|  |  |  |
| --- | --- | --- |
| 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  ${Common\_T00110}  ${Common\_T00120}  ${Common\_T00130}  ${Common\_T00140}  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. ${Common\_T00160} 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  ${Common\_T00210}Although the idea had been waiting for enough time to progress it, the final motivation came when published its in July 2012.[SAFECode](http://www.safecode.org/)[Practical Security Stories and Security Tasks for Agile Development Environments](http://www.safecode.org/publications/SAFECode_Agile_Dev_Security0712.pdf)  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/).  ${Common\_T00250} 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 (SCP), but with additional consideration of sections in the , the and David Rook’s . ${Common\_T00320}[OWASP Secure Coding Practices - Quick Reference Guide](https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide)[OWASP Application Security Verification Standard](https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project)[OWASP Testing Guide](https://www.owasp.org/index.php/OWASP_Testing_Project)[Principles of Secure Development](http://www.securityninja.co.uk/secure-development/the-principles-place/)   * 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. ${Common\_T00400}  Mappings  ${Common\_T00510} An initial aim had been to reference weakness IDs, but these proved too numerous, and instead it was decided to map each card to software attack pattern IDs which themselves are mapped to CWEs, so the desired result is achieved.[CWE](http://cwe.mitre.org/)[CAPEC](http://capec.mitre.org/)  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  ${Common\_T00710}  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. ${Common\_T00760}. These card sheets are not inexpensive, so care should be taken in deciding what to print and using what media and printer type.  ${Common\_T00780}The cut lines are shown on the penultimate page of this document, but Avery also produce a landscape A4 template () that can be used as a guide.[A-0017-01\_L.doc](http://www.avery.co.uk/avery/secure/gb_softwaredownload?downloadPath=%2Fuk%2FA-0017-01_L.doc)  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. ${Common\_T00840}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. ${Common\_T00920}  Provide feedback  ${Common\_T01010} 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.  ${Common\_T01030}   * Mailing list <https://lists.owasp.org/mailman/listinfo/owasp_cornucopia> * Project home page <https://www.owasp.org/index.php/OWASP_Cornucopia>   ${Common\_T01080} 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. ${Common\_T01040}. An example is:  *${SM\_SM2\_desc}*  ${Common\_T01060} 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.  ${Common\_T01080}<https://www.owasp.org/index.php/Cornucopia_-_Ecommerce_Website_Edition_-_Wiki_Deck>  ${Common\_T01100}   * 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. ${Common\_T01230}Instead these cards have some general tips in italicized text.  ${Common\_T01250}Here is one way, demonstrated online in a video at , which uses the new (May 2015) score/record sheet at<https://youtu.be/i5Y0akWj31k><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). ${Common\_T01430}.   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  ${Common\_T01610}   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. ${Common\_T01820} 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.  ${Common\_T01840}  ${Common\_T01850}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.  ${Common\_T01880}  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. ${Common\_T01900}  You can even play by yourself. Just use the cards to act as thought-provokers. ${Common\_T01930}  ${Common\_T01940}  ${Common\_T02000}  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.  ${Common\_T02030}Items in parentheses are “maybes”. |  | Internal coding standards and libraries  ${Common\_T02110}   |  |  |  | | --- | --- | --- | | 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  ${Common\_T02310}   |  |  |  | | --- | --- | --- | | 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. ${Common\_T02540}*  *2. How can I get involved? ${Common\_T02560}*  *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. ${Common\_T02640}*  *${Common\_T02650} 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*  *${Common\_T02690} 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. ${Common\_T02740}*  *${Common\_T02750} 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.*  *${Common\_T02790} It is better if that someone else, not playing the game, takes notes about the requirements identified and issues discussed. This could be used as training for a more junior developer, or performed by the project manager. Some organisations have made a recording to review afterwards when the requirements are written up more formally.* |  | *${Common\_T02830} 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.*  *${Common\_T02900} 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? ${Common\_T02940}See*<https://www.owasp.org/index.php/Cornucopia_-_Ecommerce_Website_Edition_-_Wiki_Deck>  *${Common\_T02970} 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) |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **${VE\_suit}** | **A** | **${VE\_suit}** |  | **${VE\_suit}** | **2** | **${VE\_suit}** | **3** |
| ${VE\_VEA\_desc} | (${Common\_NoCard}) | ${VE\_VE2\_desc} | ${VE\_VE3\_desc} |
| *${VE\_VEA\_misc}* |  | |  | | --- | | 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 | |
| **${VE\_suit}** | **4** | **${VE\_suit}** | **5** | **${VE\_suit}** | **6** | **${VE\_suit}** | **7** |
| ${VE\_VE4\_desc} | ${VE\_VE5\_desc} | ${VE\_VE6\_desc} | ${VE\_VE7\_desc} |
| |  | | --- | | 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 | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **${VE\_suit}** | **8** | **${VE\_suit}** | **9** | **${VE\_suit}** | **10** | **${VE\_suit}** | **J** |
| ${VE\_VE8\_desc} | ${VE\_VE9\_desc} | ${VE\_VE10\_desc} | ${VE\_VEJ\_desc} |
| |  | | --- | | OWASP SCP  15, 169 | | OWASP ASVS  1.7, 5.21, 5.23 | | OWASP AppSensor  - | | CAPEC  28, 31, 152, 160, 468 | | SAFECode  2, 17 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  6, 21, 22, 168 | | OWASP ASVS  5.3 | | OWASP AppSensor  IE2-3 | | CAPEC  28 | | SAFECode  3, 16, 24 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  2, 19, 92, 95, 180 | | OWASP ASVS  5.19, 10.6, 16.2, 16.3, 16.4, 16.5, 16.8 | | OWASP AppSensor  IE4, IE5 | | CAPEC  12, 51, 57, 90,111,145,194,195,202,218,463 | | SAFECode  14 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  1, 17 | | OWASP ASVS  5.5, 5.18 | | OWASP AppSensor  RE3, RE4 | | CAPEC  87, 207, 554 | | SAFECode  2, 17 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **${VE\_suit}** | **Q** | **${VE\_suit}** | **K** |  |  |  |  |
| ${VE\_VEQ\_desc} | ${VE\_VEK\_desc} | (${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 | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **${AT\_suit}** | **A** | **${AT\_suit}** |  | **${AT\_suit}** | **2** | **${AT\_suit}** | **3** |
| ${AT\_ATA\_desc} | (${Common\_NoCard}) | ${AT\_AT2\_desc} | ${AT\_AT3\_desc} |
| *${AT\_ATA\_misc}* |  | |  | | --- | | 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 | |
| **${AT\_suit}** | **4** | **${AT\_suit}** | **5** | **${AT\_suit}** | **6** | **${AT\_suit}** | **7** |
| ${AT\_AT4\_desc} | ${AT\_AT5\_desc} | ${AT\_AT6\_desc} | ${AT\_AT7\_desc} |
| |  | | --- | | 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 | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **${AT\_suit}** | **8** | **${AT\_suit}** | **9** | **${AT\_suit}** | **10** | **${AT\_suit}** | **J** |
| ${AT\_AT8\_desc} | ${AT\_AT9\_desc} | ${AT\_AT10\_desc} | ${AT\_ATJ\_desc} |
| |  | | --- | | OWASP SCP  28 | | OWASP ASVS  2.6 | | OWASP AppSensor  - | | CAPEC  115 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  55, 56 | | OWASP ASVS  2.1, 2.9, 2.26, 2.31, 4.15 | | OWASP AppSensor  - | | CAPEC  21 | | SAFECode  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  25, 26, 27 | | OWASP ASVS  1.7, 2.30 | | OWASP AppSensor  - | | CAPEC  90, 115 | | SAFECode  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  23, 32, 34 | | OWASP ASVS  2.1 | | OWASP AppSensor  - | | CAPEC  115 | | SAFECode  14, 28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **${AT\_suit}** | **Q** | **${AT\_suit}** | **K** |  |  |  |  |
