© 2012-2024 OWASP Foundation

OWASP
The Open Web Application Security Project

Cornucopia

Edição de Ecomércio v1.30-PT-BR

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 Grant Ongers

Reviewers
Tom Brennan, Johanna Curiel, Darío De Filippis 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 Grant Ongers, along with other OWASP volunteers who have helped in many ways.

OWASP does not endorse or recommend commercial products or services © 2012-2024 OWASP Foundation
This document is licensed under the Creative Commons Attribution-ShareAlike 3.0 license

© 2012-2024 OWASP Foundation

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 published its Practical Security Stories and Security Tasks for Agile Development Environments in July 2012.

The Microsoft SDL team had already published its super Elevation of Privilege: The Threat Modeling Game (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 Creative Commons Attribution License.

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, 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 (SCP), but with additional consideration of sections in the OWASP Application Security Verification Standard, the OWASP Testing Guide and David Rook's Principles of Secure Development. 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)

Smilar 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 weakness IDs, but these proved too numerous, and instead it was decided to map each card to CAPEC 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 v4.0 and AppSensor (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.

Printing the cards

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

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

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

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

Customization

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

© 2012-2024 OWASP Foundation

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.

Instruções

O texto em cada carta descreve um ataque, sendo escolhido um nome para o atacante, o texto é único entre todas as cartas do jogo. O nome pode representar um sistema de computador (por exemplo um banco de dados, um sistema de arquivos, outra aplicação qualquer, um serviço relativo, um botnet), um indivíduo (por exemplo um cidadão, um cliente, um colaborador, um criminoso, um espião), ou até mesmo um grupo de pessoas (por exemplo uma organização competitiva, ativistas com uma causa em comum). O atacante pode estar remoto em algum outro aparelho/localização, ou local/interno com acesso ao mesmo aparelho, host ou rede na qual a aplicação está rodando. O atacante sempre é nomeado no começo de cada descrição. Um exemplo segue:

William tem o controle sobre a geração de identificadores de sessão

Isso significa que o atacante (William) pode criar novos identificadores de sessão que a aplicação aceita. Os ataques foram inicialmente desenhados a partir dos requisitos listados no SCP 'Secure Coding Practices' v2, suplementados com a verificação de objetivos do OWASP ' Application Security Verification Standard for Web Applications', com histórias focadas em segurança contidas em SAFECode's 'Practical Security Sotires and Security Tasks for Agile Development Environments', e finalmente com uma revisão das cartas junto com EOP 'Elevation of Privilege': 'The Threat Modeling Game' criado pelo time da Microsoft SDL.

Um guia mais aprofundado sobre cada carta está disponível no Wiki Deck em (ref: Cornucopia Wiki Deck)

Gabaritos entre os ataques e as cinco fontes estão providas na maioria das cartas:

- Requisitos em “Secure Coding Practices (SCP) - Quick Reference Guide”, v2, OWASP, Novembro 2010 (ref: OWASP SCP Quick Reference Guide v2.1)
- Verification IDs in “Application Security Verification Standard (ASVS) for Web Applications” (ref: ASVS v3 and v4 downloads)
- Attack detection points IDs in “AppSensor”, OWASP, Agosto 2010-2015 (ref: AppSensor DetectionPoints)
- IDs in “Common Attack Pattern Enumeration and Classification (CAPEC)”, v2.8, Mitre Corporation, Novembro 2015 (ref: capec (31. July 2018)
- Security-focused stories in 'Practical Security Stories and Security Tasks for Agile Development Environments', SAFECode, Julho 2012 (ref: SAFECode Agile Dev Security)

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 (ref: Cornucopia scoresheet) , which uses the new (May 2015) score/record sheet at

© 2012-2024 OWASP Foundation

PREPAROS

Compre um baralho, ou imprima o seu próprio baralho de cartas Cornucopia (veja a página 2 deste documento
Identifique uma aplicação ou o processo de uma aplicação para revisar; podendo ser um conceito, um design ou uma implementação
Criar um diagrama de fluxo de dados, user stories, ou outros diagramas para ajudar a revisão
Identificar e convidar um grupo de 3-6 arquitetos, desenvolvedores, testers e outros stakeholders, juntá-los e se sentar ao redor de uma mesa (tente incluir alguém suficientemente familiar com segurança de aplicações)
Tenha alguns prêmios para entregar (estrelas douradas, pizza, cerveja ou flores dependendo da cultura da sua empresa

JOGO

Um naipe – Cornucopia – age como o mais forte. Áses são altos neste jogo (eles ganham de Reis). Fica mais fácil se alguém que não está jogando documente os problemas e as pontuações.

