



**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 ágil" 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

Otra 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,

## Estrategia de Juego

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

### Printing the cards

Check the Cornucopia project page for how to obtain pre-printed decks on glossy card.

The cards can be printed from this document in black & white but are more effective in color. The cards in the later pages of this document have been laid out to fit on one type of pre-scored business A4 card sheets. This appeared to be the quickest way to initially provide to create playing cards quickly. Avery product codes C32015 and C32030 have been tested successfully, but any 10 up 85mm x 54 mm cards on A4 paper should work with a little adjustment. Other stationery suppliers like Ryman and Sigel produce similar sheets. These card sheets are not inexpensive, so care should be taken in deciding what to print and using what media and printer type.

The cards can of course just be printed on any size of paper or card and then cut-up manually, or a commercial printer would be able to print larger volumes and cut the cards to size. The cut lines are shown on the penultimate page of this document, but Avery also produce a landscape A4 template (A-0017-01\_L.doc) that can be used as a guide.

Printing and cutting up can take an hour or so, and using a faster printer helps. Try to print add higher quality to increase legibility. An optional card back design (in OWASP tartan) has been provided as the last page of this document. There is no special alignment needed. Dual-sided printing needs special care taken. You could customize the card faces or the backs for your own organization's preferences.

### Customization

After you have used Cornucopia a few times, you may feel that some cards are less relevant to your applications, or the threats are different for your organization. Edit this document yourself to make the cards more suitable for your teams, or create new decks completely.

### 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](https://lists.owasp.org/mailman/listinfo/owasp_cornucopia)
- OWASP's hard-working employees, especially Kate Hartmann

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.

[https://www.owasp.org/index.php/OWASP\\_Cornucopia](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. Always try to have a mix of roles who can contribute alternative perspectives.

### *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](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

- Release.  
[https://www.owasp.org/index.php/File:OWASP\\_SCP\\_Quick\\_Reference\\_Guide\\_v2.pdf](https://www.owasp.org/index.php/File:OWASP_SCP_Quick_Reference_Guide_v2.pdf)
- Updates to alternative game rules.  
[https://www.owasp.org/images/3/33/OWASP\\_Application\\_Security\\_Verification\\_Standard\\_3.01.pdf](https://www.owasp.org/images/3/33/OWASP_Application_Security_Verification_Standard_3.01.pdf)
- Attack descriptions on cards with tinted backgrounds changed to black (from dark grey).  
[https://www.owasp.org/index.php/AppSensor\\_DetectionPoints](https://www.owasp.org/index.php/AppSensor_DetectionPoints)
- [https://www.youtube.com/watch?v=Q\\_LE-8xNXVk](https://www.youtube.com/watch?v=Q_LE-8xNXVk)  
[http://capec.mitre.org/data/archive/capec\\_v2.8.zip](http://capec.mitre.org/data/archive/capec_v2.8.zip)
- Reviewers  
[http://www.safecode.org/publications/SAFECode\\_Agile\\_Dev\\_Security0712.pdf](http://www.safecode.org/publications/SAFECode_Agile_Dev_Security0712.pdf)

Una mejora es que el ataque está incluido dentro del elemento referenciado, pero no necesariamente abarca la totalidad de su intención. For structured data like CAPEC, the most specific reference is provided but sometimes a cross-reference is provided that also has more specific (child) examples. There are no lookups on the six Aces and two Jokers. Instead these cards have some general tips in italicized text.

Es posible jugar Cornucopia de muchas formas diferentes. Here is one way, demonstrated online in a video at <https://youtu.be/i5Y0akWj31k>, which uses the new (May 2015) score/record sheet at <https://www.owasp.org/index.php/File:Cornucopia-scoresheet.pdf>

<https://youtu.be/i5Y0akWj31k>  
<https://www.owasp.org/index.php/File:Cornucopia-scoresheet.pdf>

## Reglas alternativas de juego

## 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. 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

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, déjelos 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.

correspondientes.

usuario, especificaciones y casos de prueba según sea necesario para su metodología de desarrollo.

D2. Cree historias de

### 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 [your list]	Gestión de Sesiones [your list]	Criptografía [your list]
Autenticación [your list]	Autorización [your list]	Cornucopia [your list]

### 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 [your list]	Gestión de Sesiones [your list]	Criptografía [your list]
Autenticación [your list]	Autorización [your list]	Cornucopia [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? ¿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?

Edit this document yourself to make the cards more suitable for your teams, or create new decks completely.

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 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 aprroximadamente. 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. What sort of people should play the game?

Always try to have a mix of roles who can contribute alternative perspectives. But include someone who has a reasonable knowledge of application vulnerability terminology. Otherwise try to include a mix of architects, developers, testers and a relevant project manager or business owner.

### 8. Who should take notes and record scores?

It is better if that someone else, not playing the game, takes notes about the requirements identified and issues discussed. This could be used as training for a more junior developer, or performed by the project manager. Some organisations have made a recording to review afterwards when the requirements are written up more formally.

### 9. Should we always use the full deck of cards?

No. A smaller deck is quicker to play. Start your first game with only enough cards for two or three rounds. Always consider removing cards that are not appropriate at all of the target application or function being reviewed. For the first few times people play the game it is also usually better to remove the Aces and the two Jokers. It is also usual to play the game without any trumps suit until people are more familiar with the idea.

### 10. What should players do when they have an Ace card that says "invented a new X attack"?

TOtra motivación para Cornucopia es vincular los ataques con los requisitos y las técnicas de verificación. With players new to the game, it can be better to remove these to begin with (see also FAQ 9).

### 11. I don't understand what the attack means on each card - is there more detailed information?

Yes, the online Wiki Deck at was created to help players understand the attacks. See

<https://www.owasp.org/index.php/Cornucopia - Ecommerce Website Edition - Wiki Deck>

### 12. My company wants to print its own version of OWASP Cornucopia - what license do we need to refer to? Please contact the mailing list or project leaders directly, if anyone is missing from the below lists.

[https://www.owasp.org/index.php/OWASP\\_Cornucopia - tab=FAQs](https://www.owasp.org/index.php/OWASP_Cornucopia - tab=FAQs)



DATA VALIDATION & ENCODING	<p><b>A</b></p> <p>Has creado un nuevo ataque contra validación de datos y codificación</p> <p><i>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</i></p>	<p>(No Tarjeta)</p> <p><b>DATA VALIDATION &amp; ENCODING</b></p>	<p><b>2</b></p> <p>Brian puede reunir información sobre las principales configuraciones: esquemas, lógicas, código, software, servicios e infraestructura debido al contenido de mensajes de error, configuración deficiente, o a la presencia de archivos de instalación predeterminados o antiguos, de prueba, de copia de seguridad o copias de los recursos, o exposición de código fuente</p> <p>OWASP SCP \${VE_VE2_owasp_scp} OWASP ASVS \${VE_VE2_owasp_asvs} OWASP APPSENSOR \${VE_VE2_owasp_appsensor} CAPEC 54, 541 SAFECODE \${VE_VE2_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p> <p><b>DATA VALIDATION &amp; ENCODING</b></p>
DATA VALIDATION & ENCODING	<p><b>4</b></p> <p>Dave puede ingresar datos o nombres maliciosos en campos porque actualmente no hay una revisión o monitoreo a nivel de usuario o proceso</p> <p>OWASP SCP \${VE_VE4_owasp_scp} OWASP ASVS \${VE_VE4_owasp_asvs} OWASP APPSENSOR \${VE_VE4_owasp_appsensor} CAPEC 28, 31, 48, 126, 162, 165, 213, 220-221, 261 SAFECODE \${VE_VE4_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p><b>5</b></p> <p>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</p> <p><b>DATA VALIDATION &amp; ENCODING</b></p>	<p><b>6</b></p> <p>Jason puede eludir las rutinas de validación centralizadas, ya que no se utilizan en todas las entradas</p> <p><b>DATA VALIDATION &amp; ENCODING</b></p>
DATA VALIDATION & ENCODING	<p><b>7</b></p> <p>Jan puede crear cargas especiales para frustrar la validación de entrada, porque el conjunto de caracteres no es especificado/aplicado, o los datos se codifican varias veces, o los datos no están completamente transformados en el mismo formato que la aplicación usa (por ejemplo, canonicalización) antes de ser validados, o las variables no están configuradas de manera coherente</p> <p>OWASP SCP \${VE_VE7_owasp_scp} OWASP ASVS \${VE_VE7_owasp_asvs} OWASP APPSENSOR \${VE_VE7_owasp_appsensor} CAPEC 28 SAFECODE \${VE_VE7_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p><b>DATA VALIDATION &amp; ENCODING</b></p>	<p><b>3</b></p> <p>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</p> <p>OWASP SCP \${VE_VE3_owasp_scp} OWASP ASVS \${VE_VE3_owasp_asvs} OWASP APPSENSOR \${VE_VE3_owasp_appsensor} CAPEC 28, 48, 126, 165, 213, 220-221, 261-262, 271-272 SAFECODE \${VE_VE3_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p> <p><b>DATA VALIDATION &amp; ENCODING</b></p>

