|  |  |  |
| --- | --- | --- |
| 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) |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Data validation & encoding** | **A** | **Data validation & encoding** |  | **Data validation & encoding** | **2** | **Data validation & encoding** | **3** |
| Vous avez inventé une nouvelle attaque contre la Validation des Données et l'Encodage | (${Common\_NoCard}) | Brian peut recueillir des informations sur les configurations sous-jacentes, les schémas, la logique, le code, le logiciel, les services et l'infrastructure, de par le contenu des messages d'erreur, ou une mauvaise configuration, ou la présence de fichiers d'installation par défaut, ou des ressources de test, de sauvegarde, de copie, ou l'exposition de code source | Robert peut saisir des données malveillantes, car le format attendu n'est pas vérifié, ou des duplicatas sont acceptés, ou la structure n'est pas vérifiée, ou les éléments individuels des données ne sont pas validées : type, plage, longueur, liste blanche de caractères ou de formats autorisés |
| *Apprenez-en plus à ce sujet dans les antisèches gratuites OWASP sur la Validation des Entrées, la Prévention des XSS, DOM-XSS, et des Injections SQL, ainsi que sur les Requêtes Paramétrées* |  | |  | | --- | | 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 | |
| **Data validation & encoding** | **4** | **Data validation & encoding** | **5** | **Data validation & encoding** | **6** | **Data validation & encoding** | **7** |
| Dave peut saisir des noms de champs ou des données malveillantes, car ils ne sont pas vérifiés dans le contexte de l'utilisateur ou du processus en cours | Jee peut contourner les routines d'encodage centralisées, car celles-ci ne sont pas utilisées partout, ou bien de mauvais encodages sont utilisés | Jason peut contourner les routines d'encodage centralisées, car celles-ci ne sont pas utilisées à chaque saisie | Jan peut générer des messages de sorte à tromper la validation des données, car le jeu de caractères n'est pas spécifié/imposé, ou les données sont encodées plusieurs fois, ou les données ne sont pas pleinement converties dans le format que l'application utilise (par exemple canonicalisation) avant leur validation, ou les variables sont insuffisamment typées |
| |  | | --- | | 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 | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Data validation & encoding** | **8** | **Data validation & encoding** | **9** | **Data validation & encoding** | **10** | **Data validation & encoding** | **J** |
| Sarah peut contourner les routines de sanitisation centralisées, car celles-ci ne sont pas pleinement utilisées | Shamun peut contourner la validation des saisies ou la validation des sorties, car les échecs de validation ne sont pas rejetés et/ou sanitisés | Darío peut exploiter la confiance que l'application place dans une source de données (par exemple données définies par l'utilisateur, manipulation de données stockées localement, changement de déclaration des données sur un système client, manque de vérification de l'identité pendant la validation de données de telle manière que Darío peut se faire passer pour Colin) | Dennis a le contrôle sur la validation des saisies, la validation des sorties, ou le code d'encodage des sorties, ou les routines, de telle manière que celles-ci peuvent être contournées |
| |  | | --- | | 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 | |
| **Data validation & encoding** | **Q** | **Data validation & encoding** | **K** |  |  |  |  |
| Geoff peut injecter des données dans un client ou un système interpréteur, car une interface paramétrée n'est pas utilisée, ou n'a pas été implémentée correctement, ou les données n'ont pas été encodées correctement dans ce contexte, ou il n'y a pas de politique restrictive sur le code ou les ajouts de données | Gabe peut injecter des données dans un interpréteur côté serveur (ex : SQL, commandes OS, Xpath, Server JavaScript, SMTP), car une interface paramétrée fortement typée n'est pas utilisée ou n'a pas été implémentée correctement | (${Common\_NoCard}) | (${Common\_NoCard}) |
| |  | | --- | | 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 | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Authentication** | **A** | **Authentication** |  | **Authentication** | **2** | **Authentication** | **3** |
