|  |  |  |
| --- | --- | --- |
| WHStore:watsonhall:groups:owasp:OWASP_Image_Toolbox:owasp_logo_122106.eps  **Cornucopia**  **Ecommerce Website Edition v1.20-EN**  OWASP Cornucopia is a mechanism to assist software development teams identify security requirements in Agile, conventional and formal development processes  Author  Colin Watson  Project Leaders  Colin Watson and Darío De Filippis  Reviewers  Tom Brennan, Johanna Curiel and Timo Goosen  Acknowledgments  Microsoft SDL Team for the Elevation of Privilege Threat Modelling Game, published under a Creative Commons Attribution license, as the inspiration for Cornucopia and from which many ideas, especially the game theory, were copied.  Keith Turpin and contributors to the “OWASP Secure Coding Practices - Quick Reference Guide”, originally donated to OWASP by Boeing, which is used as the primary source of security requirements information to formulate the content of the cards.  Contributors, supporters, sponsors and volunteers to the OWASP ASVS, AppSensor and Web Framework Security Matrix projects, Mitre’s Common Attack Pattern Enumeration and Classification (CAPEC), and SAFECode’s “Practical Security Stories and Security Tasks for Agile Development Environments” which are all used in the cross-references provided.  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 Darío De Filippis, along with other OWASP volunteers who have helped in many ways.  OWASP does not endorse or recommend commercial products or services  © 2012-2016 OWASP Foundation  This document is licensed under the Creative Commons Attribution-ShareAlike 3.0 license | |  |
| Introduction  The idea behind Cornucopia is to help development teams, especially those using Agile methodologies, to identify application security requirements and develop security-based user stories. Although the idea had been waiting for enough time to progress it, the final motivation came when [SAFECode](http://www.safecode.org/) published its [Practical Security Stories and Security Tasks for Agile Development Environments](http://www.safecode.org/publications/SAFECode_Agile_Dev_Security0712.pdf) in July 2012.  The Microsoft SDL team had already published its super [Elevation of Privilege: The Threat Modeling Game](http://www.microsoft.com/security/sdl/adopt/eop.aspx) (EoP) but that did not seem to address the most appropriate kind of issues that web application development teams mostly have to address. EoP is a great concept and game strategy, and was [published under a](http://blogs.msdn.com/b/sdl/archive/2010/03/02/announcing-elevation-of-privilege-the-threat-modeling-game.aspx) [Creative Commons Attribution License](http://creativecommons.org/licenses/by/3.0/).  Cornucopia Ecommerce Website Edition is based the concepts and game ideas in EoP, but those have been modified to be more relevant to the types of issues ecommerce website developers encounter. It attempts to introduce threat-modelling ideas into development teams that use Agile methodologies, or are more focused on web application weaknesses than other types of software vulnerabilities or are not familiar with STRIDE and DREAD.  Cornucopia Ecommerce Website Edition is referenced as an information resource in the PCI Security Standard Council’s Information Supplement [PCI DSS E-commerce Guidelines](https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_eCommerce_Guidelines.pdf), v2, January 2013.  The card deck (pack)  Instead of EoP’s STRIDE suits (sets of cards with matching designs), Cornucopia suits are based on the structure of the [OWASP Secure Coding Practices - Quick Reference Guide](https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide) (SCP), but with additional consideration of sections in the [OWASP Application Security Verification Standard](https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project), the [OWASP Testing Guide](https://www.owasp.org/index.php/OWASP_Testing_Project) and David Rook’s [Principles of Secure Development](http://www.securityninja.co.uk/secure-development/the-principles-place/). These provided five suits, and a sixth called “Cornucopia” was created for everything else:   * Data validation and encoding (VE) * Authentication (AT) * Session Management (SM) * Authorization (AZ) * Cryptography (CR) * Cornucopia (C)   Similar to poker-playing cards, each suit contains 13 cards (Ace, 2-10, Jack, Queen and King) but, unlike EoP, there are also two Joker cards. The content was mainly drawn from the SCP.  Mappings  The other driver for Cornucopia is to link the attacks with requirements and verification techniques. An initial aim had been to reference [CWE](http://cwe.mitre.org/) weakness IDs, but these proved too numerous, and instead it was decided to map each card to [CAPEC](http://capec.mitre.org/) software attack pattern IDs which themselves are mapped to CWEs, so the desired result is achieved.  Each card is also mapped to the 36 primary security stories in the SAFECode document, as well as to the OWASP SCP v2, ASVS v3.0.1 and [AppSensor](https://www.owasp.org/index.php/OWASP_AppSensor_Project) (application attack detection and response) to help teams create their own security-related stories for use in Agile processes. |  | Game strategy  Apart from the content differences, the game rules are virtually identical to [those for EoP](http://social.technet.microsoft.com/wiki/contents/articles/285.elevation-of-privilege-the-game.aspx).  