<p><b>DATA VALIDATION &amp; ENCODING</b></p>	<p><b>8</b></p> <p>Sarah puede pasar por alto las rutinas de sanitización centralizadas ya que no están siendo utilizadas exhaustivamente</p> <table border="1" data-bbox="339 520 662 755"> <tr><td>OWASP SCP \${VE_VE8_owasp_scp}</td></tr> <tr><td>OWASP ASVS \${VE_VE8_owasp_asvs}</td></tr> <tr><td>OWASP APPSENSOR \${VE_VE8_owasp_appsensor}</td></tr> <tr><td>CAPEC 28, 31, 152, 160, 468</td></tr> <tr><td>SAFECODE \${VE_VE8_safecode}</td></tr> <tr><td>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</td></tr> </table>	OWASP SCP \${VE_VE8_owasp_scp}	OWASP ASVS \${VE_VE8_owasp_asvs}	OWASP APPSENSOR \${VE_VE8_owasp_appsensor}	CAPEC 28, 31, 152, 160, 468	SAFECODE \${VE_VE8_safecode}	OWASP Cornucopia Ecommerce Website Edition v1.20-EN	<p><b>DATA VALIDATION &amp; ENCODING</b></p> <p><b>9</b></p> <p>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</p> <table border="1" data-bbox="795 520 1138 755"> <tr><td>OWASP SCP \${VE_VE9_owasp_scp}</td></tr> <tr><td>OWASP ASVS \${VE_VE9_owasp_asvs}</td></tr> <tr><td>OWASP APPSENSOR \${VE_VE9_owasp_appsensor}</td></tr> <tr><td>CAPEC 28</td></tr> <tr><td>SAFECODE \${VE_VE9_safecode}</td></tr> <tr><td>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</td></tr> </table>	OWASP SCP \${VE_VE9_owasp_scp}	OWASP ASVS \${VE_VE9_owasp_asvs}	OWASP APPSENSOR \${VE_VE9_owasp_appsensor}	CAPEC 28	SAFECODE \${VE_VE9_safecode}	OWASP Cornucopia Ecommerce Website Edition v1.20-EN	<p><b>DATA VALIDATION &amp; ENCODING</b></p> <p><b>10</b></p> <p>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)</p> <table border="1" data-bbox="1253 520 1596 755"> <tr><td>OWASP SCP \${VE_VE10_owasp_scp}</td></tr> <tr><td>OWASP ASVS \${VE_VE10_owasp_asvs}</td></tr> <tr><td>OWASP APPSENSOR \${VE_VE10_owasp_appsensor}</td></tr> <tr><td>CAPEC 12, 51, 57, 90, 111, 145, 194-195, 202, 218, 463</td></tr> <tr><td>SAFECODE \${VE_VE10_safecode}</td></tr> <tr><td>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</td></tr> </table>	OWASP SCP \${VE_VE10_owasp_scp}	OWASP ASVS \${VE_VE10_owasp_asvs}	OWASP APPSENSOR \${VE_VE10_owasp_appsensor}	CAPEC 12, 51, 57, 90, 111, 145, 194-195, 202, 218, 463	SAFECODE \${VE_VE10_safecode}	OWASP Cornucopia Ecommerce Website Edition v1.20-EN	<p><b>DATA VALIDATION &amp; ENCODING</b></p> <p><b>J</b></p> <p>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</p> <table border="1" data-bbox="1711 520 1980 755"> <tr><td>OWASP SCP \${VE_VEJ_owasp_scp}</td></tr> <tr><td>OWASP ASVS \${VE_VEJ_owasp_asvs}</td></tr> <tr><td>OWASP APPSENSOR \${VE_VEJ_owasp_appsensor}</td></tr> <tr><td>CAPEC 87, 207, 554</td></tr> <tr><td>SAFECODE \${VE_VEJ_safecode}</td></tr> <tr><td>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</td></tr> </table>	OWASP SCP \${VE_VEJ_owasp_scp}	OWASP ASVS \${VE_VEJ_owasp_asvs}	OWASP APPSENSOR \${VE_VEJ_owasp_appsensor}	CAPEC 87, 207, 554	SAFECODE \${VE_VEJ_safecode}	OWASP Cornucopia Ecommerce Website Edition v1.20-EN
OWASP SCP \${VE_VE8_owasp_scp}																												
OWASP ASVS \${VE_VE8_owasp_asvs}																												
OWASP APPSENSOR \${VE_VE8_owasp_appsensor}																												
CAPEC 28, 31, 152, 160, 468																												
SAFECODE \${VE_VE8_safecode}																												
OWASP Cornucopia Ecommerce Website Edition v1.20-EN																												
OWASP SCP \${VE_VE9_owasp_scp}																												
OWASP ASVS \${VE_VE9_owasp_asvs}																												
OWASP APPSENSOR \${VE_VE9_owasp_appsensor}																												
CAPEC 28																												
SAFECODE \${VE_VE9_safecode}																												
OWASP Cornucopia Ecommerce Website Edition v1.20-EN																												
OWASP SCP \${VE_VE10_owasp_scp}																												
OWASP ASVS \${VE_VE10_owasp_asvs}																												
OWASP APPSENSOR \${VE_VE10_owasp_appsensor}																												
CAPEC 12, 51, 57, 90, 111, 145, 194-195, 202, 218, 463																												
SAFECODE \${VE_VE10_safecode}																												
OWASP Cornucopia Ecommerce Website Edition v1.20-EN																												
OWASP SCP \${VE_VEJ_owasp_scp}																												
OWASP ASVS \${VE_VEJ_owasp_asvs}																												
OWASP APPSENSOR \${VE_VEJ_owasp_appsensor}																												
CAPEC 87, 207, 554																												
SAFECODE \${VE_VEJ_safecode}																												
OWASP Cornucopia Ecommerce Website Edition v1.20-EN																												
<p><b>DATA VALIDATION &amp; ENCODING</b></p>	<p><b>Q</b></p> <p>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</p> <table border="1" data-bbox="339 1183 662 1418"> <tr><td>OWASP SCP \${VE_VEQ_owasp_scp}</td></tr> <tr><td>OWASP ASVS \${VE_VEQ_owasp_asvs}</td></tr> <tr><td>OWASP APPSENSOR \${VE_VEQ_owasp_appsensor}</td></tr> <tr><td>CAPEC 28, 31, 152, 160, 468</td></tr> <tr><td>SAFECODE \${VE_VEQ_safecode}</td></tr> <tr><td>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</td></tr> </table>	OWASP SCP \${VE_VEQ_owasp_scp}	OWASP ASVS \${VE_VEQ_owasp_asvs}	OWASP APPSENSOR \${VE_VEQ_owasp_appsensor}	CAPEC 28, 31, 152, 160, 468	SAFECODE \${VE_VEQ_safecode}	OWASP Cornucopia Ecommerce Website Edition v1.20-EN	<p><b>DATA VALIDATION &amp; ENCODING</b></p> <p><b>K</b></p> <p>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</p> <table border="1" data-bbox="795 1183 1138 1418"> <tr><td>OWASP SCP \${VE_VEK_owasp_scp}</td></tr> <tr><td>OWASP ASVS \${VE_VEK_owasp_asvs}</td></tr> <tr><td>OWASP APPSENSOR \${VE_VEK_owasp_appsensor}</td></tr> <tr><td>CAPEC 23, 28, 76, 152, 160, 261</td></tr> <tr><td>SAFECODE \${VE_VEK_safecode}</td></tr> <tr><td>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</td></tr> </table>	OWASP SCP \${VE_VEK_owasp_scp}	OWASP ASVS \${VE_VEK_owasp_asvs}	OWASP APPSENSOR \${VE_VEK_owasp_appsensor}	CAPEC 23, 28, 76, 152, 160, 261	SAFECODE \${VE_VEK_safecode}	OWASP Cornucopia Ecommerce Website Edition v1.20-EN	<p>(No Tarjeta)</p>	<p>(No Tarjeta)</p>												
OWASP SCP \${VE_VEQ_owasp_scp}																												
OWASP ASVS \${VE_VEQ_owasp_asvs}																												
OWASP APPSENSOR \${VE_VEQ_owasp_appsensor}																												
CAPEC 28, 31, 152, 160, 468																												
SAFECODE \${VE_VEQ_safecode}																												
OWASP Cornucopia Ecommerce Website Edition v1.20-EN																												
OWASP SCP \${VE_VEK_owasp_scp}																												
OWASP ASVS \${VE_VEK_owasp_asvs}																												
OWASP APPSENSOR \${VE_VEK_owasp_appsensor}																												
CAPEC 23, 28, 76, 152, 160, 261																												
SAFECODE \${VE_VEK_safecode}																												
OWASP Cornucopia Ecommerce Website Edition v1.20-EN																												

