



Cornucopia

Website App Edition v1.30-NO_NB

OWASP® Cornucopia er en mekanisme for å hjelpe programvareutviklingsteam med å identifisere sikkerhetskrav i smidige, konvensjonelle og formelle utviklingsprosesser.

Forfatter

Colin Watson

Prosjektleddere

Colin Watson and Grant Ongers

Redaksjonell bearbeidelse

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

Takk til

Adam Shostack og Microsoft SDL Team for "Elevation of Privilege Threat Modeling Game", publisert under "Creative Commons Attribution" som ble brukt som inspirasjon til Cornucopia og som mange ideer, spesielt spillteorien, ble kopiert fra.

Keith Turpin og bidragsytere til "OWASP Secure Coding Practices - Quick Reference Guide", opprinnelig donert til OWASP av Boeing, som brukes som den primære kilden til informasjon om sikkerhetskrav for å formulere innholdet på kortene.

Bidragsytere, støttespillere, sponsorer og frivillige til OWASP ASVS-, AppSensor- og Web Framework Security Matrix-prosjektene, Mitre's "Common Attack Pattern Enumeration and Classification (CAPEC)", og SAFECode's "Practical Security Stories and Security Tasks for Agile Development Environments" som alle brukes i oppgitte kryssreferanser.

Playgen for å tilby et opplysende ettermiddagsseminar om oppgave gamification, og tartanmaker.com for bruk av nettverktøyet for å hjelpe til å lage mønsteret på baksiden av kortene.

Blackfoot UK Limited for å lage og donere utskriftsklare designfiler, Tom Brennan og OWASP Foundation for å ha startet opprettingen av en OWASP-merket boks og brosyre, og OWASP-ansatte, spesielt Kate Hartmann, for å administrere bestilling, lagring og forsendelse av trykte kortstokker. Oana Cornea og andre deltakere på AppSec EU 2015-prosjektoppmøtet for deres hjelp med å lage demonstrasjonsvideoen. Colin Watson som forfatter og medprosjektledder sammen med Grant Ongers, sammen med andre OWASP-frivillige som har hjulpet til på mange måter.

OWASP støtter eller anbefaler ikke kommersielle produkter eller tjenester © 2012-2024 OWASP Foundation.
Dette dokumentet er lisensiert under "Creative Commons Attribution-ShareAlike 3.0" lisensen



Introduksjon

Ideen bak Cornucopia er å hjelpe utviklingsteam, spesielt de som bruker Smidige metoder, med å identifisere applikasjonssikkerhetskrav og utvikle sikkerhetsbaserte brukerhistorier. Selv om ideen hadde ventet en stund med å komme videre, kom den endelige motivasjonen da SAFECode publiserte sine praktiske sikkerhetshistorier og sikkerhetsoppgaver for smidige utviklingsmiljøer i juli 2012.

Microsoft SDL-teamet hadde allerede publisert sin supre “Elevation of Privilege: The Threat Modeling Game (EoP)”, men det så ikke ut til å løse den mest hensiktsmessige typen problemer som utviklingsteam for nettapplikasjoner stort sett må løse. EoP er et flott konsept og spillstrategi, og ble publisert under en “Creative Commons Attribution” lisensen.

“Cornucopia Website App Edition” er basert på konseptene og spillideene i EoP, men de har blitt modifisert for å være mer relevante for den typen problemer som utviklere av webapp-nettsteder møter. Den prøver å introdusere trusselmodelleringens ideer i utviklingsteam som bruker smidige metoder, eller som er mer fokusert på svakheter i nettapplikasjoner enn andre typer programvaresårbarheter eller som ikke er kjent med STRIDE og DREAD.

“Cornucopia Website App Edition” er referert til som en informasjonsressurs i “PCI Security Standard Council's Information Supplement PCI DSS E-commerce Guidelines, v2”, januar 2013.

Kortstokken (pakke)

I stedet for EoPs STRIDE-farger (sett med kort med matchende design), er Cornucopia-fargene basert på strukturen til “OWASP Secure Coding Practices - Quick Reference Guide (SCP)”, men med ytterligere hensyn tatt fra avsnitt i “OWASP Application Security Verification Standard”, “OWASP Testing Guide” og David Rooks prinsipper for sikker utvikling. Disse har resultert i fem farger, og en sjette kalt “Cornucopia” som har blitt opprettet for alt annet:

- Datavalidering & Tegnkoding (VE)
- Autentisering (AT)
- Sesjonshåndtering (SM)
- Autorisasjon (AZ)
- Kryptografi (CR)
- Cornucopia (C)

I likhet med pokerkort, inneholder hver farge 13 kort (ess, 2-10, knekt, dronning og konge), men i motsetning til EoP, er det også to Joker-kort. Innholdet var hovedsakelig hentet fra SCP.

Referanseoversikt

Den andre driveren bak Cornucopia er å koble angrep med krav og verifiseringsteknikker. Et av de første målene var å referere til CWE-svakhets-ID-er, men disse viste seg å være for mange, og i stedet ble det besluttet å kartlegge hvert kort til CAPEC-programvareangrepsmønster-IDer som i seg selv er kartlagt til CWE-er, slik at det ønskede resultatet ble oppnådd. Hvert kort er også tilordnet de 36 primære sikkerhetshistoriene i SAFECode-dokumentet, samt til OWASP SCP v2, ASVS v4.0 og AppSensor (applikasjonsangrepsteksjon og respons) for å hjelpe team med å lage sine egne sikkerhetsrelaterte historier for bruk i smidige prosesser.

Spillstrategi

Bortsett fra forskjellene iht. innholdet, er spillereglene praktisk talt identiske med de for EoP.

Trykking av kort

Sjekk Cornucopia-prosjektsiden for å finne ut hvordan du får tak i forhåndstrykte kortstokker på glanset kort.

Kortene kan skrives ut fra dette dokumentet i svart-hvitt, men er mer effektive i farger. Kortene på de senere sidene i dette dokumentet er lagt ut for å passe til en type forhåndsstutfylte A4-kortark. Dette så ut til å være den raskeste måten å sørge for å lage kort raskt. Avery-produktkodene C32015 og C32030 har blitt testet vellykket, men en hver “10 up 85 mm x 54 mm” kort på A4-papir bør fungere med litt justering. Andre papirvareleverandører som Ryman og Sigel produserer lignende ark. Disse kortarkene er ikke billige, så det bør utvises forsiktighet når du bestemmer deg for hva du skal trykke opp og hva slags media og skrивertype du skal benytte.

Kortene kan selvfølgelig skrives ut på en hvilken som helst størrelse papir eller kartong for deretter å kuttes opp manuelt, ellers kan et kommersiell trykkeri skrive ut større volumer og kutte kortene i riktig størrelse. Kuttlinjene vises på nest siste side i dette dokumentet, men Avery produserer også en liggende A4-mal (A-0017-01_L.doc) som kan brukes som veileding.

Utskrift og oppskjæring kan ta en time eller så, det hjelper å bruke en raskere skriver. Prøv å skrive ut og velge høyere kvalitet for økt lesbarhet. Et valgfritt baksidedesign (i OWASP tartan) er opprettet som siste side i dette dokumentet. Ingen spesiell justering er nødvendig. Tosidig utskrift krever spesiell forsiktighet. Du kan tilpasse kortflatene eller baksidene etter din egen organisasjons preferanser.

Tilpasning

Etter at du har brukt Cornucopia noen ganger, kan det hende du føler at noen kort er mindre relevante for applikasjonene dine, eller at truslene er forskjellige for organisasjonen din. Rediger dette dokumentet selv for å gjøre kortene mer passende for teamene dine, eller lag nye fullstendig kortstokker.

Gi tilbakemelding

Hvis du har ideer eller tilbakemeldinger om bruken av OWASP® Cornucopia, vennligst del dem. Enda bedre hvis du lager alternative versjoner av kortene, eller produserer profesjonelle utskriftsklare versjoner, vennligst del det med de frivillige som har laget denne utgaven og med det bredere fellesskapet for applikasjonsutvikling og applikasjonssikkerhet.

Det beste stedet å bruke for å diskutere eller bidra er i listen eller gruppen for OWASP-prosjektet:

- Liste/Gruppe
https://lists.owasp.org/mailman/listinfo/owasp_cornucopia
- Prosjektets hjemmeside
https://www.owasp.org/index.php/OWASP_Cornucopia

Alle OWASP-dokumenter og -verktøy er gratis å laste ned og bruke. OWASP® Cornucopia er lisensiert under “Creative Commons Attribution-ShareAlike 3.0” lisensen.