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](http://www.avery.co.uk/avery/secure/gb_softwaredownload?downloadPath=%2Fuk%2FA-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.  Provide feedback  If you have ideas or feedback on the use of OWASP Cornucopia, please share them. Even better if you create alternative versions of the cards, or produce professional print-ready versions, please share that with the volunteers who created this edition and with the wider application development and application security community.  The best place to use to discuss or contribute is the mailing list for the OWASP project:   * Mailing list <https://lists.owasp.org/mailman/listinfo/owasp_cornucopia> * Project home page <https://www.owasp.org/index.php/OWASP_Cornucopia>   All OWASP documents and tools are free to download and use. OWASP Cornucopia is licensed under the Creative Commons Attribution-ShareAlike 3.0 license. |

|  |  |  |
| --- | --- | --- |
| Instructions  The text on each card describes an attack, but the attacker is given a name, which are unique across all the cards. The name can represent a computer system (e.g. the database, the file system, another application, a related service, a botnet), an individual person (e.g. a citizen, a customer, a client, an employee, a criminal, a spy), or even a group of people (e.g. a competitive organization, activists with a common cause). The attacker might be remote in some other device/location, or local/internal with access to the same device, host or network as the application is running on. The attacker is always named at the start of each description. An example is:  *William has control over the generation of session identifiers*  This means the attacker (William) can create new session identifiers that the application accepts. The attacks were primarily drawn from the security requirements listed in the SCP, v2 but then supplemented with verification objectives from the OWASP “Application Security Verification Standard for Web Applications”, the security focused stories in SAFECode’s “Practical Security Stories and Security Tasks for Agile Development Environments”, and finally a review of the cards in EOP.  Further guidance about each card is available in the online Wiki Deck at <https://www.owasp.org/index.php/Cornucopia_-_Ecommerce_Website_Edition_-_Wiki_Deck>  Lookups between the attacks and five resources are provided on most cards:   * Requirements in “Secure Coding Practices (SCP) - Quick Reference Guide”, v2, OWASP, November 2010 <https://www.owasp.org/index.php/File:OWASP_SCP_Quick_Reference_Guide_v2.pdf> * Verification IDs in “Application Security Verification Standard (ASVS) for Web Applications”, OWASP, v3.0.1, 2016 (excluding sections 18 and 19) <https://www.owasp.org/images/3/33/OWASP_Application_Security_Verification_Standard_3.0.1.pdf> * Attack detection points IDs in “AppSensor”, OWASP, August 2010-2015 <https://www.owasp.org/index.php/AppSensor_DetectionPoints> * IDs in “Common Attack Pattern Enumeration and Classification (CAPEC)”, v2.8, Mitre Corporation, November 2015 <http://capec.mitre.org/data/archive/capec_v2.8.zip> * Security-focused stories in "Practical Security Stories and Security Tasks for Agile Development Environments", SAFECode, July 2012 <http://www.safecode.org/publications/SAFECode_Agile_Dev_Security0712.pdf>   A look-up means the attack is included within the referenced item, but does not necessarily encompass the whole of its intent. 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.  It is possible to play Cornucopia in many different ways. 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> |  | A - Preparations   1. Obtain a deck, or print your own deck of Cornucopia cards (see page 2 of this document) and separate/cut out the cards 2. Identify an application or application process to review; this might be a concept, design or an actual implementation 3. Create a data flow diagram, user stories, or other artefacts to help the review 4. Identify and invite a group of 3-6 architects, developers, testers and other business stakeholders together and sit around a table (try to include someone fairly familiar with application security) 5. Have some prizes to hand (gold stars, chocolate, pizza, beer or flowers depending upon your office culture)   B - Play  One suit - *Cornucopia* - acts as trumps. Aces are high (i.e. they beat Kings). It helps if there is a non-player to document the issues and scores..   