OWASP
The Open Web Application Security Project

Cornucopia

Ecommerce Website Edition v1.30-ES

OWASP Cornucopia es un mecanismo para asistir a los equipos de desarrollo de software en la identificación de requerimientos de seguridad en procesos de desarrollo de software ágiles, convencionales y formales.

Author
Colin Watson

Project Leaders
Colin Watson and Grant Ongers

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

Reconocimientos del proyecto

Microsoft SDL Team para el juego de modelado de amenazas Elevation of Privilege, publicado bajo una licencia Creative Commons Attribution, como inspiración para Cornucopia y del que se copiaron muchas ideas, especialmente la teoría de juego.

Keith Turpin y colaboradores de las “Prácticas de codificación segura de OWASP - Guía de referencia rápida”, originalmente donada a OWASP por Boeing, que se utiliza como fuente principal de información sobre requisitos de seguridad para formular el contenido de las tarjetas.

Colaboradores, patrocinadores y voluntarios de los proyectos OWASP ASVS, AppSensor y Web Framework Security Matrix, la enumeración y clasificación de patrones de ataque común de Mitre (CAPEC) y las "historias prácticas de seguridad y tareas de seguridad para entornos de desarrollo ágiles" de SAFECode, que se utilizan en las referencias cruzadas proporcionadas.

Playgen for providing an illuminating afternoon seminar on task gamification, and tartanmaker.com for the online tool to help create the card back pattern.

Blackfoot UK Limited for creating and donating print-ready design files, Tom Brennan and the OWASP Foundation for instigating the creation of an OWASP-branded box and leaflet, and OWASP employees, especially Kate Hartmann, for managing the ordering, stocking and despatch of printed card decks. Oana Cornea and other participants at the AppSec EU 2015 project summit for their help in creating the demonstration video. Colin Watson as author and co-project leader with Grant Ongers, along with other OWASP volunteers who have helped in many ways.

Introducción

La idea detrás de Cornucopia es ayudar a los equipos de desarrollo, especialmente aquellos que usan metodologías ágiles, a identificar los requisitos de seguridad de las aplicaciones y desarrollar historias de usuarios basadas en la seguridad. Aunque la idea había estado esperando mucho tiempo para progresar, la motivación final llegó cuando SAFECode publicó sus Historias Prácticas de Seguridad y Tareas de seguridad para entornos de desarrollo ágil en julio de 2012.

El equipo SDL de Microsoft ya había publicado su súper Elevación de Privilegios: el juego de Modelado de Amenazas (EoP), pero eso no parecía abordar el tipo de problemas más apropiado que los equipos de desarrollo de aplicaciones web, en su mayoría, tienen que enfrentar. EoP es un gran concepto y estrategia de juego, y fue publicado bajo una Licencia de Creative Commons Attribution.

Cornucopia Ecommerce Website Edition se basa en los conceptos e ideas de juegos de EoP, pero se han modificado para que sean más relevantes para los tipos de problemas que enfrentan los desarrolladores de sitios web de comercio electrónico. Intenta introducir ideas de modelado de amenazas en los equipos de desarrollo que utilizan metodologías ágiles, o están más enfocados en las debilidades de las aplicaciones web que otros tipos de vulnerabilidades de software o no están familiarizados con STRIDE y DREAD.

Cornucopia Ecommerce Website Edition es referenciada como un recurso de información en el PCI Security Standard Council's Supplement Information PCI DSS E-commerce Guidelines, v2, enero de 2013.

El mazo de cartas (paquete)

A diferencia del juego EoP de STRIDE (juegos de tarjetas con diseños asociados), las cartas de Cornucopia se basan en la estructura de las Prácticas de codificación segura de OWASP - Guía de referencia rápida (SCP), pero con una consideración adicional de las secciones en el Estándar de verificación de seguridad de aplicaciones de OWASP (ASVS), la Guía de pruebas de OWASP y Principios de desarrollo seguro de David Rook. Estos proporcionaron cinco dominios, y un sexto llamado "Cornucopia" fue creado para todo lo demás:

- Validación de Data
- Autenticación
- Gestión de Sesiones
- Autorización
- Criptografía
- Cornucopia

Similar a las cartas de póker, cada palo contiene 13 cartas (As, 2 10, Jack, Queen y King) pero, a diferencia de EoP, también hay dos cartas Joker. El contenido se extrajo principalmente del SCP.

Mapeos

La motivación para Cornucopia es vincular los ataques con los requisitos y las técnicas de verificación. Un objetivo inicial había sido hacer referencia a los ID de debilidad de CWE, pero estos resultaron ser demasiados, y en su lugar se decidió asignar cada tarjeta a los ID de patrón de ataque de software CAPEC, que a su vez se relacionan a CWE, por lo que se logra el resultado deseado. Cada tarjeta también se asocia a las 36 historias de seguridad principales en el documento SAFECode, así como a OWASP SCP v2, ASVS v4.0 y AppSensor (detección y respuesta de ataques de aplicaciones) para ayudar a los equipos a crear sus propias historias relacionadas con la seguridad para su uso en procesos ágiles.

Estrategia de Juego

Además de las diferencias de contenido, las reglas del juego son prácticamente idénticas a las de EoP.

imprimiendo las tarjetas

Consulte la página del proyecto Cornucopia para saber cómo obtener barajas preimpresas en cartulina brillante.

Las tarjetas se pueden imprimir a partir de este documento en blanco y negro, pero son más efectivas en color. Las tarjetas de las páginas posteriores de este documento se han diseñado para que quepan en un tipo de hojas de tarjetas de visita A4 precortadas. Esta parecía ser la forma más rápida de empezar a crear cartas rápidamente. Los códigos de producto Avery C32015 y C32030 se han probado con éxito, pero cualquier tarjeta de 10 hasta 85 mm x 54 mm en papel A4 debería funcionar con un pequeño ajuste. Otros proveedores de artículos de papelería como Ryman y Sigel producen hojas similares. Estas hojas de tarjetas no son económicas, por lo que se debe tener cuidado al decidir qué imprimir y utilizar qué soporte y tipo de impresora.

