OWASP
The Open Web Application Security Project

Cornucopia

E-commerce Website Editie v1.30-NL

OWASP Cornucopia is een mechanisme om softwareontwikkelingsteams te helpen bij het identificeren van beveiligingsvereisten in Agile, conventionele en formele ontwikkelingsprocessen.

Auteur
Colin Watson

Projectleiders
Colin Watson and Grant Ongers

Recensenten
Tom Brennan, Johanna Curiel, Darío De Filippis and Timo Goosen

Erkenningen

Microsoft SDL Team for the Elevation of Privilege Threat Modeling Game, gepubliceerd onder een Creative Commons Attribution-licentie, als inspiratie voor Cornucopia en waaruit veel ideeën, vooral de speltheorie, zijn gekopieerd.

Keith Turpin en bijdragers aan de “OWASP Secure Coding Practices - Quick Reference Guide”, oorspronkelijk geschonken aan OWASP door Boeing, die wordt gebruikt als de primaire bron van informatie over beveiligingsvereisten om de inhoud van de kaarten te formuleren.

Bijdragers, supporters, sponsors en vrijwilligers aan de OWASP ASVS-, AppSensor- en Web Framework Security Matrix-projecten, Mitre's Common Attack Pattern Enumeration and Classification (CAPEC), en SAFECode's “Practical Security Stories and Security Tasks for Agile Development Environments”, die allemaal gebruikt in de verstrekte kruisverwijzingen.

Playgen voor het geven van een verhelderend middagseminar over taakgamificatie, en tartanmaker.com voor de online tool om het kaartrugpatroon te helpen creëren.

Blackfoot UK Limited voor het maken en doneren van drukklare ontwerpbestanden, Tom Brennan en de OWASP Foundation voor het aanzetten tot het maken van een doos en folder met het OWASP-merk, en OWASP-medewerkers, met name Kate Hartmann, voor het beheren van de bestelling, bevoorrading en verzending van bedrukte kaartspellen. Oana Cornea en andere deelnemers aan de AppSec EU 2015-projecttop voor hun hulp bij het maken van de demonstratievideo. Colin Watson als auteur en co-projectleider met Grant Ongers, samen met andere OWASP-vrijwilligers die op veel manieren hebben geholpen.

Inleiding

Het idee achter Cornucopia is om ontwikkelingsteams te helpen, met name degenen die Agile-methodologieën gebruiken, om beveiligingsvereisten voor applicaties te identificeren en op beveiliging gebaseerde gebruikersverhalen te ontwikkelen. Hoewel het idee lang genoeg had gewacht om het verder uit te werken, kwam de laatste motivatie toen SAFECode in juli 2012 zijn Praktische beveiligingsverhalen en beveiligingstaken voor flexibele ontwikkelomgevingen publiceerde.

Het Microsoft SDL-team had zijn super Elevation of Privilege: The Threat Modeling Game (EoP) al gepubliceerd, maar dat leek niet de meest geschikte soort problemen aan te pakken die ontwikkelingsteams voor webapplicaties meestal moeten aanpakken. EoP is een geweldig concept en een geweldige spelstrategie, en is gepubliceerd onder een Creative Commons Attribution-licentie.

Cornucopia Ecommerce Website Edition is gebaseerd op de concepten en spelideeën in EoP, maar deze zijn aangepast om relevanter te zijn voor de soorten problemen die ontwikkelaars van e-commercewebsites tegenkomen. Het probeert ideeën voor het modelleren van bedreigingen te introduceren in ontwikkelingsteams die Agile-methodologieën gebruiken, of die meer gericht zijn op zwakheden in webapplicaties dan andere soorten softwarekwetsbaarheden of die niet bekend zijn met STRIDE en DREAD.

Cornucopia Ecommerce Website Edition wordt vermeld als een informatiebron in de PCI Security Standard Council's Information Supplement PCI DSS E-commerce Guidelines, v2, januari 2013.

The card deck (pack)

In plaats van EoP's STRIDE-kleuren (sets van kaarten met bijpassende ontwerpen), zijn Cornucopia-kleuren gebaseerd op de structuur van de OWASP Secure Coding Practices - Quick Reference Guide (SCP), maar met extra aandacht voor secties in de OWASP Application Security Verification Standard, de OWASP Testing Guide en David Rook's Principles of Secure Development. Deze leverden vijf kleuren op, en een zesde genaamd “Cornucopia“ werd gemaakt voor al het andere:

- Data validatie en codering (VE)
- Authenticatie (AT)
- Sessiebeheer (SM)
- Autorisatie (AZ)
- Cryptografie (CR)
- Hoorn des overvloeds (C)

Net als bij pokerkaarten, bevat elke reeks 13 kaarten (Aas, 2-10, Boer, Vrouw en Koning), maar in tegenstelling tot EoP zijn er ook twee Joker-kaarten. De inhoud is voornamelijk afkomstig uit het SCP.

Mappings

De andere driver voor Cornucopia is om de aanvallen te koppelen aan vereisten en verificatietechnieken. Een eerste doel was om te verwijzen naar CWE-zwakte-ID's, maar deze bleken te talrijk, en in plaats daarvan werd besloten om elke kaart toe te wijzen aan CAPEC-software-aanvalspatroon-ID's die zelf zijn toegewezen aan CWE's, zodat het gewenste resultaat wordt bereikt. Elke kaart is ook toegewezen aan de 36 primaire beveiligingsverhalen in het SAFECode-document, evenals aan de OWASP SCP v2, ASVS v4.0 en AppSensor (detectie en reactie van toepassingsaanvallen) om teams te helpen hun eigen beveiligingsgerelateerde verhalen voor gebruik in Agile-processen.

Spelstrategie

Afgezien van de inhoudelijke verschillen, zijn de spelregels vrijwel identiek aan die voor EoP.

De kaarten afdrukken

Kijk op de Cornucopia-projectpagina voor het verkrijgen vanain voorgedrukte decks op glanzend karton.

De kaarten kunnen vanuit dit document in zwart-wit worden afgedrukt, maar zijn effectiever in kleur. De kaarten op de latere pagina's van dit document zijn zo opgemaakt dat ze op één type voorgescoorde zakelijke A4-kaarten passen. Dit bleek de snelste manier om in eerste instantie snel speelkaarten te kunnen maken. Avery-productcodes C32015 en C32030 zijn met succes getest, maar alle 10 tot 85 mm x 54 mm kaarten op A4-papier zouden met een kleine aanpassing moeten werken. Andere leveranciers van kantoorbenodigdheden zoals Ryman en Sigel produceren soortgelijke vellen Deze kaartvellen zijn niet goedkoop, dus wees voorzichtig bij het beslissen wat te printen en welk medium en printertype te gebruiken.

