Cornucopia

Ecommerce Website Edition v1.20-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.

Autor

Colin Watson

Index

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 y codificación de datos (VE)
- Autenticación (AT)
- Gestión de sesiones (SM)
- Autorización (AZ)
- Criptografía (CR)
- Cornucopia (C)

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

TOtra 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 v3.0.1 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.

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:

- Lista de correo
https://lists.owasp.org/mailman/listinfo/owasp_cornucopia
- Página de inicio del proyecto
https://www.owasp.org/index.php/OWASP_Cornucopia

Todos los documentos y herramientas de OWASP son de descarga y uso gratuito. OWASP Cornucopia tiene licencia de Creative Commons Attribution ShareAlike 3.0.

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. Un ejemplo es:

William tiene control sobre la generación de identificadores de sesión

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

- Requisitos en "Prácticas de codificación segura (SCP) - Guía de referencia rápida", v2, OWASP, noviembre de 2010

https://www.owasp.org/index.php/File:OWASP_SCP_Quick_Reference_Guide_v2.pdf

- ID de verificación en "Application Security Verification Standard (ASVS) para aplicaciones web", OWASP, 2016

https://www.owasp.org/images/3/33/OWASP_Application_Security_Verification_Standard_3.0.1.pdf

- ID de puntos de detección de ataque en "AppSensor", OWASP, agosto de 2012

https://www.owasp.org/index.php/AppSensor_DetectionPoints

- ID en "Enumeración y clasificación de patrones de ataque común (CAPEC)", v2.6, Mitre Corporation, noviembre de 2015

http://capec.mitre.org/data/archive/capec_v2.8.zip

- Historias centradas en la seguridad en "Historias prácticas de seguridad y tareas de seguridad para entornos de desarrollo ágil", SAFECode, julio de 2012

http://www.safecode.org/publications/SAFECode_Agile_Dev_Security0712.pdf

OWASP
Open Web Application Security Project

Reconocimientos del proyecto:

- Colin Watson y Darío De Filippis
- Blackfoot UK Limited para los diseños de tarjetas listos para imprimir
- Tom Brennan y OWASP por la caja y el folleto
- Empleados de OWASP, especialmente Kate Hartmann
- Oana Cornea y otros participantes en AppSec EU 2015
- Max Gómez-Sánchez Vergaray por la traducción al español

(continúa en la página 16)

Una mejora es que el ataque está incluido dentro del elemento referenciado, pero no necesariamente abarca la totalidad de 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 más específicos (secundarios). No hay referencias ni asociaciones directas de los seis ases ni de los dos comodines. En cambio, estas tarjetas tienen algunos consejos generales en texto en cursiva.

Es posible jugar Cornucopia de muchas formas diferentes. He aquí una forma.

A - Preparativos

A1. Use 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.

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
[your list]	[your list]	[your list]
Autenticación	Autorización	Cornucopia

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
[your list]	[your list]	[your list]
Autenticación	Autorización	Cornucopia
[your list]	[your list]	[your list]

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?

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?

EoP comienza cada descripción con palabras como "Un atacante puede ...". Deben expresarse como un ataque, pero no me gustaba la terminología anónima, quería algo más atractivo y, por lo tanto, usé nombres personales. 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. Por lo tanto, además de "Alice y Bob", utilizo los (primeros) nombres de los empleados y miembros de la junta actuales y recientes de OWASP (asignados sin orden), y luego selecciono al azar los 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.

OWASP
Open Web Application Security Project

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.