Bruksanvisning

Teksten på hvert kort beskriver et angrep, men angriperen har fått et navn som er unikt for hvert av kortene. Navnet kan representere et datasystem (f.eks. databasen, filsystemet, en annen applikasjon, en relatert tjeneste, et botnett), en enkeltperson (f.eks. en borger, en kunde, en klient, en ansatt, en kriminell, en spion), eller til og med en gruppe mennesker (f.eks. en konkurrent, aktivister med en felles sak). Angriperen kan være ekstern på en annen enhet/lokasjon, eller lokal/intern med tilgang til samme enhet, vert eller nettverk hvor applikasjonen kjører. Nåværende og tidligere OWASP® Cornucopia-prosjektbidragsyttere og ledere, spesielt de involverte som sist oppdaterte kryss-referanser, laget nettversjoner og skrev skript for dynamisk å genererert Cornucopias utdatafiler. Eksempelvis:

William har kontroll over genereringen av sesjonsidentifikatorer.

Dette betyr at angriperen (William) kan opprette nye sesjonsidentifikatorer som applikasjonen godtar. Angrepene ble primært hentet fra sikkerhetskravene oppført i SCP, v2, men deretter supplert med verifiseringskrav fra OWASP “Application Security Verification Standard for Web Applications”, de sikkerhetsfokuserte historiene i SAFECode’s “Practical Security Stories and Security Tasks for Agile Development Environments”, og til slutt en gjennomgang av kortene i EOP.

Ytterligere veiledning til hvert kort er tilgjengelig på online Wiki kortstokken på

https://wiki.owasp.org/index.php/Cornucopia - Ecommerce_Website_Edition - Wiki_Deck

Referanseoversikt til angrepene og de fem ressurser finnes på de fleste kort:

- Krav til “Secure Coding Practices (SCP) - Quick Reference Guide”, v2, OWASP®, November 2010 (ref: [OWASP SCP Quick Reference Guide v2.1](#))
- Verifiserings IDer til “Application Security Verification Standard (ASVS) for Web Applications” (ref: [ASVS v3 and v4 downloads](#))
- ID-er for angrepsdeteksjonspunkter til “AppSensor”, OWASP®, August 2010-2015 (ref: [AppSensor DetectionPoints](#))
- IDer til “Common Attack Pattern Enumeration and Classification (CAPEC)”, v2.8, Mitre Corporation, November 2015 (ref: [capec \(31. July 2018\)](#))
- Sikkerhetsfokuserte historier til 'Practical Security Stories and Security Tasks for Agile Development Environments', SAFECode, Juli 2012 (ref: [SAFECode Agile Dev Security](#))

En referanse betyr at angrepet er inkludert i det refererte elementet, men at det ikke nødvendigvis omfatter hele dens intensjon. For strukturerte data som CAPEC er den mest spesifikke referansen gitt, men noen ganger er det gitt en kryssreferanse som også har mer spesifikke (underordnede) eksempler. Det finnes ingen referanseoversikt på de seks essene og to jokerne. I stedet har disse kortene noen generelle tips i kursiv tekst.

Det er mulig å spille Cornucopia på mange forskjellige måter. Her er en måte, demonstrert online i en video: (ref: [ColinWatsonOWASP](#)), som benytter det nye skåre/funn arket fra mai (2015) lastet ned fra (refL [Cornucopia scoresheet](#))

A - Forberedelser

- A1. Skaff deg en kortstokk, eller skriv ut din egen kortstokk med Cornucopia-kort (se side 2 i dette dokumentet) og skjær/klipp ut kortene
- A2. Identifiser en applikasjon eller applikasjonsfunksjon som skal gjennomgås; dette kan være et konsept, design eller en faktisk implementering
- A3. Lag et dataflytdiagram, brukerhistorier eller andre artefakter for å hjelpe til med utforskningen
- A4. Identifiser og inviter en gruppe på 3-6; arkitekter, utviklere, testere og andre forretningsinteressenter og sett deg rundt et bord (forsøk å inkludere noen som er ganske kjent med applikasjonssikkerhet)
- A5. Ha noen premier for hånden (gullstjerner, sjokolade, pizza, øl eller blomster avhengig av organisasjonskulturen din)

B - Spill

Fargen - Cornucopia - fungerer som trumfer. Ess er høye (dvs. slår konge). Det hjelper hvis det er en ikke-spiller som kan dokumentere problemene og poengsummene.

- B1. Fjern jokerne og noen få kort med lav poengsum (2, 3, 4) fra Cornucopia-fargen for å sikre at hver spiller har samme antall kort
- B2. Bland kortene og del ut alle
- B3. For å begynne, velg en tilfeldig spiller som skal spille det første kortet - de kan spille hvilket som helst kort fra hånden deres bortsett fra trumffargen - Cornucopia
- B4. For å spille et kort, må hver spiller lese det opp, og forklare (se online Wiki Deck for tips) hvordan trusselen kan fungere (spilleren får et poeng for angrep som kan fungere som gruppen mener er en håndterbar feil) - ikke prøv å tenke på avbøtende tiltak på dette stadiet, og ikke utelukk en trussel bare på grunn av en tro på at den allerede er mitigert - noen noterer kortet og noterer problemene som tas opp
- B5. Spill med klokken, hver person må spille et kort på samme måte; hvis du har et kort i den matchende hovedfargen, må du spille ett av disse, ellers kan det spilles et kort fra en hvilken som helst annen farge. Bare et høyere kort i samme farge, eller det høyeste kortet i trumffargen Cornucopia, vinner hånden.
- B6. Personen som vinner runden, leder neste runde (dvs. de spiller først), og definerer dermed neste hovedfarge
- B7. Gjenta til alle kortene er spilt

C - Scoring

Målet er å identifisere aktuelle trusler og vinne hender (runder):

- C1. Poeng +1 for hvert kort du kan identifisere som en gyldig trussel mot applikasjonen som vurderes
- C2. Få +1 poeng hvis du vinner en runde
- C3. Når alle kortene er spilt, vinner den som har flest poeng

D - Avslutning

- D1. Gå gjennom alle gjeldende trusler og samsvarende sikkerhetskrav
- D2. Lag brukerhistorier, spesifikasjoner og testtilfeller iht. utviklingsmetodikken din.

Alternative spilleregler

Hvis du er ny i spillet, fjern ess og to Joker-kort til å begynne med. Legg til Joker-kortene igjen når folk blir mer kjent med prosessen. Bortsett fra reglene for "trumfkortspill" beskrevet ovenfor, som ligner veldig på EoP, kan kortstokken også spilles som "tjueen kortspill" (også kjent som "pontong" eller "blackjack") som normalt reduserer antall kort spilt i hver runde.

Øv på en tenkt applikasjon, eller til og med en fremtidig planlagt applikasjon, i stedet for å prøve å finne feil ved eksisterende applikasjoner til deltakerne er fornøyd med nytten av spillet.

Vurder å bare spille med en farge for å gjøre økten kortere – men prøv å dekke alle fargene for hvert prosjekt. Eller enda bedre bare spill en hånd med noen forhåndsvalgte kort, og skår poeng kun etter evnen til å identifisere sikkerhetskrav. Om mulig, arranger ett parti fra hver farge hver dag i en uke eller så hvis deltakerne ikke kan sparre lenge nok til en full kortstokk.

Noen lag har foretrukket å spille en hel hånd med kort, og deretter diskutere hva som står på kortene etter hver runde (i stedet for etter at hver person har spilt et kort).

Et annet forslag er at hvis en spiller ikke klarer å identifisere kortet som relevant, la andre spillere foreslå ideer, og muligens la dem få poenget for kortet. Vurder å gi ekstra poeng for spesielt gode bidrag.

Du kan til og med spille selv. Bare bruk kortene som tankevekkere. Å involvere flere mennesker vil imidlertid være fordelaktig.

I Microsofts EoP-veiledning anbefaler de juks som en god spillstrategi.

