|  |  |  |
| --- | --- | --- |
| 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 Grant Ongers  ${Common\_T00040}  Tom Brennan, Johanna Curiel, Darío De Filippis 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://wiki.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} ${Common\_T03070}*  [https://www.owasp.org/index.php/OWASP\_Cornucopia - tab=FAQs](https://www.owasp.org/index.php/OWASP_Cornucopia#tab=FAQs) | | | | |
|  |  |  |  |  |  | |  | |  |  |  |  |
|  | **Data validation & encoding** | **A** | **Data validation & encoding** |  | | **Data validation & encoding** | | **2** | **Data validation & encoding** | **3** |  |
|  | Je hebt een nieuwe aanval uitgevonden tegen gegevensvalidatie en -codering | (${Common\_NoCard}) | | Brian kan informatie verzamelen over de onderliggende configuraties, schema's, logica, code, software, services en infrastructuur vanwege de inhoud van foutmeldingen, of een slechte configuratie, of de aanwezigheid van standaard installatiebestanden of oude, test, back-up of kopieën van bronnen, of blootstelling van broncode | Robert kan kwaadaardige gegevens invoeren omdat het toegestane protocolformaat niet wordt gecontroleerd, of duplicaten worden geaccepteerd, of de structuur niet wordt geverifieerd, of de individuele gegevenselementen niet worden gevalideerd voor formaat, type, bereik, lengte en een witte lijst met toegestane tekens of formaten |  |
|  | *Lees meer over dit onderwerp in OWASP's gratis spiekbriefjes over invoervalidatie, XSS-preventie, op DOM gebaseerde XSS-preventie, SQL-injectiepreventie en queryparameterisatie* |  | | |  | | --- | | OWASP SCP  69, 107-109, 136-137, 153, 156, 158, 162 | | OWASP ASVS  1.6.4, 2.10.4, 4.3.2, 7.1.1, 10.2.3, 14.1.1, 14.2.2, 14.3.3 | | OWASP APPSENSOR  HT1-3 | | CAPEC  54, 541 | | SAFECODE  4, 23 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  - | | OWASP ASVS  1.5.3, 5.1.1-5.1.4, 13.2.1, 14.1.2, 14.4.1 | | OWASP APPSENSOR  RE7-8, AE4-7, IE2-3, CIE1, CIE3-4, HT1-3 | | CAPEC  28, 48, 126, 165, 213, 220-221, 261-262, 271-272 | | SAFECODE  3, 16, 24, 35 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |  |
|  | **Data validation & encoding** | **4** | **Data validation & encoding** | **5** | | **Data validation & encoding** | | **6** | **Data validation & encoding** | **7** |  |
|  | Dave kan kwaadaardige veldnamen of gegevens invoeren omdat het niet wordt gecontroleerd binnen de context van de huidige gebruiker en het huidige proces | Jee kan de gecentraliseerde coderingsroutines omzeilen omdat ze niet overal worden gebruikt, of de verkeerde coderingen worden gebruikt | | Jason kan de gecentraliseerde validatieroutines omzeilen omdat ze niet op alle invoer worden gebruikt | Jan kan speciale payloads maken om invoervalidatie te dwarsbomen omdat de tekenset niet is gespecificeerd/afgedwongen, of de gegevens meerdere keren worden gecodeerd, of de gegevens niet volledig worden geconverteerd naar hetzelfde formaat dat de toepassing gebruikt (bijv. gevalideerd, of variabelen zijn niet sterk getypt |  |
|  | |  | | --- | | OWASP SCP  8, 10, 183 | | OWASP ASVS  4.2.1, 5.1.1, 5.1.2, 11.1.1, 11.1.2 | | OWASP APPSENSOR  RE3-6, AE8-11, SE1, SE3-6, IE2-4, HT1-3 | | CAPEC  28, 31, 48, 126, 162, 165, 213, 220-221, 261 | | SAFECODE  24, 35 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  3, 15, 18-22, 168 | | OWASP ASVS  1.1.6, 5.3.3, 5.2.1, 5.2.2, 5.2.5 | | OWASP APPSENSOR  - | | CAPEC  28, 31, 152, 160, 468 | | SAFECODE  2, 17 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | | |  | | --- | | OWASP SCP  3, 168 | | OWASP ASVS  1.1.6, 1.5.3, 5.1.3, 13.2.2, 13.2.5 | | OWASP APPSENSOR  IE2-3 | | CAPEC  28 | | SAFECODE  3, 16, 24 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  4-5, 7, 150 | | OWASP ASVS  1.5.3, 13.2.2, 13.2.5 | | OWASP APPSENSOR  IE2-3, EE1-2 | | CAPEC  28, 153, 165 | | SAFECODE  3, 16, 24 | | 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 kan de gecentraliseerde reinigingsroutines omzeilen omdat ze niet volledig worden gebruikt | Shamun kan invoervalidatie of uitvoervalidatiecontroles omzeilen omdat validatiefouten niet worden afgewezen en/of opgeschoond | Darío kan misbruik maken van het vertrouwen dat de toepassing stelt in een gegevensbron (bijv. door de gebruiker te definiëren gegevens, manipulatie van lokaal opgeslagen gegevens, wijziging van statusgegevens op een clientapparaat, gebrek aan verificatie van identiteit tijdens gegevensvalidatie zoals Darío kan doe alsof je Colin bent) | Dennis heeft controle over invoervalidatie, uitvoervalidatie of uitvoercoderingscode of routines zodat ze kunnen worden omzeild |