| Vous avez inventé une nouvelle attaque contre l'Authentification | (${Common\_NoCard}) | James peut entreprendre des fonctions d'authentification sans que l'utilisateur légitime ne s'en aperçoive (par exemple tentative d'authentification, authentification avec des identifiants volés, mise à jour du mot de passe) | Muhammad peut obtenir le mot de passe d'un utilisateur ou d'autres secrets comme des questions de sécurité, de par l'observation pendant la saisie, ou à partir d'un cache local, de la mémoire, en transit, par lecture d'une ressource non protégée, parce qu'ils sont communément répandus, qu'ils n'expirent jamais, que l'utilisateur ne peut pas changer son propre mot de passe |
| *Apprenez-en plus à ce sujet dans les antisèches gratuites OWASP sur l'Authentification* |  | |  | | --- | | 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 | |
| **Authentication** | **4** | **Authentication** | **5** | **Authentication** | **6** | **Authentication** | **7** |
| Sebastien peut facilement identifier les noms des utilisateurs ou peut les énumérer | Javier peut utiliser les identifiants par défaut, de test, ou facilement devinables, ou peut utiliser un ancien compte ou un compte dont l'application n'a pas besoin | Sven peut réutiliser un mot de passe temporaire car l'utilisateur n'a pas besoin de le changer à la première connexion, ou sa durée de vie est trop longue ou n'expire pas, ou sa communication ne nécessite pas de deuxième canal distinct (par exemple voie postale, application mobile, SMS) | Cecilia peut réaliser des attaques de type brute force ou de dictionnaire contre un ou plusieurs comptes sans limitation, ou ses attaques sont simplifiées du fait d'une faible politique de mots de passe (faible complexité, longueur, historique, ou durée de vie insuffisante) |
| |  | | --- | | 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 | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Authentication** | **8** | **Authentication** | **9** | **Authentication** | **10** | **Authentication** | **J** |
| Kate peut contourner l'authentification car son échec n'est pas contrôlé (passage en accès non authentifié) | Claudia peut effectuer davantage de fonctions critiques car l'authentification est trop faible (ex : pas d'authentification forte à deux facteurs), ou la réauthentification n'est pas requise pour ces fonctions | Pravin peut contourner les contrôles d'authentification car un module/framework/service d'authentification, qui est centralisé, standardisé, testé, autorisé, et séparé de la ressource requêtée, n'est pas utilisé | Mark peut accéder à des ressources ou des services parce qu'il n'y a pas d'authentification, ou il a été pensé à tort que l'authentification était prise en compte par un autre système ou réalisée dans une action précédente |
| |  | | --- | | 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 | |
| **Authentication** | **Q** | **Authentication** | **K** |  |  |  |  |
| Jaime peut contourner l'authentification car celle-ci n'est pas implémentée avec la même rigueur dans toutes les fonctionnalités (ex : inscription, changement de mot de passe, recouvrement de mot de passe, déconnexion, administration) ou dans toutes les versions/canaux (ex : site web mobile, appli mobile, site web, API, centre d'appel) | Olga peut influencer ou modifier du code/routines d'authentification de telle manière que celle-ci soit contournée | (${Common\_NoCard}) | (${Common\_NoCard}) |
| |  | | --- | | 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 | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Session management** | **A** | **Session management** |  | **Session management** | **2** | **Session management** | **3** |
| Vous avez inventé une nouvelle attaque contre la Gestion des Sessions | (${Common\_NoCard}) | William a le contrôle sur la génération des identifiants de session | Ryan peut utiliser le même compte en parallèle, puisque les sessions concurrentes sont autorisées |
| *Apprenez-en plus à ce sujet dans les antisèches gratuites OWASP sur la Gestion des Sessions, et sur la prévention des Cross Site Request Forgery (CSRF)* |  | |  | | --- | | 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 | |
| **Session management** | **4** | **Session management** | **5** | **Session management** | **6** | **Session management** | **7** |