Por supuesto, las tarjetas pueden imprimirse en cualquier tamaño de papel o tarjeta y luego cortarse manualmente, o una imprenta comercial podría imprimir volúmenes más grandes y cortar las tarjetas al tamaño adecuado. Las líneas de corte se muestran en la penúltima página de este documento, pero Avery también produce una plantilla A4 apaisada (A-0017-01_L.doc) que puede usarse como guía.

Imprimir y cortar puede llevar aproximadamente una hora, y es útil utilizar una impresora más rápida. Intente imprimir con mayor calidad para aumentar la legibilidad. Se proporciona un diseño de reverso de tarjeta opcional (en tartan OWASP) en la última página de este documento. No se necesita ninguna alineación especial. La impresión a doble cara necesita un cuidado especial. Puede personalizar las caras o el reverso de la tarjeta según las preferencias de su propia organización.

Personalización

Después de haber utilizado Cornucopia varias veces, es posible que sienta que algunas tarjetas son menos relevantes para sus aplicaciones o que las amenazas son diferentes para su organización. Edite este documento usted mismo para hacer que las cartas sean más adecuadas para sus equipos o cree mazos completamente nuevos.

Brindar retroalimentación

Si tiene ideas o comentarios sobre el uso de OWASP Cornucopia, compártalos. Aún mejor si crea versiones alternativas de las tarjetas, o produce versiones profesionales listas para imprimir, comparta eso con los voluntarios que crearon esta edición y con la comunidad más amplia de desarrollo y seguridad de aplicaciones.

El mejor lugar para usar para discutir o contribuir es la lista de correo para el proyecto OWASP:

- Blackfoot UK Limited for gifting print-ready design files and hundreds of professionally printed card decks for distribution by post and at OWASP chapter meetings
  https://lists.owasp.org/mailman/listinfo/owasp_cornucopia
- OWASP's hard-working employees, especially Kate Hartmann
  https://www.owasp.org/index.php/OWASP_Cornucopia

Instrucciones

El texto en cada carta describe un ataque, pero el atacante recibe un nombre, que es único en todas las cartas. El nombre puede representar un sistema informático (por ejemplo, la base de datos, el sistema de archivos, otra aplicación, un servicio relacionado, una botnet), una persona individual (por ejemplo, un ciudadano, un cliente, un usuario, un empleado, un criminal, un espía), o incluso un grupo de personas (por ejemplo, una organización competitiva, activistas con una causa común). El atacante puede ser remoto en algún otro dispositivo / ubicación, o local / interno con acceso al mismo dispositivo, host o red en el que se ejecuta la aplicación. El atacante siempre se nombra al comienzo de cada descripción. Trate siempre de tener una combinación de roles que puedan aportar perspectivas alternativas.

Wiki Deck link added

Esto significa que el atacante (William) puede crear nuevos identificadores de sesión que la aplicación acepta. Los ataques se basaron principalmente en los requisitos de seguridad enumerados en SCP, v2, pero luego se complementaron con los objetivos de verificación del "Estándar de verificación de seguridad de aplicaciones para aplicaciones web" de OWASP, las historias centradas en la seguridad en "Historias Prácticas de seguridad y tareas de seguridad de SAFECode para el desarrollo ágil", y finalmente una revisión de las tarjetas en EoP.

Las relaciones entre los ataques y cinco recursos se ofrecen en la mayoría de las tarjetas

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

Las relaciones entre los ataques y cinco recursos se ofrecen en la mayoría de las tarjetas

- Requisitos en "Secure Coding Practices (SCP) - Quick Reference Guide", v2, OWASP, Noviembre de 2010 (ref: OWASP SCP Quick Reference Guide v2.1)
- ID de verificación en "Application Security Verification Standard (ASVS) for Web Applications" (ref: ASVS v3 and v4 downloads)
- ID de puntos de detección de ataques en "AppSensor", OWASP, August de 2010-2015 (ref: AppSensor DetectionPoints)
- ID en "Common Attack Pattern Enumeration and Classification (CAPEC)", v2.8, Mitre Corporation, Noviembre de 2015 (ref: capec (31. July 2018))
- Historias centradas en la seguridad en 'Practical Security Stories and Security Tasks for Agile Development Environments', SAFECode, julio de 2012 (ref: SAFECode Agile Dev Security)

Una búsqueda significa que el ataque está incluido dentro del elemento al que se hace referencia, pero no necesariamente abarca toda su intención. Para datos estructurados como CAPEC, se proporciona la referencia más específica, pero a veces se proporciona una referencia cruzada que también tiene ejemplos (secundarios) más específicos. No hay búsquedas sobre los seis ases y los dos comodines. En cambio, estas tarjetas tienen algunos consejos generales en texto en cursiva.

Es posible jugar Cornucopia de muchas formas diferentes. Aquí hay una manera, como demonstrado online en un video de (refL Cornucopia scoresheet) , qué usa la nueva (May 2015) oja para anotar puntos

A - Preparativos

A1. Usa las cartas de este paquete.
A2. Identifique una solicitud o proceso de solicitud para revisar; esto podría ser un concepto, diseño o una implementación real.
A3. Cree un diagrama de flujo de datos, historias de usuarios u otros artefactos para ayudar en la revisión.
A4. Identifique e invite a un grupo de 3 a 6 personas, Se recomienda que los roles a considerar sean arquitectos, desarrolladores, evaluadores y otras partes interesadas del negocio, Siéntelos juntos alrededor de una mesa (intente incluir a alguien bastante familiarizado con la seguridad de las aplicaciones)
A5. Tenga algunos premios a mano (estrellas doradas, chocolate, pizza, cerveza o flores según la cultura de su oficina).