| ${AT\_ATQ\_desc} | ${AT\_ATK\_desc} | (${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 | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **${SM\_suit}** | **A** | **${SM\_suit}** |  | **${SM\_suit}** | **2** | **${SM\_suit}** | **3** |
| ${SM\_SMA\_desc} | (${Common\_NoCard}) | ${SM\_SM2\_desc} | ${SM\_SM3\_desc} |
| *${SM\_SMA\_misc}* |  | |  | | --- | | 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 | |
| **${SM\_suit}** | **4** | **${SM\_suit}** | **5** | **${SM\_suit}** | **6** | **${SM\_suit}** | **7** |
| ${SM\_SM4\_desc} | ${SM\_SM5\_desc} | ${SM\_SM6\_desc} | ${SM\_SM7\_desc} |
| |  | | --- | | 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 | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **${SM\_suit}** | **8** | **${SM\_suit}** | **9** | **${SM\_suit}** | **10** | **${SM\_suit}** | **J** |
| ${SM\_SM8\_desc} | ${SM\_SM9\_desc} | ${SM\_SM10\_desc} | ${SM\_SMJ\_desc} |
| |  | | --- | | OWASP SCP  96 | | OWASP ASVS  - | | OWASP AppSensor  - | | CAPEC  21 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  69, 75, 76, 119, 138 | | OWASP ASVS  3.6, 8.7, 10.3 | | OWASP AppSensor  SE4-6 | | CAPEC  31, 60 | | SAFECode  28 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  73, 74 | | OWASP ASVS  4.13 | | OWASP AppSensor  IE4 | | CAPEC  62, 111 | | SAFECode  18 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  - | | OWASP ASVS  15.1, 15.2 | | OWASP AppSensor  IE5 | | CAPEC  60 | | SAFECode  12, 14 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **${SM\_suit}** | **Q** | **${SM\_suit}** | **K** |  |  |  |  |
| ${SM\_SMQ\_desc} | ${SM\_SMK\_desc} | (${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 | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **${AZ\_suit}** | **A** | **${AZ\_suit}** |  | **${AZ\_suit}** | **2** | **${AZ\_suit}** | **3** |
| ${AZ\_AZA\_desc} | (${Common\_NoCard}) | ${AZ\_AZ2\_desc} | ${AZ\_AZ3\_desc} |
| *${AZ\_AZA\_misc}* |  | |  | | --- | | 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 | |
| **${AZ\_suit}** | **4** | **${AZ\_suit}** | **5** | **${AZ\_suit}** | **6** | **${AZ\_suit}** | **7** |
| ${AZ\_AZ4\_desc} | ${AZ\_AZ5\_desc} | ${AZ\_AZ6\_desc} | ${AZ\_AZ7\_desc} |
| |  | | --- | | 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 | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **${AZ\_suit}** | **8** | **${AZ\_suit}** | **9** | **${AZ\_suit}** | **10** | **${AZ\_suit}** | **J** |
| ${AZ\_AZ8\_desc} | ${AZ\_AZ9\_desc} | ${AZ\_AZ10\_desc} | ${AZ\_AZJ\_desc} |
| |  | | --- | | OWASP SCP  10, 32, 93, 94, 189 | | OWASP ASVS  4.10, 4.15, 4.16, 8.13, 15.1 | | OWASP AppSensor  ACE3 | | CAPEC  25, 39, 74, 162, 166, 207 | | SAFECode  8, 10, 11, 12 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  94 | | OWASP ASVS  4.14, 15.2 | | OWASP AppSensor  AE3, FIO1-2, UT2-4, STE1-3 | | CAPEC  26, 29, 119, 261 | | SAFECode  1, 35 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  78, 91 | | OWASP ASVS  1.7, 4.11 | | OWASP AppSensor  ACE1-4 | | CAPEC  36, 95, 121, 179 | | SAFECode  8, 10, 11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  89, 90 | | OWASP ASVS  4.10, 13.2 | | OWASP AppSensor  - | | CAPEC  75, 133, 203 | | SAFECode  8, 10, 11 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **${AZ\_suit}** | **Q** | **${AZ\_suit}** | **K** |  |  |  |  |
| ${AZ\_AZQ\_desc} | ${AZ\_AZK\_desc} | (${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 | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **${CR\_suit}** | **A** | **${CR\_suit}** |  | **${CR\_suit}** | **2** | **${CR\_suit}** | **3** |
| ${CR\_CRA\_desc} | (${Common\_NoCard}) | ${CR\_CR2\_desc} | ${CR\_CR3\_desc} |
| *${CR\_CRA\_misc}* |  | |  | | --- | | 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 | |
| **${CR\_suit}** | **4** | **${CR\_suit}** | **5** | **${CR\_suit}** | **6** | **${CR\_suit}** | **7** |
| ${CR\_CR4\_desc} | ${CR\_CR5\_desc} | ${CR\_CR6\_desc} | ${CR\_CR7\_desc} |
