|  |  |  |
| --- | --- | --- |
| 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** |
| Has creado un nuevo ataque contra validación de datos y codificación | (${Common\_NoCard}) | Brian puede reunir información sobre las principales configuraciones: esquemas, lógicas, código, software, servicios e infraestructura debido al contenido de mensajes de error, configuración deficiente, o a la presencia de archivos de instalación predeterminados o antiguos, de prueba, de copia de seguridad o copias de los recursos, o exposición de código fuente | Robert puede ingresar datos maliciosos porque el formato de protocolo permitido no está siendo revisado, los duplicados son aceptados, la estructura no está siendo validada, los elementos de datos individuales no están siendo validados por: formato, tipo, rango, longitud y una lista blanca de formatos o caracteres permitidos |
| *Lea más sobre este tema en Cheat Sheets de OWASP libre, XSS Prevención, basada en DOM Prevención XSS, SQL Prevención de inyecciones, y Parametrización 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 puede ingresar datos o nombres maliciosos en campos porque actualmente no hay una revisión o monitoreo a nivel de usuario o proceso | Jee puede eludir las rutinas de codificación centralizadas, ya que dichas rutinas no son usadas por todos los activos o se están utilizando codificaciones incorrectas | Jason puede eludir las rutinas de validación centralizadas, ya que no se utilizan en todas las entradas | Jan puede crear cargas especiales para frustrar la validación de entrada, porque el conjunto de caracteres no es especificado/aplicado, o los datos se codifican varias veces, o los datos no están completamente transformados en el mismo formato que la aplicación usa (por ejemplo, canonicalización) antes de ser validados, o las variables no están configuradas de manera robusta |
| |  | | --- | | 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 puede pasar por alto las rutinas de sanitización centralizadas ya que no están siendo utilizadas exhaustivamente | Shamun puede pasar por alto los checks de validaciones de entrada o salida porque los fallos en las validaciones no son rechazados y/o sanitizados | Darío puede explotar la confianza que la aplicación deposita en una fuente de datos (por ejemplo, datos definibles por el usuario, manipulación de datos almacenados localmente, alteración de los datos del estado en un dispositivo cliente, falta de verificación de identidad durante la validación de datos, como Darío puede pretender ser Colin) | Dennis tiene control sobre la validación de entrada, la validación de salida o código de codificación de salida o rutinas para que puedan ser evitados |
| |  | | --- | | 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  ${VE\_VEJ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Data validation & encoding** | **Q** | **Data validation & encoding** | **K** |  |  |  |  |
| Geoff puede inyectar datos en el lado del cliente o en el dispositivo porque no se está utilizando una interfaz parametrizada, o no ha sido implementada correctamente, o los datos no han sido codificados correctamente, o no hay una política restrictiva en el código o los datos incluidos | Gabe puede inyectar datos en un intérprete del lado del servidor (por ejemplo, SQL, comandos del sistema operativo, Xpath, servidor JavaScript, SMTP) porque no se está utilizando una interfaz parametrizada fuertemente tipificada o no se ha implementado correctamente | (${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** |
| Usted tiene inventado un nuevo ataque contra la autenticación | (${Common\_NoCard}) | James puede emprender funciones de autenticación sin que el usuario real se dé cuenta alguna vez de lo ocurrido (por ejemplo, intento de logueo, inicio de sesión con credenciales robadas, restablecimiento de la contraseña) | Muhammad puede obtener una contraseña de usuario u otros secretos tales como preguntas de seguridad, por observación durante el ingreso o desde el cache, o desde la memoria, o en tránsito, o leyéndolo de alguna ubicación desprotegida, o porque es ampliamente conocido, o porque nunca caduca, o porque el usuario no puede cambiar su propia contraseña |
| *Leer mas sobre este tema en OWASP's free 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 puede fácilmente identificar nombres de usuario o puede enumerarlos | Javier puede usar credenciales por defecto, de prueba o fáciles de adivinar para autenticar, o puede usar una cuenta antigua o una cuenta no necesaria para la aplicación | Sven puede reutilizar contraseñas temporales porque el usuario no realizó el cambio en el primer logueo. o tiene demasiado tiempo y no tiene vencimiento, o no usa un método correcto de entrega (por ejemplo, publicación, aplicación móvil, SMS) | Cecilia puede usar ataques de fuerza bruta y ataques de diccionario sin límites contra uno o muchas cuentas, o estos ataques se simplifican debido a una complejidad insuficiente, longitud, caducidad inadecuada y reutilización de requisitos para las contraseñas |