1. Remove the Jokers and a few low-score (2, 3, 4) cards from *Cornucopia* suit to ensure each player will have the same number of cards 2. Shuffle the deck and deal all the cards 3. To begin, choose a player randomly who will play the first card - they can play any card from their hand except from the trump suit - *Cornucopia* 4. To play a card, each player must read it out aloud, and explain (see the online Wiki Deck for tips) how the threat could apply (the player gets a point for attacks that might work which the group thinks is an actionable bug) - do not try to think of mitigations at this stage, and do not exclude a threat just because of a belief that it is already mitigated - someone note the card and record the issues raised 5. Play clockwise, each person must play a card in the same way; if you have any card of the matching lead suit you must play one of those, otherwise they can play a card from any other suit. Only a higher card of the same suit, or the highest card in the trump suit *Cornucopia*, wins the hand 6. The person who wins the round, leads the next round (i.e. they play first), and thus defines the next lead suit 7. Repeat until all the cards are played   C - Scoring  The objective is to identify applicable threats, and win hands (rounds):   1. Score +1 for each card you can identify as a valid threat to the application under consideration 2. Score +1 if you win a round 3. Once all cards have been played, whoever has the most points wins   D - Closure   1. Review all the applicable threats and the matching security requirements 2. Create user stories, specifications and test cases as required for your development methodology. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alternative game rules  If you are new to the game, remove the Aces and two Joker cards to begin with. Add the Joker cards back in once people become more familiar with the process. Apart from the “trumps card game” rules described above which are very similar to the EoP, the deck can also be played as the “twenty-one card game” (also known as “pontoon” or “blackjack”) which normally reduces the number of cards played in each round.  Practice on an imaginary application, or even a future planned application, rather than trying to find fault with existing applications until the participants are happy with the usefulness of the game.  Consider just playing with one suit to make a shorter session – but try to cover all the suits for every project. Or even better just play one hand with some pre-selected cards, and score only on the ability to identify security requirements. Perhaps have one game of each suit each day for a week or so, if the participants cannot spare long enough for a full deck.  Some teams have preferred to play a full hand of cards, and then discuss what is on the cards after each round (instead of after each person plays a card).  Another suggestion is that if a player fails to identify the card is relevant, allow other players to suggest ideas, and potentially let them gain the point for the card. Consider allowing extra points for especially good contributions.  You can even play by yourself. Just use the cards to act as thought-provokers. Involving more people will be beneficial though.  In Microsoft's EoP guidance, they recommend cheating as a good game strategy.  Development framework-specific modified card decks  At the end of 2012, the [OWASP Framework Security Matrix](https://www.owasp.org/index.php/Category:Framework_Security_Matrix) was published which documents built in security controls in some commonly used languages and frameworks for web and mobile application development. With [certain provisos](http://blogs.computerworld.com/application-security/21545/security-why-choosing-frameworks-platforms-and-language-matter) it is useful to consider how using these controls can simplify the identification of additional requirements – provided of course the controls are included, enabled and configured correctly.  Consider removing the following cards from the decks if you are confidence they are addressed by the way you are using the language/framework. Items in parentheses are “maybes”. |  | Internal coding standards and libraries  Add your own list of excluded cards based on your organisation’s coding standards (provided they are confirmed by appropriate verification steps in the development lifecycle).   |  |  |  | | --- | --- | --- | | Your coding standards and libraries | | | | Data validation and encoding  *[your list]*  Authentication  *[your list]* | Session management  *[your list]*  Authorization  *[your list]* | Cryptography  *[your list]*  Cornucopia  *[your list]* |   Compliance requirement decks  Create a smaller deck by only including cards for a particular compliance requirement.   |  |  |  | | --- | --- | --- | | Compliance requirement | | | | Data validation and encoding  *[compliance list]*  Authentication  *[compliance list]* | Session management  *[compliance list]*  Authorization  *[compliance list]* | Cryptography  *[compliance list]*  Cornucopia  *[compliance list]* | |

|  |  |  |
| --- | --- | --- |