De kaarten kunnen natuurlijk gewoon op elk formaat papier of karton worden afgedrukt en vervolgens handmatig worden versneden, of een commerciële drukker zou grotere volumes kunnen printen en de kaarten op maat kunnen snijden. De snijlijnen worden weergegeven op de voorlaatste pagina van dit document, maar Avery maakt ook een liggend A4-sjabloon (A-0017-01_L.doc) dat als richtlijn kan worden gebruikt.

Afdrukken en versnijden kan ongeveer een uur duren, en het gebruik van een snellere printer helpt. Probeer af te drukken, voeg een hogere kwaliteit toe om de leesbaarheid te vergroten. Een optioneel kaartontwerp (in OWASP-tartan) is verstrekt als de laatste pagina van dit document. Er is geen speciale uitlijning nodig. Dubbelzijdig afdrukken vereist speciale zorg. U kunt de kaartvlakken of de achterkant aanpassen aan de voorkeuren van uw eigen organisatie.

Maatwerk

Nadat je Cornucopia een paar keer hebt gebruikt, heb je misschien het gevoel dat sommige kaarten minder relevant zijn voor je applicaties, of dat de bedreigingen anders zijn voor je organisatie. Bewerk dit document zelf om de kaarten geschikter te maken voor je teams, of maak volledig nieuwe kaartspellen.

Geef feedback

Als u ideeën of feedback heeft over het gebruik van OWASP Cornucopia, deel deze dan alstublieft. Nog beter als je alternatieve versies van de kaarten maakt, of professionele drukklare versies maakt, deel dat dan met de vrijwilligers die deze editie hebben gemaakt en met de bredere gemeenschap voor applicatieontwikkeling en applicatiebeveiliging.

De beste plaats om te discussiëren of bij te dragen is de mailinglijst voor het OWASP-project:

- Mailinglijst
  https://lists.owasp.org/mailman/listinfo/owasp_cornucopia
- Project startpagina
  https://www.owasp.org/index.php/OWASP_Cornucopia

Instructies

De tekst op elke kaart beschrijft een aanval, maar de aanvaller krijgt een naam, die uniek is voor alle kaarten. De naam kan een computersysteem vertegenwoordigen (bijv. de database, het bestandssysteem, een andere toepassing, een gerelateerde dienst, een botnet), een individuele persoon (bijv. een burger, een klant, een klant, een werknemer, een crimineel, een spion), of zelfs een groep mensen (bijvoorbeeld een concurrerende organisatie, activisten met een gemeenschappelijk doel). De aanvaller bevindt zich mogelijk op afstand op een ander apparaat/locatie, of lokaal/intern met toegang tot hetzelfde apparaat, dezelfde host of hetzelfde netwerk als waarop de applicatie wordt uitgevoerd. De aanvaller wordt altijd genoemd aan het begin van elke beschrijving Een voorbeeld is:

William heeft controle over het genereren van sessie-ID's.

Dit betekent dat de aanvaller (William) nieuwe sessie-ID's kan maken die de toepassing accepteert. De aanvallen waren voornamelijk afgeleid van de beveiligingsvereisten die zijn vermeld in het SCP, v2, maar vervolgens aangevuld met verificatiedoelstellingen uit de OWASP "Application Security Verification Standard for Web Applications", de op beveiliging gerichte verhalen in SAFECode's "Practical Security Stories and Security Tasks for Agile Development Environments", en tot slot een overzicht van de kaarten in EOP.

Meer informatie over elke kaart is beschikbaar in het online Wiki Deck op

https://wiki.owasp.org/index.php/Cornucopia_-_Ecommerce_Website_Edition_-_Wiki_Deck

Lookups tussen de aanvallen en fOp de meeste kaarten staan hulpmiddelen:

- Vereisten in "Secure Coding Practices (SCP) - Quick Reference Guide", v2, OWASP, november 2010 (ref: OWASP SCP Quick Reference Guide v2.1)
- Verificatie-ID's in "Application Security Verification Standard (ASVS) for Web Applications" (ref: ASVS v3 and v4 downloads)
- Aanvalsdetectiepunten-ID's in "AppSensor", OWASP, augustus 2010-2015 (ref: AppSensor DetectionPoints)
- ID's in "Common Attack Pattern Enumeration and Classification (CAPEC)", v2.8, Mitre Corporation, november 2015 (ref: capec (31. July 2018))
- Op veiligheid gerichte verhalen in 'Practical Security Stories and Security Tasks for Agile Development Environments', SAFECode, juli 2012 (ref: SAFECode Agile Dev Security)

Een look-up betekent dat de aanval is opgenomen in het item waarnaar wordt verwezen, maar niet noodzakelijkerwijs de volledige bedoeling ervan omvat. Voor gestructureerde gegevens zoals CAPEC wordt de meest specifieke verwijzing gegeven, maar soms wordt een kruisverwijzing gegeven die ook meer specifieke (kinder)voorbeelden bevat. Er zijn geen zoekopdrachten voor de zes azen en twee jokers. In plaats daarvan hebben deze kaarten enkele algemene tips in cursieve tekst.

Het is mogelijk om Cornucopia op veel verschillende manieren te spelen. Hier is een manier, online gedemonstreerd in een video op (refL Cornucopia scoresheet) , die het nieuwe (mei 2015) score-/recordblad gebruikt op

A - Voorbereidingen

A1. Verkrijg een stapel kaarten, of print uw eigen stapel Cornucopia-kaarten (zie pagina 2 van dit document) en scheid/knip de kaarten uit
A2. Identificeer een aanvraag of aanvraagproces om te beoordelen; dit kan een concept, ontwerp of een daadwerkelijke implementatie zijn
A3. Maak een gegevensstroomdiagram, gebruikersverhalen of andere artefacten om de beoordeling te vergemakkelijken
A4. Identificeer en nodig een groep van 3-6 architecten, ontwikkelaars, testers en andere zakelijke belanghebbenden samen uit en ga rond een tafel zitten (probeer iemand die redelijk bekend is met applicatiebeveiliging erbij te betrekken)
A5. Houd wat prijzen bij de hand (gouden sterren, chocolade, pizza, bier of bloemen, afhankelijk van je kantoorcultuur)

B - Spelen

Eén kleur - Cornucopia - fungeert als troef. Azen zijn hoog (d.w.z. ze verslaan koningen). Het helpt als er een niet-speler is om de problemen en scores te documenteren.