| |  | | --- | | OWASP SCP  15, 169 | | OWASP ASVS  1.1.6, 5.2.2, 5.2.5 | | OWASP APPSENSOR  - | | CAPEC  28, 31, 152, 160, 468 | | SAFECODE  2, 17 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  6, 21-22, 168 | | OWASP ASVS  7.1.3 | | OWASP APPSENSOR  IE2-3 | | CAPEC  28 | | SAFECODE  3, 16, 24 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  2, 19, 92, 95, 180 | | OWASP ASVS  1.12.2, 5.1.3, 9.2.3, 12.2.1, 12.3.1-12.3.3, 12.4.2, 12.5.2, 14.5.3 | | OWASP APPSENSOR  IE4, IE5 | | CAPEC  12, 51, 57, 90, 111, 145, 194-195, 202, 218, 463 | | SAFECODE  14 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  1, 17 | | OWASP ASVS  1.5.3 | | OWASP APPSENSOR  RE3, RE4 | | CAPEC  87, 207, 554 | | SAFECODE  2, 17 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Data validation & encoding** | **Q** | **Data validation & encoding** | **K** |  |  |  |  |
| Geoff kan gegevens in een client- of device-side-interpreter injecteren omdat een geparametriseerde interface niet wordt gebruikt, of niet correct is geïmplementeerd, of de gegevens niet correct zijn gecodeerd voor de context, of er is geen beperkend beleid ten aanzien van code of gegevens omvat | Gabe kan gegevens injecteren in een server-side interpreter (bijv. SQL, OS-commando's, Xpath, Server JavaScript, SMTP) omdat een sterk getypeerde geparametriseerde interface niet wordt gebruikt of niet correct is geïmplementeerd | (${Common\_NoCard}) | (${Common\_NoCard}) |
| |  | | --- | | OWASP SCP  10, 15-16, 19-20 | | OWASP ASVS  5.2.1, 5.2.5, 5.3.3, 5.5.4 | | OWASP APPSENSOR  IE1, RP3 | | CAPEC  28, 31, 152, 160, 468 | | SAFECODE  2, 17 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  15, 19-22, 167, 180, 204, 211-212 | | OWASP ASVS  5.2.1, 5.2.2, 5.3.4, 5.3.7-5.3.10 | | OWASP APPSENSOR  CIE1, CIE2 | | CAPEC  23, 28, 76, 152, 160, 261 | | SAFECODE  2, 19-20 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Authentication** | **A** | **Authentication** |  | **Authentication** | **2** | **Authentication** | **3** |
| Je hebt een nieuwe aanval tegen authenticatie uitgevonden | (${Common\_NoCard}) | James kan authenticatiefuncties uitvoeren zonder dat de echte gebruiker er ooit van op de hoogte is dat dit is gebeurd (bijv. poging om in te loggen, inloggen met gestolen inloggegevens, het wachtwoord opnieuw instellen) | Mohammed kan het wachtwoord van een gebruiker of andere geheimen, zoals beveiligingsvragen, verkrijgen door observatie tijdens invoer, of uit een lokale cache, of uit het geheugen, of tijdens het transport, of door het te lezen vanaf een onbeveiligde locatie, of omdat het op grote schaal wordt gebruikt. bekend is, of omdat het nooit verloopt, of omdat de gebruiker haar eigen wachtwoord niet kan wijzigen |
| *Lees meer over dit onderwerp in de gratis verificatie-cheatsheet van OWASP* |  | |  | | --- | | OWASP SCP  47, 52 | | OWASP ASVS  2.5.2, 7.1.2, 7.1.4, 7.2.1, 8.2.1-8.2.3, 8.3.6 | | OWASP APPSENSOR  UT1 | | CAPEC  - | | SAFECODE  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  36-37, 40, 43, 48, 51, 119, 139-140, 146 | | OWASP ASVS  2.5.2, 2.5.3 | | OWASP APPSENSOR  - | | CAPEC  37, 546 | | SAFECODE  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Authentication** | **4** | **Authentication** | **5** | **Authentication** | **6** | **Authentication** | **7** |