| Frequently asked questions  *1. Can I copy or edit the game?* Yes of course. All OWASP materials are free to do with as you like provided you comply with the Creative Commons Attribution-ShareAlike 3.0 license. Perhaps if you create a new version, you might donate it to the OWASP Cornucopia Project?  *2. How can I get involved?* Please send ideas or offers of help to the project’s mailing list.  *3. How were the attackers’ names chosen?* EoP begins every description with words like "An attacker can...". These have to be phrased as an attack but I was not keen on the anonymous terminology, wanting something more engaging, and therefore used personal names. These can be thought of as external or internal people or aliases for computer systems. But instead of just random names, I thought how they might reflect the OWASP community aspect. Therefore, apart from "Alice and Bob", I use the given (first) names of current and recent OWASP employees and Board members (assigned in no order), and then randomly selected the remaining 50 or so names from the current list of paying individual OWASP members. No name was used more than once, and where people had provided two personal names, I dropped one part to try to ensure no-one can be easily identified. Names were not deliberately allocated to any particular attack, defence or requirement. The cultural and gender mix simply reflects theses sources of names, and is not meant to be world-representative. In v1.20, the name on VE-10 changed to reflect the project’s new co-leader - this card is also the only one with two names in the attack.  *4. Why aren’t there any images on the card faces?* There is quite a lot of text on the cards, and the cross-referencing takes up space too. But it would be great to have additional design elements included. Any volunteer  *5. Are the attacks ranked by the number on the card?* Only approximately. The risk will be application and organisation dependent, due to varying security and compliance requirements, so your own severity rating may place the cards in some other order than the numbers on the cards.  *6. How long does it take to play a round of cards using the full deck?* This depends upon the amount of discussion and how familiar the players are with application security concepts. But perhaps allow 1.5 to 2.0 hours for 4-6 people.  *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”?* The player can make up any attack they think is valid, but must match the suit of the card e.g. data validation and encoding). 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 refer to the full answer to this question on the project’s web pages at [https://www.owasp.org/index.php/OWASP\_Cornucopia - tab=FAQs](https://www.owasp.org/index.php/OWASP_Cornucopia#tab=FAQs) |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Validación de datos & Codificación** | **A** | **Validación de datos & Codificación** |  | **Validación de datos & Codificación** | **2** | **Validación de datos & Codificación** | **3** |
| Has creado un nuevo ataque contra validación de datos y codificación | (No Tarjeta) | 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 | 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 |
| *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* |  | |  | | --- | | OWASP SCP  69, 107-109, 136, 137, 153, 156, 158, 162 | | OWASP ASVS  1.10, 4.5, 8.1, 11.5, 19.1, 19.5 | | OWASP AppSensor  HT1-3 | | CAPEC  54, 541 | | SAFECode  4, 23 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  8, 9, 11-14, 16, 159, 190, 191 | | OWASP ASVS  5.1, 5.16, 5.17, 5.18, 5.19, 5.20, 11.1, 11.2 | | 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 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Validación de datos & Codificación** | **4** | **Validación de datos & Codificación** | **5** | **Validación de datos & Codificación** | **6** | **Validación de datos & Codificación** | **7** |
| Dave puede ingresar datos o nombres maliciosos en campos porque actualmente no hay una revisión o monitoreo a nivel de usuario o proceso | 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 | Jason puede eludir las rutinas de validación centralizadas, ya que no se utilizan en todas las entradas | 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 robusta |
| |  | | --- | | OWASP SCP  8, 10, 183 | | OWASP ASVS  4.16, 5.16, 5.17, 15.1 | | OWASP AppSensor  RE3-6,AE8-11,SE1,3-6,IE2-4,HT1-3 | | CAPEC  28, 31, 48, 126, 162, 165, 213, 220, 221,261 | | SAFECode  24, 35 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  3, 15, 18-22 168 | | OWASP ASVS  1.7, 5.15, 5.21, 5.22, 5.23 | | OWASP AppSensor  - | | CAPEC  28, 31, 152, 160, 468 | | SAFECode  2, 17 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  3, 168 | | OWASP ASVS  1.7, 5.6, 5.19 | | OWASP AppSensor  IE2-3 | | CAPEC  28 | | SAFECode  3, 16, 24 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  4, 5, 7, 150 | | OWASP ASVS  5.6, 11.8 | | OWASP AppSensor  IE2-3, EE1-2 | | CAPEC  28, 153, 165 | | SAFECode  3, 16, 24 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Validación de datos & Codificación** | **8** | **Validación de datos & Codificación** | **9** | **Validación de datos & Codificación** | **10** | **Validación de datos & Codificación** | **J** |