| Alison peut régler les cookies d'identification de session vers une autre application web, car le chemin et le domaine sont insuffisamment restreints | John peut prédire ou deviner les identifiants de session car ceux-ci ne sont pas modifiés lorsque le rôle de l'utilisateur change (par exemple pré et post authentification) et lors de la bascule entre communications chiffrées et non chiffrées, ou ne sont pas suffisamment longs et aléatoires, ou ne sont pas changés périodiquement | Gary peut prendre la main sur une session d'un utilisateur car le délai d'attente sur l'inactivité est trop long ou inexistant, ou la même session peut être utilisée depuis plus d'un équipement/site | Casey peut utiliser la session d'Adam après qu'il ait terminé, car il n'existe pas de fonction de déconnexion, ou il ne peut pas se déconnecter facilement, ou la déconnexion ne clôt pas proprement la session |
| |  | | --- | | 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 | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Session management** | **8** | **Session management** | **9** | **Session management** | **10** | **Session management** | **J** |
| Matt peut profiter abusivement de sessions longues car l'application ne réauthentifie pas régulièrement pour vérifier si les privilèges ont changé | Ivan peut voler des identifiants de session car ceux-ci sont transmis via des canaux non sécurisés, ou sont journalisés, ou sont révélés dans les messages d'erreur, ou sont inutilement accessibles par du code que l'attaquant peut influencer ou modifier | Marce peut contrefaire des requêtes car des tokens per-session, ou per-request pour des actions plus critiques (ex : tokens anti-CSRF ou similaires), ne sont pas utilisés lors des actions qui changent l'état d'une session | Jeff peut rejouer une interaction identique (ex : requête HTTP, signal, click sur bouton), celle-ci est acceptée et non rejetée |
| |  | | --- | | 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 | |
| **Session management** | **Q** | **Session management** | **K** |  |  |  |  |
| Salim peut contourner la gestion de session car celle-ci n'est pas globalement et régulièrement appliquée à travers l'application | Peter peut contourner les contrôles de gestion de session car ceux-ci ont été développés en interne, au lieu d'utiliser un framework standard ou un module approuvé et testé | (${Common\_NoCard}) | (${Common\_NoCard}) |
| |  | | --- | | 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 | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Authorization** | **A** | **Authorization** |  | **Authorization** | **2** | **Authorization** | **3** |
| Vous avez inventé une nouvelle attaque contre les Habilitations | (${Common\_NoCard}) | Tim peut modifier l'emplacement où la donnée est envoyée ou renvoyée | Christian peut accéder à des informations auxquelles il n'est pas habilité via un autre canal pour lequel il l'est (ex : résultats de recherche, journaux, reporting) ou parce que celles-ci sont en cache, ou l'information est conservée plus longtemps que nécessaire, ou toute autre fuite de données |
| *Apprenez-en plus à ce sujet dans les guides gratuits OWASP sur le Développement et les Tests* |  | |  | | --- | | 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 | |
| **Authorization** | **4** | **Authorization** | **5** | **Authorization** | **6** | **Authorization** | **7** |
| Kelly peut contourner les contrôles d'habilitation car ils n'échouent pas de façon sécurisée (c'est-à-dire qu'en cas d'échec, retour au comportement par défaut qui est un accès autorisé) | Chad peut accéder à des ressources (services, processus, AJAX, Flash, vidéo, images, documents, fichiers temporaires, données de session, de configuration, propriétés système, registre, journaux) auxquelles il ne devrait pas à cause d'habilitations défaillantes ou de privilèges excessifs (par exemple en n'appliquant pas le principe de moindre privilège) | Eduardo peut avoir accès à des données auxquelles il n'est pas habilité, même s'il a un accès légitime au formulaire/page/ URL/point d'entrée | Yuanjing peut accéder à des fonctions de l'application, des objets ou des propriétés auxquels elle n'est pas habilitée |
| |  | | --- | | 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 | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Authorization** | **8** | **Authorization** | **9** | **Authorization** | **10** | **Authorization** | **J** |