B - El juego

Un palo, Cornucopia, actúa como triunfo. Los ases son altos (es decir, vencieron a los reyes). Ayuda si hay alguien que no es jugador para documentar los problemas y las puntuaciones.

B1. Retire los comodines y algunas cartas de puntuación baja (2, 3, 4) del palo de Cornucopia para asegurarse de que cada jugador tenga la misma cantidad de cartas.
B2. Baraja la baraja y reparte todas las cartas.
B3. Para comenzar, elija un jugador al azar que jugará la primera carta; puede jugar cualquier carta de su mano, excepto del palo de triunfo: Cornucopia.
B4. Para jugar una carta, cada jugador debe leerla en voz alta y explicar (consulte el Wiki Deck en línea para obtener consejos) cómo podría aplicarse la amenaza (el jugador obtiene un punto por los ataques que podrían funcionar y que el grupo cree que es un error procesable). No intente pensar en mitigaciones en esta etapa, y no excluya una amenaza solo por creer que ya está mitigada; alguien anote la tarjeta y registre los problemas planteados.
B5. Juegue en el sentido de las agujas del reloj, cada persona debe jugar una carta de la misma manera; si tienes una carta del mismo palo, debes jugar una de esas; de lo contrario, pueden jugar una carta de cualquier otro palo, sólo una carta más alta del mismo palo, o la carta más alta del palo de triunfo Cornucopia, gana la mano. Only a higher card of the same suit, or the highest card in the trump suit Cornucopia, wins the hand.
B6. La persona que gana la ronda lidera la siguiente ronda (es decir, juega primero) y, por lo tanto, define el siguiente palo principal.
B7. Repita hasta que se jueguen todas las cartas.

C - Puntuación

El objetivo es identificar las amenazas aplicables y ganar manos (rondas):

C1. Obtenga +1 por cada tarjeta que pueda identificar como una amenaza válida para la aplicación en cuestión.
C2. Obtén +1 si ganas una ronda.
C3. Una vez que se han jugado todas las cartas, gana el que tenga más puntos.

D - Cierre

D1. Revise todas las amenazas aplicables y los requisitos de seguridad correspondientes.
D2. Cree historias de usuario, especificaciones y casos de prueba según sea necesario para su metodología de desarrollo.

Reglas alternativas de juego

Si es nuevo en el juego, elimine los Ases y dos cartas de Joker para empezar. Vuelva a agregar las tarjetas Joker una vez que la gente se familiarice con el proceso. Aparte de las reglas del "juego de cartas de triunfos" descritas anteriormente que son muy similares a la EoP, el mazo también se puede jugar como el "juego de veintiún cartas" (también conocido como "pontón" o "blackjack") que normalmente reduce el número de cartas jugadas en cada ronda.

Practique con una aplicación imaginaria, o incluso una aplicación planificada para el futuro, en lugar de tratar de encontrar fallas en las aplicaciones existentes hasta que los participantes estén contentos con la utilidad del juego.

Considere simplemente jugar con un dominio para hacer una sesión más corta, pero trate de cubrir todos los dominios para cada proyecto. O incluso mejor, simplemente juegue una mano con algunas cartas preseleccionadas y puntúe solo en la capacidad de identificar los requisitos de seguridad. Quizás tenga un juego de cada palo cada día durante una semana más o menos, si los participantes no pueden disponer del tiempo suficiente para una baraja completa.

Algunos equipos han preferido jugar una mano completa de cartas y luego discutir lo que hay en las cartas después de cada ronda (en lugar de después de que cada persona juegue una carta).

Otra sugerencia es que, si un jugador no identifica que la carta es relevante, permita que otros jugadores sugieran ideas y, potencialmente, déjeles ganar el punto por la carta. Considere la posibilidad de conceder puntos extra por contribuciones especialmente buenas.

Incluso puedes jugar solo. Solo usa las tarjetas para que actúen como lluvia de ideas. Sin embargo, involucrar a más personas siempre será beneficioso.

En la guía EoP de Microsoft, recomiendan hacer trampa como una buena estrategia de juego.

Marco de desarrollo específico - barajas de cartas modificadas

A finales de 2012, se publicó la Matriz de seguridad del marco de OWASP, cuyos documentos incorporaron controles de seguridad en algunos lenguajes y marcos de uso común para el desarrollo de aplicaciones web y móviles. Con ciertas salvedades, es útil considerar cómo el uso de estos controles puede simplificar la identificación de requisitos adicionales, siempre que, por supuesto, los controles estén incluidos, habilitados y configurados correctamente.

Considere quitar las siguientes cartas de los mazos si está seguro de que se tratan por la forma en que está usando el lenguaje / marco ork. Los elementos entre paréntesis son "maybes". Bibliotecas y estándares de codificación internos.

Estándares de codificación internos

Agregue su propia lista de tarjetas excluidas según los estándares de codificación de su organización (siempre que estén confirmados por los pasos de verificación apropiados en el ciclo de vida del desarrollo).

Tus estándares de Codificación y Librerías		
Validación de Data	Gestión de Sesiones	Criptografía
[lista tuya]	*[lista tuya]*	*[lista tuya]*
Autenticación	Autorización	Cornucopia
[lista tuya]	*[lista tuya]*	*[lista tuya]*

Mazos de requisitos de cumplimiento

Cree una baraja más pequeña al incluir solo tarjetas para un requisito de cumplimiento particular.