Spesifikke modifiserte kortstokker til utviklingsrammeverk

Det kan bygges inn sikkerhetskontroller fra noen av de vanligste språkene og rammeverkene for utvikling av nett- og mobilapplikasjoner. Med visse forbehold er det nyttig å vurdere hvordan bruk av disse kontrollene kan forenkle identifiseringen av tilleggskrav – forutsatt at kontrollene selvfolgtelig er inkludert, aktivert og konfigurert riktig.

Vurder å fjerne kort fra kortstokkene hvis du er sikker på at de blir adressert på den måten du bruker programmeringsspråket/rammeverket på. Elementer i parentes er "mulige".

Interne kodenormer og biblioteker

Legg til din egen liste over ekskluderte kort basert på organisasjonens kodenormer (forutsatt at de bekreftes av passende verifiseringstrinn i utviklingslivssyklusen).

Dine kodenormer og biblioteker		
Datavalidering & Tegnkoding [din liste]	Sesjonshåndtering [din liste]	Kryptografi [din liste]
Autentisering [din liste]	Autorisasjon [din liste]	Cornucopia [din liste]

Kortstokk knyttet til overholdelse av standarder, lover og regler

Lag en mindre kortstokk ved kun å inkludere kort for et bestemt krav knyttet til overholdelse av standarder, lover og regler.

Krav knyttet til overholdelse av standarder, lover og regler		
Datavalidering & Tegnkoding [overholdelsesliste iht. standarder, lover og regler]	Sesjonshåndtering [overholdelsesliste iht. standarder, lover og regler]	Kryptografi [overholdelsesliste iht. standarder, lover og regler]
Autentisering [overholdelsesliste iht. standarder, lover og regler]	Autorisasjon [overholdelsesliste iht. standarder, lover og regler]	Cornucopia [overholdelsesliste iht. standarder, lover og regler]

Oftre stilte spørsmål

1. Kan jeg kopiere eller redigere spillet?

Ja, selvfølgelig. Alt OWASP-materiale er gjort fritt tilgjengelig for å gjøre med som du vil, forutsatt at du overholder "Creative Commons Attribution-Share Alike 3.0" lisensen. Hvis du lager en ny versjon, kan du kanskje donere den til OWASP® Cornucopia Project?

2. Hvordan kan jeg hjelpe til?

Send gjerne ideer eller tilbud om hjelp til prosjektets e-postliste.

3. Hvordan ble angripernes navn valgt?

EoP begynner hver beskrivelse med ord som "En angriper kan...". Disse må formuleres som et angrep, men jeg var ikke begeistret for den anonyme terminologien, ville ha noe mer engasjerende, og brukte derfor personnavn. Disse kan betraktes som eksterne eller interne personer eller aliaser for datasystemer. Men i stedet for bare tilfeldige navn, tenkte jeg på hvordan de kunne reflektere OWASP-felleskapsaspektet. Derfor, bortsett fra 'Alice og Bob', bruker jeg de oppgitte (for)navnnene til nåværende og nylige OWASP-ansatte og styremedlemmer (tildelt uten rekkefølge), og valgte deretter tilfeldig de resterende 50 eller så navnene fra gjeldende liste over betalende personer OWASP medlemmer. Ingen navn ble brukt mer enn en gang, og der folk hadde oppgitt to personnavn, droppet jeg én del for å prøve å sikre at ingen lett kan identifiseres. Navn ble ikke berørt tildelt noe spesielt angrep, forsvar eller krav. Den kulturelle og kjønnsblandingen gjenspeiler ganske enkelt disse navnene, og er ikke ment å være verdensrepresentativ. I v1.20 ble navnet på VE-10 endret fra å gjenspeile prosjektets nye medledder - dette kortet er også det eneste med to navn i angrepet.

4. Hvorfor er det ingen bilder på kortflatene?

Det er ganske mye tekst på kortene, og kryssreferansene tar også plass. Men det ville vært flott å ha flere designelementer inkludert. Finnes det noen frivillige?

5. Er angrepene rangert etter nummeret på kortet?

Bare sånn ca. Risikooen vil være avhengig av bruk og organisasjon, på grunn av varierende sikkerhets- og samsvarskrav, så din egen alvorlighetsgrad kan plassere kortene i en annen rekkefølge enn tallene på kortene.

6. Hvor lang tid tar det å spille en runde med kort med hele kortstokken?

Dette avhenger av størrelsen på applikasjonen, mengden diskusjoner og hvor kjent spillerne er med applikasjonsikkerhetskonsepter. Men kanskje tillat 1,5 til 2,0 timer for 4-6 personer.

7. Hva slags folk bør spille spillet?

Prøv alltid å ha en blanding av roller som kan bidra med alternative perspektiver. Men ta med noen som har en rimelig kunnskap om terminologi for applikasjonssårbarhet. Prøv ellers å inkludere en blanding av arkitekter, utviklere, testere og en relevant prosjektleder eller bedriftscheier.

8. Hjem skal ta notater og notere poeng?

Det er bedre hvis noen andre, som ikke spiller spillet, tar notater om kravene som er identifisert og diskuterte problemer. Dette kan brukes som oppfølging for en junior utvikler, eller utføres av prosjektleder. Noen organisasjoner har gjort videoopptak for gjennomgang i etterkant når kravene er skrevet opp mer formelt.

9. Bør vi alltid bruke hele kortstokken?

Nei. En mindre kortstokk er raskere å spille. Start ditt første spill med bare nok kort for to eller tre runder. Start ditt første spill med bare nok kort for to eller tre runder. For de første gangene folk spiller spillet er det også vanligvis bedre å fjerne essene og de to jokerne. Det er også vanlig å spille spillet uten trumfjär til folk er mer kjent med ideen.

10. Hva bør spillere gjøre når de har et ess-kort som sier "oppfunnet et nytt X angrep"?

Spilleren kan gjøre opp ethvert angrep de tror er gyldige, men må matche fargen på kortet (f.eks. Datavalidering & Tegnkoding). Med spillere som er nye i spillet, kan det være bedre å fjerne disse til å begynne med (se også FAQ 9).

11. Jeg forstår ikke hva angrepet betyr på hvert kort - finnes det mer detaljert informasjon?

Ja, online Wiki Deck ble opprettet for å hjelpe spillere med å forstå angrepene. See

https://www.owasp.org/index.php/Cornucopia - Ecommerce_Website_Edition - Wiki_Deck

12. Firmaet mitt ønsker å skrive ut sin egen versjon av OWASP® Cornucopia – hvilken lisens må vi referere til? Vennligst se det fullstendige svaret på dette spørsmålet på prosjektets nettsider:

https://www.owasp.org/index.php/OWASP_Cornucopia - tab=FAQs

	A	(Ikke et kort)		2		3
DATAVALIDERING & TEGNKODING			DATAVALIDERING & TEGNKODING		DATAVALIDERING & TEGNKODING	
	Du har funnet opp et nytt angrep mot Datavalidering og Tegnkoding			Brian kan samle informasjon om underliggende konfigurasjoner, skjemaer, logikk, kode, programvare, tjenester og infrastruktur på grunn av innholdet i feilmeldinger, eller dårlig konfigurasjon, eller tilstedevarelsen av standard installasjonsfiler eller gamle-, test-, sikkerhetskopier eller kopier av ressurser, eller eksponering av kildekode		Robert kan legge inn ondsinnede data fordi det tillatte protokollformatet ikke blir sjekket, duplikater akseptert, strukturen blir ikke verifisert, eller de individuelle dataelementene blir ikke validert iht. format, type, rekkevidde, lengde og en hvitliste over tillatte data, tegn eller formater
	<i>Les mer om dette emnet i OWASPs gratis jukseark om "Input Validation, XSS Prevention, DOM-basert XSS Prevention, SQL Injection Prevention og Query Parameterization"</i>			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}		OWASP SCP - OWASP ASVS 1.5.3, 5.1.1-4, 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}
	4		5	Jee kan omgå de sentraliserte datakodingsrutinene siden de ikke brukes overalt, eller feil datakoding blir brukt	6	7
DATAVALIDERING & TEGNKODING			DATAVALIDERING & TEGNKODING		DATAVALIDERING & TEGNKODING	
	Dave kan legge inn ondsinnede feltnavn eller data fordi de ikke blir sjekket innenfor konteksten til gjeldende bruker og prosess			Jason kan omgå de sentraliserte valideringsrutinene siden de ikke brukes på all input		Jan kan lage spesielle datalast for å hindre inndatavalidering fordi tegnsettet ikke er spesifisert/håndhevet, dataene er kodet flere ganger, dataene er ikke fullstendig konvertert til det samme formatet som applikasjonen bruker (f.eks. kanonisering) før de valideres, eller hvis variabler ikke benytter sterke typer
	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}			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}		OWASP SCP 4-5, 7, 150 OWASP ASVS 1.5.3, 13.2.2, 13.2.5 OWASP APPSENSOR IE2, IE3, EE1, EE2 CAPEC 28, 153, 165 SAFECODE 3, 16, 24 \$Common_Title_full}