<p><b>AUTHENTICATION</b></p>	<p><b>AUTHENTICATION</b></p> <p><b>A</b></p> <p>Usted tiene inventado un nuevo ataque contra la autenticación</p> <p>(No Tarjeta)</p> <p><i>Leer mas sobre este tema en OWASP's free Authentication Cheat Sheet</i></p>	<p><b>AUTHENTICATION</b></p> <p><b>2</b></p> <p>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)</p>	<p><b>AUTHENTICATION</b></p> <p><b>3</b></p> <p>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</p>	
<p><b>AUTHENTICATION</b></p>	<p><b>AUTHENTICATION</b></p> <p><b>4</b></p> <p>Sebastien puede fácilmente identificar nombres de usuario o puede enumerarlos</p> <p>OWASP SCP \${AT_AT4_owasp_scp} OWASP ASVS \${AT_AT4_owasp_asvs} OWASP APPSENSOR \${AT_AT4_owasp_appsensor} CAPEC 383 SAFECODE \${AT_AT4_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p><b>AUTHENTICATION</b></p> <p><b>5</b></p> <p>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</p> <p>OWASP SCP \${AT_AT5_owasp_scp} OWASP ASVS \${AT_AT5_owasp_asvs} OWASP APPSENSOR \${AT_AT5_owasp_appsensor} CAPEC 70 SAFECODE \${AT_AT5_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p><b>AUTHENTICATION</b></p> <p><b>6</b></p> <p>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)</p> <p>OWASP SCP \${AT_AT6_owasp_scp} OWASP ASVS \${AT_AT6_owasp_asvs} OWASP APPSENSOR \${AT_AT6_owasp_appsensor} CAPEC 50 SAFECODE \${AT_AT6_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p><b>AUTHENTICATION</b></p> <p><b>7</b></p> <p>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</p> <p>OWASP SCP \${AT_AT7_owasp_scp} OWASP ASVS \${AT_AT7_owasp_asvs} OWASP APPSENSOR \${AT_AT7_owasp_appsensor} CAPEC 2, 16 SAFECODE \${AT_AT7_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>