B1. Verwijder de jokers en een paar kaarten met een lage score (2, 3, 4) uit de Cornucopia-reeks om ervoor te zorgen dat elke speler hetzelfde aantal kaarten heeft
B2. Schud de stapel en deel alle kaarten
B3. Om te beginnen, kies willekeurig een speler die de eerste kaart zal spelen - ze kunnen elke kaart uit hun hand spelen behalve die van de troefkleur - Hoorn des overvloeds
B4. Om een kaart te spelen, moet elke speler deze hardop voorlezen en uitleggen (zie het online Wiki Deck voor tips) hoe de dreiging van toepassing kan zijn (de speler krijgt een punt voor aanvallen die mogelijk werken waarvan de groep denkt dat een bruikbare bug) - probeer in dit stadium geen oplossingen te bedenken en sluit een bedreiging niet uit alleen omdat u denkt dat deze al is verholpen - iemand noteert de kaart en noteert de problemen die aan de orde zijn gesteld
B5. Speel met de klok mee, elke persoon moet een kaart op dezelfde manier spelen; als je een kaart van de overeenkomende eerste reeks hebt, moet je een van die kaarten spelen, anders kunnen ze een kaart uit een andere reeks spelen. Alleen een hogere kaart van dezelfde kleur, of de hoogste kaart in de troefkleur Cornucopia, wint de hand.
B6. De persoon die de ronde wint, leidt de volgende ronde (d.w.z. zij spelen eerst), en bepaalt zo de volgende leidende kleur
B7. Herhaal totdat alle kaarten zijn gespeeld

C - Scoren

Het doel is om toepasselijke bedreigingen te identificeren en handen te winnen (rondes):

C1. Score +1 voor elke kaart die u kunt identificeren als een geldige bedreiging voor de betreffende toepassing
C2. Scoor +1 als je een ronde wint
C3. Als alle kaarten zijn gespeeld, wint degene die de meeste punten heeft

D - Sluiting

D1. Bekijk alle van toepassing zijnde dreigingen en de bijbehorende beveiligingseisen
D2. Maak gebruiker stories, specificaties en testcases zoals vereist voor uw ontwikkelingsmethodologie.

Alternatieve spelregels

Als je nieuw bent in het spel, verwijder dan eerst de azen en twee jokerkaarten. Voeg de Joker-kaarten weer toe zodra mensen meer vertrouwd raken met het proces. Naast de hierboven beschreven regels van het "troefkaartspel" die erg lijken op de EoP, kan het kaartspel ook worden gespeeld als het "eenentwintig kaartspel" (ook bekend als "ponton" of "blackjack") dat vermindert normaal gesproken het aantal kaarten dat in elke ronde wordt gespeeld.

Oefen op een denkbeeldige applicatie, of zelfs een toekomstige geplande applicatie, in plaats van te proberen fouten te vinden in bestaande applicaties totdat de deelnemers tevreden zijn met het nut van het spel.

Overweeg om gewoon met één kleur te spelen om een kortere sessie te maken - maar probeer alle kleuren voor elk project te dekken. Of nog beter, speel gewoon één hand met een aantal vooraf geselecteerde kaarten en scoor alleen op het vermogen om beveiligingsvereisten te identificeren. Misschien één spel van elke reeks elke dag gedurende een week of zo, als de deelnemers niet lang genoeg kunnen sparen voor een volledig kaartspel.

Sommige teams geven er de voorkeur aan om een volledige hand kaarten te spelen en na elke ronde te bespreken wat er op de kaarten staat (in plaats van nadat elke persoon een kaart heeft gespeeld).

Een andere suggestie is dat als een speler de kaart niet identificeert relevant is, andere spelers ideeën moet laten voorstellen en hen mogelijk het punt voor de kaart laat verdienen. Overweeg om extra punten toe te kennen voor bijzonder goede bijdragen.

Je kunt zelfs alleen spelen. Gebruik de kaarten gewoon om als gedachte-opwekkers te fungeren. Meer mensen erbij betrekken zal wel voordelig zijn.

In de EoP-richtlijnen van Microsoft raden ze valsspelen aan als een goede spelstrategie.

Ontwikkelingsraamwerk-specifieke aangepaste kaartspellen

Eind 2012 werd de OWASP Framework Security Matrix gepubliceerd waarin beveiligingscontroles zijn ingebouwd in enkele veelgebruikte talen en frameworks voor de ontwikkeling van web- en mobiele applicaties. Onder bepaalde voorwaarden is het nuttig om na te gaan hoe het gebruik van deze bedieningselementen de identificatie van aanvullende vereisten kan vereenvoudigen - op voorwaarde natuurlijk dat de bedieningselementen correct zijn opgenomen, ingeschakeld en geconfigureerd.

Overweeg om de volgende kaarten van de stapels te verwijderen als je er zeker van bent dat ze worden aangesproken door de manier waarop je de taal/het kader gebruikt. Items tussen haakjes zijn "misschien".

Interne codeerstandaarden en bibliotheken

Voeg uw eigen lijst met uitgesloten kaarten toe op basis van de coderingsnormen van uw organisatie (op voorwaarde dat ze worden bevestigd door de juiste verificatiestappen in de ontwikkelingslevenscyclus).

Uw codeerstandaarden en bibliotheken		
Datavalidatie en codering *[uw lijst]*	Sessiebeheer *[uw lijst]*	Cryptografie *[uw lijst]*
Authenticatie *[uw lijst]*	Autorisatie *[uw lijst]*	Hoorn des overvloeds *[uw lijst]*

Compliance vereisten decks

Maak een kleiner kaartspel door alleen kaarten op te nemen voor een bepaalde nalevingsvereiste.

Compliance-eis		
Datavalidatie en codering *[nalevingslijst]*	Sessiebeheer *[nalevingslijst]*	Cryptografie *[nalevingslijst]*
Authenticatie *[nalevingslijst]*	Autorisatie *[nalevingslijst]*	Hoorn des overvloeds *[nalevingslijst]*

Veel gestelde vragen

1. Kan ik het spel kopiëren of bewerken?

Ja natuurlijk. Alle OWASP-materialen zijn vrij om mee te doen wat je wilt, op voorwaarde dat je voldoet aan de Creative Commons Attribution-ShareAlike 3.0-licentie. Als u een nieuwe versie maakt, kunt u deze misschien doneren aan het OWASP Cornucopia Project?