Requerimientos de Cumplimiento		
Validación de Data	Gestión de Sesiones	Criptografía
[lista tuya]	*[lista tuya]*	*[lista tuya]*
Autenticación	Autorización	Cornucopia
[lista tuya]	*[lista tuya]*	*[lista tuya]*

Preguntas frecuentes

1. ¿Puedo copiar o editar el juego?

Sí, por supuesto. Son libres de hacer lo que desee con todos los materiales de OWASP, siempre que cumpla con la licencia Creative Commons Attribution ShareAlike 3.0. Quizás si crea una nueva versión, ¿podría donarla al Proyecto Cornucopia de OWASP? ¿podría donarla al Proyecto Cornucopia de OWASP?

2. ¿Cómo puedo involucrarme?

Envíe ideas u ofertas de ayuda a la lista de distribución del proyecto.

3. ¿Cómo se eligieron los nombres de los atacantes?

Edite este documento usted mismo para hacer que las cartas sean más adecuadas para sus equipos o cree mazos completamente nuevos. Estos pueden considerarse personas externas o internas o alias para sistemas informáticos. Pero en lugar de solo nombres aleatorios, pensé en cómo podrían reflejar el aspecto de la comunidad OWASP. Hay mucho texto en las tarjetas y las referencias cruzadas también ocupan espacio. 50 nombres restantes de la lista actual de pagos miembros individuales de OWASP. No se usó ningún nombre más de una vez, y cuando las personas habían proporcionado dos nombres personales, eliminé una parte para tratar de asegurar que nadie pueda ser identificado fácilmente. Los nombres no se asignaron deliberadamente a ningún ataque, defensa o requisito en particular. La mezcla cultural y de género simplemente refleja estas fuentes de nombres, y no pretende ser representativa mundial.

4. ¿Por qué no hay imágenes en las caras de las tarjetas?

Hay mucho texto en las tarjetas y las referencias cruzadas también ocupan espacio. Pero sería genial tener elementos de diseño adicionales incluidos. ¿Algún voluntario?

5. ¿Se clasifican los ataques según el número de la tarjeta?

Solo aproximadamente. El riesgo dependerá de la aplicación y la organización, debido a los diferentes requisitos de seguridad y cumplimiento, por lo que su propia clasificación de criticidad puede colocar las tarjetas en un orden diferente al de los números de las tarjetas.

6. ¿Cuánto tiempo se tarda en jugar una ronda de cartas con la baraja completa?

Esto depende de la cantidad de discusión y de lo familiarizados que estén los jugadores con los conceptos de seguridad de las aplicaciones. Pero quizás tome de 1,5 a 2,0 horas para 4-6 personas.

7. ¿Qué tipo de personas deberían jugar?

Trate siempre de tener una combinación de roles que puedan aportar perspectivas alternativas. Pero incluya a alguien que tenga un conocimiento razonable de la terminología de vulnerabilidad de aplicaciones. De lo contrario, intente incluir una combinación de arquitectos, desarrolladores, evaluadores y un gerente de proyecto o propietario de negocio relevante.

8. ¿Quién debería tomar notas y registrar partituras?

Es mejor si otra persona, que no esté jugando, tome notas sobre los requisitos identificados y los problemas discutidos. Esto podría usarse como capacitación para un desarrollador más joven o ser realizado por el gerente del proyecto. Algunas organizaciones han realizado una grabación para revisarla posteriormente cuando los requisitos se redacten de manera más formal.

9. ¿Deberíamos utilizar siempre la baraja completa?

No. Un mazo más pequeño es más rápido de jugar. Comienza tu primer juego con sólo cartas suficientes para dos o tres rondas. Considere siempre eliminar las tarjetas que no sean apropiadas en absoluto para la aplicación o función de destino que se está revisando. Las primeras veces que la gente juega, también suele ser mejor eliminar los ases y los dos comodines. También es habitual jugar sin ningún palo de triunfo hasta que la gente esté más familiarizada con la idea.

10. ¿Qué deben hacer los jugadores cuando tienen una carta As que dice "inventó un nuevo ataque X"?

El jugador puede inventar cualquier ataque que considere válido, pero debe coincidir con el palo de la carta (por ejemplo, validación y codificación de datos). Para los jugadores nuevos en el juego, puede ser mejor eliminarlos para empezar (consulte también la pregunta frecuente 9).

11. No entiendo qué significa el ataque en cada tarjeta. ¿Hay información más detallada?

Sí, el Wiki Deck en línea en fue creado para ayudar a los jugadores a comprender los ataques. Ver

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

12. Mi empresa quiere imprimir su propia versión de OWASP Cornucopia: ¿a qué licencia debemos referirnos? Comuníquese directamente con la lista de correo o con los líderes del proyecto si falta alguien en las listas a continuación.

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

DATA VALIDATION & ENCODING

A

Has creado un nuevo ataque contra validación de datos y codificación

Lea más sobre este tema en Cheat Sheets de OWASP libre, XSS Prevención, basada en DOM Prevención XSS, SQL Prevención de inyecciones, y Parametrización de consultas

DATA VALIDATION & ENCODING

(No Tarjeta)

DATA VALIDATION & ENCODING

2

Brian puede reunir información sobre las principales configuraciones: esquemas, lógicas, código, software, servicios e infraestructura debido al contenido de mensajes de error, configuración deficiente, a la presencia de archivos de instalación predeterminados o antiguos, prueba, copia de seguridad o los recursos, o exposición de código fuente

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 puede ingresar datos maliciosos porque el formato de protocolo permitido no está siendo revisado, los duplicados son aceptados, la estructura no está siendo validada, los elementos de datos individuales no están siendo validados por: formato, tipo, rango, longitud y una lista blanca de formatos o caracteres permitidos