<p><b>AUTHENTICATION</b></p>	<p><b>8</b></p> <p>Kate puede pasar por alto la autenticación porque ésta no falla de forma segura (es decir, por defecto permite acceso no autenticado)</p> <table border="1" data-bbox="332 525 646 754"> <tr><td>OWASP SCP \${AT_AT8_owasp_sc}</td></tr> <tr><td>OWASP ASVS \${AT_AT8_owasp_asvs}</td></tr> <tr><td>OWASP APPSENSOR \${AT_AT8_owasp_appsens}</td></tr> <tr><td>CAPEC 115</td></tr> <tr><td>SAFECODE \${AT_AT8_safecode}</td></tr> <tr><td>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</td></tr> </table>	OWASP SCP \${AT_AT8_owasp_sc}	OWASP ASVS \${AT_AT8_owasp_asvs}	OWASP APPSENSOR \${AT_AT8_owasp_appsens}	CAPEC 115	SAFECODE \${AT_AT8_safecode}	OWASP Cornucopia Ecommerce Website Edition v1.20-EN	<p><b>AUTHENTICATION</b></p>	<p><b>9</b></p> <p>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</p> <table border="1" data-bbox="765 525 1102 754"> <tr><td>OWASP SCP \${AT_AT9_owasp_sep}</td></tr> <tr><td>OWASP ASVS \${AT_AT9_owasp_asvs}</td></tr> <tr><td>OWASP APPSENSOR \${AT_AT9_owasp_appsens}</td></tr> <tr><td>CAPEC 21</td></tr> <tr><td>SAFECODE \${AT_AT9_safecode}</td></tr> <tr><td>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</td></tr> </table>	OWASP SCP \${AT_AT9_owasp_sep}	OWASP ASVS \${AT_AT9_owasp_asvs}	OWASP APPSENSOR \${AT_AT9_owasp_appsens}	CAPEC 21	SAFECODE \${AT_AT9_safecode}	OWASP Cornucopia Ecommerce Website Edition v1.20-EN	<p><b>AUTHENTICATION</b></p>	<p><b>10</b></p> <p>Pravín 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</p> <table border="1" data-bbox="1230 525 1545 754"> <tr><td>OWASP SCP \${AT_AT10_owasp_sep}</td></tr> <tr><td>OWASP ASVS \${AT_AT10_owasp_asvs}</td></tr> <tr><td>OWASP APPSENSOR \${AT_AT10_owasp_appsens}</td></tr> <tr><td>CAPEC 90, 115</td></tr> <tr><td>SAFECODE \${AT_AT10_safecode}</td></tr> <tr><td>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</td></tr> </table>	OWASP SCP \${AT_AT10_owasp_sep}	OWASP ASVS \${AT_AT10_owasp_asvs}	OWASP APPSENSOR \${AT_AT10_owasp_appsens}	CAPEC 90, 115	SAFECODE \${AT_AT10_safecode}	OWASP Cornucopia Ecommerce Website Edition v1.20-EN	<p><b>AUTHENTICATION</b></p>
OWASP SCP \${AT_AT8_owasp_sc}																								
OWASP ASVS \${AT_AT8_owasp_asvs}																								
OWASP APPSENSOR \${AT_AT8_owasp_appsens}																								
CAPEC 115																								
SAFECODE \${AT_AT8_safecode}																								
OWASP Cornucopia Ecommerce Website Edition v1.20-EN																								
OWASP SCP \${AT_AT9_owasp_sep}																								
OWASP ASVS \${AT_AT9_owasp_asvs}																								
OWASP APPSENSOR \${AT_AT9_owasp_appsens}																								
CAPEC 21																								
SAFECODE \${AT_AT9_safecode}																								
OWASP Cornucopia Ecommerce Website Edition v1.20-EN																								
OWASP SCP \${AT_AT10_owasp_sep}																								
OWASP ASVS \${AT_AT10_owasp_asvs}																								
OWASP APPSENSOR \${AT_AT10_owasp_appsens}																								
CAPEC 90, 115																								
SAFECODE \${AT_AT10_safecode}																								
OWASP Cornucopia Ecommerce Website Edition v1.20-EN																								
<p><b>AUTHENTICATION</b></p>	<p><b>Q</b></p> <p>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)</p> <table border="1" data-bbox="332 847 646 1445"> <tr><td>OWASP SCP \${AT_ATQ_owasp_sc}</td></tr> <tr><td>OWASP ASVS \${AT_ATQ_owasp_asvs}</td></tr> <tr><td>OWASP APPSENSOR \${AT_ATQ_owasp_appsens}</td></tr> <tr><td>CAPEC 36, 50, 115, 121, 179</td></tr> <tr><td>SAFECODE \${AT_ATQ_safecode}</td></tr> <tr><td>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</td></tr> </table>	OWASP SCP \${AT_ATQ_owasp_sc}	OWASP ASVS \${AT_ATQ_owasp_asvs}	OWASP APPSENSOR \${AT_ATQ_owasp_appsens}	CAPEC 36, 50, 115, 121, 179	SAFECODE \${AT_ATQ_safecode}	OWASP Cornucopia Ecommerce Website Edition v1.20-EN	<p><b>AUTHENTICATION</b></p>	<p><b>K</b></p> <p>Olga puede influir o alterar el código o rutina de autenticación o puede evitarlo</p> <table border="1" data-bbox="765 847 1102 1445"> <tr><td>OWASP SCP \${AT_ATK_owasp_sep}</td></tr> <tr><td>OWASP ASVS \${AT_ATK_owasp_asvs}</td></tr> <tr><td>OWASP APPSENSOR \${AT_ATK_owasp_appsens}</td></tr> <tr><td>CAPEC 115, 207, 554</td></tr> <tr><td>SAFECODE \${AT_ATK_safecode}</td></tr> <tr><td>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</td></tr> </table>	OWASP SCP \${AT_ATK_owasp_sep}	OWASP ASVS \${AT_ATK_owasp_asvs}	OWASP APPSENSOR \${AT_ATK_owasp_appsens}	CAPEC 115, 207, 554	SAFECODE \${AT_ATK_safecode}	OWASP Cornucopia Ecommerce Website Edition v1.20-EN									
OWASP SCP \${AT_ATQ_owasp_sc}																								
OWASP ASVS \${AT_ATQ_owasp_asvs}																								
OWASP APPSENSOR \${AT_ATQ_owasp_appsens}																								
CAPEC 36, 50, 115, 121, 179																								
SAFECODE \${AT_ATQ_safecode}																								
OWASP Cornucopia Ecommerce Website Edition v1.20-EN																								
OWASP SCP \${AT_ATK_owasp_sep}																								
OWASP ASVS \${AT_ATK_owasp_asvs}																								
OWASP APPSENSOR \${AT_ATK_owasp_appsens}																								
CAPEC 115, 207, 554																								
SAFECODE \${AT_ATK_safecode}																								
OWASP Cornucopia Ecommerce Website Edition v1.20-EN																								

<p><b>SESSION MANAGEMENT</b></p>	<p><b>A</b></p> <p>Has inventado un nuevo ataque contra la gestión de sesión</p> <p><i>Read more about this topic in OWASP's free Cheat Sheets on Session Management, and Cross Site Request Forgery (CSRF) Prevention</i></p>	<p><b>SESSION MANAGEMENT</b></p> <p><b>5</b></p> <p>(No Tarjeta)</p>	<p><b>SESSION MANAGEMENT</b></p> <p><b>2</b></p> <p>William tiene el control sobre la generación de identificadores de sesión</p>	<p><b>SESSION MANAGEMENT</b></p> <p><b>3</b></p> <p>Ryan puede usar una sola cuenta en paralelo ya que permite sesiones concurrentes</p>
<p><b>SESSION MANAGEMENT</b></p>	<p><b>4</b></p> <p>Alison puede configurar cookies de identificación de sesión en otra aplicación web porque el dominio y la ruta no están suficientemente restringidos</p> <p>OWASP SCP \${SM_SM4_owasp_scp} OWASP ASVS \${SM_SM4_owasp_asvs} OWASP APPSENSOR \${SM_SM4_owasp_appsensor} CAPEC 31, 61 SAFECODE \${SM_SM4_safecode} OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p><b>SESSION MANAGEMENT</b></p> <p><b>5</b></p> <p>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</p> <p>OWASP SCP \${SM_SM5_owasp_scp} OWASP ASVS \${SM_SM5_owasp_asvs} OWASP APPSENSOR \${SM_SM5_owasp_appsensor} CAPEC 31 SAFECODE \${SM_SM5_safecode} OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p><b>SESSION MANAGEMENT</b></p> <p><b>6</b></p> <p>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</p> <p>OWASP SCP \${SM_SM6_owasp_scp} OWASP ASVS \${SM_SM6_owasp_asvs} OWASP APPSENSOR \${SM_SM6_owasp_appsensor} CAPEC 21 SAFECODE \${SM_SM6_safecode} OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p><b>SESSION MANAGEMENT</b></p> <p><b>7</b></p> <p>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</p> <p>OWASP SCP \${SM_SM7_owasp_scp} OWASP ASVS \${SM_SM7_owasp_asvs} OWASP APPSENSOR \${SM_SM7_owasp_appsensor} CAPEC 21 SAFECODE \${SM_SM7_safecode} OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>