| |  | | --- | | 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 puede pasar por alto la autenticación porque ésta no falla de forma segura (es decir, por defecto permite acceso no autenticado) | Claudia puede utilizar Funciones más críticas porque los requisitos de autenticación son demasiado débiles (por ejemplo, no usa autenticación robusta como el doble factor), o no hay requisitos de re-autenticación para éstos | Pravin puede omitir el control de autenticación porque no se está utilizando un módulo/framework/servicio de autenticación centralizado, estándar, testeado, probado y aprobado, separado del recurso solicitado | Mark puede acceder a los recursos o servicios porque no hay requisitos de autenticación, o fue asumido erróneamente que la autentificación sería realizada por algún otro sistema o realizada en alguna acción previa |
| |  | | --- | | 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  ${AT\_ATJ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Authentication** | **Q** | **Authentication** | **K** |  |  |  |  |
| Jaime puede omitir la autenticación porque no se aplica con igual rigor para todos los tipos de funcionalidad de autenticación (por ejemplo, registro, cambio de contraseña, recuperación de contraseña, cierre de sesión, administración) o en todas las versiones / canales (por ejemplo, sitio web móvil, aplicación móvil, sitio web completo, API, call center) | Olga puede influir o alterar el código o rutina de autenticación o puede evitarlo | (${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** |
| Has inventado un nuevo ataque contra la gestión de sesión | (${Common\_NoCard}) | William tiene el control sobre la generación de identificadores de sesión | Ryan puede usar una sola cuenta en paralelo ya que permite sesiones concurrentes |
| *Read more about this topic in OWASP's free Cheat Sheets on Session Management, and Cross Site Request Forgery (CSRF) Prevention* |  | |  | | --- | | 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 puede configurar cookies de identificación de sesión en otra aplicación web porque el dominio y la ruta no están suficientemente restringidos | John puede predecir o adivinar los identificadores de sesión porque no se cambian cuando se modifica la función del usuario (por ejemplo, la autenticación previa y posterior) y cuando se cambia entre comunicaciones no cifradas y cifradas, o no son lo suficientemente largas y aleatorias, o no se cambian periódicamente | Gary puede hacerse cargo de la sesión de un usuario porque hay un tiempo de espera de inactividad largo o nulo, un límite de tiempo de sesión general largo o nulo, o la misma sesión puede usarse desde más de un dispositivo / ubicación | Casey puede utilizar la sesión de Adam después de que haya terminado, porque no hay una función de cierre de sesión, o no puede cerrar sesión fácilmente, o el cierre de sesión no termina la sesión correctamente |
| |  | | --- | | 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 puede abusar de sesiones largas porque la aplicación no requiere una autenticación periódica para verificar si los privilegios han cambiado | Ivan puede robar identificadores de sesión porque se envían a través de canales inseguros, se registran, se revelan en mensajes de error, se incluyen en URL o son accesibles de manera innecesaria mediante el código que el atacante puede influir o modificar | Marce puede forjar solicitudes porque las sesiones por sesión o por acciones más críticas, los tokens aleatorios fuertes (es decir, los tokens anti-CSRF) o similares no se utilizan para acciones que cambian de estado | Jeff puede reenviar una interacción de repetición idéntica (por ejemplo, solicitud HTTP, señal, pulsación de botón) y se acepta, no se rechaza |
| |  | | --- | | 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  ${SM\_SMJ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Session management** | **Q** | **Session management** | **K** |  |  |  |  |
| Salim puede omitir la administración de sesiones porque no se aplica de manera integral y coherente en toda la aplicación | Peter puede omitir los controles de administración de la sesión porque se construyeron por sí mismos y / o son débiles, en lugar de usar un marco estándar o un módulo aprobado aprobado | (${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** |