| Sebastien kan gebruikersnamen gemakkelijk identificeren of opsommen | Javier kan standaard-, test- of gemakkelijk te raden inloggegevens gebruiken om te verifiëren, of kan een oud account gebruiken of een account dat niet nodig is voor de toepassing | Sven kan een tijdelijk wachtwoord opnieuw gebruiken omdat de gebruiker het bij het eerste gebruik niet hoeft te wijzigen, of omdat het te lang of niet verloopt, of omdat het geen out-of-band bezorgingsmethode gebruikt (bijv. post, mobiele app , SMS) | Cecilia kan brute kracht en woordenboekaanvallen gebruiken tegen een of meerdere accounts zonder limiet, of deze aanvallen worden vereenvoudigd vanwege onvoldoende complexiteit, lengte, vervaldatum en hergebruikvereisten voor wachtwoorden |
| |  | | --- | | OWASP SCP  33, 53 | | OWASP ASVS  2.2.1, 4.1.5 | | OWASP APPSENSOR  AE1 | | CAPEC  383 | | SAFECODE  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  54, 175, 178 | | OWASP ASVS  4.1.5 | | OWASP APPSENSOR  AE12, HT3 | | CAPEC  70 | | SAFECODE  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  37, 45-46, 178 | | OWASP ASVS  2.5.6 | | OWASP APPSENSOR  - | | CAPEC  50 | | SAFECODE  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  33, 38-39, 41, 50, 53 | | OWASP ASVS  2.1.2, 2.1.7, 2.1.10, 2.2.1, 2.2.1 | | OWASP APPSENSOR  AE2, AE3 | | CAPEC  2, 16 | | SAFECODE  27 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Authentication** | **8** | **Authentication** | **9** | **Authentication** | **10** | **Authentication** | **J** |
| Kate kan authenticatie omzeilen omdat het niet beveiligd is (d.w.z. het staat standaard niet-geverifieerde toegang toe) | Claudia kan meer kritieke functies uitvoeren omdat de authenticatievereisten te zwak zijn (gebruik bijvoorbeeld geen sterke authenticatie zoals two-factor), of er is geen vereiste om opnieuw te authenticeren voor deze | Pravin kan authenticatiecontroles omzeilen omdat een gecentraliseerde standaard, geteste, bewezen en goedgekeurde authenticatiemodule/framework/service, los van de resource die wordt aangevraagd, niet wordt gebruikt | Mark heeft toegang tot bronnen of services omdat er geen authenticatievereiste is, of er werd ten onrechte aangenomen dat authenticatie zou worden uitgevoerd door een ander systeem of uitgevoerd in een eerdere actie |
| |  | | --- | | OWASP SCP  28 | | OWASP ASVS  4.1.5 | | OWASP APPSENSOR  - | | CAPEC  115 | | SAFECODE  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  55-56 | | OWASP ASVS  1.4.3, 1.4.5, 2.1.6, 2.2.4, 4.3.3 | | OWASP APPSENSOR  - | | CAPEC  21 | | SAFECODE  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  25-27 | | OWASP ASVS  1.1.6, 1.4.4 | | OWASP APPSENSOR  - | | CAPEC  90, 115 | | SAFECODE  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  23, 32, 34 | | OWASP ASVS  1.4.3, 1.4.5 | | OWASP APPSENSOR  - | | CAPEC  115 | | SAFECODE  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Authentication** | **Q** | **Authentication** | **K** |  |  |  |  |
| Jaime kan authenticatie omzeilen omdat het niet even strikt wordt afgedwongen voor alle soorten authenticatiefunctionaliteit (bijv. registreren, wachtwoordwijziging, wachtwoordherstel, uitloggen, beheer) of voor alle versies/kanalen (bijv. mobiele website, mobiele app, volledige website, API, callcenter) | Olga kan authenticatiecode/routines beïnvloeden of wijzigen zodat ze kunnen worden omzeild | (${Common\_NoCard}) | (${Common\_NoCard}) |
| |  | | --- | | OWASP SCP  23, 29, 42, 49 | | OWASP ASVS  1.4.3, 1.4.5, 2.5.6, 2.5.7 | | OWASP APPSENSOR  - | | CAPEC  36, 50, 115, 121, 179 | | SAFECODE  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  24 | | OWASP ASVS  4.1.1, 10.2.3-10.2.6 | | OWASP APPSENSOR  - | | CAPEC  115, 207, 554 | | SAFECODE  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Session management** | **A** | **Session management** |  | **Session management** | **2** | **Session management** | **3** |
| Je hebt een nieuwe aanval tegen Session Management uitgevonden | (${Common\_NoCard}) | William heeft controle over het genereren van sessie-ID's | Ryan kan één account parallel gebruiken, aangezien gelijktijdige sessies zijn toegestaan |
| *Lees meer over dit onderwerp in OWASP's gratis spiekbriefjes over sessiebeheer en preventie van Cross Site Request Forgery (CSRF)* |  | |  | | --- | | OWASP SCP  58-59 | | OWASP ASVS  3.7.1 | | OWASP APPSENSOR  SE2 | | CAPEC  31, 60-61 | | SAFECODE  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  68 | | OWASP ASVS  3.3.3, 3.3.4 | | OWASP APPSENSOR  - | | CAPEC  - | | SAFECODE  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Session management** | **4** | **Session management** | **5** | **Session management** | **6** | **Session management** | **7** |