2. Hoe kan ik meedoen?

Stuur ideeën of aanbiedingen van hulp naar de mailinglijst van het project.

3. Hoe zijn de namen van de aanvallers gekozen?

EoP begint elke beschrijving met woorden als 'Een aanvaller kan...'. Deze moeten als een aanval worden geformuleerd, maar ik was niet enthousiast over de anonieme terminologie, wilde iets boeienders en gebruikte daarom persoonlijke namen. Deze kunnen worden gezien als externe of interne mensen of aliassen voor computersystemen. Maar in plaats van alleen willekeurige namen, bedacht ik hoe ze het OWASP-gemeenschapsaspect zouden kunnen weerspiegelen. Daarom gebruik ik, afgezien van 'Alice en Bob', de opgegeven (voor)namen van huidige en recente OWASP-medewerkers en bestuursleden (in willekeurige volgorde toegewezen), en selecteerde vervolgens willekeurig de resterende 50 of zo namen uit de huidige lijst van het betalen van individuele OWASP-leden. Er is geen enkele naam meer dan één keer gebruikt, en waar mensen twee persoonlijke namen hadden opgegeven, liet ik een deel vallen om te proberen ervoor te zorgen dat niemand gemakkelijk kan worden geïdentificeerd. Namen zijn niet opzettelijk toegewezen aan een bepaalde aanval, verdediging of vereiste. De culturele en gendermix weerspiegelt eenvoudig deze bronnen van namen en is niet bedoeld om wereldrepresentatief te zijn. In v1.20 is de naam op VE-10 veranderd om de nieuwe co-leider van het project weer te geven - deze kaart is ook de enige met twee namen in de aanval.

4. Waarom staan er geen afbeeldingen op de kaartvlakken?

Er staat best veel tekst op de kaartjes en de kruisverwijzingen nemen ook ruimte in beslag. Maar het zou geweldig zijn om extra ontwerpelementen toe te voegen. Elke vrijwilliger

5. Staan de aanvallen gerangschikt op het nummer op de kaart?

Slechts bij benadering. Het risico is afhankelijk van de toepassing en de organisatie, vanwege verschillende beveiligings- en nalevingsvereisten, dus uw eigen ernstclassificatie kan de kaarten in een andere volgorde plaatsen dan de nummers op de kaarten.

6. Hoe lang duurt het om een ronde kaarten te spelen met het volledige kaartspel?

Dit hangt af van de hoeveelheid discussie en hoe vertrouwd de spelers zijn met applicatiebeveiligingsconcepten. Maar misschien 1,5 tot 2,0 uur voor 4-6 personen.

7. Wat voor soort mensen zouden het spel moeten spelen?

Probeer altijd een mix van rollen te hebben die alternatieve perspectieven kunnen bijdragen. Maar neem iemand mee die een redelijke kennis heeft van de terminologie van applicatiekwetsbaarheid. Probeer anders een mix van architecten, ontwikkelaars, testers en een relevante projectmanager of bedrijfseigenaar.

8. Wie moet aantekeningen maken en scores opnemen?

Het is beter als iemand anders, die het spel niet speelt, aantekeningen maakt over de geïdentificeerde vereisten en besproken problemen. Dit kan gebruikt worden als training voor een meer junior ontwikkelaar, of uitgevoerd worden door de projectmanager. Sommige organisaties hebben een opname gemaakt om achteraf te bekijken als de eisen wat formeler worden opgeschreven.

9. Moeten we altijd het volledige spel kaarten gebruiken?

Nee. Een kleiner kaartspel is sneller te spelen. Begin je eerste spel met slechts genoeg kaarten voor twee of drie rondes. Overweeg altijd om kaarten te verwijderen die helemaal niet geschikt zijn voor de doeltoepassing of functie die wordt beoordeeld. Voor de eerste paar keer dat mensen het spel spelen, is het meestal ook beter om de azen en de twee jokers te verwijderen. Het is ook gebruikelijk om het spel zonder troefkleur te spelen totdat mensen meer bekend zijn met het idee.

10. Wat moeten spelers doen als ze een aaskaart hebben met de tekst 'inve'een nieuwe X-aanval gedaan"?

De speler kan elke aanval verzinnen waarvan hij denkt dat deze geldig is, maar moet overeenkomen met de kleur van de kaart (bijvoorbeeld gegevensvalidatie en codering). Bij spelers die nieuw zijn in het spel, kan het beter zijn om deze te verwijderen om mee te beginnen (zie ook FAQ 9).

11. Ik begrijp niet wat de aanval op elke kaart betekent - is er meer gedetailleerde informatie?

Ja, het online Wiki Deck at is gemaakt om spelers te helpen de aanvallen te begrijpen. Zie

https://www.owasp.org/index.php/Cornucopia_-_Ecommerce_Website_Edition_-_Wiki_Deck

12. Mijn bedrijf wil zijn eigen versie van OWASP Cornucopia afdrukken - naar welke licentie moeten we verwijzen? Raadpleeg het volledige antwoord op deze vraag op de webpagina's van het project op

https://www.owasp.org/index.php/OWASP_Cornucopia_-_tab=FAQs

DATA VALIDATION & ENCODING

A

Je hebt een nieuwe aanval uitgevonden tegen gegevensvalidatie en -codering

Lees meer over dit onderwerp in OWASP's gratis spiekbriefjes over invoervalidatie, XSS-preventie, op DOM gebaseerde XSS-preventie, SQL-injectiepreventie en queryparameterisatie

DATA VALIDATION & ENCODING

(Geen kaart)

DATA VALIDATION & ENCODING

2

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

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

${Common_Title_full}

DATA VALIDATION & ENCODING

3

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

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

${Common_Title_full}

DATA VALIDATION & ENCODING

4

Dave kan kwaadaardige veldnamen of gegevens invoeren omdat het niet wordt gecontroleerd binnen de context van de huidige gebruiker en het huidige proces

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

${Common_Title_full}

DATA VALIDATION & ENCODING

5

Jee kan de gecentraliseerde coderingsroutines omzeilen omdat ze niet overal worden gebruikt, of de verkeerde coderingen worden gebruikt