DATAVALIDERING & TEGNKODING	8 DATAVALIDERING & TEGNKODING	9 DATAVALIDERING & TEGNKODING	10 DATAVALIDERING & TEGNKODING	J Toby has control over input validation, output validation or output encoding code or routines so they can be bypassed
	<p>Oana kan omgå de sentraliserte datarensingsrutinene siden de ikke brukes fullt ut</p> <p>OWASP SCP <u>15, 169</u></p> <p>OWASP ASVS <u>1.1.6, 5.2.2, 5.2.5</u></p> <p>OWASP APPSENSOR <u>-</u></p> <p>CAPEC <u>28, 31, 152, 160, 468</u></p> <p>SAFECODE <u>2, 17</u></p> <p>{Common_Title_full}</p>	<p>Shamun kan omgå innadatavaliderings- eller utdatavalideringskontroller fordi valideringsfeil ikke blir avvist og/eller renset</p> <p>OWASP SCP <u>6, 21-22, 168</u></p> <p>OWASP ASVS <u>7.1.3</u></p> <p>OWASP APPSENSOR <u>IE2, IE3</u></p> <p>CAPEC <u>28</u></p> <p>SAFECODE <u>3, 16, 24</u></p> <p>{Common_Title_full}</p>	<p>Dario kan utnytte tilliten applikasjonen har til en datakilde (f.eks. brukerdefinerte data, manipulering av lokalt lagrede data, endring av tilstandsdata på en klientenhet, mangl på verifisering av identitet under datavalidering slik at Dario kan utgi seg for å være Colin)</p> <p>OWASP SCP <u>2, 19, 92, 95, 180</u></p> <p>OWASP ASVS <u>1.12.2, 5.1.3, 9.2.3, 12.2.1, 12.3.1-3, 12.4.2, 12.5.2, 14.5.3</u></p> <p>OWASP APPSENSOR <u>IE4, IE5</u></p> <p>CAPEC <u>12, 51, 57, 90, 111, 145, 194-195, 202, 218, 463</u></p> <p>SAFECODE <u>14</u></p> <p>{Common_Title_full}</p>	<p>OWASP SCP <u>1, 17</u></p> <p>OWASP ASVS <u>1.5.3</u></p> <p>OWASP APPSENSOR <u>RE3, RE4</u></p> <p>CAPEC <u>87, 207, 554</u></p> <p>SAFECODE <u>2, 17</u></p> <p>{Common_Title_full}</p>
DATAVALIDERING & TEGNKODING	<p>Q DATAVALIDERING & TEGNKODING</p> <p>Xavier kan injisere data inn i en datatolk på klient- eller enhetssiden fordi et parameterisert grensesnitt ikke blir brukt, eller ikke har blitt implementert riktig, eller fordi dataene ikke er kodet riktig innenfor konteksten, eller det er ingen restriktive retningslinjer for kode eller datainkludering</p> <p>OWASP SCP <u>10, 15-16, 19-20</u></p> <p>OWASP ASVS <u>5.2.1, 5.2.5, 5.3.3, 5.5.4</u></p> <p>OWASP APPSENSOR <u>IE1, RP3</u></p> <p>CAPEC <u>28, 31, 152, 160, 468</u></p> <p>SAFECODE <u>2, 17</u></p> <p>{Common_Title_full}</p>	<p>K DATAVALIDERING & TEGNKODING</p> <p>Gabe kan injisere data inn i en tolk på serversiden (f.eks. SQL, OS-kommandoer, Xpath, Server JavaScript, SMTP) fordi et parameterisert grensesnitt med sterke typer ikke brukes eller ikke er implementert riktig</p> <p>OWASP SCP <u>15, 19-22, 167, 180, 204, 211, 212</u></p> <p>OWASP ASVS <u>5.2.1, 5.2.2, 5.3.4, 5.3.7-10</u></p> <p>OWASP APPSENSOR <u>CIE1, CIE2</u></p> <p>CAPEC <u>23, 28, 76, 152, 160, 261</u></p> <p>SAFECODE <u>2, 19-20</u></p> <p>{Common_Title_full}</p>	<p>(Ikke et kort)</p>	<p>(Ikke et kort)</p>

AUTENTISERING	A	AUTENTISERING	2	AUTENTISERING	3
	Du har funnet opp et nytt angrep mot Autentisering <i>Les mer om dette emnet i OWASP's gratis jukseark om "Authentication"</i>	(Ikke et kort)	James kan utføre autentiseringsfunksjoner uten at den virkelige brukeren noen gang er klar over at dette har skjedd (f.eks. forsøk på å logge på, logge på med stjålet legitimasjon, tilbakestille passordet)	Muhammad kan få tak i en brukers passord eller andre hemmeligheter som sikkerhetsspørsmål, ved observasjon under innreise, eller fra en lokal cache, eller fra minnet, eller under transport, eller ved å lese det fra et ubeskyttet sted, eller fordi det er allment kjent, eller fordi det aldri utløper, eller fordi brukeren ikke kan endre sitt eget passord	
AUTENTISERING	4	AUTENTISERING	5	AUTENTISERING	6
	Sebastien kan enkelt identifisere brukernavn eller samle dem inn	Javier kan bruke forhåndsvalgte-, testrelaterte- eller lett-gjettelige autentiseringsfaktorer for å autentisere, eller bruke en gammel konto eller en konto som ikke nødvendig er tiltenkt applikasjonen	Sven kan gjenbruke et midlertidig passord fordi brukeren ikke trenger å endre det ved første gangs bruk, eller det har for lang- eller ingen utløpstid, eller det ikke bruker en leveringsmetode utenfor det spesifikte telekommunikasjonsfrekvensbåndet (f.eks. post, mobilapp, SMS)	Cecilia kan bruke brute-force og ordbokangrep mot en eller flere kontoer uten å møte en øvre grense, eller fordi disse angrepene er forenklet på grunn av utilstrekkelig kompleksitet, lengde-, utløps- og gjenbrukskrav for passord	7
AUTENTISERING					
	OWASP SCP 33, 53 OWASP ASVS 2.2.1, 4.1.5 OWASP APPSENSOR AE1 CAPEC 383 SAFECODE 28 \$Common_Title_full}	OWASP SCP 54, 175, 178 OWASP ASVS 4.1.5 OWASP APPSENSOR AE12, HT3 CAPEC 70 SAFECODE 28 \$Common_Title_full}	OWASP SCP 37, 45-46, 178 OWASP ASVS 2.5.6 OWASP APPSENSOR - CAPEC 50 SAFECODE 28 \$Common_Title_full}	OWASP SCP 33, 38-39, 41, 50, 53 OWASP ASVS 2.1.2, 2.1.7, 2.1.10, 2.2.1 OWASP APPSENSOR AE2, AE3 CAPEC 2, 16 SAFECODE 27 \$Common_Title_full}	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}