| Sarah puede pasar por alto las rutinas de sanitización centralizadas ya que no están siendo utilizadas exhaustivamente | 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 | 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) | 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  15, 169 | | OWASP ASVS  1.7, 5.21, 5.23 | | OWASP AppSensor  - | | CAPEC  28, 31, 152, 160, 468 | | SAFECode  2, 17 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  6, 21, 22, 168 | | OWASP ASVS  5.3 | | OWASP AppSensor  IE2-3 | | CAPEC  28 | | SAFECode  3, 16, 24 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  2, 19, 92, 95, 180 | | OWASP ASVS  5.19, 10.6, 16.2, 16.3, 16.4, 16.5, 16.8 | | OWASP AppSensor  IE4, IE5 | | CAPEC  12, 51, 57, 90,111,145,194,195,202,218,463 | | SAFECode  14 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  1, 17 | | OWASP ASVS  5.5, 5.18 | | OWASP AppSensor  RE3, RE4 | | CAPEC  87, 207, 554 | | SAFECode  2, 17 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Validación de datos & Codificación** | **Q** | **Validación de datos & Codificación** | **K** |  |  |  |  |
| 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 | 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 | (No Tarjeta) | (No Tarjeta) |
| |  | | --- | | OWASP SCP  10, 15, 16, 19, 20 | | OWASP ASVS  5.15, 5.22, 5.23, 5.24, 5.25 | | OWASP AppSensor  IE1, RP3 | | CAPEC  28, 31, 152, 160, 468 | | SAFECode  2, 17 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  15, 19-22, 167, 180, 204, 211, 212 | | OWASP ASVS  5.10, 5.11, 5.12, 5.13, 5.14, 5.16, 5.21 | | OWASP AppSensor  CIE1-2 | | CAPEC  23, 28, 76, 152, 160, 261 | | SAFECode  2, 19, 20 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Autenticación** | **A** | **Autenticación** |  | **Autenticación** | **2** | **Autenticación** | **3** |
| Usted tiene inventado un nuevo ataque contra la autenticación | (No Tarjeta) | 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) | 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 |
| *Leer mas sobre este tema en OWASP's free Authentication Cheat Sheet* |  | |  | | --- | | OWASP SCP  47, 52 | | OWASP ASVS  2.12, 8.4, 8.10 | | OWASP AppSensor  UT1 | | CAPEC  - | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  36-7, 40, 43, 48, 51, 119, 139-40, 146 | | OWASP ASVS  2.2, 2.17, 2.24, 8.7, 9.1, 9.4, 9.5, 9.9, 9.11 | | OWASP AppSensor  - | | CAPEC  37, 546 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Autenticación** | **4** | **Autenticación** | **5** | **Autenticación** | **6** | **Autenticación** | **7** |
| Sebastien puede fácilmente identificar nombres de usuario o puede enumerarlos | 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 | 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) | 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, 53 | | OWASP ASVS  2.18, 2.28 | | OWASP AppSensor  AE1 | | CAPEC  383 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  54, 175, 178 | | OWASP ASVS  2.19 | | OWASP AppSensor  AE12, HT3 | | CAPEC  70 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  37, 45, 46, 178 | | OWASP ASVS  2.22 | | OWASP AppSensor  - | | CAPEC  50 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  33, 38, 39, 41, 50, 53 | | OWASP ASVS  2.7, 2.20, 2.23, 2.25, 2.27 | | OWASP AppSensor  AE2, AE3 | | CAPEC  2, 16 | | SAFECode  27 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Autenticación** | **8** | **Autenticación** | **9** | **Autenticación** | **10** | **Autenticación** | **J** |
| Kate puede pasar por alto la autenticación porque ésta no falla de forma segura (es decir, por defecto permite acceso no autenticado) | 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 | 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 | 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  28 | | OWASP ASVS  2.6 | | OWASP AppSensor  - | | CAPEC  115 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  55, 56 | | OWASP ASVS  2.1, 2.9, 2.26, 2.31, 4.15 | | OWASP AppSensor  - | | CAPEC  21 | | SAFECode  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  25, 26, 27 | | OWASP ASVS  1.7, 2.30 | | OWASP AppSensor  - | | CAPEC  90, 115 | | SAFECode  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  23, 32, 34 | | OWASP ASVS  2.1 | | OWASP AppSensor  - | | CAPEC  115 | | SAFECode  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Autenticación** | **Q** | **Autenticación** | **K** |  |  |  |  |
| 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) | Olga puede influir o alterar el código o rutina de autenticación o puede evitarlo | (No Tarjeta) | (No Tarjeta) |
| |  | | --- | | OWASP SCP  23, 29, 42, 49 | | OWASP ASVS  2.1, 2.8 | | OWASP AppSensor  - | | CAPEC  36, 50, 115, 121, 179 | | SAFECode  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  24 | | OWASP ASVS  2.4, 13.2 | | OWASP AppSensor  - | | CAPEC  115, 207, 554 | | SAFECode  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Gestión de Sesión** | **A** | **Gestión de Sesión** |  | **Gestión de Sesión** | **2** | **Gestión de Sesión** | **3** |
| Has inventado un nuevo ataque contra la gestión de sesión | (No Tarjeta) | William tiene el control sobre la generación de identificadores de sesión | Ryan puede usar una sola cuenta en paralelo ya que permite sesiones concurrentes |
| *Read more about this topic in OWASP's free Cheat Sheets on Session Management, and Cross Site Request Forgery (CSRF) Prevention* |  | |  | | --- | | OWASP SCP  58, 59 | | OWASP ASVS  3.10 | | OWASP AppSensor  SE2 | | CAPEC  31, 60, 61 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  68 | | OWASP ASVS  3.16, 3.17, 3.18 | | OWASP AppSensor  - | | CAPEC  - | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Gestión de Sesión** | **4** | **Gestión de Sesión** | **5** | **Gestión de Sesión** | **6** | **Gestión de Sesión** | **7** |