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

${Common_Title_full}

DATA VALIDATION & ENCODING

6

Jason kan de gecentraliseerde validatieroutines omzeilen omdat ze niet op alle invoer worden gebruikt

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

${Common_Title_full}

DATA VALIDATION & ENCODING

7

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
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

${Common_Title_full}

DATA VALIDATION & ENCODING

8

Sarah kan de gecentraliseerde reinigingsroutines omzeilen omdat ze niet volledig worden gebruikt

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

${Common_Title_full}

DATA VALIDATION & ENCODING

9

Shamun kan invoervalidatie of uitvoervalidatiecontroles omzeilen omdat validatiefouten niet worden afgewezen en/of opgeschoond

OWASP SCP
6, 21-22, 168

OWASP ASVS
7.1.3

OWASP APPSENSOR
IE2-3

CAPEC
28

SAFECODE
3, 16, 24

${Common_Title_full}

DATA VALIDATION & ENCODING

10

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)

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

${Common_Title_full}

DATA VALIDATION & ENCODING

J

Dennis heeft controle over invoervalidatie, uitvoervalidatie of uitvoercoderingscode of routines zodat ze kunnen worden omzeild

OWASP SCP
1, 17

OWASP ASVS
1.5.3

OWASP APPSENSOR
RE3, RE4

CAPEC
87, 207, 554

SAFECODE
2, 17

${Common_Title_full}

DATA VALIDATION & ENCODING

Q

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

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

${Common_Title_full}

DATA VALIDATION & ENCODING

K

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

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

${Common_Title_full}

(Geen kaart)

(Geen kaart)

AUTHENTICATION

A

Je hebt een nieuwe aanval tegen authenticatie uitgevonden

Lees meer over dit onderwerp in de gratis verificatie-cheatsheet van OWASP

AUTHENTICATION

(Geen kaart)

AUTHENTICATION

2

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)

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

${Common_Title_full}

AUTHENTICATION

3

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

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

${Common_Title_full}

AUTHENTICATION

4

Sebastien kan gebruikersnamen gemakkelijk identificeren of opsommen

OWASP SCP
33, 53

OWASP ASVS
2.2.1, 4.1.5

OWASP APPSENSOR
AE1

CAPEC
383

SAFECODE
28

${Common_Title_full}

AUTHENTICATION

5

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

OWASP SCP
54, 175, 178

OWASP ASVS
4.1.5

OWASP APPSENSOR
AE12, HT3

CAPEC
70

SAFECODE
28

${Common_Title_full}

AUTHENTICATION

6

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)

OWASP SCP
37, 45-46, 178

OWASP ASVS
2.5.6

OWASP APPSENSOR
-

CAPEC
50

SAFECODE
28

${Common_Title_full}

AUTHENTICATION

7

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, 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

Kate kan authenticatie omzeilen omdat het niet beveiligd is (d.w.z. het staat standaard niet-geverifieerde toegang toe)

OWASP SCP
28

OWASP ASVS
4.1.5

OWASP APPSENSOR
-

CAPEC
115

SAFECODE
28

${Common_Title_full}

AUTHENTICATION

9

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

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

${Common_Title_full}

AUTHENTICATION

10

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

OWASP SCP
25-27

OWASP ASVS
1.1.6, 1.4.4

OWASP APPSENSOR
-

CAPEC
90, 115

SAFECODE
14, 28

${Common_Title_full}

AUTHENTICATION

J

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
23, 32, 34

OWASP ASVS
1.4.3, 1.4.5

OWASP APPSENSOR
-

CAPEC
115

SAFECODE
14, 28

${Common_Title_full}

AUTHENTICATION

Q

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)

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

${Common_Title_full}

AUTHENTICATION

K

Olga kan authenticatiecode/routines beïnvloeden of wijzigen zodat ze kunnen worden omzeild

OWASP SCP
24

OWASP ASVS
4.1.1, 10.2.3-10.2.6

OWASP APPSENSOR
-

CAPEC
115, 207, 554

SAFECODE
14, 28

${Common_Title_full}

(Geen kaart)

(Geen kaart)

SESSION MANAGEMENT

A

Je hebt een nieuwe aanval tegen Session Management uitgevonden

Lees meer over dit onderwerp in OWASP's gratis spiekbriefjes over sessiebeheer en preventie van Cross Site Request Forgery (CSRF)

SESSION MANAGEMENT

(Geen kaart)

SESSION MANAGEMENT

2

William heeft controle over het genereren van sessie-ID's

OWASP SCP
58-59

OWASP ASVS
3.7.1

OWASP APPSENSOR
SE2

CAPEC
31, 60-61

SAFECODE
28

${Common_Title_full}

SESSION MANAGEMENT

3

Ryan kan één account parallel gebruiken, aangezien gelijktijdige sessies zijn toegestaan

OWASP SCP
68

OWASP ASVS
3.3.3, 3.3.4

OWASP APPSENSOR
-

CAPEC
-

SAFECODE
28

${Common_Title_full}

SESSION MANAGEMENT

4

Alison kan sessie-identificatiecookies instellen op een andere webtoepassing omdat het domein en pad niet voldoende zijn beperkt

OWASP SCP
59, 61

OWASP ASVS
3.4.1-3.4.5

OWASP APPSENSOR
SE2

CAPEC
31, 61

SAFECODE
28

${Common_Title_full}

SESSION MANAGEMENT

5

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

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

${Common_Title_full}

SESSION MANAGEMENT

6

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

OWASP SCP
64-65

OWASP ASVS
3.3.2-3.3.4

OWASP APPSENSOR
SE5, SE6

CAPEC
21

SAFECODE
28

${Common_Title_full}

SESSION MANAGEMENT

7

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
62-63

OWASP ASVS
3.3.1, 3.3.4

OWASP APPSENSOR
-

CAPEC
21

SAFECODE
28

${Common_Title_full}

SESSION MANAGEMENT

8

Matt kan misbruik maken van lange sessies omdat de applicatie geen periodieke herauthenticatie vereist om te controleren of de rechten zijn gewijzigd