| Alison kan sessie-identificatiecookies instellen op een andere webtoepassing omdat het domein en pad niet voldoende zijn beperkt | John kan sessie-ID's voorspellen of raden omdat ze niet worden gewijzigd wanneer de rol van de gebruiker verandert (bijv. pre- en postauthenticatie) en bij het schakelen tussen niet-versleutelde en versleutelde communicatie, of niet lang genoeg en willekeurig zijn, of niet worden gewijzigd periodiek | Gary kan de sessie van een gebruiker overnemen omdat er een lange of geen time-out voor inactiviteit is, of een lange of geen algemene sessietijdslimiet, of dezelfde sessie kan worden gebruikt vanaf meer dan één apparaat/locatie | Casey kan de sessie van Adam gebruiken nadat hij klaar is, omdat er geen uitlogfunctie is, of hij kan niet gemakkelijk uitloggen, of uitloggen beëindigt de sessie niet correct |
| |  | | --- | | OWASP SCP  59, 61 | | OWASP ASVS  3.4.1-3.4.5 | | OWASP APPSENSOR  SE2 | | CAPEC  31, 61 | | SAFECODE  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  60, 62, 66-67, 71-72 | | OWASP ASVS  3.2.1, 3.2.2, 3.2.4, 3.3.1 | | OWASP APPSENSOR  SE4-6 | | CAPEC  31 | | SAFECODE  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  64-65 | | OWASP ASVS  3.3.2-3.3.4 | | OWASP APPSENSOR  SE5, SE6 | | CAPEC  21 | | SAFECODE  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  62-63 | | OWASP ASVS  3.3.1, 3.3.4 | | OWASP APPSENSOR  - | | CAPEC  21 | | SAFECODE  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Session management** | **8** | **Session management** | **9** | **Session management** | **10** | **Session management** | **J** |
| Matt kan misbruik maken van lange sessies omdat de applicatie geen periodieke herauthenticatie vereist om te controleren of de rechten zijn gewijzigd | Ivan kan sessie-ID's stelen omdat ze via onveilige kanalen worden verzonden, of worden vastgelegd, of worden onthuld in foutmeldingen, of zijn opgenomen in URL's, of onnodig toegankelijk zijn via code die de aanvaller kan beïnvloeden of wijzigen | Marce kan verzoeken vervalsen omdat per sessie, of per verzoek voor meer kritieke acties, sterke willekeurige tokens (d.w.z. anti-CSRF-tokens) of iets dergelijks niet worden gebruikt voor acties die van status veranderen | Jeff kan een identieke herhaalde interactie opnieuw verzenden (bijv. HTTP-verzoek, signaal, druk op de knop) en het wordt geaccepteerd, niet afgewezen |
| |  | | --- | | OWASP SCP  96 | | OWASP ASVS  3.6.1, 3.3.2 | | OWASP APPSENSOR  - | | CAPEC  21 | | SAFECODE  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  69, 75-76, 119, 138 | | OWASP ASVS  1.9.1, 3.1.1, 7.1.1, 7.1.2, 7.2.1, 9.1.3, 9.2.2 | | OWASP APPSENSOR  SE4-6 | | CAPEC  31, 60 | | SAFECODE  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  73-74 | | OWASP ASVS  4.2.2 | | OWASP APPSENSOR  IE4 | | CAPEC  62, 111 | | SAFECODE  18 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  - | | OWASP ASVS  11.1.1-11.1.3 | | OWASP APPSENSOR  IE5 | | CAPEC  60 | | SAFECODE  12, 14 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Session management** | **Q** | **Session management** | **K** |  |  |  |  |
| Salim kan sessiebeheer omzeilen omdat het niet volledig en consistent wordt toegepast in de hele applicatie | Peter kan de sessiebeheer controles omzeilen omdat ze zelf gebouwd zijn en/of zwak zijn, in plaats van een standaard framework of goedgekeurde geteste module te gebruiken | (${Common\_NoCard}) | (${Common\_NoCard}) |
| |  | | --- | | OWASP SCP  58 | | OWASP ASVS  1.1.6, 3.7.1 | | OWASP APPSENSOR  - | | CAPEC  21 | | SAFECODE  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  58, 60 | | OWASP ASVS  1.1.6 | | OWASP APPSENSOR  - | | CAPEC  21 | | SAFECODE  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Authorization** | **A** | **Authorization** |  | **Authorization** | **2** | **Authorization** | **3** |