| Tom peut contourner les règles métier en altérant la séquence normale du processus ou du flux, ou en réalisant celui-ci dans un ordre incorrect, ou en manipulant la date et l'heure utilisée par l'application, ou en détournant l'usage d'outils légitimes, ou encore en manipulant les données de contrôle. | Mike peut altérer le fonctionnement d'une application en utilisant une fonctionnalité légitime trop rapidement ou trop fréquemment, ou d'une façon différente de celle qui est prévue, ou consomme les ressources de l'application, ou cause des situations de compétition (accès concurrent), ou surutilise une fonctionnalité | Richard peut contourner les contrôles d'habilitation centralisés puisqu'ils ne sont pas utilisés de façon exhaustive pour toutes les interactions. | Dinis peut accéder à des informations sur la configuration de sécurité, ou des listes des contrôles d'accès |
| |  | | --- | | 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 | |
| **Authorization** | **Q** | **Authorization** | **K** |  |  |  |  |
| Christopher peut injecter une commande que l'application exécutera avec un niveau de privilège plus élevé | Ryan peut influencer ou altérer les contrôles d'habilitations et les permissions, et peut ainsi les contourner | (${Common\_NoCard}) | (${Common\_NoCard}) |
| |  | | --- | | 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 | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Cryptography** | **A** | **Cryptography** |  | **Cryptography** | **2** | **Cryptography** | **3** |
| Vous avez inventé une nouvelle attaque contre la Cryptographie | (${Common\_NoCard}) | Kyun peut accéder aux données parce qu'elles ont été obfusquées au lieu d'être protégées par une fonction de cryptographie approuvée | Axel peut modifier des données temporaires ou permanentes (stockées ou en transit), ou du code source, ou des mises à jour/patchs, ou des données de configuration, parce qu'elles ne sont protégées par aucun contrôle d'intégrité |
| *Apprenez-en plus à ce sujet dans les antisèches gratuites OWASP sur le Stockage Cryptographique et la Protection de la Couche de Transport* |  | |  | | --- | | 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 | |
| **Cryptography** | **4** | **Cryptography** | **5** | **Cryptography** | **6** | **Cryptography** | **7** |
| Paulo peut accéder aux données en transit qui ne sont pas chiffrées, même si le canal de communication est chiffré | Kyle peut contourner les contrôles cryptographiques car ils n'échouent pas de façon sécurisée (c'est-à-dire qu'ils reviennent à leur état non protégé par défaut) | Romain peut lire et modifier des données non chiffrées en mémoire ou en transit (ex. secrets cryptographiques, informations d'identification, identifiants de session, données à caractère personnel et commercialement sensibles), en cours d'utilisation, dans les échanges au sein de l'application, entre l'application et des utilisateurs, entre l'application et des systèmes externes | Gunter peut intercepter ou modifier des données chiffrées en transit parce que le protocole est mal déployé, ou faiblement configuré, ou les certificats sont invalides, or les certificats ne sont pas fiables, ou la connexion peut être dégradée plus faible ou en communication non chiffrée |
| |  | | --- | | 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 | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Cryptography** | **8** | **Cryptography** | **9** | **Cryptography** | **10** | **Cryptography** | **J** |
| Eoin peut accéder à des données métier stockées (par exemple des mots de passe, des identifiants de session, des informations à caractère personnel, des données de titulaires de cartes bancaires) parce qu'elles ne sont pas chiffrées ou hachées de façon sécurisée | Andy peut contourner les fonctions de génération de nombres aléatoires, de génération de GUID aléatoires, de hachage ou de chiffrement parce qu'elles ont été construites par lui-même, ou sont faibles | Susanna peut casser la cryptographie utilisée parce qu'elle n'est pas suffisamment robuste vis-à-vis du niveau de protection requis, ou elle n'est pas suffisamment robuste vis-à-vis de la quantité d'effort que l'attaquant est prêt à faire | Justin peut lire des informations d'identification pour l'accès à des ressources internes ou externes, des services ou d'autres systèmes parce qu'elles sont stockées dans un format non chiffré, ou intégrées dans le code source |
| |  | | --- | | 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 | |
| **Cryptography** | **Q** | **Cryptography** | **K** |  |  |  |  |