OWASP SCP
96

OWASP ASVS
3.6.1, 3.3.2

OWASP APPSENSOR
-

CAPEC
21

SAFECODE
28

${Common_Title_full}

SESSION MANAGEMENT

9

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

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

${Common_Title_full}

SESSION MANAGEMENT

10

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

OWASP SCP
73-74

OWASP ASVS
4.2.2

OWASP APPSENSOR
IE4

CAPEC
62, 111

SAFECODE
18

${Common_Title_full}

SESSION MANAGEMENT

J

Jeff kan een identieke herhaalde interactie opnieuw verzenden (bijv. HTTP-verzoek, signaal, druk op de knop) en het wordt geaccepteerd, niet afgewezen

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

Salim kan sessiebeheer omzeilen omdat het niet volledig en consistent wordt toegepast in de hele applicatie

OWASP SCP
58

OWASP ASVS
1.1.6, 3.7.1

OWASP APPSENSOR
-

CAPEC
21

SAFECODE
14, 28

${Common_Title_full}

SESSION MANAGEMENT

K

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

OWASP SCP
58, 60

OWASP ASVS
1.1.6

OWASP APPSENSOR
-

CAPEC
21

SAFECODE
14, 28

${Common_Title_full}

(Geen kaart)

(Geen kaart)

AUTHORIZATION

A

Je hebt een nieuwe aanval tegen Autorisatie uitgevonden

Lees meer over dit onderwerp in de ontwikkelings- en testhandleidingen van OWASP

AUTHORIZATION

(Geen kaart)

AUTHORIZATION

2

Tim kan beïnvloeden waar gegevens naartoe worden gestuurd of doorgestuurd

OWASP SCP
44

OWASP ASVS
4.1.3, 4.2.1, 5.1.5

OWASP APPSENSOR
-

CAPEC
153

SAFECODE
8, 10-11

${Common_Title_full}

AUTHORIZATION

3

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

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

${Common_Title_full}

AUTHORIZATION

4

Kelly kan autorisatiecontroles omzeilen omdat ze niet veilig falen (d.w.z. ze geven standaard toegang)

OWASP SCP
79-80

OWASP ASVS
4.1.5

OWASP APPSENSOR
-

CAPEC
122

SAFECODE
8, 10-11

${Common_Title_full}

AUTHORIZATION

5

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)

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

${Common_Title_full}

AUTHORIZATION

6

Eduardo heeft toegang tot gegevens waar hij geen toestemming voor heeft, ook al heeft hij toestemming voor het formulier/pagina/URL/toegangspunt

OWASP SCP
81, 88, 131

OWASP ASVS
4.1.3, 4.2.1

OWASP APPSENSOR
ACE1-4

CAPEC
122

SAFECODE
8, 10-11

${Common_Title_full}

AUTHORIZATION

7

Yuanjing heeft toegang tot applicatiefuncties, objecten of eigenschappen waartoe hij geen toegang heeft

OWASP SCP
81, 85-86, 131

OWASP ASVS
4.1.3, 4.2.1

OWASP APPSENSOR
ACE1-4

CAPEC
122

SAFECODE
8, 10-11

${Common_Title_full}

AUTHORIZATION

8

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

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

${Common_Title_full}

AUTHORIZATION

9

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

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

${Common_Title_full}

AUTHORIZATION

10

Richard kan de gecentraliseerde autorisatiecontroles omzeilen omdat ze niet volledig worden gebruikt voor alle interacties

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

${Common_Title_full}

AUTHORIZATION

J

Dinis heeft toegang tot informatie over de beveiligingsconfiguratie of heeft toegang tot controlelijsten

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

${Common_Title_full}

AUTHORIZATION

Q

Christopher kan een commando injecteren dat de applicatie op een hoger privilegeniveau zal draaien

OWASP SCP
209

OWASP ASVS
5.3.8

OWASP APPSENSOR
-

CAPEC
17, 30, 69, 234

SAFECODE
8, 10-11

${Common_Title_full}

AUTHORIZATION

K

Ryan kan autorisatiecontroles en machtigingen beïnvloeden of wijzigen, en kan ze daarom omzeilen

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

${Common_Title_full}

(Geen kaart)

(Geen kaart)

CRYPTOGRAPHY

A

Je hebt een nieuwe aanval tegen cryptografie uitgevonden

Lees meer over dit onderwerp in de gratis spiekbriefjes van OWASP over cryptografische opslag en bescherming van transportlagen

CRYPTOGRAPHY

(Geen kaart)

CRYPTOGRAPHY

2

Kyun heeft toegang tot gegevens omdat deze zijn verdoezeld in plaats van een goedgekeurde cryptografische functie te gebruiken

OWASP SCP
105, 133, 135

OWASP ASVS
6.2.2

OWASP APPSENSOR
-

CAPEC
-

SAFECODE
21, 29

$Common_Title_full}

CRYPTOGRAPHY

3

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

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

$Common_Title_full}

CRYPTOGRAPHY

4

Paulo heeft toegang tot gegevens in transit die niet versleuteld zijn, ook al is het kanaal versleuteld

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

$Common_Title_full}

CRYPTOGRAPHY

5

Kyle kan cryptografische controles omzeilen omdat ze niet veilig falen (d.w.z. ze zijn standaard onbeschermd)

OWASP SCP
103, 145

OWASP ASVS
1.9.1, 6.2.1, 9.1.3, 9.2.2

OWASP APPSENSOR
-

CAPEC
-

SAFECODE
21, 29

$Common_Title_full}

CRYPTOGRAPHY

6

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

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

$Common_Title_full}

CRYPTOGRAPHY

7

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
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

$Common_Title_full}

CRYPTOGRAPHY

8

Eoin heeft toegang tot opgeslagen bedrijfsgegevens (bijv. wachtwoorden, sessie-ID's, PII, kaarthoudergegevens) omdat deze niet veilig versleuteld of gehasht zijn

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
${Common_Title_full}

CRYPTOGRAPHY

9

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

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
${Common_Title_full}

CRYPTOGRAPHY

10

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

OWASP SCP
104-105
OWASP ASVS
6.3.3
OWASP APPSENSOR
-
CAPEC
97, 463
SAFECODE
14, 21, 29, 31-33
${Common_Title_full}

CRYPTOGRAPHY

J

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
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
${Common_Title_full}

CRYPTOGRAPHY

Q

Randolph kan de hoofdcryptografische geheimen openen of voorspellen

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
${Common_Title_full}

CRYPTOGRAPHY

K

Dan kan cryptografiecode/routines beïnvloeden of wijzigen (encryptie, hashing, digitale handtekeningen, willekeurige getallen en GUID-generatie) en kan ze daarom omzeilen