| Je hebt een nieuwe aanval tegen Autorisatie uitgevonden | (${Common\_NoCard}) | Tim kan beïnvloeden waar gegevens naartoe worden gestuurd of doorgestuurd | Christenen hebben toegang tot informatie waarvoor ze geen toestemming zouden moeten hebben, via een ander mechanisme dat wel toestemming heeft (bijv. zoekindexer, logger, rapportage), of omdat het in de cache is opgeslagen, of langer dan nodig wordt bewaard, of andere informatielekkage |
| *Lees meer over dit onderwerp in de ontwikkelings- en testhandleidingen van OWASP* |  | |  | | --- | | OWASP SCP  44 | | OWASP ASVS  4.1.3, 4.2.1, 5.1.5 | | OWASP APPSENSOR  - | | CAPEC  153 | | SAFECODE  8, 10-11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  51, 100, 135, 139-141, 150 | | OWASP ASVS  1.12.1, 4.1.3, 4.1.5, 8.1.2, 8.2.1, 8.3.1, 8.3.4, 8.3.6, 8.3.8, 12.4.1 | | OWASP APPSENSOR  - | | CAPEC  69, 213 | | SAFECODE  8, 10-11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Authorization** | **4** | **Authorization** | **5** | **Authorization** | **6** | **Authorization** | **7** |
| Kelly kan autorisatiecontroles omzeilen omdat ze niet veilig falen (d.w.z. ze geven standaard toegang) | Chad heeft toegang tot bronnen (inclusief services, processen, AJAX, Flash, video, afbeeldingen, documenten, tijdelijke bestanden, sessiegegevens, systeemeigenschappen, configuratiegegevens, registerinstellingen, logboeken) die hij niet zou moeten kunnen vanwege ontbrekende autorisatie , of als gevolg van overmatigeprivileges (bijvoorbeeld het niet gebruiken van het principe van de minste privileges) | Eduardo heeft toegang tot gegevens waar hij geen toestemming voor heeft, ook al heeft hij toestemming voor het formulier/pagina/URL/toegangspunt | Yuanjing heeft toegang tot applicatiefuncties, objecten of eigenschappen waartoe hij geen toegang heeft |
| |  | | --- | | OWASP SCP  79-80 | | OWASP ASVS  4.1.5 | | OWASP APPSENSOR  - | | CAPEC  122 | | SAFECODE  8, 10-11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  70, 81, 83-4, 87-9, 99, 117, 131-2, 142, 154, 170, 179 | | OWASP ASVS  1.2.2, 4.1.1, 4.1.3, 4.2.1 | | OWASP APPSENSOR  ACE1, ACE2, ACE3, ACE4, HT2 | | CAPEC  75, 87, 95, 126, 149, 155, 203, 213, 264-265 | | SAFECODE  8, 10-11, 13 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  81, 88, 131 | | OWASP ASVS  4.1.3, 4.2.1 | | OWASP APPSENSOR  ACE1-4 | | CAPEC  122 | | SAFECODE  8, 10-11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  81, 85-86, 131 | | OWASP ASVS  4.1.3, 4.2.1 | | OWASP APPSENSOR  ACE1-4 | | CAPEC  122 | | SAFECODE  8, 10-11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Authorization** | **8** | **Authorization** | **9** | **Authorization** | **10** | **Authorization** | **J** |
| Tom kan bedrijfsregels omzeilen door de gebruikelijke procesvolgorde of -stroom te wijzigen, of door het proces in de verkeerde volgorde uit te voeren, of door datum- en tijdwaarden te manipuleren die door de applicatie worden gebruikt, of door geldige functies te gebruiken voor onbedoelde doeleinden, of door anderszins manipuleren van besturingsgegevens | Mike kan een applicatie misbruiken door een geldige functie te snel of te vaak te gebruiken, of op een andere manier die niet de bedoeling is, of verbruikt de bronnen van de applicatie, veroorzaakt race-omstandigheden of maakt teveel gebruik van een functie | Richard kan de gecentraliseerde autorisatiecontroles omzeilen omdat ze niet volledig worden gebruikt voor alle interacties | Dinis heeft toegang tot informatie over de beveiligingsconfiguratie of heeft toegang tot controlelijsten |
| |  | | --- | | OWASP SCP  10, 32, 93-94, 189 | | OWASP ASVS  4.1.2, 4.2.1, 4.3.3, 7.3.4, 11.1.1, 11.1.2 | | OWASP APPSENSOR  ACE3 | | CAPEC  25, 39, 74, 162, 166, 207 | | SAFECODE  8, 10-12 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  94 | | OWASP ASVS  11.1.3, 11.1.4 | | OWASP APPSENSOR  AE3, FIO1-2, UT2-4, STE1-3 | | CAPEC  26, 29, 119, 261 | | SAFECODE  1, 35 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  78, 91 | | OWASP ASVS  1.1.6, 4.1.1 | | OWASP APPSENSOR  ACE1-4 | | CAPEC  36, 95, 121, 179 | | SAFECODE  8, 10-11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  89-90 | | OWASP ASVS  4.1.2, 10.2.3, 10.2.3-10.2.6 | | OWASP APPSENSOR  - | | CAPEC  75, 133, 203 | | SAFECODE  8, 10-11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Authorization** | **Q** | **Authorization** | **K** |  |  |  |  |