<p><b>SESSION MANAGEMENT</b></p>	<p><b>8</b></p> <p>Matt puede abusar de sesiones largas porque la aplicación no requiere una autenticación periódica para verificar si los privilegios han cambiado</p> <table border="1"> <tr><td>OWASP SCP \${SM_SM8_owasp_sc}</td></tr> <tr><td>OWASP ASVS \${SM_SM8_owasp_asvs}</td></tr> <tr><td>OWASP APPSENSOR \${SM_SM8_owasp_appsens}</td></tr> <tr><td>CAPEC 21</td></tr> <tr><td>SAFECODE \${SM_SM8_safecode}</td></tr> <tr><td>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</td></tr> </table>	OWASP SCP \${SM_SM8_owasp_sc}	OWASP ASVS \${SM_SM8_owasp_asvs}	OWASP APPSENSOR \${SM_SM8_owasp_appsens}	CAPEC 21	SAFECODE \${SM_SM8_safecode}	OWASP Cornucopia Ecommerce Website Edition v1.20-EN	<p><b>SESSION MANAGEMENT</b></p>	<p><b>9</b></p> <p>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</p> <table border="1"> <tr><td>OWASP SCP \${SM_SM9_owasp_sc}</td></tr> <tr><td>OWASP ASVS \${SM_SM9_owasp_asvs}</td></tr> <tr><td>OWASP APPSENSOR \${SM_SM9_owasp_appsens}</td></tr> <tr><td>CAPEC 31, 60</td></tr> <tr><td>SAFECODE \${SM_SM9_safecode}</td></tr> <tr><td>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</td></tr> </table>	OWASP SCP \${SM_SM9_owasp_sc}	OWASP ASVS \${SM_SM9_owasp_asvs}	OWASP APPSENSOR \${SM_SM9_owasp_appsens}	CAPEC 31, 60	SAFECODE \${SM_SM9_safecode}	OWASP Cornucopia Ecommerce Website Edition v1.20-EN	<p><b>SESSION MANAGEMENT</b></p>	
OWASP SCP \${SM_SM8_owasp_sc}																	
OWASP ASVS \${SM_SM8_owasp_asvs}																	
OWASP APPSENSOR \${SM_SM8_owasp_appsens}																	
CAPEC 21																	
SAFECODE \${SM_SM8_safecode}																	
OWASP Cornucopia Ecommerce Website Edition v1.20-EN																	
OWASP SCP \${SM_SM9_owasp_sc}																	
OWASP ASVS \${SM_SM9_owasp_asvs}																	
OWASP APPSENSOR \${SM_SM9_owasp_appsens}																	
CAPEC 31, 60																	
SAFECODE \${SM_SM9_safecode}																	
OWASP Cornucopia Ecommerce Website Edition v1.20-EN																	
<p><b>SESSION MANAGEMENT</b></p>	<p><b>Q</b></p> <p>Salim puede omitir la administración de sesiones porque no se aplica de manera integral y coherente en toda la aplicación</p> <table border="1"> <tr><td>OWASP SCP \${SM_SMQ_owasp_sc}</td></tr> <tr><td>OWASP ASVS \${SM_SMQ_owasp_asvs}</td></tr> <tr><td>OWASP APPSENSOR \${SM_SMQ_owasp_appsens}</td></tr> <tr><td>CAPEC 21</td></tr> <tr><td>SAFECODE \${SM_SMQ_safecode}</td></tr> <tr><td>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</td></tr> </table>	OWASP SCP \${SM_SMQ_owasp_sc}	OWASP ASVS \${SM_SMQ_owasp_asvs}	OWASP APPSENSOR \${SM_SMQ_owasp_appsens}	CAPEC 21	SAFECODE \${SM_SMQ_safecode}	OWASP Cornucopia Ecommerce Website Edition v1.20-EN	<p><b>SESSION MANAGEMENT</b></p>	<p><b>K</b></p> <p>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</p> <table border="1"> <tr><td>OWASP SCP \${SM_SMK_owasp_sc}</td></tr> <tr><td>OWASP ASVS \${SM_SMK_owasp_asvs}</td></tr> <tr><td>OWASP APPSENSOR \${SM_SMK_owasp_appsens}</td></tr> <tr><td>CAPEC 21</td></tr> <tr><td>SAFECODE \${SM_SMK_safecode}</td></tr> <tr><td>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</td></tr> </table>	OWASP SCP \${SM_SMK_owasp_sc}	OWASP ASVS \${SM_SMK_owasp_asvs}	OWASP APPSENSOR \${SM_SMK_owasp_appsens}	CAPEC 21	SAFECODE \${SM_SMK_safecode}	OWASP Cornucopia Ecommerce Website Edition v1.20-EN	<p>(No Tarjeta)</p>	
OWASP SCP \${SM_SMQ_owasp_sc}																	
OWASP ASVS \${SM_SMQ_owasp_asvs}																	
OWASP APPSENSOR \${SM_SMQ_owasp_appsens}																	
CAPEC 21																	
SAFECODE \${SM_SMQ_safecode}																	
OWASP Cornucopia Ecommerce Website Edition v1.20-EN																	
OWASP SCP \${SM_SMK_owasp_sc}																	
OWASP ASVS \${SM_SMK_owasp_asvs}																	
OWASP APPSENSOR \${SM_SMK_owasp_appsens}																	
CAPEC 21																	
SAFECODE \${SM_SMK_safecode}																	
OWASP Cornucopia Ecommerce Website Edition v1.20-EN																	

<p><b>AUTHORIZATION</b></p>	<p><b>A</b></p> <p>Has inventado un nuevo ataque contra la Autorización</p> <p><i>Read more about this topic in OWASP's Development and Testing Guides</i></p>	<p><b>AUTHORIZATION</b></p> <p>(No Tarjeta)</p>	<p><b>AUTHORIZATION</b></p> <p>Tim puede influir a donde se envía o reenvía la data</p>	<p><b>AUTHORIZATION</b></p> <p>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</p>
<p><b>AUTHORIZATION</b></p>	<p><b>4</b></p> <p>Kelly puede eludir los controles de autorización porque no fallan de forma segura (es decir, por defecto permiten el acceso)</p> <p>OWASP SCP \${AZ_AZ4_owasp_sc}</p> <p>OWASP ASVS \${AZ_AZ4_owasp_asvs}</p> <p>OWASP APPSENSOR \${AZ_AZ4_owasp_appsensor}</p> <p>CAPEC 122</p> <p>SAFECODE \${AZ_AZ4_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p><b>AUTHORIZATION</b></p> <p><b>5</b></p> <p>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)</p> <p>OWASP SCP \${AZ_AZ5_owasp_sc}</p> <p>OWASP ASVS \${AZ_AZ5_owasp_asvs}</p> <p>OWASP APPSENSOR \${AZ_AZ5_owasp_appsensor}</p> <p>CAPEC 75, 87, 95, 126, 149, 155, 203, 213, 264-265</p> <p>SAFECODE \${AZ_AZ5_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p><b>AUTHORIZATION</b></p> <p><b>6</b></p> <p>Eduardo puede acceder a los datos a los que él no tiene permiso, incluso aunque tiene permiso para formulario / página / URL / punto de entrada</p> <p>OWASP SCP \${AZ_AZ6_owasp_sc}</p> <p>OWASP ASVS \${AZ_AZ6_owasp_asvs}</p> <p>OWASP APPSENSOR \${AZ_AZ6_owasp_appsensor}</p> <p>CAPEC 122</p> <p>SAFECODE \${AZ_AZ6_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p><b>AUTHORIZATION</b></p> <p><b>7</b></p> <p>Yuanjing puede acceder a funciones de la aplicación, objetos o propiedades a las que él no está autorizado para acceder</p> <p>OWASP SCP \${AZ_AZ7_owasp_sc}</p> <p>OWASP ASVS \${AZ_AZ7_owasp_asvs}</p> <p>OWASP APPSENSOR \${AZ_AZ7_owasp_appsensor}</p> <p>CAPEC 122</p> <p>SAFECODE \${AZ_AZ7_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>