| |  | | --- | | 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 | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **${CR\_suit}** | **8** | **${CR\_suit}** | **9** | **${CR\_suit}** | **10** | **${CR\_suit}** | **J** |
| ${CR\_CR8\_desc} | ${CR\_CR9\_desc} | ${CR\_CR10\_desc} | ${CR\_CRJ\_desc} |
| |  | | --- | | OWASP SCP  30, 31, 70, 133, 135 | | OWASP ASVS  2.13, 7.7, 7.8, 9.2 | | OWASP AppSensor  - | | CAPEC  31, 37, 55 | | SAFECode  21, 29, 31 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  60, 104, 105 | | OWASP ASVS  7.6, 7.7, 7.8, 7.15 | | OWASP AppSensor  - | | CAPEC  97 | | SAFECode  14, 21, 29, 32, 33 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  104, 105 | | OWASP ASVS  - | | OWASP AppSensor  - | | CAPEC  97, 463 | | SAFECode  14, 21, 29, 31, 32, 33 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  35, 90, 171, 172 | | OWASP ASVS  2.29 | | OWASP AppSensor  - | | CAPEC  116 | | SAFECode  21, 29 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **${CR\_suit}** | **Q** | **${CR\_suit}** | **K** |  |  |  |  |
| ${CR\_CRQ\_desc} | ${CR\_CRK\_desc} | (${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 | |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **${CO\_suit}** | **A** | **${CO\_suit}** |  | **${CO\_suit}** | **2** | **${CO\_suit}** | **3** |
| ${CO\_COA\_desc} | (${Common\_NoCard}) | ${CO\_CO2\_desc} | ${CO\_CO3\_desc} |
| *${CO\_COA\_misc}* |  | |  | | --- | | 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 | |
| **${CO\_suit}** | **4** | **${CO\_suit}** | **5** | **${CO\_suit}** | **6** | **${CO\_suit}** | **7** |
| ${CO\_CO4\_desc} | ${CO\_CO5\_desc} | ${CO\_CO6\_desc} | ${CO\_CO7\_desc} |
| |  | | --- | | 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 | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **${CO\_suit}** | **8** | **${CO\_suit}** | **9** | **${CO\_suit}** | **10** | **${CO\_suit}** | **J** |
| ${CO\_CO8\_desc} | ${CO\_CO9\_desc} | ${CO\_CO10\_desc} | ${CO\_COJ\_desc} |
| |  | | --- | | OWASP SCP  151, 152, 156, 160, 161, 173-177 | | OWASP ASVS  19.1, 19.4, 19.6, 19.7, 19.8 | | OWASP AppSensor  RE1, RE2 | | CAPEC  37, 220, 310, 436, 536 | | SAFECode  - | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  23, 29, 56, 81, 82, 84-90 | | OWASP ASVS  2.1, 2.32 | | OWASP AppSensor  - | | CAPEC  122, 233 | | SAFECode  - | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  57, 151, 152, 204, 205, 213, 214 | | OWASP ASVS  1.11- | | OWASP AppSensor  - | | CAPEC  68, 438, 439, 442, 524, 538 | | SAFECode  15 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  90, 137, 148, 151-154, 175-179, 186, 192 | | OWASP ASVS  19.5, 19.9 | | OWASP AppSensor  - | | CAPEC  - | | SAFECode  4 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | |
| **${CO\_suit}** | **Q** | **${CO\_suit}** | **K** | **${WC\_suit}** | **${WC\_Joker}** | **${WC\_suit}** | **${WC\_Joker}** |
| ${CO\_COQ\_desc} | ${CO\_COK\_desc} | ${WC\_JokerA\_desc} | ${WC\_JokerB\_desc} |
| |  | | --- | | OWASP SCP  - | | OWASP ASVS  4.14, 9.8, 15.1, 15.2 | | OWASP AppSensor  (All) | | CAPEC  - | | SAFECode  1, 27 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | |  | | --- | | OWASP SCP  41, 55 | | OWASP ASVS  - | | OWASP AppSensor  UT1-4, STE3 | | CAPEC  2, 25, 119, 125 | | SAFECode  1 | | OWASP Cornucopia Ecommerce Website Edition v1.20-EN | | *${WC\_JokerA\_misc}* | *${WC\_JokerB\_misc}* |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | ${Common\_T03180} |
| 0.40 | 25 Feb 2013 | ${Common\_T03200}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 | ${Common\_T03270}. 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. ${Common\_T03400}Project contributors added. |
| 1.03 | 18 Sep 2013 | ${Common\_T03430}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 | ${Common\_T03480} |
| 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. ${Common\_T03570} |
| 1.20 | 29 Jun 2016 | Video mentioned/linked. Separate score sheet mentioned/linked. ${Common\_T03610}. 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. ${Common\_T03830}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  ${Common\_T03910}   * 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>   ${Common\_T03980} |  |