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 puede ingresar datos o nombres maliciosos en campos porque actualmente no hay una revisión o monitoreo a nivel de usuario o proceso

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 puede eludir las rutinas de codificación centralizadas, ya que dichas rutinas no son usadas por todos los activos o se están utilizando codificaciones incorrectas

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 puede eludir las rutinas de validación centralizadas, ya que no se utilizan en todas las entradas

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 puede crear cargas especiales para frustrar la validación de entrada, porque el conjunto de caracteres no es especificado/aplicado, los datos se codifican varias veces, los datos no están completamente transformados en el mismo formato que la aplicación usa (p. ej. canonicalización) antes de ser validados, o las variables no están configuradas de manera robusta

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 puede pasar por alto las rutinas de sanitización centralizadas ya que no están siendo utilizadas exhaustivamente

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 puede pasar por alto los checks de validaciones de entrada o salida porque los fallos en las validaciones no son rechazados y/o sanitizados

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 puede explotar la confianza que la aplicación deposita en una fuente de datos (por ejemplo, datos definibles por el usuario, manipulación de datos almacenados localmente, alteración de los datos del estado en un dispositivo cliente, falta de verificación de identidad durante la validación de datos, como Darío puede pretender ser Colin)

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 tiene control sobre la validación de entrada, la validación de salida o código de codificación de salida o rutinas para que puedan ser evitados

OWASP SCP
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 puede inyectar datos en el lado del cliente o en el dispositivo porque no se está utilizando una interfaz parametrizada, o no ha sido implementada correctamente, o los datos no han sido codificados correctamente, o no hay una política restrictiva en el código o los datos incluidos

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 puede inyectar datos en un intérprete del lado del servidor (por ejemplo, SQL, comandos del sistema operativo, Xpath, servidor JavaScript, SMTP) porque no se está utilizando una interfaz parametrizada fuertemente tipificada o no se ha implementado correctamente

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}

(No Tarjeta)

(No Tarjeta)

AUTHENTICATION

A

Usted tiene inventado un nuevo ataque contra la autenticación

Leer mas sobre este tema en OWASP's free Authentication Cheat Sheet

AUTHENTICATION

(No Tarjeta)

AUTHENTICATION

2

James puede emprender funciones de autenticación sin que el usuario real se dé cuenta alguna vez de lo ocurrido (por ejemplo, intento de logueo, inicio de sesión con credenciales robadas, restablecimiento de la contraseña)

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

Muhammad puede obtener una contraseña de usuario u otros secretos tales como preguntas de seguridad, por observación durante el ingreso o desde el cache, o desde la memoria, o en tránsito, o leyéndolo de alguna ubicación desprotegida, o porque es ampliamente conocido, o porque nunca caduca, o porque el usuario no puede cambiar su propia contraseña

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 puede fácilmente identificar nombres de usuario o puede enumerarlos

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 puede usar credenciales por defecto, de prueba o fáciles de adivinar para autenticar, o puede usar una cuenta antigua o una cuenta no necesaria para la aplicación

OWASP SCP
54, 175, 178

OWASP ASVS
4.1.5

OWASP APPSENSOR
AE12, HT3

CAPEC
70

SAFECODE
28

${Common_Title_full}

AUTHENTICATION

6

Sven puede reutilizar contraseñas temporales porque el usuario no realizó el cambio en el primer logueo. o tiene demasiado tiempo y no tiene vencimiento, o no usa un método correcto de entrega (por ejemplo, publicación, aplicación móvil, SMS)

OWASP SCP
37, 45-46, 178

OWASP ASVS
2.5.6

OWASP APPSENSOR
-

CAPEC
50

SAFECODE
28

${Common_Title_full}

AUTHENTICATION

7

Cecilia puede usar ataques de fuerza bruta y ataques de diccionario sin límites contra uno o muchas cuentas, o estos ataques se simplifican debido a una complejidad insuficiente, longitud, caducidad inadecuada y reutilización de requisitos para las contraseñas

OWASP SCP
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 puede pasar por alto la autenticación porque ésta no falla de forma segura (es decir, por defecto permite acceso no autenticado)

OWASP SCP
28

OWASP ASVS
4.1.5

OWASP APPSENSOR
-

CAPEC
115

SAFECODE
28

${Common_Title_full}

AUTHENTICATION

9

Claudia puede utilizar Funciones más críticas porque los requisitos de autenticación son demasiado débiles (por ejemplo, no usa autenticación robusta como el doble factor), o no hay requisitos de re-autenticación para éstos

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 puede omitir el control de autenticación porque no se está utilizando un módulo/framework/servicio de autenticación centralizado, estándar, testeado, probado y aprobado, separado del recurso solicitado

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 puede acceder a los recursos o servicios porque no hay requisitos de autenticación, o fue asumido erróneamente que la autentificación sería realizada por algún otro sistema o realizada en alguna acción previa

OWASP SCP
23, 32, 34

OWASP ASVS
1.4.3, 1.4.5

OWASP APPSENSOR
-

CAPEC
115

SAFECODE
14, 28

${Common_Title_full}

AUTHENTICATION

Q

Jaime puede omitir la autenticación porque no se aplica con igual rigor para todos los tipos de funcionalidad de autenticación (por ejemplo, registro, cambio de contraseña, recuperación de contraseña, cierre de sesión, administración) o en todas las versiones / canales (por ejemplo, sitio web móvil, aplicación móvil, sitio web completo, API, call center)

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 puede influir o alterar el código o rutina de autenticación o puede evitarlo

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}

(No Tarjeta)

(No Tarjeta)

SESSION MANAGEMENT

A

Has inventado un nuevo ataque contra la gestión de sesión

Read more about this topic in OWASP's free Cheat Sheets on Session Management, and Cross Site Request Forgery (CSRF) Prevention