| Christopher kan een commando injecteren dat de applicatie op een hoger privilegeniveau zal draaien | Ryan kan autorisatiecontroles en machtigingen beïnvloeden of wijzigen, en kan ze daarom omzeilen | (${Common\_NoCard}) | (${Common\_NoCard}) |
| |  | | --- | | OWASP SCP  209 | | OWASP ASVS  5.3.8 | | OWASP APPSENSOR  - | | CAPEC  17, 30, 69, 234 | | SAFECODE  8, 10-11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  77, 89, 91 | | OWASP ASVS  4.1.1, 4.1.2, 10.2.3-10.2.6 | | OWASP APPSENSOR  - | | CAPEC  207, 554 | | SAFECODE  8, 10-11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Cryptography** | **A** | **Cryptography** |  | **Cryptography** | **2** | **Cryptography** | **3** |
| Je hebt een nieuwe aanval tegen cryptografie uitgevonden | (${Common\_NoCard}) | Kyun heeft toegang tot gegevens omdat deze zijn verdoezeld in plaats van een goedgekeurde cryptografische functie te gebruiken | Axel kan tijdelijke of permanente gegevens (opgeslagen of in transit), of broncode, of updates/patches, of configuratiegegevens wijzigen, omdat deze niet onderworpen zijn aan integriteitscontrole |
| *Lees meer over dit onderwerp in de gratis spiekbriefjes van OWASP over cryptografische opslag en bescherming van transportlagen* |  | |  | | --- | | OWASP SCP  105, 133, 135 | | OWASP ASVS  6.2.2 | | OWASP APPSENSOR  - | | CAPEC  - | | SAFECODE  21, 29 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  92, 205, 212 | | OWASP ASVS  14.1.1, 14.1.4, 14.1.5, 10.2.3-10.2.6, 10.3.1, 10.3.2 | | OWASP APPSENSOR  SE1, IE4 | | CAPEC  31, 39, 68, 75, 133, 145, 162, 203, 438-439, 442 | | SAFECODE  12, 14 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Cryptography** | **4** | **Cryptography** | **5** | **Cryptography** | **6** | **Cryptography** | **7** |
| Paulo heeft toegang tot gegevens in transit die niet versleuteld zijn, ook al is het kanaal versleuteld | Kyle kan cryptografische controles omzeilen omdat ze niet veilig falen (d.w.z. ze zijn standaard onbeschermd) | Romain kan niet-versleutelde gegevens in het geheugen of onderweg lezen en wijzigen (bijv. cryptografische geheimen, inloggegevens, sessie-ID's, persoonlijke en commercieel gevoelige gegevens), in gebruik of in communicatie binnen de applicatie, of tussen de applicatie en gebruikers, of tussen de applicatie en externe systemen | Gunter kan versleutelde gegevens tijdens het transport onderscheppen of wijzigen omdat het protocol slecht is geïmplementeerd of zwak is geconfigureerd, of certificaten ongeldig zijn, of certificaten niet worden vertrouwd, of de verbinding kan worden verslechterd tot een zwakkere of niet-versleutelde communicatie |
| |  | | --- | | OWASP SCP  37, 88, 143, 214 | | OWASP ASVS  6.1.1, 8.3.4, 9.1.1 | | OWASP APPSENSOR  - | | CAPEC  185-187 | | SAFECODE  14, 29-30 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  103, 145 | | OWASP ASVS  1.9.1, 6.2.1, 9.1.3, 9.2.2 | | OWASP APPSENSOR  - | | CAPEC  - | | SAFECODE  21, 29 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  36-37, 143, 146-147 | | OWASP ASVS  1.9.1, 2.2.5, 2.5.1, 8.3.4, 8.3.6, 9.1.3, 9.2.2 | | OWASP APPSENSOR  - | | CAPEC  31, 57, 102, 157-158, 384, 466, 546 | | SAFECODE  29 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  75, 144-145, 148 | | OWASP ASVS  1.9.2, 6.2.7, 9.1.1, 9.2.1, 9.2.4, 14.4.5 | | OWASP APPSENSOR  IE4 | | CAPEC  31, 216 | | SAFECODE  14, 29-30 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Cryptography** | **8** | **Cryptography** | **9** | **Cryptography** | **10** | **Cryptography** | **J** |
| Eoin heeft toegang tot opgeslagen bedrijfsgegevens (bijv. wachtwoorden, sessie-ID's, PII, kaarthoudergegevens) omdat deze niet veilig versleuteld of gehasht zijn | Andy kan het genereren van willekeurige getallen, het genereren van willekeurige GUID's, hashing en versleuteling omzeilen omdat ze zelf zijn gemaakt en/of zwak zijn | Susanna kan de gebruikte cryptografie breken omdat deze niet sterk genoeg is voor de vereiste mate van bescherming, of niet sterk genoeg is voor de hoeveelheid inspanning die de aanvaller bereid is te leveren | Justin kan inloggegevens lezen voor toegang tot interne of externe bronnen, services en andere systemen omdat ze zijn opgeslagen in een niet-versleuteld formaat of opgeslagen in de broncode |