Retire os coringas e algumas cartas de pontuação baixa (2, 3, 4) do naipe Cornucopia para garantir que cada jogador tenha o mesmo número de cartas.
Embaralhe o baralho e dê as cartas
Para começar, escolha aleatoriamente quem irá jogar a primeira carta – pode-se jogar qualquer carta da sua mão com exceção do naipe mais forte – Cornucopia
Para jogar uma carta, cada jogar deve lê-la em voz alta, e explicar (veja as dicas do Wiki Deck na internet) como a ameaça pode ser aplicada (o jogador ganha um ponto por ataques que podem funcionar o qual o grupo acha que é um possível bug)
Jogue em sentido horário, cada jogador deve jogar a carta do mesmo modo, se você tem alguma carta do mesmo naipe que foi jogado você deve jogá-la, caso contrário pode-se jogar uma carta de qualquer outro naipe.
Apenas a carta mais alta do mesmo naipe, ou a mais alta do naipe Cornucopia ganha a mão
O jogador que ganhar a rodada, começa a próxima mão, decidindo assim o próximo naipe
Repita o modo de jogo até que todas as cartas tenham sido jogadas

C - Scoring

The objective is to identify applicable threats, and win hands (rounds):

C1. Score +1 for each card you can identify as a valid threat to the application under consideration
C2. Score +1 if you win a round
C3. Once all cards have been played, whoever has the most points wins

D - Closure

D1. Review all the applicable threats and the matching security requirements
D2. Create user stories, specifications and test cases as required for your development methodology.

© 2012-2024 OWASP Foundation

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 was published which documents built in security controls in some commonly used languages and frameworks for web and mobile application development. With certain provisos 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	Session management	Cryptography
[your list]	*[your list]*	*[your list]*
Authentication	Authorization	Cornucopia
[your list]	*[your list]*	*[your list]*

Compliance requirement decks

Create a smaller deck by only including cards for a particular compliance requirement.

Compliance requirement		
Data validation and encoding	Session management	Cryptography
[compliance list]	*[compliance list]*	*[compliance list]*
Authentication	Authorization	Cornucopia
[compliance list]	*[compliance list]*	*[compliance list]*

© 2012-2024 OWASP Foundation

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

© 2012-2024 OWASP Foundation

DATA VALIDATION & ENCODING

A

Você inventou um novo ataque contra a Validação de Dados de Entrada e Codificação de Dados de Saída

Leia mais sobre este tópico em OWASP Cheat Sheets. Pesquise sobre validação dos dados de entrada, Prevenção de XSS(Cross-site Scripting), Prevenção do DOM baseado em XSS, Prevenção de SQL Injection e Parametrização de Consultas

DATA VALIDATION & ENCODING

(Nenhum Cartão)

DATA VALIDATION & ENCODING

2

Brian consegue reunir o básico de informações sobre a utilização e configuração de base de dados, lógica, codificação, além da utilização de softwares, serviços e infraestrutura nas mensagens de erro ou em mensagens de configuração, ou na presença de arquivos de instalação (padrões ou antigos), ou em evidências de testes, ou em backups ou em exposição de código fonte

OWASP SCP
69, 107-109, 136-137, 153, 156, 158, 162

OWASP ASVS
1.6.4, 2.10.4, 4.3.2, 7.1.1, 10.2.3, 14.1.1, 14.2.2, 14.3.3

OWASP APPSENSOR
HT1-3

CAPEC
54, 541

SAFECODE
4, 23

DATA VALIDATION & ENCODING

3

Robert consegue inserir dados maliciosos pois o formato de protocolo não foi checado, ou duplicações são aceitas, ou a estrutura não está sendo verificada, ou os dados individuais não foram validados por formato, tipo, intervalo, tamanho e por uma lista de caracteres ou formatos possíveis

OWASP SCP
-

OWASP ASVS
1.5.3, 5.1.1-5.1.4, 13.2.1, 14.1.2, 14.4.1

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

DATA VALIDATION & ENCODING

4

Dave consegue inserir nomes ou dados de campos mal intencionados porque isto não está sendo verificado no contexto de cada usuário e processo

OWASP SCP
8, 10, 183

OWASP ASVS
4.2.1, 5.1.1, 5.1.2, 11.1.1, 11.1.2

OWASP APPSENSOR
RE3-6, AE8-11, SE1, SE3-6, IE2-4, HT1-3

CAPEC
28, 31, 48, 126, 162, 165, 213, 220-221, 261

SAFECODE
24, 35

DATA VALIDATION & ENCODING

5

Jee consegue ignorar as rotinas centralizadas de codificação de saída pois elas não estão sendo usadas em todos os lugares, ou a codificação errada está sendo usada

OWASP SCP
3, 15, 18-22, 168

OWASP ASVS
1.1.6, 5.3.3, 5.2.1, 5.2.2, 5.2.5

OWASP APPSENSOR
-

CAPEC
28, 31, 152, 160, 468

SAFECODE
2, 17

DATA VALIDATION & ENCODING

6

Jason consegue ignorar as rotinas centralizadas de validação de dados de entrada pois elas não estão sendo usadas em todos os campos de entrada de dados

OWASP SCP
3, 168

OWASP ASVS
1.1.6, 1.5.3, 5.1.3, 13.2.2, 13.2.5

OWASP APPSENSOR
IE2-3

CAPEC
28

SAFECODE
3, 16, 24

DATA VALIDATION & ENCODING

7

Jan consegue carregar/enviar informações especiais visando evitar validações de campos porque o conjunto de caracteres não é especificado e aplicado, ou o dado de entrada é codificado diversas vezes, ou o dado não é totalmente convertido no mesmo formado que a aplicação usa (ex: canonicalização) antes da validação, ou as variáveis não são fortemente tipadas

OWASP SCP
4-5, 7, 150

OWASP ASVS
1.5.3, 13.2.2, 13.2.5

OWASP APPSENSOR
IE2-3, EE1-2

CAPEC
28, 153, 165

SAFECODE
3, 16, 24

© 2012-2024 OWASP Foundation

DATA VALIDATION & ENCODING

8

Sarah consegue ignorar as rotinas centralizadas de tratamento (sanitização) pois elas não estão sendo usadas de forma abrangente