AUTENTISERING	8	AUTENTISERING	9	AUTENTISERING	10	AUTENTISERING	J
	Kate kan omgå autentisering fordi den ikke feiler på en sikker måte (dvs. den tillater som standard uautentisert tilgang)		Claudia kan utføre mer kritiske funksjoner fordi autentiseringskravene er for svake (f.eks. mangler tofaktorautentisering), eller fordi krav om re-autentisering for disse ikke er tilstede		Pravin kan omgå autentiseringskontroll fordi en sentralisert standard-, testet-, utprøvd- og godkjent autentiseringsmodul/rammeverk/tjeneste, separat fra ressursen som forespørres, ikke benyttes		Mark kan få tilgang til ressurser eller tjenester fordi det ikke finnes noe autentiseringskrav, eller fordi det ble feilaktig antatt at autentisering skulle bli utført av et annet system eller utført av en tidligere handling
AUTENTISERING	OWASP SCP 28	AUTENTISERING	OWASP SCP 55-56	AUTENTISERING	OWASP SCP 25-27	AUTENTISERING	OWASP SCP 23, 32, 34
	OWASP ASVS 4.1.5		OWASP ASVS 1.4.5, 2.1.6, 2.2.4, 4.1.3, 4.3.3		OWASP ASVS 1.1.6, 1.4.4		OWASP ASVS 1.4.5, 4.3.1
AUTENTISERING	OWASP APPSENSOR ~	AUTENTISERING	OWASP APPSENSOR ~	AUTENTISERING	OWASP APPSENSOR ~	AUTENTISERING	OWASP APPSENSOR ~
	CAPEC 115		CAPEC 21		CAPEC 90, 115		CAPEC 115
AUTENTISERING	SAFECODE 28	AUTENTISERING	SAFECODE 14, 28	AUTENTISERING	SAFECODE 14, 28	AUTENTISERING	SAFECODE 14, 28
	Common_Title_full		Common_Title_full		Common_Title_full		Common_Title_full
AUTENTISERING	Q	AUTENTISERING	K				
	Johan kan omgå autentisering fordi den ikke håndheves med like styrke for alle typer autentiseringsrelatert funksjonalitet (f.eks. registrering, passordendring, passordgjenopprettning, utlogging, administrasjon) eller på tvers av alle versjoner/kanaler (f.eks. mobil nettsted, mobilapp, nettsted, API, hjelpesenter)		Olga kan påvirke eller endre autentiseringskode/rutiner slik at de kan omgås		(Ikke et kort)		(Ikke et kort)
AUTENTISERING	OWASP SCP 23, 29, 42, 49	AUTENTISERING	OWASP SCP 24				
	OWASP ASVS 1.4.5, 2.5.6, 2.5.7, 4.3.1		OWASP ASVS 4.1.1, 10.2.3, 10.2.4-6				
AUTENTISERING	OWASP APPSENSOR ~	AUTENTISERING	OWASP APPSENSOR ~				
	CAPEC 36, 50, 115, 121, 179		CAPEC 115, 207, 554				
AUTENTISERING	SAFECODE 14, 28	AUTENTISERING	SAFECODE 14, 28				
	Common_Title_full		Common_Title_full				

SESJONSHÅNDTERING	A			2	3
	Du har funnet opp et nytt angrep mot Sesjonshåndtering <i>Les mer om dette emnet i OWASP's gratis jukseark om "Session Management, and Cross Site Request Forgery (CSRF) Prevention"</i>	(Ikke et kort)		William har kontroll over genereringen av sesjonsidentifikatorer	Ryan kan bruke en enkelt konto parallelt siden parallelle økter er tillatt
SESJONSHÅNDTERING	4		5	6	7
	Alison kan tilordne sesjonsidentifikasjons-cookies en annen nettapplikasjon fordi domenet og tilleggsstien ikke tilstrekkelig er begrenset OWASP SCP 59, 61 OWASP ASVS 3.4.1-5 OWASP APPSENSOR SE2 CAPEC 31, 61 SAFECODE 28 \$Common_Title_full}	John kan forutsi eller gjette sesjonsidentifikatorer fordi de ikke endres når brukerens rolle endres (f.eks. før og etter autentisering) og når det byttes mellom ikke-kryptert- og kryptert kommunikasjon, eller fordi de ikke er tilstrekkelig lange og tilfeldige, eller fordi de ikke endres med jevne mellomrom 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}	SESJONSHÅNDTERING	SESJONSHÅNDTERING	Graham kan benytte Adams økt etter at han er ferdig, fordi det ikke er noen utloggingsfunksjon, fordi han ikke enkelt kan logge ut, eller fordi utlogging ikke avslutter økten på riktig måte OWASP SCP 62-63 OWASP ASVS 3.3.1, 3.3.4 OWASP APPSENSOR - CAPEC 21 SAFECODE 28 \$Common_Title_full}

SESJONSHÅNDTERING	8	SESJONSHÅNDTERING	9	SESJONSHÅNDTERING	10	SESJONSHÅNDTERING	J
	Matt kan misbruke lange økter fordi applikasjonen ikke krever periodisk re-autentisering for å sjekke om privilegiene har endret seg		Ivan kan stjele sesjonsidentifikatorer fordi de sendes over usikre kanaler, blir avslørt i logger/feilmeldinger/URL-er, eller er unodvendig tilgjengelig i kode som angriperen kan påvirke eller endre		Marce kan forfalske forespørsler fordi hoyt, tilfeldige token (dvs. anti-CSRF-tokens, eller lignende) som skal benyttes per-sesjon, eller per-forespørsel for kritiske handlinger, ikke benyttes for handlinger som endrer tilstand		Jeff kan sende en identisk gjentatt interaksjon på nytt (f.eks. HTTP-forespørsel, signal, knappetrykk) som blir akseptert, ikke avvist
SESJONSHÅNDTERING	OWASP SCP 96	SESJONSHÅNDTERING	OWASP SCP 69, 75-76, 119, 138	SESJONSHÅNDTERING	OWASP SCP 73-74	SESJONSHÅNDTERING	OWASP SCP -
	OWASP ASVS 3.3.2, 3.6.1		OWASP ASVS 1.9.1, 3.1.1, 7.1.1, 7.1.2, 7.2.1, 9.1.3, 9.2.2		OWASP ASVS 4.2.2		OWASP ASVS 11.1.1, 11.1.2, 11.1.3
SESJONSHÅNDTERING	OWASP APPSENSOR -	SESJONSHÅNDTERING	OWASP APPSENSOR SE4-6	SESJONSHÅNDTERING	OWASP APPSENSOR IE4	SESJONSHÅNDTERING	OWASP APPSENSOR IE5
	CAPEC 21		CAPEC 31, 60		CAPEC 62, 111		CAPEC 60
SESJONSHÅNDTERING	SAFECODE 28	SESJONSHÅNDTERING	SAFECODE 28	SESJONSHÅNDTERING	SAFECODE 18	SESJONSHÅNDTERING	SAFECODE 12, 14
	Common_Title_full}		Common_Title_full}		Common_Title_full}		OWASP Cornucopia Ecommerce Website Edition v1.20-EN
SESJONSHÅNDTERING	Q	SESJONSHÅNDTERING	K				
	Salim kan omgå øktadministrasjon fordi den ikke benyttes omfattende og konsekvent i hele applikasjonen		Peter kan omgå sesjonshåndteringskontrollene fordi de er selvbygde og/eller svake, i stedet for å bruke et standard rammeverk eller en godkjent testet modul		(Ikke et kort)		(Ikke et kort)
SESJONSHÅNDTERING	OWASP SCP 58	SESJONSHÅNDTERING	OWASP SCP 58, 60				
	OWASP ASVS 1.1.6, 3.7.1		OWASP ASVS 1.1.6				
SESJONSHÅNDTERING	OWASP APPSENSOR -	SESJONSHÅNDTERING	OWASP APPSENSOR -				
	CAPEC 21		CAPEC 21				
SESJONSHÅNDTERING	SAFECODE 14, 28	SESJONSHÅNDTERING	SAFECODE 14, 28				
	Common_Title_full}		Common_Title_full}				

AUTORISASJON	A	AUTORISASJON		AUTORISASJON	2	AUTORISASJON	3
Du har funnet opp et nytt angrep mot Autorisasjon		(Ikke et kort)		Tim kan påvirke hvor data sendes eller videresendes til		Christian kan få tilgang til informasjon, som han ikke skal ha tillatelse til, gjennom en annen mekanisme som har tillatelse (f.eks. søkeindeks, logger, rapporter), eller fordi den er bufret, eller lagret lenger enn nødvendig, eller gjennom en annen informasjonslekkasje	
<i>Les mer om dette emnet i “OWASP's Development and Testing Guides”</i>				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}		OWASP SCP 51, 100, 135, 139-141, 150 OWASP ASVS 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}	
Kelly kan omgå autorisasjonskontroller fordi de ikke feiler sikkert (dvs. at de som standard gir tilgang)	4	AUTORISASJON	5	Chad kan få tilgang til ressurser (inkludert tjenester, prosesser, AJAX, Flash, video, bilder, dokumenter, midlertidige filer, sesjonsdata, systemegenskaper, konfigurasjonsdata, registerinnstillinger, logger) han ikke skal kunne få grunn av manglende autorisasjon, eller pga. overdrevne privilegier (f.eks. ufullstendig bruk av prinsippet om minste privilegium)	6	Eduardo kan få tilgang til data han ikke har tillatelse til, selv om han har tillatelse til skjemaut/etterspørrelse/URL/tilgangspunkt	7
OWASP SCP 79-80 OWASP ASVS 4.1.5 OWASP APPSENSOR - CAPEC 122 SAFECODE 8, 10-11 \$Common_Title_full}				OWASP SCP 70, 81, 83, 84, 87-9, 99, 117, 131, 132, 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}		OWASP SCP 81, 88, 151 OWASP ASVS 4.1.3, 4.2.1 OWASP APPSENSOR ACE1-4 CAPEC 122 SAFECODE 8, 10-11 \$Common_Title_full}	