<p><b>AUTHORIZATION</b></p>	<p><b>8</b></p> <p>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</p> <table border="1"> <tr><td>OWASP SCP \${AZ_AZ8_owasp_scp}</td></tr> <tr><td>OWASP ASVS \${AZ_AZ8_owasp_asvs}</td></tr> <tr><td>OWASP APPSENSOR \${AZ_AZ8_owasp_appsensor}</td></tr> <tr><td>CAPEC 25, 39, 74, 162, 166, 207</td></tr> <tr><td>SAFECODE \${AZ_AZ8_safecode}</td></tr> <tr><td>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</td></tr> </table>	OWASP SCP \${AZ_AZ8_owasp_scp}	OWASP ASVS \${AZ_AZ8_owasp_asvs}	OWASP APPSENSOR \${AZ_AZ8_owasp_appsensor}	CAPEC 25, 39, 74, 162, 166, 207	SAFECODE \${AZ_AZ8_safecode}	OWASP Cornucopia Ecommerce Website Edition v1.20-EN	<p><b>AUTHORIZATION</b></p>	<p><b>9</b></p> <p>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</p> <table border="1"> <tr><td>OWASP SCP \${AZ_AZ9_owasp_scp}</td></tr> <tr><td>OWASP ASVS \${AZ_AZ9_owasp_asvs}</td></tr> <tr><td>OWASP APPSENSOR \${AZ_AZ9_owasp_appsensor}</td></tr> <tr><td>CAPEC 26, 29, 119, 261</td></tr> <tr><td>SAFECODE \${AZ_AZ9_safecode}</td></tr> <tr><td>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</td></tr> </table>	OWASP SCP \${AZ_AZ9_owasp_scp}	OWASP ASVS \${AZ_AZ9_owasp_asvs}	OWASP APPSENSOR \${AZ_AZ9_owasp_appsensor}	CAPEC 26, 29, 119, 261	SAFECODE \${AZ_AZ9_safecode}	OWASP Cornucopia Ecommerce Website Edition v1.20-EN	<p><b>AUTHORIZATION</b></p>	<p><b>10</b></p> <p>Richard puede eludir los controles de autorización centralizados ya que no están siendo utilizados exhaustivamente en todas las interacciones</p> <table border="1"> <tr><td>OWASP SCP \${AZ_AZ10_owasp_scp}</td></tr> <tr><td>OWASP ASVS \${AZ_AZ10_owasp_asvs}</td></tr> <tr><td>OWASP APPSENSOR \${AZ_AZ10_owasp_appsensor}</td></tr> <tr><td>CAPEC 36, 95, 121, 179</td></tr> <tr><td>SAFECODE \${AZ_AZ10_safecode}</td></tr> <tr><td>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</td></tr> </table>	OWASP SCP \${AZ_AZ10_owasp_scp}	OWASP ASVS \${AZ_AZ10_owasp_asvs}	OWASP APPSENSOR \${AZ_AZ10_owasp_appsensor}	CAPEC 36, 95, 121, 179	SAFECODE \${AZ_AZ10_safecode}	OWASP Cornucopia Ecommerce Website Edition v1.20-EN
OWASP SCP \${AZ_AZ8_owasp_scp}																							
OWASP ASVS \${AZ_AZ8_owasp_asvs}																							
OWASP APPSENSOR \${AZ_AZ8_owasp_appsensor}																							
CAPEC 25, 39, 74, 162, 166, 207																							
SAFECODE \${AZ_AZ8_safecode}																							
OWASP Cornucopia Ecommerce Website Edition v1.20-EN																							
OWASP SCP \${AZ_AZ9_owasp_scp}																							
OWASP ASVS \${AZ_AZ9_owasp_asvs}																							
OWASP APPSENSOR \${AZ_AZ9_owasp_appsensor}																							
CAPEC 26, 29, 119, 261																							
SAFECODE \${AZ_AZ9_safecode}																							
OWASP Cornucopia Ecommerce Website Edition v1.20-EN																							
OWASP SCP \${AZ_AZ10_owasp_scp}																							
OWASP ASVS \${AZ_AZ10_owasp_asvs}																							
OWASP APPSENSOR \${AZ_AZ10_owasp_appsensor}																							
CAPEC 36, 95, 121, 179																							
SAFECODE \${AZ_AZ10_safecode}																							
OWASP Cornucopia Ecommerce Website Edition v1.20-EN																							
<p><b>AUTHORIZATION</b></p>	<p><b>Q</b></p> <p>Christopher puede injectar un comando para que la aplicación se ejecute con un nivel de privilegios más alto</p> <table border="1"> <tr><td>OWASP SCP \${AZ_AZQ_owasp_scp}</td></tr> <tr><td>OWASP ASVS \${AZ_AZQ_owasp_asvs}</td></tr> <tr><td>OWASP APPSENSOR \${AZ_AZQ_owasp_appsensor}</td></tr> <tr><td>CAPEC 17, 30, 69, 234</td></tr> <tr><td>SAFECODE \${AZ_AZQ_safecode}</td></tr> <tr><td>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</td></tr> </table>	OWASP SCP \${AZ_AZQ_owasp_scp}	OWASP ASVS \${AZ_AZQ_owasp_asvs}	OWASP APPSENSOR \${AZ_AZQ_owasp_appsensor}	CAPEC 17, 30, 69, 234	SAFECODE \${AZ_AZQ_safecode}	OWASP Cornucopia Ecommerce Website Edition v1.20-EN	<p><b>AUTHORIZATION</b></p>	<p><b>K</b></p> <p>Ryan puede influir o alterar controles y permisos de autorización, y por ende puede</p> <table border="1"> <tr><td>OWASP SCP \${AZ_AZK_owasp_scp}</td></tr> <tr><td>OWASP ASVS \${AZ_AZK_owasp_asvs}</td></tr> <tr><td>OWASP APPSENSOR \${AZ_AZK_owasp_appsensor}</td></tr> <tr><td>CAPEC 207, 554</td></tr> <tr><td>SAFECODE \${AZ_AZK_safecode}</td></tr> <tr><td>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</td></tr> </table>	OWASP SCP \${AZ_AZK_owasp_scp}	OWASP ASVS \${AZ_AZK_owasp_asvs}	OWASP APPSENSOR \${AZ_AZK_owasp_appsensor}	CAPEC 207, 554	SAFECODE \${AZ_AZK_safecode}	OWASP Cornucopia Ecommerce Website Edition v1.20-EN	<p>(No Tarjeta)</p>	<p>(No Tarjeta)</p>						
OWASP SCP \${AZ_AZQ_owasp_scp}																							
OWASP ASVS \${AZ_AZQ_owasp_asvs}																							
OWASP APPSENSOR \${AZ_AZQ_owasp_appsensor}																							
CAPEC 17, 30, 69, 234																							
SAFECODE \${AZ_AZQ_safecode}																							
OWASP Cornucopia Ecommerce Website Edition v1.20-EN																							
OWASP SCP \${AZ_AZK_owasp_scp}																							
OWASP ASVS \${AZ_AZK_owasp_asvs}																							
OWASP APPSENSOR \${AZ_AZK_owasp_appsensor}																							
CAPEC 207, 554																							
SAFECODE \${AZ_AZK_safecode}																							
OWASP Cornucopia Ecommerce Website Edition v1.20-EN																							