OWASP SCP
15, 169

OWASP ASVS
1.1.6, 5.2.2, 5.2.5

OWASP APPSENSOR
-

CAPEC
28, 31, 152, 160, 468

SAFECODE
2, 17

OWASP Cornucopia Edição de Ecomércio v1.30-PT-BR

DATA VALIDATION & ENCODING

9

Shamun consegue ignorar as verificações de validação de entrada ou de saída porque as falhas de validação não são rejeitadas e/ou tratadas (sanitização)

OWASP SCP
6, 21-22, 168

OWASP ASVS
7.1.3

OWASP APPSENSOR
IE2-3

CAPEC
28

SAFECODE
3, 16, 24

OWASP Cornucopia Edição de Ecomércio v1.30-PT-BR

DATA VALIDATION & ENCODING

10

Dario consegue explorar a confiabilidade da aplicação em fonte de dados (ex: dados definidos pelo usuário, manipulação de dados armazenados localmente, mudança do estado dos dados em dispositivos clientes, falta de verificação da identidade durante uma validação de dados, como Dario pode fingir ser Colin)

OWASP SCP
2, 19, 92, 95, 180

OWASP ASVS
1.12.2, 5.1.3, 9.2.3, 12.2.1, 12.3.1-12.3.3, 12.4.2, 12.5.2, 14.5.3

OWASP APPSENSOR
IE4, IE5

CAPEC
12, 51, 57, 90, 111, 145, 194-195, 202, 218, 463

SAFECODE
14

OWASP Cornucopia Edição de Ecomércio v1.30-PT-BR

DATA VALIDATION & ENCODING

J

Dennis tem o controle sobre validações de entrada de dados, validações de saída de dados ou codificação de saída ou rotinas que ele consegue ignorar/burlar

OWASP SCP
1, 17

OWASP ASVS
1.5.3

OWASP APPSENSOR
RE3, RE4

CAPEC
87, 207, 554

SAFECODE
2, 17

OWASP Cornucopia Ecommerce Website Edition v1.20-EN

DATA VALIDATION & ENCODING

Q

Geoff consegue injetar dados num dispositivo ou num interpretador no lado do cliente porque uma interface parametrizada não foi usada, ou não foi implementada corretamente, ou os dados não foram codificados corretamente para o contexto proposto, ou não há uma política restritiva para a codificação ou a inclusão de dados

OWASP SCP
10, 15-16, 19-20

OWASP ASVS
5.2.1, 5.2.5, 5.3.3, 5.5.4

OWASP APPSENSOR
IE1, RP3

CAPEC
28, 31, 152, 160, 468

SAFECODE
2, 17

OWASP Cornucopia Edição de Ecomércio v1.30-PT-BR

DATA VALIDATION & ENCODING

K

Gabe consegue injetar dados num interpretador no lado do servidor (ex: SQL, comandos para o sistema operacional, Xpath, Server JavaScript, SMTP) porque uma interface parametrizada não foi usada ou não foi implementada corretamente

OWASP SCP
15, 19-22, 167, 180, 204, 211-212

OWASP ASVS
5.2.1, 5.2.2, 5.3.4, 5.3.7-5.3.10

OWASP APPSENSOR
CIE1, CIE2

CAPEC
23, 28, 76, 152, 160, 261

SAFECODE
2, 19-20

OWASP Cornucopia Edição de Ecomércio v1.30-PT-BR

(Nenhum Cartão)

(Nenhum Cartão)

© 2012-2024 OWASP Foundation

AUTHENTICATION

A

Você inventou um novo ataque contra a Autenticação e Gerenciamento de Credenciais

Leia mais sobre este tópico em OWASP Authentication Cheat Sheet

AUTHENTICATION

(Nenhum Cartão)

AUTHENTICATION

2

James pode assumir as funções de autenticação sem que o usuário real esteja ciente do uso destas funções (ex: tente fazer login, logar com credenciais, redefinir a senha)

OWASP SCP
47, 52
OWASP ASVS
2.5.2, 7.1.2, 7.1.4, 7.2.1, 8.2.1-8.2.3, 8.3.6
OWASP APPSENSOR
UT1
CAPEC
-
SAFECODE
28

AUTHENTICATION

3

Muhammad consegue obter a senha de um usuário ou outros dados, pela observação durante a autenticação, ou cache local, ou pela memória, ou pelo tráfego de dados, ou pela leitura de algum local desprotegido, ou porque isto é amplamente conhecido, ou porque não há expiração de dados, ou por que o usuário não consegue trocar sua própria senha

OWASP SCP
36-37, 40, 43, 48, 51, 119, 139-140, 146
OWASP ASVS
2.5.2, 2.5.3
OWASP APPSENSOR
-
CAPEC
37, 546
SAFECODE
28

AUTHENTICATION

4

Sebastien pode identificar facilmente nomes de usuários ou consegue elencar quem eles são

OWASP SCP
33, 53
OWASP ASVS
2.2.1, 4.1.5
OWASP APPSENSOR
AE1
CAPEC
383
SAFECODE
28

AUTHENTICATION

5

Javier pode usar credenciais padrões (default), de teste ou facilmente adivinhadas para autenticação, ou consegue autenticar através de contas inativas ou autentica-se por contas não necessariamente da aplicação