AUTORISASJON	8	AUTORISASJON	9	AUTORISASJON	10	AUTORISASJON	J
	<p>Tom kan omgå forretningsregler ved å endre den vanlige prosessekvensen eller -flyten, eller ved å gjennomføre prosessen i feil rekkefølge, eller ved å manipulere dato- og klokkeslettverdier som benyttes av applikasjonen, eller ved å bruke gyldige funksjoner til utilsiktede formål, eller, på annen måte, manipulere kontrolldata</p> <p>OWASP SCP 10, 32, 93-94, 189</p> <p>OWASP ASVS 4.1.2, 4.2.1, 4.3.3, 7.3.4, 11.1.1, 11.1.2</p> <p>OWASP APPSENSOR ACE3</p> <p>CAPEC 25, 39, 74, 162, 166, 207</p> <p>SAFECODE 8, 10-12</p> <p>Common_Title_full</p>	<p>Mike kan misbruke en applikasjon ved å bruke en gyldig funksjon for raskt, eller for ofte, eller på en måte som ikke er tiltenkt, eller som forbruker applikasjonens ressurser, forårsaker en kappløpssituasjon, eller overutnyttelse av en funksjon</p> <p>OWASP SCP 94</p> <p>OWASP ASVS 11.1.3, 11.1.4</p> <p>OWASP APPSENSOR AE3, FIO1-2, UT2-4, STE1-3</p> <p>CAPEC 26, 29, 119, 261</p> <p>SAFECODE 1, 35</p> <p>Common_Title_full</p>	<p>Richard kan omgå de sentraliserte autorisasjonskontrollene siden de ikke blir benyttet fullstendig på alle interaksjoner</p> <p>OWASP SCP 78, 91</p> <p>OWASP ASVS 1.1.6, 4.1.1</p> <p>OWASP APPSENSOR ACE1-4</p> <p>CAPEC 36, 95, 121, 179</p> <p>SAFECODE 8, 10-11</p> <p>Common_Title_full</p>	<p>Dinis kan få tilgang til sikkerhetskonfigurasjonsinformasjon eller tilgangskontrolllister</p> <p>OWASP SCP 89-90</p> <p>OWASP ASVS 4.1.2, 10.2.3-6</p> <p>OWASP APPSENSOR -</p> <p>CAPEC 75, 133, 203</p> <p>SAFECODE 8, 10-11</p> <p>Common_Title_full</p>			
AUTORISASJON	Q	AUTORISASJON	K				
	<p>Christopher kan injisere en kommando som applikasjonen vil kjøre på et høyere rettighetsnivå</p> <p>OWASP SCP 209</p> <p>OWASP ASVS 5.3.8</p> <p>OWASP APPSENSOR -</p> <p>CAPEC 17, 30, 69, 234</p> <p>SAFECODE 8, 10-11</p> <p>Common_Title_full</p>	<p>Ryan kan påvirke eller endre autorisasjonskontroller og tillatelser, og kan derfor omgå dem</p> <p>OWASP SCP 77, 89, 91</p> <p>OWASP ASVS 4.1.1, 4.1.2, 10.2.3-6</p> <p>OWASP APPSENSOR -</p> <p>CAPEC 207, 554</p> <p>SAFECODE 8, 10-11</p> <p>Common_Title_full</p>	<p>(Ikke et kort)</p>				<p>(Ikke et kort)</p>

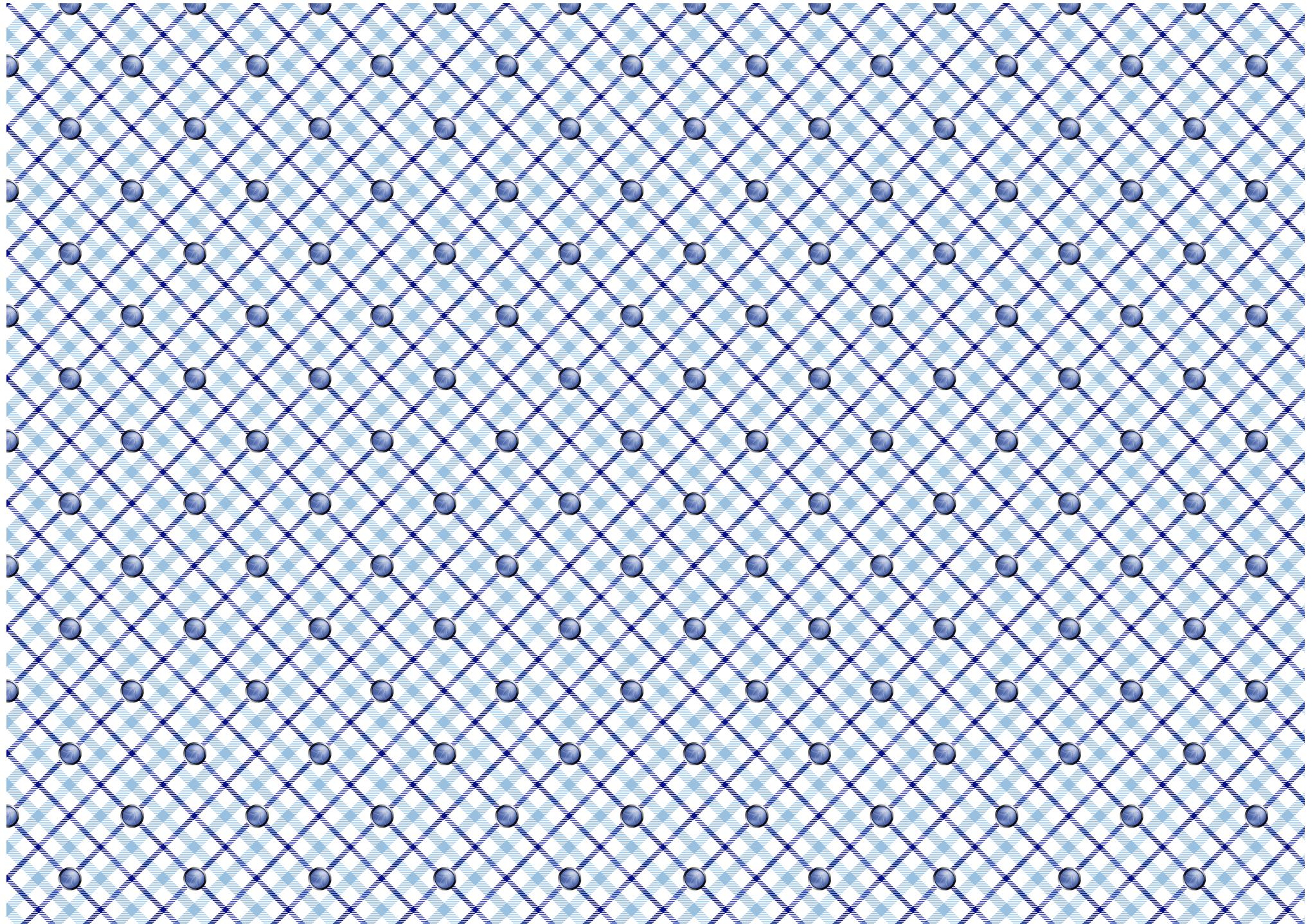
KRYPTOGRAFI	A	KRYPTOGRAFI	5	KRYPTOGRAFI	2	KRYPTOGRAFI	3
	Du har funnet opp et nytt angrep mot Kryptografi <i>Les mer om dette emnet i OWASP's gratis jukseark om "Cryptographic Storage, and Transport Layer Protection"</i>	(Ikke et kort)		Kyun kan få tilgang til data fordi de har blitt tilslørt i steden for kryptert/hashet med en godkjent kryptografisk funksjon		Axel kan endre midlertidige eller permanente data (lagret eller under transport), kildekode, oppdateringer/patcher eller konfigurasjonsdata, fordi de ikke er gjenstand for integritetskontroll	
KRYPTOGRAFI	4	KRYPTOGRAFI	5	KRYPTOGRAFI	6	KRYPTOGRAFI	7
	Paulo kan få tilgang til data under overføring som ikke er kryptert, selv om kommunikasjonskanalen er kryptert	Kyle kan omgå kryptografiske kontroller fordi de ikke svikter sikkert (dvs. at de som standard er ubeskyttet)		Romain kan lese og endre ukrypterte data i minnet eller under overføring (f.eks. kryptografiske hemmeligheter, autentiseringsdata, sesjonsidentifikatorer, personlige og kommersielt sensitive data), i bruk eller under kommunikasjon innenfor applikasjonen, mellom applikasjonen og brukerne, eller mellom applikasjonen og eksterne systemer		Gunter kan avskjære eller endre krypterte data under overføring fordi protokollen er dårlig distribuert, svakt konfigurerert, sertifikater ugyldige, sertifikater uklarert, eller fordi tilkobling kan bli degradert til en svakere eller ukryptert kommunikasjonskanal	
KRYPTOGRAFI	OWASP SCP 37, 88, 143, 214 OWASP ASVS 8.3.4, 9.1.1 OWASP APPSENSOR - CAPEC 185-187 SAFECODE 14, 29-30 \$Common_Title_full}	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}		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}		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}	