SESSION MANAGEMENT

(No Tarjeta)

SESSION MANAGEMENT

2

William tiene el control sobre la generación de identificadores de sesión

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 puede usar una sola cuenta en paralelo ya que permite sesiones concurrentes

OWASP SCP
68
OWASP ASVS
3.3.3, 3.3.4
OWASP APPSENSOR
-
CAPEC
-
SAFECODE
28
${Common_Title_full}

SESSION MANAGEMENT

4

Alison puede configurar cookies de identificación de sesión en otra aplicación web porque el dominio y la ruta no están suficientemente restringidos

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 puede predecir o adivinar los identificadores de sesión porque no se cambian cuando se modifica la función del usuario (por ejemplo, la autenticación previa y posterior) y cuando se cambia entre comunicaciones no cifradas y cifradas, o no son lo suficientemente largas y aleatorias, o no se cambian periódicamente

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 puede hacerse cargo de la sesión de un usuario porque hay un tiempo de espera de inactividad largo o nulo, un límite de tiempo de sesión general largo o nulo, o la misma sesión puede usarse desde más de un dispositivo / ubicación

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 puede utilizar la sesión de Adam después de que haya terminado, porque no hay una función de cierre de sesión, o no puede cerrar sesión fácilmente, o el cierre de sesión no termina la sesión correctamente

OWASP SCP
62-63
OWASP ASVS
3.3.1, 3.3.4
OWASP APPSENSOR
-
CAPEC
21
SAFECODE
28
${Common_Title_full}

SESSION MANAGEMENT

8

Matt puede abusar de sesiones largas porque la aplicación no requiere una autenticación periódica para verificar si los privilegios han cambiado

OWASP SCP
96

OWASP ASVS
3.6.1, 3.3.2

OWASP APPSENSOR
-

CAPEC
21

SAFECODE
28

${Common_Title_full}

SESSION MANAGEMENT

9

Ivan puede robar identificadores de sesión porque se envían a través de canales inseguros, se registran, se revelan en mensajes de error, se incluyen en URL o son accesibles de manera innecesaria mediante el código que el atacante puede influir o modificar

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 puede forjar solicitudes porque las sesiones por sesión o por acciones más críticas, los tokens aleatorios fuertes (es decir, los tokens anti-CSRF) o similares no se utilizan para acciones que cambian de estado

OWASP SCP
73-74

OWASP ASVS
4.2.2

OWASP APPSENSOR
IE4

CAPEC
62, 111

SAFECODE
18

${Common_Title_full}

SESSION MANAGEMENT

J

Jeff puede reenviar una interacción de repetición idéntica (por ejemplo, solicitud HTTP, señal, pulsación de botón) y se acepta, no se rechaza

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 puede omitir la administración de sesiones porque no se aplica de manera integral y coherente en toda la aplicación

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 puede omitir los controles de administración de la sesión porque se construyeron por sí mismos y / o son débiles, en lugar de usar un marco estándar o un módulo aprobado aprobado

OWASP SCP
58, 60

OWASP ASVS
1.1.6

OWASP APPSENSOR
-

CAPEC
21

SAFECODE
14, 28

${Common_Title_full}

(No Tarjeta)

(No Tarjeta)

AUTHORIZATION

A

Has inventado un nuevo ataque contra la Autorización

Read more about this topic in OWASP's Development and Testing Guides

AUTHORIZATION

(No Tarjeta)

AUTHORIZATION

2

Tim puede influir a donde se envía o reenvía la data

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

Christian puede acceder a información, a la que no debería tener permiso, a través de otro mecanismo al que sí tiene permiso (por ejemplo, indexador de búsqueda, registrador, reporte), o porque está en caché, o guardada por más tiempo del necesario u otro medio de fuga de información

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 puede eludir los controles de autorización porque no fallan de forma segura (es decir, por defecto permiten el acceso)

OWASP SCP
79-80

OWASP ASVS
4.1.5

OWASP APPSENSOR
-

CAPEC
122

SAFECODE
8, 10-11

${Common_Title_full}

AUTHORIZATION

5

Chad puede acceder a los recursos (incluidos servicios, procesos, AJAX, Flash, video, imágenes, documentos, archivos temporales, datos de sesión, propiedades del sistema, datos de configuración, registro de configuración, logs) a los que no debería poder acceder debido a la falta de autorización, o debido a privilegios excesivos(por ejemplo, no usar el principio de menor privilegio)

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 puede acceder a los datos a los que él no tiene permiso, incluso aunque tiene permiso para formulario / página / URL / punto de entrada

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 puede acceder a funciones de la aplicación, objetos o propiedades a las que él no está autorizado para acceder

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 puede omitir las reglas de negocios al alterar la secuencia o flujo de proceso habitual, o realizar el proceso en el orden incorrecto, o manipular los valores de fecha y hora utilizados por la aplicación, o usar características válidas para propósitos no intencionados, o manipulando los datos de control

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 puede hacer uso incorrecto de una aplicación al usar una función válida demasiado rápido, o con demasiada frecuencia, o de otra forma sin intención, o que consuma los recursos de la aplicación, o cause condiciones de carrera, o sobreutilice una función

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 puede eludir los controles de autorización centralizados ya que no están siendo utilizados exhaustivamente en todas las interacciones

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 puede acceder a la información de configuración de seguridad, o listas de control de acceso

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 puede inyectar un comando para que la aplicación se ejecute con un nivel de privilegios más alto

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 puede influir o alterar controles y permisos de autorización, y por ende puede

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}

(No Tarjeta)

(No Tarjeta)

CRYPTOGRAPHY

A

Has inventado un nuevo ataque contra la Criptografía

Read more about this topic in OWASP's free Cheat Sheets on Cryptographic Storage, and Transport Layer Protection