OWASP SCP
54, 175, 178
OWASP ASVS
4.1.5
OWASP APPSENSOR
AE12, HT3
CAPEC
70
SAFECODE
28

AUTHENTICATION

6

Sven consegue reutilizar uma senha temporária porque o usuário não precisa troca-la no primeiro acesso, ou o tempo de expiração é muito longo, ou o tempo de expiração não existe, ou não é usado um método de entrega out-of-band (ex: aplicação mobile, SMS)

OWASP SCP
37, 45-46, 178
OWASP ASVS
2.5.6
OWASP APPSENSOR
-
CAPEC
50
SAFECODE
28

AUTHENTICATION

7

Cecilia consegue usar força bruta e ataques de dicionário (dictionary attacks) contra uma ou muitas contas sem limitação, ou estes ataques são simplificados pois as senhas tem baixa complexidade, tamanho reduzido, inexistência de expiração e regras para reuso

OWASP SCP
33, 38-39, 41, 50, 53
OWASP ASVS
2.1.2, 2.1.7, 2.1.10, 2.2.1, 2.2.1
OWASP APPSENSOR
AE2, AE3
CAPEC
2, 16
SAFECODE
27

© 2012-2024 OWASP Foundation

AUTHENTICATION

8

Kate consegue ignorar a autenticação porque isto não é uma falha de segurança (ex: o acesso sem autenticação está assinalado como padrão)

OWASP SCP
28

OWASP ASVS
4.1.5

OWASP APPSENSOR
-

CAPEC
115

SAFECODE
28

AUTHENTICATION

9

Claudia consegue assumir funções críticas porque os requisitos de autenticação são muito fracos (ex: não é usado autenticação com força de senha), ou não é um requisito revalidar a autenticação com frequência

OWASP SCP
55-56

OWASP ASVS
1.4.3, 1.4.5, 2.1.6, 2.2.4, 4.3.3

OWASP APPSENSOR
-

CAPEC
21

SAFECODE
14, 28

AUTHENTICATION

10

Pravin consegue ignorar controle de autenticação porque não está sendo usado um módulo/framework/serviço de autenticação que seja centralizado, testado, comprovado e aprovado para gerir requisições

OWASP SCP
25-27

OWASP ASVS
1.1.6, 1.4.4

OWASP APPSENSOR
-

CAPEC
90, 115

SAFECODE
14, 28

AUTHENTICATION

J

Mark consegue acessar recursos ou serviços porque não há requisitos de autenticação, ou, por engano, um outro sistema ou outra ação realizou autenticação

OWASP SCP
23, 32, 34

OWASP ASVS
1.4.3, 1.4.5

OWASP APPSENSOR
-

CAPEC
115

SAFECODE
14, 28

AUTHENTICATION

Q

Jaime consegue ignorar a autenticação porque não é aplicado o mesmo rigor para todas as funções de autenticação (ex: logar, troca de senha, recuperação de senha, logout, acesso administrador) ou não é aplicado o mesmo rigor nos diversos locais de acesso e versões do sistema(ex:mobile website, mobile app, full website, API, call center)

OWASP SCP
23, 29, 42, 49

OWASP ASVS
1.4.3, 1.4.5, 2.5.6, 2.5.7

OWASP APPSENSOR
-

CAPEC
36, 50, 115, 121, 179

SAFECODE
14, 28

AUTHENTICATION

K

Olga consegue influenciar ou alterar o código ou a rotina de autenticação e com isto ignorar a autenticação

OWASP SCP
24

OWASP ASVS
4.1.1, 10.2.3-10.2.6

OWASP APPSENSOR
-

CAPEC
115, 207, 554

SAFECODE
14, 28

(Nenhum Cartão)

(Nenhum Cartão)

© 2012-2024 OWASP Foundation

SESSION MANAGEMENT

A

Você inventou um novo ataque contra o Gerenciamento de Sessões

Leia mais sobre este tópico em OWASP Session Management Cheat Sheet e prevenção de ataques do tipo Cross Site Request Forgery (CSRF)

SESSION MANAGEMENT

(Nenhum Cartão)

SESSION MANAGEMENT

2

William tem o controle sobre a geração de identificadores de sessão

OWASP SCP
58-59
OWASP ASVS
3.7.1
OWASP APPSENSOR
SE2
CAPEC
31, 60-61
SAFECODE
28

SESSION MANAGEMENT

3

Ryan consegue usar uma única conta em paralelo, pois as sessões simultâneas são permitidas

OWASP SCP
68
OWASP ASVS
3.3.3, 3.3.4
OWASP APPSENSOR
-
CAPEC
-
SAFECODE
28

SESSION MANAGEMENT

4

Alison consegue configurar identificadores de cookies em outras aplicações web porque o domínio ou o caminho não são suficientemente limitados

OWASP SCP
59, 61
OWASP ASVS
3.4.1-3.4.5
OWASP APPSENSOR
SE2
CAPEC
31, 61
SAFECODE
28

SESSION MANAGEMENT

5

John consegue prever ou adivinhar identificadores de sessão porque estes não são alterados quando uma regra de usuário é alterada (ex: antes e depois da autenticação) e quando uma troca entre meios de comunicação criptografados e não criptografados acontece, ou os identificadores são curtos e não randômicos, ou não são modificados periodicamente