| Has inventado un nuevo ataque contra la Autorización | (${Common\_NoCard}) | Tim puede influir a donde se envía o reenvía la data | Christian puede acceder a información, a la que no debería tener permiso, a través de otro mecanismo al que sí tiene permiso (por ejemplo, indexador de búsqueda, registrador, reporte), o porque está en caché, o guardada por más tiempo del necesario u otro medio de fuga de información |
| *Read more about this topic in OWASP's Development and Testing Guides* |  | |  | | --- | | 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 puede eludir los controles de autorización porque no fallan de forma segura (es decir, por defecto permiten el acceso) | Chad puede acceder a los recursos (incluidos servicios, procesos, AJAX, Flash, video, imágenes, documentos, archivos temporales, datos de sesión, propiedades del sistema, datos de configuración, registro de configuración, logs) a los que no debería poder acceder debido a la falta de autorización, o debido a privilegios excesivos(por ejemplo, no usar el principio de menor privilegio) | Eduardo puede acceder a los datos a los que él no tiene permiso, incluso aunque tiene permiso para formulario / página / URL / punto de entrada | Yuanjing puede acceder a funciones de la aplicación, objetos o propiedades a las que él no está autorizado para acceder |
| |  | | --- | | 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 puede omitir las reglas de negocios al alterar la secuencia o flujo de proceso habitual, o realizar el proceso en el orden incorrecto, o manipular los valores de fecha y hora utilizados por la aplicación, o usar características válidas para propósitos no intencionados, o manipulando los datos de control | Mike puede hacer uso incorrecto de una aplicación al usar una función válida demasiado rápido, o con demasiada frecuencia, o de otra forma sin intención, o que consuma los recursos de la aplicación, o cause condiciones de carrera, o sobreutilice una función | Richard puede eludir los controles de autorización centralizados ya que no están siendo utilizados exhaustivamente en todas las interacciones | Dinis puede acceder a la información de configuración de seguridad, o listas de control de acceso |
| |  | | --- | | 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  ${AZ\_AZJ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Authorization** | **Q** | **Authorization** | **K** |  |  |  |  |
| Christopher puede inyectar un comando para que la aplicación se ejecute con un nivel de privilegios más alto | Ryan puede influir o alterar controles y permisos de autorización, y por ende puede | (${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** |
| Has inventado un nuevo ataque contra la Criptografía | (${Common\_NoCard}) | Kyun puede acceder a los datos porque ha sido ofuscado en lugar de utilizar una función criptográfica aprobada | Axel puede modificar datos transitorios o permanentes (almacenados o en tránsito), código fuente, actualizaciones / parches o datos de configuración, ya que no están sujetos a verificación de integridad |
| *Read more about this topic in OWASP's free Cheat Sheets on Cryptographic Storage, and Transport Layer Protection* |  | |  | | --- | | 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 puede acceder a datos en tránsito que no están encriptados, incluso aunque el canal está encriptado | Kyle puede pasar por alto controles criptográficos porque estos no fallan de forma segura (es decir, por defecto no protegen) | Romain puede leer y modificar datos sin cifrar en la memoria o en tránsito (por ejemplo, secretos criptográficos, credenciales, identificadores de sesión, datos personales y comerciales), en uso o en comunicaciones dentro de la aplicación, o entre la aplicación y los usuarios, o entre la aplicación y sistemas externos | Gunter puede interceptar o modificar datos encriptados en tránsito porque el protocolo está mal implementado o configurado de manera débil, o los certificados no son válidos, los certificados no son confiables o la conexión puede degradarse a una comunicación más débil o no encriptada |
| |  | | --- | | 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 puede acceder a los datos comerciales almacenados (por ejemplo, contraseñas, identificadores de sesión, PII, datos del titular de la tarjeta) porque no está cifrado de forma segura ni hash de forma segura | Andy puede omitir la generación de números aleatorios, la generación aleatoria de GUID, el hash y las funciones de cifrado porque han sido construidos por sí mismos y / o son débiles | Susanna puede romper la criptografía en uso porque no es lo suficientemente fuerte para el grado de protección requerido, o no lo es para la cantidad de esfuerzo que el atacante está dispuesto a hacer | Justin puede leer las credenciales para acceder a recursos, servicios y otros sistemas internos o externos porque se almacenan en un formato no cifrado o se guardan en el código fuente |