CRYPTOGRAPHY

(No Tarjeta)

CRYPTOGRAPHY

2

Kyun puede acceder a los datos porque ha sido ofuscado en lugar de utilizar una función criptográfica aprobada

OWASP SCP
105, 133, 135

OWASP ASVS
6.2.2

OWASP APPSENSOR
-

CAPEC
-

SAFECODE
21, 29

${Common_Title_full}

CRYPTOGRAPHY

3

Axel puede modificar datos transitorios o permanentes (almacenados o en tránsito), código fuente, actualizaciones / parches o datos de configuración, ya que no están sujetos a verificación de integridad

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 puede acceder a datos en tránsito que no están encriptados, incluso aunque el canal está encriptado

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 puede pasar por alto controles criptográficos porque estos no fallan de forma segura (es decir, por defecto no protegen)

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 puede leer y modificar datos sin cifrar en la memoria o en tránsito (por ejemplo, secretos criptográficos, credenciales, identificadores de sesión, datos personales y comerciales), en uso o en comunicaciones dentro de la aplicación, o entre la aplicación y los usuarios, o entre la aplicación y sistemas externos

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 puede interceptar o modificar datos encriptados en tránsito porque el protocolo está mal implementado o configurado de manera débil, o los certificados no son válidos, los certificados no son confiables o la conexión puede degradarse a una comunicación más débil o no encriptada

OWASP SCP
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 puede acceder a los datos comerciales almacenados (por ejemplo, contraseñas, identificadores de sesión, PII, datos del titular de la tarjeta) porque no está cifrado de forma segura ni hash de forma segura

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 puede omitir la generación de números aleatorios, la generación aleatoria de GUID, el hash y las funciones de cifrado porque han sido construidos por sí mismos y / o son débiles

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 puede romper la criptografía en uso porque no es lo suficientemente fuerte para el grado de protección requerido, o no lo es para la cantidad de esfuerzo que el atacante está dispuesto a hacer

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 puede leer las credenciales para acceder a recursos, servicios y otros sistemas internos o externos porque se almacenan en un formato no cifrado o se guardan en el código fuente

OWASP SCP
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 puede acceder o predecir los algoritmos o llaves de los secretos criptográficos

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 puede influir o alterar el código / las rutinas criptográficas (cifrado, hash, firmas digitales, números aleatorios y generación de GUID) y, por lo tanto, puede omitirlos

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}

(No Tarjeta)

(No Tarjeta)

CORNUCOPIA

A

Has inventado un nuevo ataque de cualquier tipo

Read more about application security in OWASP's free Guides on Requirements, Development, Code Review and Testing, the Cheat Sheet series, and the Open Software Assurance Maturity Model

CORNUCOPIA

(No Tarjeta)

CORNUCOPIA

2

Lee puede omitir los controles de la aplicación porque se han usado funciones de programación peligrosas/riesgosas en lugar de alternativas más seguras, errores de conversión de tipo, porque la aplicación no es confiable porque un recurso externo no está disponible, o por las problemas con condición de carrera, - inicialización / asignación de recursos o - desbordamientos

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 puede acceder al código fuente, o descompilar, o de otro modo acceder a la lógica de negocio para entender cómo la aplicación y cualquier secreto contenido funciona

OWASP SCP
134

OWASP ASVS
14.1.1

OWASP APPSENSOR
-

CAPEC
189, 207

SAFECODE
-

${Common_Title_full}

CORNUCOPIA

4

Keith puede realizar una acción y no es posible atribuirla a él

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 puede influir en la confianza que otras partes, incluidos los usuarios tienen en la aplicación, o abusar de esa confianza en otra parte (por ejemplo, en otra aplicación)

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 puede omitir los controles porque falta el manejo de errores/excepciones, o se implementa de manera inconsistente o parcial, o no niega el acceso por defecto (es decir, los errores deben terminar el acceso / ejecución), o se basan en el manejo por parte de otro servicio o sistema

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

Las acciones de Mwengu no se pueden investigar porque no hay un registro adecuado de los eventos de seguridad con una marca de tiempo adecuada, o no hay un registro de auditoría completo, o Mwengu puede modificarlas o eliminarlas, o no existe un servicio de registro centralizado

OWASP SCP
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 puede omitir la aplicación para obtener acceso a los datos debido a que la red y la infraestructura del host, y los servicios/aplicaciones compatibles, no se han configurado de manera segura, la configuración no se verificó periódicamente ni se aplicaron parches de seguridad, los datos se almacenaron localmente o no se guardaron protegidos físicamente

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 puede pasar por alto la aplicación para acceder a los datos porque las herramientas administrativas o las interfaces administrativas no están aseguradas adecuadamente

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 puede eludir los controles de la aplicación porque los frameworks de código, librerías y componentes contienen código malicioso o vulnerabilidades (por ejemplo, inhouse, software comercial, servicio tercerizado, de código abierto, ubicado externamente)

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 puede explotar la aplicación porque fue compilada utilizando herramientas obsoletas, o su configuración no es segura por defecto, o la seguridad de la información no fue documentada y pasada a equipos operacionales

OWASP SCP
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 puede emprender acciones maliciosas, no normales sin detección y respuesta por la aplicación en tiempo real

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 puede utilizar la aplicación para negar el servicio a algunos o todos sus usuarios

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}

JOKER

Joker

Alice puede utilizar la aplicación para atacar los sistemas y datos de los usuarios.

Has pensado convertirte en un individuo Miembro de OWASP? Todas las herramientas, orientación y reuniones locales son gratis para todos, pero la membresía individual ayuda Apoyar el trabajo de OWASP.