OWASP SCP
60, 62, 66-67, 71-72
OWASP ASVS
3.2.1, 3.2.2, 3.2.4, 3.3.1
OWASP APPSENSOR
SE4-6
CAPEC
31
SAFECODE
28

SESSION MANAGEMENT

6

Gary consegue ter o controle da sessão de um usuário porque o tempo de encerramento(timeout) da sessão é longo ou inexiste, ou o tempo limite da sessão é longo ou inexiste, ou a mesma sessão pode ser usada para mais de um dispositivo/local

OWASP SCP
64-65
OWASP ASVS
3.3.2-3.3.4
OWASP APPSENSOR
SE5, SE6
CAPEC
21
SAFECODE
28

SESSION MANAGEMENT

7

Casey consegue utilizar a sessão de Adam depois dele ter finalizado o uso da aplicação, porque a função de logout inexiste, ou Adam não fez logout, ou a função de logout não termina a sessão de forma adequada

OWASP SCP
62-63
OWASP ASVS
3.3.1, 3.3.4
OWASP APPSENSOR
-
CAPEC
21
SAFECODE
28

© 2012-2024 OWASP Foundation

SESSION MANAGEMENT

8

Matt consegue utilizar longas sessões porque a aplicação não solicita uma nova autenticação de forma periódica para validar se os privilégios do usuário foram alterados

OWASP SCP
96

OWASP ASVS
3.6.1, 3.3.2

OWASP APPSENSOR
-

CAPEC
21

SAFECODE
28

SESSION MANAGEMENT

9

Ivan consegue roubar identificadores de sessão porque estes são transmitidos em canais inseguros, ou estão logados, ou são exibidos em mensagens de erros, ou estão em URLs, ou são acessíveis pelo código que o atacante consegue alterar ou influenciar

OWASP SCP
69, 75-76, 119, 138

OWASP ASVS
1.9.1, 3.1.1, 7.1.1, 7.1.2, 7.2.1, 9.1.3, 9.2.2

OWASP APPSENSOR
SE4-6

CAPEC
31, 60

SAFECODE
28

SESSION MANAGEMENT

10

Marce consegue inventar requisições porque tokens randômicos e fortes (ou seja, tokens anti-CSRF) ou similares não estão sendo usados para ações que mudam estado. Estas requisições podem ser por sessão ou por requisição (request) em ações mais críticas

OWASP SCP
73-74

OWASP ASVS
4.2.2

OWASP APPSENSOR
IE4

CAPEC
62, 111

SAFECODE
18

SESSION MANAGEMENT

J

Jeff consegue reenviar uma interação de repetição idêntica (ex: requisição HTTP, sinal, botão pressionado) e ela é aceita, sem rejeição

OWASP SCP
-

OWASP ASVS
11.1.1-11.1.3

OWASP APPSENSOR
IE5

CAPEC
60

SAFECODE
12, 14

SESSION MANAGEMENT

Q

Salim consegue ignorar o gerenciamento de sessão porque este não é aplicado de forma abrangente e consistente por toda a aplicação

OWASP SCP
58

OWASP ASVS
1.1.6, 3.7.1

OWASP APPSENSOR
-

CAPEC
21

SAFECODE
14, 28

SESSION MANAGEMENT

K

Peter consegue ignorar o controle de gerenciamento de sessão porque este foi autoconstruído e/ou é fraco, ao invés de ter sido usado a estrutura padrão de um framework ou um modulo testado e aprovado

OWASP SCP
58, 60

OWASP ASVS
1.1.6

OWASP APPSENSOR
-

CAPEC
21

SAFECODE
14, 28

(Nenhum Cartão)

(Nenhum Cartão)

© 2012-2024 OWASP Foundation

AUTHORIZATION

A

Você inventou um novo ataque contra Controle de Acessos

Leia mais sobre este tópico em OWASP Development Guide e OWAPS Testing Guide

AUTHORIZATION

(Nenhum Cartão)

AUTHORIZATION

2

Tim consegue alterar nomes/endereços (paths) onde os dados são enviados ou encaminhados para alguém

OWASP SCP
44

OWASP ASVS
4.1.3, 4.2.1, 5.1.5

OWASP APPSENSOR
-

CAPEC
153

SAFECODE
8, 10-11

AUTHORIZATION

3

Christian consegue acessar informações, que ele não deveria ter permissão, por meio de outro mecanismo que tenha permissão (ex: indexador de pesquisa, log, relatórios) ou porque a informação está armazenada em cache, ou mantida por mais tempo do que o necessário, ou outra vazamento de informação

OWASP SCP
51, 100, 135, 139-141, 150

OWASP ASVS
1.12.1, 4.1.3, 4.1.5, 8.1.2, 8.2.1, 8.3.1, 8.3.4, 8.3.6, 8.3.8, 12.4.1

OWASP APPSENSOR
-

CAPEC
69, 213

SAFECODE
8, 10-11

AUTHORIZATION

4

Kelly consegue ignorar controles de acesso porque estes não falham seguramente (ex: a permissão de acesso está assinalada como padrão)