OWASP SCP
31, 101
OWASP ASVS
1.6.2, 6.2.5-6.2.8
OWASP APPSENSOR
-
CAPEC
207, 554
SAFECODE
14, 21, 29
${Common_Title_full}

(Geen kaart)

(Geen kaart)

CORNUCOPIA

A

Je hebt een nieuwe aanval van elk type uitgevonden

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

CORNUCOPIA

(Geen kaart)

CORNUCOPIA

2

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

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

${Common_Title_full}

CORNUCOPIA

3

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

OWASP SCP
134

OWASP ASVS
14.1.1

OWASP APPSENSOR
-

CAPEC
189, 207

SAFECODE
-

${Common_Title_full}

CORNUCOPIA

4

Keith kan een actie uitvoeren en het is niet mogelijk om deze aan hem toe te schrijven

OWASP SCP
23, 32, 34, 42, 51, 181

OWASP ASVS
7.2.1, 7.2.2

OWASP APPSENSOR
-

CAPEC
-

SAFECODE
-

${Common_Title_full}

CORNUCOPIA

5

Larry kan het vertrouwen van andere partijen, inclusief gebruikers, in de applicatie beïnvloeden, of dat vertrouwen ergens anders misbruiken (bijvoorbeeld in een andere applicatie)

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
-

${Common_Title_full}

CORNUCOPIA

6

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

OWASP SCP
109-112, 155

OWASP ASVS
4.1.5, 7.1.4

OWASP APPSENSOR
-

CAPEC
54, 98, 164

SAFECODE
4, 11, 23

${Common_Title_full}

CORNUCOPIA

7

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
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

${Common_Title_full}

CORNUCOPIA

8

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

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
-

${Common_Title_full}

CORNUCOPIA

9

Michael kan de applicatie omzeilen om toegang te krijgen tot gegevens omdat administratieve tools of administratieve interfaces niet adequaat zijn beveiligd

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
-

${Common_Title_full}

CORNUCOPIA

10

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)

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

${Common_Title_full}

CORNUCOPIA

J

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
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

${Common_Title_full}

CORNUCOPIA

Q

Jim kan kwaadaardige, niet-normale acties ondernemen zonder realtime detectie en reactie door de applicatie

OWASP SCP
-

OWASP ASVS
8.1.4, 11.1.1-11.1.4

OWASP APPSENSOR
(All)

CAPEC
-

SAFECODE
1, 27

${Common_Title_full}

CORNUCOPIA

K

Gareth kan de applicatie gebruiken om service aan sommige of alle gebruikers te weigeren

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

${Common_Title_full}

WILD CARD

Joker

Alice kan de applicatie gebruiken om systemen en gegevens van gebruikers aan te vallen

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

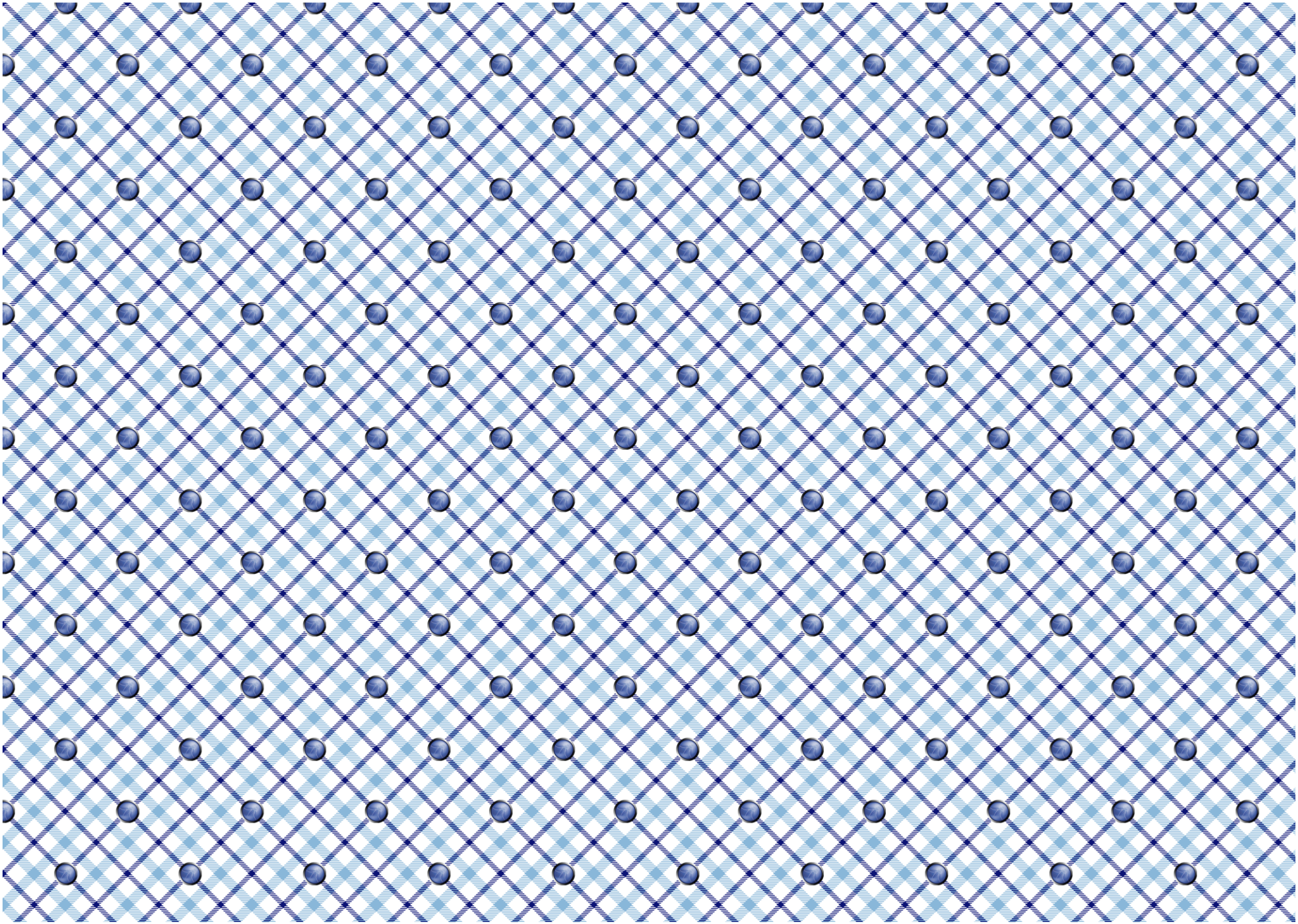
WILD CARD

Joker

Bob kan de applicatie beïnvloeden, wijzigen of beïnvloeden zodat deze niet langer voldoet aan wettelijke, reglementaire, contractuele of andere organisatorische mandaten