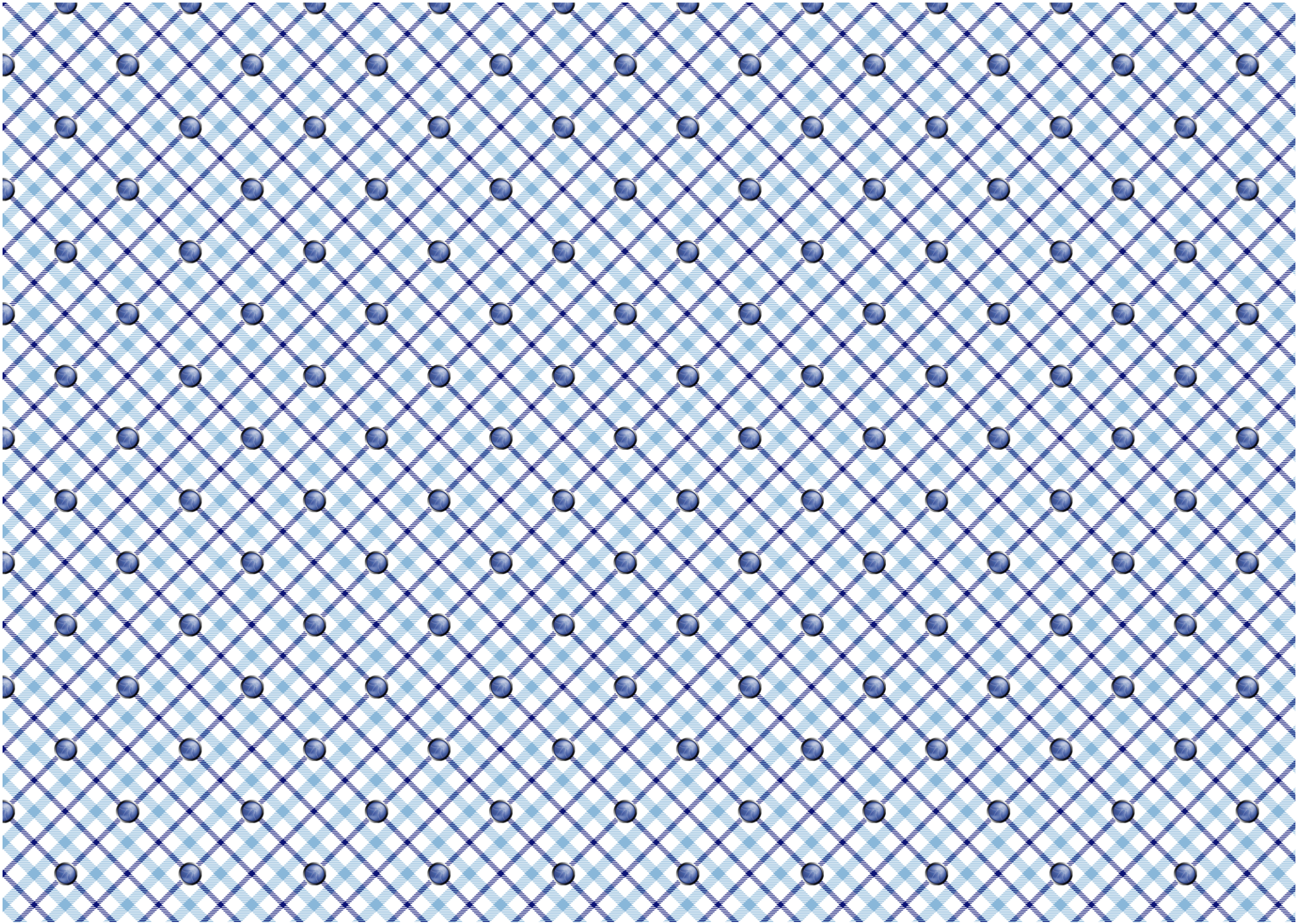
JOKER

Joker

Bob puede influir, alterar o afectar la aplicación para que ya no cumpla con mandatos legales, regulatorios, contractuales u otros mandatos organizacionales

Examine las vulnerabilidades y descubre cómo se pueden arreglar usando aplicaciones de entrenamiento en OWASP Broken Web Applications VM gratis, o utilizando los desafíos en línea en el laboratorio de hacking gratis

Cut here



Registro de cambios

Versión / Fecha		Comentarios
0,4	30 Jul 2012	Original Draft
0,4	10 Aug 2012	Draft reviewed and updated
0,4	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. Darío 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.

Project contributors

All OWASP projects rely on the voluntary efforts of people in the software development and information security sectors.

They have contributed their time and energy to make suggestions, provide feedback, write, review and edit documentation, give encouragement, trial the game, and promote the concept.

Without all their efforts, the project would not have progressed to this point.

Please contact the mailing list or project leaders directly, if anyone is missing from the below lists.

- 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 hard-working employees, especially Kate Hartmann
- Attendees at OWASP London, OWASP Manchester, OWASP Netherlands and OWASP Scotland chapter meetings, and the London Gamification meetup, who made helpful suggestions and asked challenging questions
- Blackfoot UK Limited for gifting print-ready design files and hundreds of professionally printed card decks for distribution by post and at OWASP chapter meetings
- Video of presentation, OWASP EU Tour 2013 London, 3rd June 2013

Podcasts and videos

Video of presentation, OWASP EU Tour 2013 London, 3rd June 2013

- Version / Date
  https://www.youtube.com/watch?v=i5Y0akWj31k
- Podcast and video links added.
  http://trustedsoftwarealliance.com/2014/03/21/the-owasp-cornucopia-project-with-colin-watson/
- Video of presentation, OWASP EU Tour 2013 London, 3rd June 2013
  https://www.youtube.com/watch?v=Q_LE-8xNXVk

See the project website for further information and presentation materials.