OWASP SCP
79-80

OWASP ASVS
4.1.5

OWASP APPSENSOR
-

CAPEC
122

SAFECODE
8, 10-11

AUTHORIZATION

5

Chad consegue acessar recursos que não deveria ter acesso devido a inexistência de uma autorização ou por concessão de privilégios excessivos (ex: não usar o princípio de menor privilégio possível). Os recursos podem ser serviços, processos, AJAX, Flash, vídeo, imagens, documentos, arquivos temporários, dados de sessão, propriedades do sistema, dados de configuração, logs

OWASP SCP
70, 81, 83-4, 87-9, 99, 117, 131-2, 142, 154, 170, 179

OWASP ASVS
1.2.2, 4.1.1, 4.1.3, 4.2.1

OWASP APPSENSOR
ACE1, ACE2, ACE3, ACE4, HT2

CAPEC
75, 87, 95, 126, 149, 155, 203, 213, 264-265

SAFECODE
8, 10-11, 13

AUTHORIZATION

6

Eduardo consegue acessar dados que ele não tem permissão embora ele tem permissão em formulários, páginas, URL ou pontos de entrada

OWASP SCP
81, 88, 131

OWASP ASVS
4.1.3, 4.2.1

OWASP APPSENSOR
ACE1-4

CAPEC
122

SAFECODE
8, 10-11

AUTHORIZATION

7

Yuanjing consegue acessar funções, telas e propriedades do aplicativo, a qual ele não está autorizado a ter acesso

OWASP SCP
81, 85-86, 131

OWASP ASVS
4.1.3, 4.2.1

OWASP APPSENSOR
ACE1-4

CAPEC
122

SAFECODE
8, 10-11

© 2012-2024 OWASP Foundation

AUTHORIZATION

8

Tom consegue ignorar regras de negócios alterando o fluxo/sequência usual do processo, ou realizando o processo na forma incorreta, ou manipulando valores de data e hora usados pela aplicação, ou usando recursos válidos para fins não intencionais, ou pela manipulação incorreta do controle de dados

OWASP SCP
10, 32, 93-94, 189

OWASP ASVS
4.1.2, 4.2.1, 4.3.3, 7.3.4, 11.1.1, 11.1.2

OWASP APPSENSOR
ACE3

CAPEC
25, 39, 74, 162, 166, 207

SAFECODE
8, 10-12

OWASP Cornucopia Edição de Ecomércio v1.30-PT-BR

AUTHORIZATION

9

Mike consegue usar indevidamente uma aplicação quando uma funcionalidade é usada de forma muito rápida, ou com muita frequência, ou de outra maneira a qual a funcionalidade não se destina, ou pelo consumo de recursos da aplicação ou pela condição de corrida (race conditions) ou utilização excessiva da funcionalidade

OWASP SCP
94

OWASP ASVS
11.1.3, 11.1.4

OWASP APPSENSOR
AE3, FIO1-2, UT2-4, STE1-3

CAPEC
26, 29, 119, 261

SAFECODE
1, 35

OWASP Cornucopia Edição de Ecomércio v1.30-PT-BR

AUTHORIZATION

10

Richard consegue ignorar os controles de acesso centralizados pois estes não estão sendo utilizados de forma abrangente em todas as interações

OWASP SCP
78, 91

OWASP ASVS
1.1.6, 4.1.1

OWASP APPSENSOR
ACE1-4

CAPEC
36, 95, 121, 179

SAFECODE
8, 10-11

OWASP Cornucopia Edição de Ecomércio v1.30-PT-BR

AUTHORIZATION

J

Dinis consegue acessar informações referente a configurações de segurança ou consegue acessar a lista de controle de acesso

OWASP SCP
89-90

OWASP ASVS
4.1.2, 10.2.3, 10.2.3-10.2.6

OWASP APPSENSOR
-

CAPEC
75, 133, 203

SAFECODE
8, 10-11

OWASP Cornucopia Edição de Ecomércio v1.30-PT-BR

AUTHORIZATION

Q

Christopher consegue injetar um comando que a aplicação vai executar no mais alto nível de privilégio

OWASP SCP
209

OWASP ASVS
5.3.8

OWASP APPSENSOR
-

CAPEC
17, 30, 69, 234

SAFECODE
8, 10-11

OWASP Cornucopia Edição de Ecomércio v1.30-PT-BR

AUTHORIZATION

K

Ryan consegue influenciar ou alterar controles de acesso e permissões e consegue ignora-los

OWASP SCP
77, 89, 91

OWASP ASVS
4.1.1, 4.1.2, 10.2.3-10.2.6

OWASP APPSENSOR
-

CAPEC
207, 554

SAFECODE
8, 10-11

OWASP Cornucopia Edição de Ecomércio v1.30-PT-BR

(Nenhum Cartão)

(Nenhum Cartão)

© 2012-2024 OWASP Foundation

CRYPTOGRAPHY

A

Você inventou um novo ataque contra Práticas de Criptografia

Leia mais sobre este tópico em OWASP Cryptographic Storage Cheat Sheet e OWASP Transport Layer Protection Cheat Sheet

CRYPTOGRAPHY

(Nenhum Cartão)

CRYPTOGRAPHY

2

Kyun consegue acesso a dados porque isto foi ocultado/ofuscado/escondido ao invés de ser usada uma função de criptografia aprovada