| Alison puede configurar cookies de identificación de sesión en otra aplicación web porque el dominio y la ruta no están suficientemente restringidos | 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 | 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 | 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  59, 61 | | OWASP ASVS  3.12 | | OWASP AppSensor  SE2 | | CAPEC  31, 61 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  60, 62, 66, 67, 71, 72 | | OWASP ASVS  3.2, 3.7, 3.11 | | OWASP AppSensor  SE4-6 | | CAPEC  31 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  64, 65 | | OWASP ASVS  3.3, 3.4, 3.16, 3.17, 3.18 | | OWASP AppSensor  SE5, SE6 | | CAPEC  21 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  62, 63 | | OWASP ASVS  3.2, 3.5 | | OWASP AppSensor  - | | CAPEC  21 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Gestión de Sesión** | **8** | **Gestión de Sesión** | **9** | **Gestión de Sesión** | **10** | **Gestión de Sesión** | **J** |
| Matt puede abusar de sesiones largas porque la aplicación no requiere una autenticación periódica para verificar si los privilegios han cambiado | 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 | 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 | Jeff puede reenviar una interacción de repetición idéntica (por ejemplo, solicitud HTTP, señal, pulsación de botón) y se acepta, no se rechaza |
| |  | | --- | | OWASP SCP  96 | | OWASP ASVS  - | | OWASP AppSensor  - | | CAPEC  21 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  69, 75, 76, 119, 138 | | OWASP ASVS  3.6, 8.7, 10.3 | | OWASP AppSensor  SE4-6 | | CAPEC  31, 60 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  73, 74 | | OWASP ASVS  4.13 | | OWASP AppSensor  IE4 | | CAPEC  62, 111 | | SAFECode  18 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  - | | OWASP ASVS  15.1, 15.2 | | OWASP AppSensor  IE5 | | CAPEC  60 | | SAFECode  12, 14 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Gestión de Sesión** | **Q** | **Gestión de Sesión** | **K** |  |  |  |  |
| Salim puede omitir la administración de sesiones porque no se aplica de manera integral y coherente en toda la aplicación | 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 | (No Tarjeta) | (No Tarjeta) |
| |  | | --- | | OWASP SCP  58 | | OWASP ASVS  3.1 | | OWASP AppSensor  - | | CAPEC  21 | | SAFECode  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  58, 60 | | OWASP ASVS  1.7 | | OWASP AppSensor  - | | CAPEC  21 | | SAFECode  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Autorización** | **A** | **Autorización** |  | **Autorización** | **2** | **Autorización** | **3** |
| Has inventado un nuevo ataque contra la Autorización | (No Tarjeta) | Tim puede influir a donde se envía o reenvía la data | 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 |
| *Read more about this topic in OWASP's Development and Testing Guides* |  | |  | | --- | | OWASP SCP  44 | | OWASP ASVS  4.1, 4.16, 16.1 | | OWASP AppSensor  - | | CAPEC  153 | | SAFECode  8, 10, 11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  51, 100, 135, 139, 140, 141, 150 | | OWASP ASVS  4.1, 8.2, 9.1-9.6, 9.11, 16.6, 16.7 | | OWASP AppSensor  - | | CAPEC  69, 213 | | SAFECode  8, 10, 11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Autorización** | **4** | **Autorización** | **5** | **Autorización** | **6** | **Autorización** | **7** |
| Kelly puede eludir los controles de autorización porque no fallan de forma segura (es decir, por defecto permiten el acceso) | 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) | Eduardo puede acceder a los datos a los que él no tiene permiso, incluso aunque tiene permiso para formulario / página / URL / punto de entrada | Yuanjing puede acceder a funciones de la aplicación, objetos o propiedades a las que él no está autorizado para acceder |
| |  | | --- | | OWASP SCP  79, 80 | | OWASP ASVS  4.8 | | OWASP AppSensor  - | | CAPEC  122 | | SAFECode  8, 10, 11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP 70,81,83-4,87-9, 99,117,131-2,142,154,170,179 | | OWASP ASVS  4.1, 4.4, 4.9,, 19.3 | | OWASP AppSensor  ACE1-4, HT2 | | CAPEC  75, 87, 95, 126, 149, 155, 203, 213, 264-5 | | SAFECode  8, 10, 11, 13 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  81, 88, 131 | | OWASP ASVS  4.1, 4.4 | | OWASP AppSensor  ACE1-4 | | CAPEC  122 | | SAFECode  8, 10, 11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  81, 85, 86, 131 | | OWASP ASVS  4.1, 4.4 | | OWASP AppSensor  ACE1-4 | | CAPEC  122 | | SAFECode  8, 10, 11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Autorización** | **8** | **Autorización** | **9** | **Autorización** | **10** | **Autorización** | **J** |
| 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 | 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 | Richard puede eludir los controles de autorización centralizados ya que no están siendo utilizados exhaustivamente en todas las interacciones | Dinis puede acceder a la información de configuración de seguridad, o listas de control de acceso |