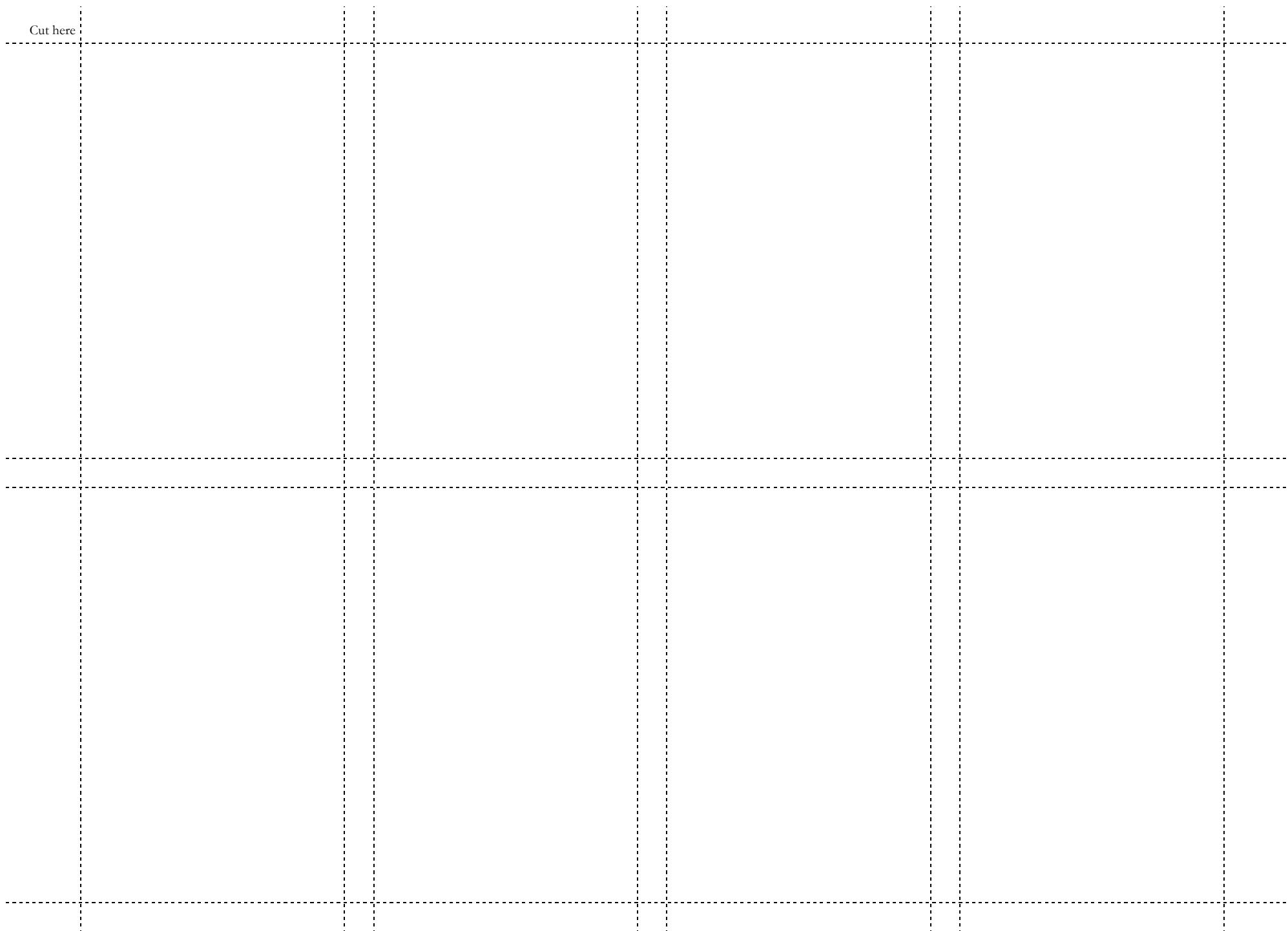
CRYPTOGRAPHY	A	Has inventado un nuevo ataque contra la Criptografía	(No Tarjeta)	CRYPTOGRAPHY	2	Kyun puede acceder a los datos porque ha sido ofuscado en lugar de utilizar una función criptográfica aprobada	CRYPTOGRAPHY	3	Axel puede modificar datos transitorios o permanentes (almacenados o en tránsito), código fuente, actualizaciones / parches o datos de configuración, ya que no están sujetos a verificación de integridad
		<i>Read more about this topic in OWASP's free Cheat Sheets on Cryptographic Storage, and Transport Layer Protection</i>							
CRYPTOGRAPHY	4	Paulo puede acceder a datos en tránsito que no están encriptados, incluso aunque el canal está encriptado		CRYPTOGRAPHY	5	Kyle puede pasar por alto controles criptográficos porque estos no fallan de forma segura (es decir, por defecto no protegen)	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 \${CR_CR4_owasp_scp} OWASP ASVS \${CR_CR4_owasp_asvs} OWASP APPSENSOR \${CR_CR4_owasp_appsensor} CAPEC 185-187 SAFECODE \${CR_CR4_safecode}		CRYPTOGRAPHY		OWASP SCP \${CR_CR5_owasp_scp} OWASP ASVS \${CR_CR5_owasp_asvs} OWASP APPSENSOR \${CR_CR5_owasp_appsensor} CAPEC - SAFECODE \${CR_CR5_safecode}	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

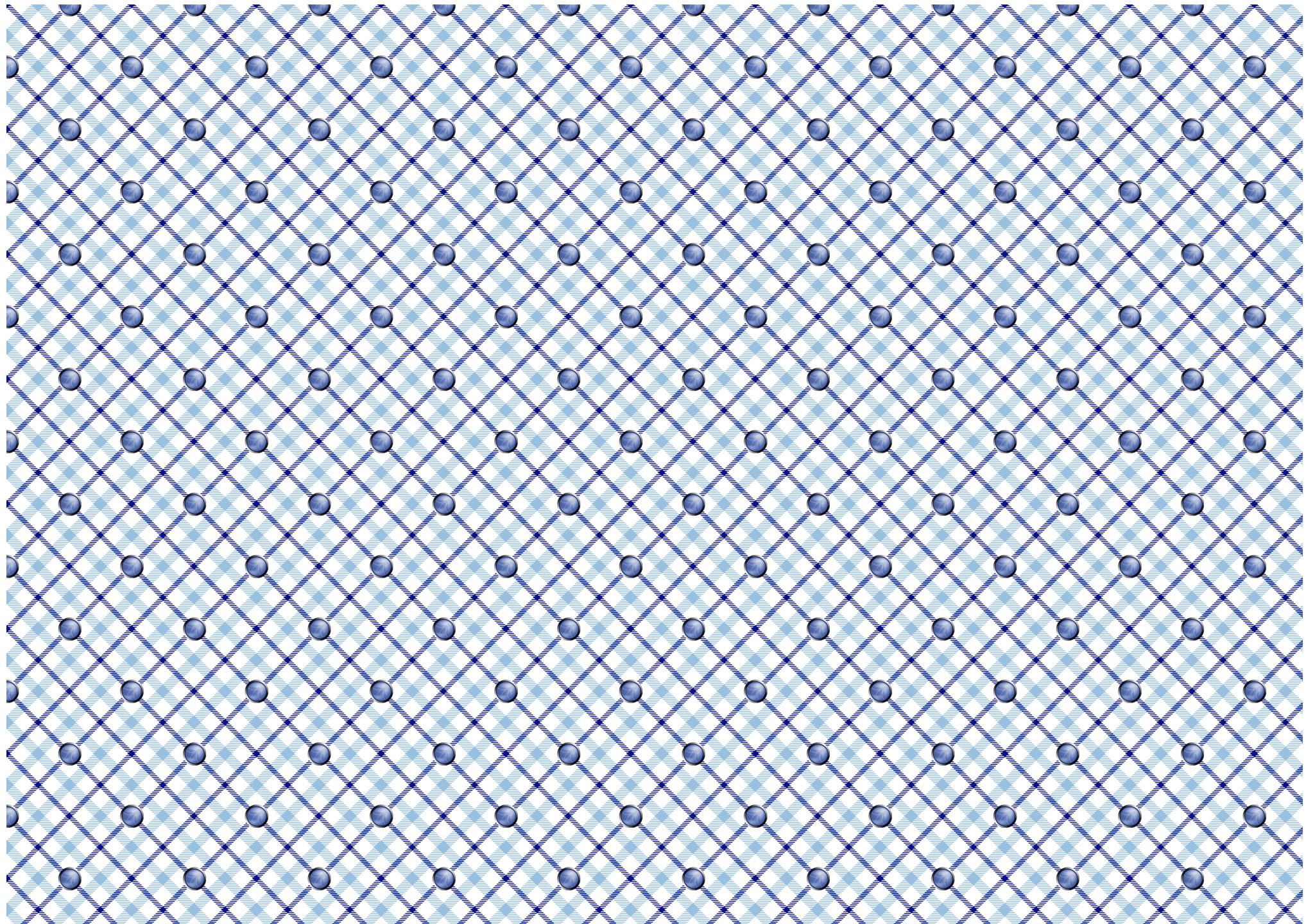
<p><b>CRYPTOGRAPHY</b></p>	<p><b>8</b></p> <p>Eoin puede acceder a los datos comerciales almacenados (por ejemplo, contraseñas, identificadores de sesión, PII, datos del titular de la tarjeta) porque no está cifrado de forma segura ni hash de forma segura</p>	<p><b>CRYPTOGRAPHY</b></p>	<p><b>9</b></p> <p>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</p>
<p>OWASP SCP \${CR_CR8_owasp_scp}</p> <p>OWASP ASVS \${CR_CR8_owasp_asvs}</p> <p>OWASP APPSENSOR \${CR_CR8_owasp_appsensor}</p> <p>CAPEC 31, 37, 55</p> <p>SAFECODE \${CR_CR8_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p>OWASP SCP \${CR_CR9_owasp_sep}</p> <p>OWASP ASVS \${CR_CR9_owasp_asvs}</p> <p>OWASP APPSENSOR \${CR_CR9_owasp_appsensor}</p> <p>CAPEC 97</p> <p>SAFECODE \${CR_CR9_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p>OWASP SCP \${CR_CR10_owasp_sep}</p> <p>OWASP ASVS \${CR_CR10_owasp_asvs}</p> <p>OWASP APPSENSOR \${CR_CR10_owasp_appsensor}</p> <p>CAPEC 97, 463</p> <p>SAFECODE \${CR_CR10_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p>OWASP SCP \${CR_CR10_owasp_scp}</p> <p>OWASP ASVS \${CR_CR10_owasp_asvs}</p> <p>OWASP APPSENSOR \${CR_CR10_owasp_appsensor}</p> <p>CAPEC 116</p> <p>SAFECODE \${CR_CR10_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>
<p><b>CRYPTOGRAPHY</b></p>	<p><b>Q</b></p> <p>Randolph puede acceder o predecir los algoritmos o llaves de los secretos criptográficos</p>	<p><b>CRYPTOGRAPHY</b></p>	<p><b>K</b></p> <p>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</p>
	<p>OWASP SCP \${CR_CRQ_owasp_scp}</p> <p>OWASP ASVS \${CR_CRQ_owasp_asvs}</p> <p>OWASP APPSENSOR \${CR_CRQ_owasp_appsensor}</p> <p>CAPEC 116-117</p> <p>SAFECODE \${CR_CRQ_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p>OWASP SCP \${CR_CRK_owasp_sep}</p> <p>OWASP ASVS \${CR_CRK_owasp_asvs}</p> <p>OWASP APPSENSOR \${CR_CRK_owasp_appsensor}</p> <p>CAPEC 207, 554</p> <p>SAFECODE \${CR_CRK_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p>(No Tarjeta)</p> <p>(No Tarjeta)</p>