OWASP SCP
105, 133, 135

OWASP ASVS
6.2.2

OWASP APPSENSOR
-

CAPEC
-

SAFECODE
21, 29

CRYPTOGRAPHY

3

Axel consegue modificar dados que estão armazenados ou que são temporários ou transitórios, ou consegue modificar código fonte, ou consegue modificar patches/atualizações, ou alterar dados de configuração, pois a integridade não foi checada

OWASP SCP
92, 205, 212

OWASP ASVS
14.1.1, 14.1.4, 14.1.5, 10.2.3-10.2.6, 10.3.1, 10.3.2

OWASP APPSENSOR
SE1, IE4

CAPEC
31, 39, 68, 75, 133, 145, 162, 203, 438-439, 442

SAFECODE
12, 14

CRYPTOGRAPHY

4

Paulo consegue acesso a dados transitórios não criptografados, embora o canal de comunicação esteja criptografado

OWASP SCP
37, 88, 143, 214

OWASP ASVS
6.1.1, 8.3.4, 9.1.1

OWASP APPSENSOR
-

CAPEC
185-187

SAFECODE
14, 29-30

CRYPTOGRAPHY

5

Kyle consegue ignorar controles criptográficos porque eles não falham de forma segura (ex: eles são desprotegidos por padrão)

OWASP SCP
103, 145

OWASP ASVS
1.9.1, 6.2.1, 9.1.3, 9.2.2

OWASP APPSENSOR
-

CAPEC
-

SAFECODE
21, 29

CRYPTOGRAPHY

6

Romain consegue ler e modificar dados descriptografados que estão na memória ou são transitórios (ex: credenciais, identificadores de sessão, dados pessoais e comercialmente relevantes), em uso ou em comunicação dentro da aplicação, ou entre aplicação e usuário, ou entre a aplicação e sistemas externos

OWASP SCP
36-37, 143, 146-147

OWASP ASVS
1.9.1, 2.2.5, 2.5.1, 8.3.4, 8.3.6, 9.1.3, 9.2.2

OWASP APPSENSOR
-

CAPEC
31, 57, 102, 157-158, 384, 466, 546

SAFECODE
29

CRYPTOGRAPHY

7

Gunter consegue interceptar ou modificar dados criptografados em trânsito porque o protocolo está mal implantado, ou configurado de forma fraca, ou os certificados estão inválidos, ou os certificados não são confiáveis, ou a conexão pode ser deteriorada para uma comunicação mais fraca ou descriptografada

OWASP SCP
75, 144-145, 148

OWASP ASVS
1.9.2, 6.2.7, 9.1.1, 9.2.1, 9.2.4, 14.4.5

OWASP APPSENSOR
IE4

CAPEC
31, 216

SAFECODE
14, 29-30

© 2012-2024 OWASP Foundation

CRYPTOGRAPHY

8

Eoin consegue acesso a dados de negócios armazenados (ex: senhas, identificadores de sessão, informações de identificação pessoal - PII, dados de titular de cartão) pois estes dados não estão criptografados de forma segura ou com segurança

OWASP SCP
30-31, 70, 133, 135
OWASP ASVS
2.4.1, 6.2.2, 6.2.3, 8.3.4
OWASP APPSENSOR
-
CAPEC
31, 37, 55
SAFECODE
21, 29, 31

CRYPTOGRAPHY

9

Andy consegue ignorar a geração de números aleatórios/randômicos, ou ignorar a geração aleatória de GUID, ou ignorar as funções de criptografia e hashing porque eles são fracos ou foram autoconstruídos

OWASP SCP
60, 104-105
OWASP ASVS
6.2.2, 6.2.3, 6.3.1, 6.3.3
OWASP APPSENSOR
-
CAPEC
97
SAFECODE
14, 21, 29, 32-33

CRYPTOGRAPHY

10

Susanna consegue quebrar a criptografia em uso pois a criptografia não é forte o suficiente para oferecer a proteção exigida, ou esta não é forte o suficiente para tratar a quantidade de esforço que o atacante está disposto a fazer

OWASP SCP
104-105
OWASP ASVS
6.3.3
OWASP APPSENSOR
-
CAPEC
97, 463
SAFECODE
14, 21, 29, 31-33

CRYPTOGRAPHY

J

Justin consegue ler credenciais para acessar recursos internos e externos, serviços e outros sistemas porque estas credenciais estão armazenadas num formato descriptografado ou salvos no código fonte

OWASP SCP
35, 90, 171-172
OWASP ASVS
1.6.1, 1.6.2, 1.6.4, 2.10.4, 6.4.1, 6.4.2
OWASP APPSENSOR
-
CAPEC
116
SAFECODE
21, 29

CRYPTOGRAPHY

Q

Randolph consegue acessar ou prever os dados mestres de criptografia

OWASP SCP
35, 102
OWASP ASVS
1.6.1, 1.6.2, 1.6.3, 6.2.3, 8.3.6
OWASP APPSENSOR
-
CAPEC
116-117
SAFECODE
21, 29

CRYPTOGRAPHY

K

Dan consegue influenciar ou alternar as rotinas/codificações de criptografia (encriptação, hashing, assinaturas digitais, números aleatórios e geração de GUID) e consegue ignorá-los também

OWASP SCP
31, 101
OWASP ASVS
1.6.2, 6.2.5-6.2.8
OWASP APPSENSOR
-
CAPEC
207, 554
SAFECODE
14, 21, 29

(Nenhum Cartão)