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



Wijzig logboek

Versie / Datum		Opmerkingen
0.1	30 Jul 2012	Origineel ontwerp
0.2	10 Aug 2012	Concept herzien en bijgewerkt
0.3	15 Aug 2012	Concept heeft OWASP SCP-mailinglijst aangekondigd voor commentaar.
0.4	25 Feb 2013	Speelregels bijgewerkt op basis van feedback tijdens workshops. Toegevoegde verwijzing naar PCI SSC-informatiesupplement: PCI DSS-richtlijnen voor e-commerce. Beschrijvende tekst uitgebreid en bijgewerkt. Sectie met bijdragers, paginanummering, veelgestelde vragen en wijzigingslogboek toegevoegd.
1	25 Feb 2013	Laat los.
1.01	03 Jun 2013	Framework-specifieke kaartspel discussie toegevoegd Aanvullende veelgestelde vragen gemaakt. Beschrijvende tekst bijgewerkt. Nieuwe omslagafbeelding en vorige omslagafbeelding naar achteren verplaatst. Snijlijnen toegevoegd. FAQ's 5 en 6 toegevoegd. Aanvalbeschrijvingen op kaarten met getinte achtergrond veranderd in zwart (van donkergrijs). Projectbijdragers toegevoegd.
1.02	14 Aug 2013	Waarschuwing over tijd om af te drukken toegevoegd. Aanvullende alternatieve spelregels toegevoegd (eenentwintig, speel een kaartspel over een week, speel de volledige hand en bespreek dan). Compliance deck concept toegevoegd. FAQ's 5 en 6 toegevoegd. Aanvalbeschrijvingen op kaarten met getinte achtergrond veranderd in zwart (van donkergrijs). Projectbijdragers toegevoegd.
1.03	18 Sep 2013	Kleine wijziging in de bewoording van de aanval op twee kaarten. OWASP SCP en ASVS kruisverwijzingen gecontroleerd en bijgewerkt. Codeletters toegevoegd voor pakken. Alle resterende aanvalsbeschrijvingen op kaarten zijn gewijzigd in zwart (van donkergrijs) en de achtergrondkleuren zijn gewijzigd om meer contrast te bieden en de leesbaarheid te vergroten.
1.04	01 Feb 2014	Tekst “wachtwoordwijziging, wachtwoordwijziging”, gecorrigeerd in “wachtwoordwijziging, wachtwoordherstel”, op Queen of Authentication-kaart.
1,05	21 Mar 2014	Updates van alternatieve spelregels. Aanvullende veelgestelde vragen gemaakt. Bijdragers bijgewerkt. Podcast- en videolinks toegevoegd.
1.1	04 Mar 2015	Wijzig logboekdatum gecorrigeerd voor v1.05. Kruisverwijzingen bijgewerkt voor 2014-versie van ASVS. Bijdragers bijgewerkt. Kleine tekstwijzigingen op kaarten om de leesbaarheid te verbeteren.
1.2	29 Jun 2016	Video vermeld/gelinkt Apart scoreblad vermeld/gekoppeld. Vorige ingesloten scorebladpagina's verwijderd Correctie (geïdentificeerd door Tom Brennan) en toevoeging aan tekst op kaart 8 Authenticatie. Oana Cornea en andere deelnemers aan de AppSec EU 2015-projecttop toegevoegd aan de lijst met bijdragers. Darío De Filippis toegevoegd als co-leider van het project. Wiki Deck-link toegevoegd Kruisverwijzingen bijgewerkt voor ASVS v3.0.1 en CAPEC v2.8. Kleine tekstwijzigingen in een klein aantal kaarten. “-EN” toegevoegd aan versienummer ter voorbereiding op “-ES”-versie. Susana Romaniz toegevoegd als bijdrage aan de Spaanse vertaling. Kleine tekstwijzigingen in instructies en veelgestelde vragen.
1.3	01 Jan 2023	Kruisverwijzingen bijgewerkt van ASVS v3.0.1 naar ASVS v4.0 door Johan Sydseter.

Projectbijdragers

Alle OWASP-projecten zijn afhankelijk van de vrijwillige inspanningen van mensen in de sectoren softwareontwikkeling en informatiebeveiliging.

Ze hebben hun tijd en energie gestoken in het doen van suggesties, het geven van feedback, het schrijven, beoordelen en bewerken van documentatie, het geven van aanmoediging, het uitproberen van het spel en het promoten van het concept.

Zonder al hun inspanningen zou het project niet zover zijn gevorderd.

Neem rechtstreeks contact op met de mailinglijst of met de projectleiders als er iemand ontbreekt op de onderstaande lijsten.

- 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
- Johan Sydseter

- OWASP's hardwerkende medewerkers, vooral Kate Hartmann
- Aanwezigen bij OWASP Londen, OWASP Manchester, OWASP Nederland en OWASP Schotland Chapter meetings, en de London Gamification meetup, die nuttige suggesties deden en uitdagende vragen stelden
- Blackfoot UK Limited voor het schenken van drukklare ontwerpbestanden en honderden professioneel bedrukte kaartendecks voor distributie per post en op OWASP-hoofdstukvergaderingen
- OWASP NYC voor het maken van een OWASP-doosontwerp en het distribueren van pakketten op AppSec USA 2014.

Podcasts en video's

De volgende ondersteunende OWASP Cornucopia-bronnen zijn online beschikbaar:

- Video - Gebruik van de kaarten, gemaakt tijdens de AppSec EU 2015-projecttop, 20 mei 2015
  https://www.youtube.com/watch?v=i5Y0akWj31k
- Podcast-interview, OWASP 24/7 Podcast-kanaal, 21 maart 2014
  http://trustedsoftwarealliance.com/2014/03/21/the-owasp-cornucopia-project-with-colin-watson/
- Video presentatie, OWASP EU Tour 2013 London, 3rd June 2013

https://www.youtube.com/watch?v=Q_LE-8xNXVk

Zie de projectwebsite voor meer informatie en presentatiemateriaal.