secrets cryptographiques, informations d'identification, identifiants de session, données à caractère personnel et commercialement sensibles), en cours d'utilisation, dans les échanges au sein de l'application, entre l'application et des utilisateurs, entre l'application et des systèmes externes | Gunter peut intercepter ou modifier des données chiffrées en transit parce que le protocole est mal déployé, ou faiblement configuré, ou les certificats sont invalides, or les certificats ne sont pas fiables, ou la connexion peut être dégradée plus faible ou en communication non chiffrée |
| |  | | --- | | 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 peut accéder à des données métier stockées (par exemple des mots de passe, des identifiants de session, des informations à caractère personnel, des données de titulaires de cartes bancaires) parce qu'elles ne sont pas chiffrées ou hachées de façon sécurisée | Andy peut contourner les fonctions de génération de nombres aléatoires, de génération de GUID aléatoires, de hachage ou de chiffrement parce qu'elles ont été construites par lui-même, ou sont faibles | Susanna peut casser la cryptographie utilisée parce qu'elle n'est pas suffisamment robuste vis-à-vis du niveau de protection requis, ou elle n'est pas suffisamment robuste vis-à-vis de la quantité d'effort que l'attaquant est prêt à faire | Justin peut lire des informations d'identification pour l'accès à des ressources internes ou externes, des services ou d'autres systèmes parce qu'elles sont stockées dans un format non chiffré, ou intégrées dans le code source |
| |  | | --- | | 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  ${CR\_CRJ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Cryptography** | **Q** | **Cryptography** | **K** |  |  |  |  |
| Randolph peut accéder ou prédire les secrets cryptographiques maîtres | Dan peut influencer ou altérer le code/les routines de cryptographie (chiffrement, hachage, signatures numériques, nombre aléatoire et génération de GUID) et peut ainsi les contourner | (${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** |
| Vous avez inventé une nouvelle attaque de n'importe quel type | (${Common\_NoCard}) | Lee peut contourner les contrôles applicatifs car des fonctions à risque ont été utilisées à la place d'alternatives plus sûres, ou il y a des erreurs de conversion de type, ou car l'application n'est pas fiable lorsqu'une ressource externe est indisponible, ou il y a des situations d'accès concurrent, des problèmes d'initialisation ou d'allocation de ressources, ou des débordements peuvent survenir | Andrew peut accéder au code source, ou décompiler, ou accéder à la logique métier pour comprendre le fonctionnement de l'application et les secrets qu'elle contient |
| *Apprenez-en plus à propos de la sécurité applicative dans les guides gratuits OWASP : Exigences, Développement, Revue de Code et Tests, antisèches, et framework Open 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 peut effectuer une action et il n'est pas possible de la lui attribuer. | Larry peut influencer la confiance que les autres parties, y compris les utilisateurs, ont dans l'application, ou abuser de cette confiance ailleurs (par exemple dans une autre application). | Aaron peut contourner les contrôles parce que la gestion des erreurs/exceptions est absente, ou est implémentée de manière incohérente ou partielle, ou ne refuse pas l'accès par défaut (c'est-à-dire que les erreurs doivent mettre fin à l'accès/à l'exécution), ou dépend de la gestion par un autre service ou système. | Les actions de Mwengu ne peuvent pas être étudiées parce qu'il n'y a pas d'enregistrement des événements de sécurité correctement horodaté, parce qu'il n'y a pas de piste d'audit complète, ou parce que ceux-ci peuvent être modifiées ou supprimées par Mwengu, ou parce qu'il n'y a pas de service de centralisation des traces |
| |  | | --- | | 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 peut contourner l'application pour accéder aux données car l'infrastructure réseau et hôte et les services / applications de support n'ont pas été configurés de manière sécurisée, ni la configuration périodiquement vérifiée, ni les correctifs de sécurité appliqués, ou les données sont stockées localement, ou les données ne sont pas physiquement protégées | Michael peut contourner l'application pour accéder aux données car les outils ou les interfaces d'administration ne sont pas sécurisés de manière adéquate | Xavier peut contourner les contrôles de l'application car les frameworks, les bibliothèques et les composants applicatifs contiennent du code malveillant ou des vulnérabilités (par exemple: interne, sur étagère, externalisé, open source, externe) | Roman peut exploiter l'application car elle a été compilée à l'aide d'outils obsolètes ou sa configuration n'est pas sécurisée par défaut, ou les informations de sécurité n'ont pas été documentées et transmises aux équipes opérationnelles |
| |  | | --- | | 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 peut entreprendre des actions malveillantes, non légitimes, sans détection et réponse en temps réel par l'application | Gareth peut utiliser l'application pour refuser le service à certains ou à tous ses utilisateurs | Alice peut utiliser l'application pour attaquer les systèmes et les données des utilisateurs | Bob peut influencer, altérer ou affecter l'application de façon à ce qu'elle ne soit plus conforme aux exigences légales, réglementaires, contractuelles ou autres exigences de l'organisation |
| |  | | --- | | 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 | | *Avez-vous déjà songé à devenir membre OWASP? Tous les outils, conseils et réunions locales sont gratuits pour tous, mais l'adhésion individuelle aide à soutenir le travail de l'OWASP* | *Découvrez comment les vulnérabilités peuvent être corrigées dans les applications de formation de la VM gratuite OWASP Broken Web Applications, ou en utilisant les défis en ligne du Hacking Lab gratuit* |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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} |  |