	<b>CORNUCOPIA</b>	<b>A</b>	<b>CORNUCOPIA</b>		<b>CORNUCOPIA</b>	<b>2</b>	<b>CORNUCOPIA</b>	<b>3</b>
		Has inventado un nuevo ataque de cualquier tipo		(No Tarjeta)			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	
		<i>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</i>						
	<b>CORNUCOPIA</b>	<b>4</b>	<b>CORNUCOPIA</b>	<b>5</b>	<b>CORNUCOPIA</b>	<b>6</b>	<b>CORNUCOPIA</b>	<b>7</b>
		Keith puede realizar una acción y no es posible atribuirla a él		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)		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 \${CO_CO4_owasp_scp}		OWASP SCP \${CO_CO5_owasp_scp}		OWASP SCP \${CO_CO6_owasp_sep}		OWASP SCP \${CO_CO7_owasp_sep}
		OWASP ASVS \${CO_CO4_owasp_asvs}		OWASP ASVS \${CO_CO5_owasp_asvs}		OWASP ASVS \${CO_CO6_owasp_asvs}		OWASP ASVS \${CO_CO7_owasp_asvs}
		OWASP APPSENSOR \${CO_CO4_owasp_appsensor}		OWASP APPSENSOR \${CO_CO5_owasp_appsensor}		OWASP APPSENSOR \${CO_CO6_owasp_appsensor}		OWASP APPSENSOR \${CO_CO7_owasp_appsensor}
		CAPEC		CAPEC		CAPEC		CAPEC
		-		89, 103, 181, 459		93		93
		SAFECODE \${CO_CO4_safecode}		SAFECODE \${CO_CO5_safecode}		SAFECODE \${CO_CO6_safecode}		SAFECODE \${CO_CO7_safecode}
		OWASP Cornucopia Ecommerce Website Edition v1.20-EN		OWASP Cornucopia Ecommerce Website Edition v1.20-EN		OWASP Cornucopia Ecommerce Website Edition v1.20-EN		OWASP Cornucopia Ecommerce Website Edition v1.20-EN

CORNUCOPIA	8	CORNUCOPIA	9	CORNUCOPIA	10	CORNUCOPIA	J
	<p>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, o los datos se almacenaron localmente, o los datos no se guardaron protegidos físicamente</p> <p>OWASP SCP \${CO_CO8_owasp_sc}</p> <p>OWASP ASVS \${CO_CO8_owasp_asvs}</p> <p>OWASP APPSENSOR \${CO_CO8_owasp_appsensor}</p> <p>CAPEC 37, 220, 310, 436, 536</p> <p>SAFECODE \${CO_CO8_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p>Michael puede pasar por alto la aplicación para acceder a los datos porque las herramientas administrativas o las interfaces administrativas no están aseguradas adecuadamente</p> <p>OWASP SCP \${CO_CO9_owasp_sc}</p> <p>OWASP ASVS \${CO_CO9_owasp_asvs}</p> <p>OWASP APPSENSOR \${CO_CO9_owasp_appsensor}</p> <p>CAPEC 122, 233</p> <p>SAFECODE \${CO_CO9_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p>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)</p> <p>OWASP SCP \${CO_CO10_owasp_sc}</p> <p>OWASP ASVS \${CO_CO10_owasp_asvs}</p> <p>OWASP APPSENSOR \${CO_CO10_owasp_appsensor}</p> <p>CAPEC 68, 438-439, 442, 524, 538</p> <p>SAFECODE \${CO_CO10_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p>OWASP SCP \${CO_CO1_owasp_sc}</p> <p>OWASP ASVS \${CO_CO1_owasp_asvs}</p> <p>OWASP APPSENSOR \${CO_CO1_owasp_appsensor}</p> <p>CAPEC -</p> <p>SAFECODE \${CO_CO1_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p>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</p>		
CORNUCOPIA	Q	CORNUCOPIA	K	JOKER	Joker	JOKER	Joker
	<p>Jim puede emprender acciones maliciosas, no normales sin detección y respuesta por la aplicación en tiempo real</p> <p>OWASP SCP \${CO_COQ_owasp_sc}</p> <p>OWASP ASVS \${CO_COQ_owasp_asvs}</p> <p>OWASP APPSENSOR \${CO_COQ_owasp_appsensor}</p> <p>CAPEC -</p> <p>SAFECODE \${CO_COQ_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p>Gareth puede utilizar la aplicación para negar el servicio a algunos o todos sus usuarios</p> <p>OWASP SCP \${CO_COK_owasp_sc}</p> <p>OWASP ASVS \${CO_COK_owasp_asvs}</p> <p>OWASP APPSENSOR \${CO_COK_owasp_appsensor}</p> <p>CAPEC 2, 25, 119, 125</p> <p>SAFECODE \${CO_COK_safecode}</p> <p>OWASP Cornucopia Ecommerce Website Edition v1.20-EN</p>	<p>Alice puede utilizar la aplicación para atacar los sistemas y datos de los usuarios.</p> <p><i>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.</i></p>		<p>Bob puede influir, alterar o afectar la aplicación para que ya no cumpla con mandatos legales, regulatorios, contractuales u otros mandatos organizacionales</p> <p><i>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</i></p>		

Cut here





## Change Log

Version / Date		Comments
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. 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 2024	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
- 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
- Ken Ferris
- Antonis Manaras
- Dario De Filippis
- Jim Manico
- 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=j5Y0akWj31k>
- 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](https://www.youtube.com/watch?v=Q_LE-8xNXVk)

See the project website for further information and presentation materials.