KRYPTOGRAFI	8	KRYPTOGRAFI	9	KRYPTOGRAFI	10	KRYPTOGRAFI	J
	Eoin kan få tilgang til lagrede forretningsdata (f.eks. passord, sesjonsidentifikatorer, PII, kortholderdata) fordi de ikke er sikkert kryptert eller sikkert hashet		Andy kan omgå generering av tilfeldige tall, generering av tilfeldig GUID, hashing og krypteringsfunksjoner fordi de er selvbygde og/eller svake		Susanna kan bryte kryptografien i bruk fordi den ikke er sterk nok for den nødvendige beskyttelsesgraden, eller den er ikke sterk nok i forhold til innsatsen angriperen er villig til å legge inn		Justin kan lese autensieringsdata for å få tilgang til interne eller eksterne ressurser, tjenester og andre systemer fordi de er lagret i et ukryptert format, eller lagret i kildekoden
KRYPTOGRAFI	OWASP SCP 30-31, 70, 133, 135	KRYPTOGRAFI	OWASP SCP 60, 104-105	KRYPTOGRAFI	OWASP SCP 104-105	KRYPTOGRAFI	OWASP SCP 35, 90, 171-172
	OWASP ASVS 2.4.1, 6.2.2, 6.2.3, 8.3.4		OWASP ASVS 6.2.2, 6.2.3, 6.3.1, 6.3.3		OWASP ASVS 6.3.3		OWASP ASVS 1.6.1, 1.6.2, 1.6.4, 2.10.4, 6.4.1, 6.4.2
KRYPTOGRAFI	OWASP APPSENSOR -	KRYPTOGRAFI	OWASP APPSENSOR -	KRYPTOGRAFI	OWASP APPSENSOR -	KRYPTOGRAFI	OWASP APPSENSOR -
	CAPEC 31, 37, 55		CAPEC 97		CAPEC 97, 463		CAPEC 116
KRYPTOGRAFI	SAFECODE 21, 29, 31	KRYPTOGRAFI	SAFECODE 14, 21, 29, 32-33		SAFECODE 14, 21, 29, 31-33		SAFECODE 21, 29
	\$(Common_Title_full}		\$(Common_Title_full}		\$(Common_Title_full}		\$(Common_Title_full}
KRYPTOGRAFI	Q	KRYPTOGRAFI	K		(Ikke et kort)		(Ikke et kort)
	Dartim kan få tilgang til eller forutsi kryptografiske hovednokler		Dan kan påvirke eller endre kryptokode/rutiner (kryptering, hashing, digitale signaturer, tilfeldig tall og GUID-generering) og kan derfor omgå dem				
KRYPTOGRAFI	OWASP SCP 35, 102	KRYPTOGRAFI	OWASP SCP 31, 101				
	OWASP ASVS 1.6.1-3, 6.2.3, 8.3.6		OWASP ASVS 1.6.2, 6.2.5-8				
KRYPTOGRAFI	OWASP APPSENSOR -	KRYPTOGRAFI	OWASP APPSENSOR -				
	CAPEC 116-117		CAPEC 207, 554				
KRYPTOGRAFI	SAFECODE 21, 29	KRYPTOGRAFI	SAFECODE 14, 21, 29				
	\$(Common_Title_full}		\$(Common_Title_full}				

CORNUCOPIA	A	CORNUCOPIA		2	CORNUCOPIA	3
	Du har funnet opp et nytt angrep av hvilken som helst type	(Ikke et kort)		Lee kan omgå applikasjonskontroller fordi farlige/risikofylte programmeringsfunksjoner har blitt brukt istf. sikrere alternativer, fordi typekonverteringsfeil finnes, applikasjonen er upålitelig når ekstern ressurs er utilgjengelig, eller pga. kapplopssituasjons-, ressursinitialisering-, ,allokerings- eller overflytproblemer		Andrew kan få tilgang til kildekode, dekompilere, eller på annen måte få tilgang til forretningslogikk for å forstå hvordan applikasjonen fungerer og avdekke eventuelle hemmeligheter den inneholder
CORNUCOPIA	<i>Les mer om applikasjonssikkerhet i OWASPs gratis guider som omhandler krav, utvikling, kodegjennomgang og testing, the "Cheat Sheet series", og OWASPs "Software Assurance Maturity Model"</i>			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}	OWASP SCP 134 OWASP ASVS 14.1.1 OWASP APPSENSOR ~ CAPEC 189, 207 SAFECODE ~ \$Common_Title_full}	
	4	CORNUCOPIA	5	CORNUCOPIA	6	CORNUCOPIA
CORNUCOPIA	Keith kan utføre en handling og det er ikke mulig å tilskrive ham den		Larry kan påvirke tilliten andre parter, inkludert brukere, har til applikasjonen, eller misbruke denne tilliten andre steder (f.eks. i en annen applikasjon)	Aaron kan omgå kontroller fordi feil/unntakshåndtering mangler, eller er implementert inkonsekvent eller delvis, eller nekter ikke tilgang som standard (dvs. feil bør avslutte tilgang/utførelse), eller er avhengig av håndtering fra en annen tjeneste eller system		Mwengus handlinger kan ikke undersøkes fordi det ikke finnes tilstrekkelig nøyaktige tidsstempelregistrering av sikkerhetshendelsene, eller fordi det ikke finnes et fullstendig revisjonsspor, eller fordi disse kan endres eller slettes av Mwengu, eller fordi det ikke finnes enentralisert loggingstjeneste
	OWASP SCP 23, 32, 34, 42, 51, 181 OWASP ASVS 7.2.1, 7.2.2 OWASP APPSENSOR ~ CAPEC ~ SAFECODE ~ \$Common_Title_full}		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}	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}	OWASP SCP 113, 114, 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	CORNUCOPIA	9	CORNUCOPIA	10	CORNUCOPIA	J
	<p>David kan omgå applikasjonen for å få tilgang til data fordi nettverket og vertsinfrastrukturen, og støttetjenester/applikasjoner, ikke er sikkert konfigurert, konfigurasjonen sjekket på nytt med jevne mellomrom og sikkerhetsoppdateringer utført, eller fordi dataene er lagret lokalt, eller fordi dataene ikke er fysisk beskyttet</p> <p>OWASP SCP 151, 152, 156, 160, 161, 173-177</p> <p>OWASP ASVS 1.4.5, 10.3.1, 10.3.2, 14.1.4, 14.1.5, 14.2.1, 14.2.2</p> <p>OWASP APPSENSOR REF1, RE2</p> <p>CAPEC 37, 220, 310, 436, 536</p> <p>SAFECODE -</p> <p>{Common_Title_full}</p>		<p>Michael kan omgå applikasjonen for å få tilgang til data fordi administrative verktøy eller administrative grensesnitt ikke er tilstrekkelig sikret</p> <p>OWASP SCP 23, 29, 56, 81, 82, 84-90</p> <p>OWASP ASVS 1.4.5, 4.3.1</p> <p>OWASP APPSENSOR -</p> <p>CAPEC 122, 233</p> <p>SAFECODE -</p> <p>{Common_Title_full}</p>		<p>Spyros kan omgå applikasjonens kontroller fordi koderammeverk, biblioteker og komponenter inneholder ondsinnet kode eller sårbarheter i (f.eks. internt utviklede-, kommersielt ikke-standardiserte- eller tjenesteutsette systemer, eller i systemer som benytter åpen kildekode eller er eksternt plassert)</p> <p>OWASP SCP 57, 151-152, 204-205, 213-214</p> <p>OWASP ASVS 1.14.3, 10.1.1, 10.2.3-6, 14.2.1</p> <p>OWASP APPSENSOR -</p> <p>CAPEC 68, 438-439, 442, 524, 538</p> <p>SAFECODE 15</p> <p>{Common_Title_full}</p>		<p>Roman kan utnytte applikasjonen fordi den ble kompilert ved hjelp av utdaterte verktøy, eller fordi konfigurasjonen ikke er sikker som standard, eller fordi sikkerhetsinformasjon ikke ble dokumentert og gitt videre til operative team</p> <p>OWASP SCP 90, 137, 148, 151-154, 175-179, 186, 192</p> <p>OWASP ASVS 1.14.3, 14.1.1-5, 14.2.1</p> <p>OWASP APPSENSOR -</p> <p>CAPEC -</p> <p>SAFECODE 4</p> <p>{Common_Title_full}</p>
CORNUCOPIA	Q	CORNUCOPIA	K	JOKER	Joker	JOKER	Joker
	<p>Jim kan utføre ondsinnde-, ikke-normale handlinger uten sanntidsdeteksjon og respons fra applikasjonen</p> <p>OWASP SCP -</p> <p>OWASP ASVS 8.1.4, 11.1.4</p> <p>OWASP APPSENSOR (All)</p> <p>CAPEC -</p> <p>SAFECODE 1, 27</p> <p>{Common_Title_full}</p>		<p>Grant kan bruke applikasjonen til å nekte noen eller alle brukerne tjenesten</p> <p>OWASP SCP 41, 55</p> <p>OWASP ASVS 2.2.1, 11.1.3, 11.1.4</p> <p>OWASP APPSENSOR UT1-4, STE3</p> <p>CAPEC 2, 25, 119, 125</p> <p>SAFECODE 1</p> <p>{Common_Title_full}</p>		<p>Alice kan bruke applikasjonen til å angripe brukernes systemer og data</p> <p><i>Har du tenkt på å bli et individuelt OWASP-medlem? Alle verktøy, veiledering og lokale møter er gratis for alle, men individuelt medlemskap er med på å støtte OWASPs arbeid</i></p>		<p>Bob kan øve innflytelse over, endre eller påvirke applikasjonen slik at den ikke lenger overholder juridiske, regulatoriske, kontraktsmessige eller andre organisatoriske mандater</p> <p><i>Undersøk sårbarheter og oppdag hvordan de kan fikses ved å bruke OWASPs Juice Shop, Security Shepherd, eller ved å bruke netttutfordringene i OWASPs hacking-lab gratis</i></p>