| Randolph peut accéder ou prédire les secrets cryptographiques maîtres | Dan peut influencer ou altérer le code/les routines de cryptographie (chiffrement, hachage, signatures numériques, nombre aléatoire et génération de GUID) et peut ainsi les contourner | (${Common\_NoCard}) | (${Common\_NoCard}) |
| |  | | --- | | 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** |
| Vous avez inventé une nouvelle attaque de n'importe quel type | (${Common\_NoCard}) | Lee peut contourner les contrôles applicatifs car des fonctions à risque ont été utilisées à la place d'alternatives plus sûres, ou il y a des erreurs de conversion de type, ou car l'application n'est pas fiable lorsqu'une ressource externe est indisponible, ou il y a des situations d'accès concurrent, des problèmes d'initialisation ou d'allocation de ressources, ou des débordements peuvent survenir | Andrew peut accéder au code source, ou décompiler, ou accéder à la logique métier pour comprendre le fonctionnement de l'application et les secrets qu'elle contient |
| *Apprenez-en plus à propos de la sécurité applicative dans les guides gratuits OWASP : Exigences, Développement, Revue de Code et Tests, antisèches, et framework 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 peut effectuer une action et il n'est pas possible de la lui attribuer. | Larry peut influencer la confiance que les autres parties, y compris les utilisateurs, ont dans l'application, ou abuser de cette confiance ailleurs (par exemple dans une autre application). | Aaron peut contourner les contrôles parce que la gestion des erreurs/exceptions est absente, ou est implémentée de manière incohérente ou partielle, ou ne refuse pas l'accès par défaut (c'est-à-dire que les erreurs doivent mettre fin à l'accès/à l'exécution), ou dépend de la gestion par un autre service ou système. | Les actions de Mwengu ne peuvent pas être étudiées parce qu'il n'y a pas d'enregistrement des événements de sécurité correctement horodaté, parce qu'il n'y a pas de piste d'audit complète, ou parce que ceux-ci peuvent être modifiées ou supprimées par Mwengu, ou parce qu'il n'y a pas de service de centralisation des traces |
| |  | | --- | | 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 peut contourner l'application pour accéder aux données car l'infrastructure réseau et hôte et les services / applications de support n'ont pas été configurés de manière sécurisée, ni la configuration périodiquement vérifiée, ni les correctifs de sécurité appliqués, ou les données sont stockées localement, ou les données ne sont pas physiquement protégées | Michael peut contourner l'application pour accéder aux données car les outils ou les interfaces d'administration ne sont pas sécurisés de manière adéquate | Xavier peut contourner les contrôles de l'application car les frameworks, les bibliothèques et les composants applicatifs contiennent du code malveillant ou des vulnérabilités (par exemple: interne, sur étagère, externalisé, open source, externe) | Roman peut exploiter l'application car elle a été compilée à l'aide d'outils obsolètes ou sa configuration n'est pas sécurisée par défaut, ou les informations de sécurité n'ont pas été documentées et transmises aux équipes opérationnelles |
| |  | | --- | | 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 peut entreprendre des actions malveillantes, non légitimes, sans détection et réponse en temps réel par l'application | Gareth peut utiliser l'application pour refuser le service à certains ou à tous ses utilisateurs | Alice peut utiliser l'application pour attaquer les systèmes et les données des utilisateurs | Bob peut influencer, altérer ou affecter l'application de façon à ce qu'elle ne soit plus conforme aux exigences légales, réglementaires, contractuelles ou autres exigences de l'organisation |
| |  | | --- | | 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 | | *Avez-vous déjà songé à devenir membre OWASP? Tous les outils, conseils et réunions locales sont gratuits pour tous, mais l'adhésion individuelle aide à soutenir le travail de l'OWASP* | *Découvrez comment les vulnérabilités peuvent être corrigées dans les applications de formation de la VM gratuite OWASP Broken Web Applications, ou en utilisant les défis en ligne du Hacking Lab gratuit* |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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. |  |