| |  | | --- | | OWASP SCP  10, 32, 93, 94, 189 | | OWASP ASVS  4.10, 4.15, 4.16, 8.13, 15.1 | | OWASP AppSensor  ACE3 | | CAPEC  25, 39, 74, 162, 166, 207 | | SAFECode  8, 10, 11, 12 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  94 | | OWASP ASVS  4.14, 15.2 | | OWASP AppSensor  AE3, FIO1-2, UT2-4, STE1-3 | | CAPEC  26, 29, 119, 261 | | SAFECode  1, 35 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  78, 91 | | OWASP ASVS  1.7, 4.11 | | OWASP AppSensor  ACE1-4 | | CAPEC  36, 95, 121, 179 | | SAFECode  8, 10, 11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  89, 90 | | OWASP ASVS  4.10, 13.2 | | OWASP AppSensor  - | | CAPEC  75, 133, 203 | | SAFECode  8, 10, 11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Autorización** | **Q** | **Autorización** | **K** |  |  |  |  |
| Christopher puede inyectar un comando para que la aplicación se ejecute con un nivel de privilegios más alto | Ryan puede influir o alterar controles y permisos de autorización, y por ende puede | (No Tarjeta) | (No Tarjeta) |
| |  | | --- | | OWASP SCP  209 | | OWASP ASVS  5.12 | | OWASP AppSensor  - | | CAPEC  17, 30, 69, 234 | | SAFECode  8, 10, 11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  77, 89, 91 | | OWASP ASVS  4.9, 4.10, 13.2 | | OWASP AppSensor  - | | CAPEC  207, 554 | | SAFECode  8, 10, 11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Criptografía** | **A** | **Criptografía** |  | **Criptografía** | **2** | **Criptografía** | **3** |
| Has inventado un nuevo ataque contra la Criptografía | (No Tarjeta) | Kyun puede acceder a los datos porque ha sido ofuscado en lugar de utilizar una función criptográfica aprobada | 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 |
| *Read more about this topic in OWASP's free Cheat Sheets on Cryptographic Storage, and Transport Layer Protection* |  | |  | | --- | | OWASP SCP  105, 133, 135 | | OWASP ASVS  - | | OWASP AppSensor  - | | CAPEC  - | | SAFECode  21, 29 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  92, 205, 212 | | OWASP ASVS  8.11, 11.7, 13.2, 19.5, 19.6, 19.7, 19.8 | | OWASP AppSensor  SE1, IE4 | | CAPEC  31, 39, 68, 75, 133, 145, 162, 203,438-9,442 | | SAFECode  12, 14 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Criptografía** | **4** | **Criptografía** | **5** | **Criptografía** | **6** | **Criptografía** | **7** |
| Paulo puede acceder a datos en tránsito que no están encriptados, incluso aunque el canal está encriptado | Kyle puede pasar por alto controles criptográficos porque estos no fallan de forma segura (es decir, por defecto no protegen) | 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 | 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  37, 88, 143, 214 | | OWASP ASVS  7.12, 9.2 | | OWASP AppSensor  - | | CAPEC  185, 186, 187 | | SAFECode  14, 29, 30 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  103, 145 | | OWASP ASVS  7.2, 10.3 | | OWASP AppSensor  - | | CAPEC  - | | SAFECode  21, 29 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  36, 37, 143, 146, 147 | | OWASP ASVS  2.16, 9.2, 9.11, 10.3, 19.2 | | OWASP AppSensor  - | | CAPEC  31, 57, 102, 157, 158, 384, 466, 546 | | SAFECode  29 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  75, 144, 145, 148 | | OWASP ASVS  10.1, 10.5, 10.10, 10.11, 10.12, 10.13, 10.14 | | OWASP AppSensor  IE4 | | CAPEC  31, 216 | | SAFECode  14, 29, 30 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Criptografía** | **8** | **Criptografía** | **9** | **Criptografía** | **10** | **Criptografía** | **J** |
| 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 | 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 | 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 | 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  30, 31, 70, 133, 135 | | OWASP ASVS  2.13, 7.7, 7.8, 9.2 | | OWASP AppSensor  - | | CAPEC  31, 37, 55 | | SAFECode  21, 29, 31 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  60, 104, 105 | | OWASP ASVS  7.6, 7.7, 7.8, 7.15 | | OWASP AppSensor  - | | CAPEC  97 | | SAFECode  14, 21, 29, 32, 33 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  104, 105 | | OWASP ASVS  - | | OWASP AppSensor  - | | CAPEC  97, 463 | | SAFECode  14, 21, 29, 31, 32, 33 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  35, 90, 171, 172 | | OWASP ASVS  2.29 | | OWASP AppSensor  - | | CAPEC  116 | | SAFECode  21, 29 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Criptografía** | **Q** | **Criptografía** | **K** |  |  |  |  |
| Randolph puede acceder o predecir los algoritmos o llaves de los secretos criptográficos | 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 | (No Tarjeta) | (No Tarjeta) |
| |  | | --- | | OWASP SCP  35, 102 | | OWASP ASVS  7.8, 7.9, 7.11, 7.13, 7.14 | | OWASP AppSensor  - | | CAPEC  116, 117 | | SAFECode  21, 29 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  31, 101 | | OWASP ASVS  7.11 | | OWASP AppSensor  - | | CAPEC  207, 554 | | SAFECode  14, 21, 29 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Cornucopia** | **A** | **Cornucopia** |  | **Cornucopia** | **2** | **Cornucopia** | **3** |