Cut
here



Endrings logg

Version / Dato	Kommentarer
0.1	30 Jul 2012 Original Draft
0.2	10 Aug 2012 Draft reviewed and updated
0.3	15 Aug 2012 Draft announced OWASP SCP mailing list for comment.
0.4	25 Feb 2013 Play rules updated based on feedback during workshops. Added reference to PCI SSC Information Supplement: PCI DSS E-commerce Guidelines. Descriptive text extended and updated. Added contributors section, page numbering, FAQs and change log.
1	25 Feb 2013 Release.
1.01	03 Jun 2013 Framework-specific card deck discussion added Additional FAQs created. Descriptive text updated. New cover image, and previous cover image moved to back. Cut lines added. FAQs 5 and 6 added. Attack descriptions on cards with tinted backgrounds changed to black (from dark grey). Project contributors added.
1.02	14 Aug 2013 Warning about time to print added. Additional alternative game rules added (twenty-one, play a deck over a week, play full hand and then discuss). Compliance deck concept added. FAQs 5 and 6 added. Attack descriptions on cards with tinted backgrounds changed to black (from dark grey). Project contributors added.
1.03	18 Sep 2013 Minor attack wording changes on two cards. OWASP SCP and ASVS cross-references checked and updated. Code letters added for suits. All remaining attack descriptions on cards changed to black (from dark grey) and background colours amended to provide more contrast and increase readability.
1.04	01 Feb 2014 Text “password change, password change,” corrected to “password change, password recovery,” on Queen of Authentication card.
1.05	21 Mar 2014 Updates to alternative game rules. Additional FAQs created. Contributors updated. Podcast and video links added.
1.1	04 Mar 2015 Change log date corrected for v1.05. Cross-references updated for 2014 version of ASVS. Contributors updated. Minor text changes to cards to improve readability.
1.2	29 Jun 2016 Video mentioned/linked Separate score sheet mentioned/linked. Previous embedded score sheet pages deleted Correction (identified by Tom Brennan) and addition to text on card 8 Authentication. Oana Cornea and other participants at the AppSec EU 2015 project summit added to list of contributors. Dario De Filippis added as project co-leader. Wiki Deck link added Cross-references updated for ASVS v3.0.1 and CAPEC v2.8. Minor text changes to a small number of cards. Added “-EN” to version number in preparation for “-ES” version. Susana Romaniz added as a contributor to the Spanish translation. Minor text changes to instructions and FAQs.
1.3	01 Jan 2023 - Cross-references updated from ASVS v3.0.1 to ASVS v4.0 by Johan Sydseter. - Norwegian language version added.

Prosjektbidragsytere

Alle OWASP-prosjekter er avhengige av frivillig innsats fra personer i programvareutviklings- og informasjonssikkerhetsektorene.

De har bidratt med tid og energi til å komme med forslag, gi tilbakemeldinger, skrive, gjennomgå og redigere dokumentasjon, gi oppmuntringer, prøve spillet og promotere konseptet.

Uten all deres innsats ville ikke prosjektet ha kommet så langt.

Ta kontakt med e-postlisten eller prosjektleddere direkte, hvis noen mangler på listene nedenfor.

- Simon Bennetts
- Sebastien Gioria
- Mark Miller
- Tom Brennan
- Tobias Gondrom
- Cam Morris
- Fabio Cerullo
- Timo Goosen
- Susana Romaniz
- Oana Cornea
- Anthony Harrison
- Ravishankar Sahadevan
- Johanna Curiel
- John Herrlin
- Tao Sauvage
- Todd Dahl
- Jerry Hoff
- Stephen de Vries
- Luis Enriquez
- Marios Kourtesis
- Colin Watson
- Ken Ferris
- Antonis Manaras
- Johan Sydseter
- Darío De Filippis
- Jim Manico

- OWASPs hardtarbeidende ansatte.
- Deltakere på OWASP London, OWASP Manchester, OWASP Netherlands og OWASP Scotland chapter meetings, og London Gamification Meetup, som kom med nyttige forslag og stilte utfordrende spørsmål
- Blackfoot UK Limited for å gi utskriftsklare designfiler og hundrevis av profesjonelt trykte kortstokker for distribusjon via post og på OWASP-chapter meetings
- OWASP NYC for å lage en OWASP-boksdesign og distribuere pakker på AppSec USA 2014.

Podcasts and videoer

Følgende støttende OWASP® Cornucopia ressurser er tilgjengelige online:

- Video – Bruk av kortene, opprettet under AppSec EU 2015 project summit, 20. mai 2015 <https://www.youtube.com/watch?v=i5Y0akWj31k>
- Podcastintervju, OWASP 24/7 Podcast-kanal, 21. mars 2014 <http://trustedsoftwarealliance.com/2014/03/21/the-owasp-cornucopia-project-with-colin-watson/>
- Video av presentasjonen, OWASP EU Tour 2013 London, 3. juni 2013 <https://www.youtube.com/watch?v=Q LE-8xNXVk>

Se prosjektets hjemmeside for mer informasjon og presentasjonsmateriell.