| |  | | --- | | 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  ${CR\_CRJ\_safecode} | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Cryptography** | **Q** | **Cryptography** | **K** |  |  |  |  |
| Randolph puede acceder o predecir los algoritmos o llaves de los secretos criptográficos | Dan puede influir o alterar el código / las rutinas criptográficas (cifrado, hash, firmas digitales, números aleatorios y generación de GUID) y, por lo tanto, puede omitirlos | (${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** |
| Has inventado un nuevo ataque de cualquier tipo | (${Common\_NoCard}) | Lee puede omitir los controles de la aplicación porque se han usado funciones de lenguaje de programación peligrosas/riesgosas en lugar de alternativas más seguras, o hay errores de conversión de tipo, o porque la aplicación no es confiable cuando un recurso externo no está disponible, o hay race conditions, o hay problemas en la inicialización/asignación de recursos, o pueden ocurrir desbordamientos | Andrew puede acceder al código fuente, o descompilar, o de otro modo acceder a la lógica de negocio para entender cómo la aplicación y cualquier secreto contenido funciona |
| *Read more about application security in OWASP's free Guides on Requirements, Development, Code Review and Testing, the Cheat Sheet series, and the 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 puede realizar una acción y no es posible atribuirla a él | Larry puede influir en la confianza que otras partes, incluidos los usuarios tienen en la aplicación, o abusar de esa confianza en otra parte (por ejemplo, en otra aplicación) | Aaron puede omitir los controles porque falta el manejo de errores/excepciones, o se implementa de manera inconsistente o parcial, o no niega el acceso por defecto (es decir, los errores deben terminar el acceso / ejecución), o se basan en el manejo por parte de otro servicio o sistema | Las acciones de Mwengu no se pueden investigar porque no hay un registro adecuado de los eventos de seguridad con una marca de tiempo adecuada, o no hay un registro de auditoría completo, o Mwengu puede modificarlas o eliminarlas, o no existe un servicio 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 puede omitir la aplicación para obtener acceso a los datos debido a que la red y la infraestructura del host, y los servicios/aplicaciones compatibles, no se han configurado de manera segura, la configuración no se verificó periódicamente ni se aplicaron parches de seguridad, o los datos se almacenaron localmente, o los datos no se guardaron protegidos físicamente | Michael puede pasar por alto la aplicación para acceder a los datos porque las herramientas administrativas o las interfaces administrativas no están aseguradas adecuadamente | Xavier puede eludir los controles de la aplicación porque los frameworks de código, librerías y componentes contienen código malicioso o vulnerabilidades (por ejemplo, inhouse, software comercial, servicio tercerizado, de código abierto, ubicado externamente) | Roman puede explotar la aplicación porque fue compilada utilizando herramientas obsoletas, o su configuración no es segura por defecto, o la seguridad de la información no fue documentada y pasada a equipos operacionales |
| |  | | --- | | 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 puede emprender acciones maliciosas, no normales sin detección y respuesta por la aplicación en tiempo real | Gareth puede utilizar la aplicación para negar el servicio a algunos o todos sus usuarios | Alice puede utilizar la aplicación para atacar los sistemas y datos de los usuarios. | Bob puede influir, alterar o afectar la aplicación para que ya no cumpla con mandatos legales, regulatorios, contractuales u otros mandatos organizacionales |
| |  | | --- | | 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 | | *Has pensado convertirte en un individuo Miembro de OWASP? Todas las herramientas, orientación y reuniones locales son gratis para todos, pero la membresía individual ayuda Apoyar el trabajo de OWASP.* | *Examine las vulnerabilidades y descubre cómo se pueden arreglar usando aplicaciones de entrenamiento en OWASP Broken Web Applications VM gratis, o utilizando los desafíos en línea en el laboratorio de hacking gratis* |

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