| |  | | --- | | OWASP SCP  30-31, 70, 133, 135 | | OWASP ASVS  2.4.1, 6.2.2, 6.2.3, 8.3.4 | | OWASP APPSENSOR  - | | CAPEC  31, 37, 55 | | SAFECODE  21, 29, 31 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  60, 104-105 | | OWASP ASVS  6.2.2, 6.2.3, 6.3.1, 6.3.3 | | OWASP APPSENSOR  - | | CAPEC  97 | | SAFECODE  14, 21, 29, 32-33 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  104-105 | | OWASP ASVS  6.3.3 | | OWASP APPSENSOR  - | | CAPEC  97, 463 | | SAFECODE  14, 21, 29, 31-33 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  35, 90, 171-172 | | OWASP ASVS  1.6.1, 1.6.2, 1.6.4, 2.10.4, 6.4.1, 6.4.2 | | OWASP APPSENSOR  - | | CAPEC  116 | | SAFECODE  21, 29 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Cryptography** | **Q** | **Cryptography** | **K** |  |  |  |  |
| Randolph kan de hoofdcryptografische geheimen openen of voorspellen | Dan kan cryptografiecode/routines beïnvloeden of wijzigen (encryptie, hashing, digitale handtekeningen, willekeurige getallen en GUID-generatie) en kan ze daarom omzeilen | (${Common\_NoCard}) | (${Common\_NoCard}) |
| |  | | --- | | OWASP SCP  35, 102 | | OWASP ASVS  1.6.1, 1.6.2, 1.6.3, 6.2.3, 8.3.6 | | OWASP APPSENSOR  - | | CAPEC  116-117 | | SAFECODE  21, 29 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  31, 101 | | OWASP ASVS  1.6.2, 6.2.5-6.2.8 | | OWASP APPSENSOR  - | | CAPEC  207, 554 | | SAFECODE  14, 21, 29 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Cornucopia** | **A** | **Cornucopia** |  | **Cornucopia** | **2** | **Cornucopia** | **3** |
| Je hebt een nieuwe aanval van elk type uitgevonden | (${Common\_NoCard}) | Lee kan applicatiecontroles omzeilen omdat er gevaarlijke/risicovolle programmeertaalfuncties zijn gebruikt in plaats van veiligere alternatieven, of omdat er typeconversiefouten zijn, of omdat de applicatie onbetrouwbaar is wanneer een externe bron niet beschikbaar is, of er race-omstandigheden zijn, of er zijn resource-initialisatie- of toewijzingsproblemen, of er kunnen overflows optreden | Andrew heeft toegang tot de broncode of kan decompileren, of anderszins toegang krijgen tot bedrijfslogica om te begrijpen hoe de applicatie werkt en eventuele geheimen die erin zitten |
| *Lees meer over applicatiebeveiliging in OWASP's gratis Guides on Requirements, Development, Code Review and Testing, de Cheat Sheet-serie en het Open Software Assurance Maturity Model* |  | |  | | --- | | OWASP SCP  194-202, 205-209 | | OWASP ASVS  14.1.2 | | OWASP APPSENSOR  - | | CAPEC  25-26, 29, 96, 123-124, 128-129, 264-265 | | SAFECODE  3, 5-7, 9, 22, 25-26, 34 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  134 | | OWASP ASVS  14.1.1 | | OWASP APPSENSOR  - | | CAPEC  189, 207 | | SAFECODE  - | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Cornucopia** | **4** | **Cornucopia** | **5** | **Cornucopia** | **6** | **Cornucopia** | **7** |
| Keith kan een actie uitvoeren en het is niet mogelijk om deze aan hem toe te schrijven | Larry kan het vertrouwen van andere partijen, inclusief gebruikers, in de applicatie beïnvloeden, of dat vertrouwen ergens anders misbruiken (bijvoorbeeld in een andere applicatie) | Aaron kan controles omzeilen omdat de afhandeling van fouten/uitzonderingen ontbreekt, of inconsistent of gedeeltelijk is geïmplementeerd, of de toegang niet standaard weigert (d.w.z. fouten zouden de toegang/uitvoering moeten beëindigen), of vertrouwt op afhandeling door een andere service of systeem | Mwengu's acties kunnen niet worden onderzocht omdat er geen adequaat nauwkeurig tijdstempel is van beveiligingsgebeurtenissen, of er is geen volledige audittrail, of deze kunnen worden gewijzigd of verwijderd door Mwengu, of er is geen gecentraliseerde logservice |