| Has inventado un nuevo ataque de cualquier tipo | (No Tarjeta) | Lee puede omitir los controles de la aplicación porque se han usado funciones de lenguaje de programación peligrosas/riesgosas en lugar de alternativas más seguras, o hay errores de conversión de tipo, o porque la aplicación no es confiable cuando un recurso externo no está disponible, o hay race conditions, o hay problemas en la inicialización/asignación de recursos, o pueden ocurrir desbordamientos | 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 |
| *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* |  | |  | | --- | | OWASP SCP  194-202, 205-209 | | OWASP ASVS  5.1 | | OWASP AppSensor  - | | CAPEC  25, 26, 29, 96, 123-4, 128-9, 264-5 | | SAFECode  3, 5-7, 9, 22, 25-26, 34 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  134 | | OWASP ASVS  19.5 | | OWASP AppSensor  - | | CAPEC  189, 207 | | SAFECode  - | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Cornucopia** | **4** | **Cornucopia** | **5** | **Cornucopia** | **6** | **Cornucopia** | **7** |
| 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 | 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  23, 32, 34, 42, 51, 181 | | OWASP ASVS  8.10 | | OWASP AppSensor  - | | CAPEC  - | | SAFECode  - | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  - | | OWASP ASVS  - | | OWASP AppSensor  - | | CAPEC  89, 103, 181, 459 | | SAFECode  - | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  109, 110, 111, 112, 155 | | OWASP ASVS  8.2, 8.4 | | OWASP AppSensor  - | | CAPEC  54, 98, 164 | | SAFECode  4, 11, 23 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  113-115, 117, 118, 121-130 | | OWASP ASVS  2.12, 8.3-8.12, 9.10, 10.4 | | OWASP AppSensor  - | | CAPEC  93 | | SAFECode  4 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Cornucopia** | **8** | **Cornucopia** | **9** | **Cornucopia** | **10** | **Cornucopia** | **J** |
| 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 | Michael puede pasar por alto la aplicación para acceder a los datos porque las herramientas administrativas o las interfaces administrativas no están aseguradas adecuadamente | 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) | 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  151, 152, 156, 160, 161, 173-177 | | OWASP ASVS  19.1, 19.4, 19.6, 19.7, 19.8 | | OWASP AppSensor  RE1, RE2 | | CAPEC  37, 220, 310, 436, 536 | | SAFECode  - | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  23, 29, 56, 81, 82, 84-90 | | OWASP ASVS  2.1, 2.32 | | OWASP AppSensor  - | | CAPEC  122, 233 | | SAFECode  - | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  57, 151, 152, 204, 205, 213, 214 | | OWASP ASVS  1.11- | | OWASP AppSensor  - | | CAPEC  68, 438, 439, 442, 524, 538 | | SAFECode  15 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  90, 137, 148, 151-154, 175-179, 186, 192 | | OWASP ASVS  19.5, 19.9 | | OWASP AppSensor  - | | CAPEC  - | | SAFECode  4 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **Cornucopia** | **Q** | **Cornucopia** | **K** | **Joker** | **Joker** | **Joker** | **Joker** |
| Jim puede emprender acciones maliciosas, no normales sin detección y respuesta por la aplicación en tiempo real | Gareth puede utilizar la aplicación para negar el servicio a algunos o todos sus usuarios | Alice puede utilizar la aplicación para atacar los sistemas y datos de los usuarios. | Bob puede influir, alterar o afectar la aplicación para que ya no cumpla con mandatos legales, regulatorios, contractuales u otros mandatos organizacionales |
| |  | | --- | | OWASP SCP  - | | OWASP ASVS  4.14, 9.8, 15.1, 15.2 | | OWASP AppSensor  (All) | | CAPEC  - | | SAFECode  1, 27 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  41, 55 | | OWASP ASVS  - | | OWASP AppSensor  UT1-4, STE3 | | CAPEC  2, 25, 119, 125 | | SAFECode  1 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | *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.* | *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 |  |  |  |  |  |  |  |  |
|  | **${ }** |  |  |  |  |  | **J** |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |



Change Log

| Version / Date | | Comments |
| --- | --- | --- |
| 0.10 | 30 Jul 2012 | Original draft. |
| 0.20 | 10 Aug 2012 | Draft reviewed and updated. |
| 0.30 | 15 Aug 2012 | Draft announced OWASP SCP mailing list for comment. |
| 0.40 | 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. |
| 1.00 | 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. Alternative rules and deck subset descriptions added. Project website and mailing list added. Cornucopia King cross-reference to AppSensor updated. |
| 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. |
| 1.10 | 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. |
| 1.20 | 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. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 |  * 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 * OWASP NYC for creating an OWASP box design and distributing packs at AppSec USA 2014.   Podcasts and videos  The following supporting OWASP Cornucopia resources are available online:   * Video - Using the cards, created during AppSec EU 2015 project summit, 20th May 2015 <https://www.youtube.com/watch?v=i5Y0akWj31k> * Podcast interview, OWASP 24/7 Podcast channel, 21st March 2014 <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. |  |