| |  | | --- | | OWASP SCP  23, 32, 34, 42, 51, 181 | | OWASP ASVS  7.2.1, 7.2.2 | | OWASP APPSENSOR  - | | CAPEC  - | | SAFECODE  - | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  - | | OWASP ASVS  1.9.2, 9.1.1, 5.1.5, 9.2.1, 9.2.4 | | OWASP APPSENSOR  - | | CAPEC  89, 103, 181, 459 | | SAFECODE  - | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  109-112, 155 | | OWASP ASVS  4.1.5, 7.1.4 | | OWASP APPSENSOR  - | | CAPEC  54, 98, 164 | | SAFECODE  4, 11, 23 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  113-115, 117-118, 121-130 | | OWASP ASVS  7.1.2, 7.1.4, 7.2.1, 7.2.2, 7.3.1-7.3.3, 8.3.5, 9.2.5 | | OWASP APPSENSOR  - | | CAPEC  93 | | SAFECODE  4 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Cornucopia** | **8** | **Cornucopia** | **9** | **Cornucopia** | **10** | **Cornucopia** | **J** |
| David kan de applicatie omzeilen om toegang te krijgen tot gegevens omdat de netwerk- en hostinfrastructuur en ondersteunende services/applicaties niet veilig zijn geconfigureerd, de configuratie periodiek opnieuw is gecontroleerd en beveiligingspatches zijn toegepast, of de gegevens lokaal zijn opgeslagen, of de gegevens zijn niet fysiek beschermd | Michael kan de applicatie omzeilen om toegang te krijgen tot gegevens omdat administratieve tools of administratieve interfaces niet adequaat zijn beveiligd | Xavier kan de controles van de applicatie omzeilen omdat codeframeworks, bibliotheken en componenten kwaadaardige code of kwetsbaarheden bevatten (bijv. intern, commercieel kant-en-klaar, uitbesteed, open source, extern gelokaliseerd) | Roman kan de applicatie misbruiken omdat deze is gecompileerd met verouderde tools, of de configuratie ervan is niet standaard beveiligd, of de beveiligingsinformatie is niet gedocumenteerd en doorgegeven aan operationele teams |
| |  | | --- | | OWASP SCP  151-152, 156, 160-161, 173-177 | | OWASP ASVS  1.4.5, 10.3.1, 10.3.2, 14.1.4, 14.1.5, 14.2.1, 14.2.2 | | OWASP APPSENSOR  RE1, RE2 | | CAPEC  37, 220, 310, 436, 536 | | SAFECODE  - | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  23, 29, 56, 81-82, 84-90 | | OWASP ASVS  1.4.3, 1.4.5, 4.3.1 | | OWASP APPSENSOR  - | | CAPEC  122, 233 | | SAFECODE  - | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  57, 151-152, 204-205, 213-214 | | OWASP ASVS  1.14..3, 10.1.1, 10.2.3-10.2.6, 14.2.1 | | OWASP APPSENSOR  - | | CAPEC  68, 438-439, 442, 524, 538 | | SAFECODE  15 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  90, 137, 148, 151-154, 175-179, 186, 192 | | OWASP ASVS  1.14.3, 14.1.1-14.1.5, 14.2.1 | | OWASP APPSENSOR  - | | CAPEC  - | | SAFECODE  4 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Cornucopia** | **Q** | **Cornucopia** | **K** | **Wild Card** | **Joker** | **Wild Card** | **Joker** |
| Jim kan kwaadaardige, niet-normale acties ondernemen zonder realtime detectie en reactie door de applicatie | Gareth kan de applicatie gebruiken om service aan sommige of alle gebruikers te weigeren | Alice kan de applicatie gebruiken om systemen en gegevens van gebruikers aan te vallen | Bob kan de applicatie beïnvloeden, wijzigen of beïnvloeden zodat deze niet langer voldoet aan wettelijke, reglementaire, contractuele of andere organisatorische mandaten |
| |  | | --- | | OWASP SCP  - | | OWASP ASVS  8.1.4, 11.1.1-11.1.4 | | OWASP APPSENSOR  (All) | | CAPEC  - | | SAFECODE  1, 27 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  41, 55 | | OWASP ASVS  2.2.1, 11.1.3, 11.1.4 | | OWASP APPSENSOR  UT1-4, STE3 | | CAPEC  2, 25, 119, 125 | | SAFECODE  1 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | *Heb je erover nagedacht om individueel OWASP-lid te worden? Alle tools, begeleiding en lokale bijeenkomsten zijn gratis voor iedereen, maar individueel lidmaatschap helpt het werk van OWASP te ondersteunen* | *Bestudeer kwetsbaarheden en ontdek hoe ze kunnen worden opgelost met behulp van trainingsapplicaties in de gratis OWASP Broken Web Applications VM, of met behulp van de online uitdagingen in het gratis Hacking Lab* |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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\_T03710} | 01 Jan 2023 | ${Common\_T03720} |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ${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} |  |