(Nenhum Cartão)

© 2012-2024 OWASP Foundation

CORNUCOPIA

A

Você inventou um novo ataque de qualquer tipo

Leia mais sobre segurança da aplicação nos guias da OWASP (Requirements, Development, Code Review and Testing) e na série OWASP Cheat Sheet, e no modelo de maturidade Open SAMM (Software Assurance Maturity Model)

CORNUCOPIA

(Nenhum Cartão)

CORNUCOPIA

2

Lee consegue ignorar os controles do aplicativo pois foram usadas funções arriscadas da linguagem de programação ao invés de opções seguras, ou há erros de conversão, ou porque o aplicativo está inseguro quando um recurso externo está indisponível, ou há race condition, ou há problemas na inicialização ou alocação de recursos, ou quando há sobrecarga

OWASP SCP
194-202, 205-209

OWASP ASVS
14.1.2

OWASP APPSENSOR
-

CAPEC
25-26, 29, 96, 123-124, 128-129, 264-265

SAFECODE
3, 5-7, 9, 22, 25-26, 34

CORNUCOPIA

3

Andrew consegue acessar o código fonte, ou descompilar o aplicativo, ou consegue acessar a lógica do negócio para entender como a aplicação funciona e quais segredos ela contêm

OWASP SCP
134

OWASP ASVS
14.1.1

OWASP APPSENSOR
-

CAPEC
189, 207

SAFECODE
-

CORNUCOPIA

4

Keith consegue realizar uma ação e isto não é atribuído a ele

OWASP SCP
23, 32, 34, 42, 51, 181

OWASP ASVS
7.2.1, 7.2.2

OWASP APPSENSOR
-

CAPEC
-

SAFECODE
-

CORNUCOPIA

5

Larry consegue induzir a confiança de outras partes, incluindo usuários autenticados, ou violar esta confiança em outro lugar (ex: em outro aplicativo)

OWASP SCP
-

OWASP ASVS
1.9.2, 9.1.1, 5.1.5, 9.2.1, 9.2.4

OWASP APPSENSOR
-

CAPEC
89, 103, 181, 459

SAFECODE
-

CORNUCOPIA

6

Aaron consegue ignorar os controles porque a manipulação de erros/exceções é perdida/ignorada, ou é implementada de forma inconsistente ou parcial, ou não há negação de acesso por padrão (ex: erros devem terminar o acesso/execução da funcionalidade), ou depende do tratamento por algum outro serviço ou sistema

OWASP SCP
109-112, 155

OWASP ASVS
4.1.5, 7.1.4

OWASP APPSENSOR
-

CAPEC
54, 98, 164

SAFECODE
4, 11, 23

CORNUCOPIA

7

As ações de Mwengu não podem ser investigadas porque não há um registro correto de eventos de segurança com precisão, ou não há uma trilha de auditoria completa, ou estas podem ser alteradas ou excluídas pelo Mwengu, ou não existe um serviço de registro centralizado

OWASP SCP
113-115, 117-118, 121-130

OWASP ASVS
7.1.2, 7.1.4, 7.2.1, 7.2.2, 7.3.1-7.3.3, 8.3.5, 9.2.5

OWASP APPSENSOR
-

CAPEC
93

SAFECODE
4

© 2012-2024 OWASP Foundation

CORNUCOPIA

8

David consegue ignorar o aplicativo para obter acesso aos dados porque a infraestrutura de rede e servidores e os serviços suportados não foram configurados de forma segura, as configurações não são verificadas periodicamente e os patches de segurança não são aplicados, ou os dados armazenados localmente não são fisicamente protegidos

OWASP SCP
151-152, 156, 160-161, 173-177

OWASP ASVS
1.4.5, 10.3.1, 10.3.2, 14.1.4, 14.1.5, 14.2.1, 14.2.2

OWASP APPSENSOR
RE1, RE2

CAPEC
37, 220, 310, 436, 536

SAFECODE
-

CORNUCOPIA

9

Michael consegue ignorar o aplicativo para obter acesso aos dados porque ferramentas ou interfaces administrativas não estão adequadamente seguras

OWASP SCP
23, 29, 56, 81-82, 84-90

OWASP ASVS
1.4.3, 1.4.5, 4.3.1

OWASP APPSENSOR
-

CAPEC
122, 233

SAFECODE
-

CORNUCOPIA

10

Xavier consegue contornar os controles do aplicativo porque os códigos fontes tanto dos frameworks, como de bibliotecas e componentes utilizados contêm código malicioso ou vulnerabilidades

OWASP SCP
57, 151-152, 204-205, 213-214

OWASP ASVS
1.14..3, 10.1.1, 10.2.3-10.2.6, 14.2.1

OWASP APPSENSOR
-

CAPEC
68, 438-439, 442, 524, 538

SAFECODE
15

CORNUCOPIA

J

Roman consegue explorar o aplicativo pois este foi compilado usando ferramentas desatualizadas ou configurações não seguras como padrão ou informações de segurança não foram documentadas e passadas para o time operacional

OWASP SCP
90, 137, 148, 151-154, 175-179, 186, 192

OWASP ASVS
1.14.3, 14.1.1-14.1.5, 14.2.1

OWASP APPSENSOR
-

CAPEC
-

SAFECODE
4

CORNUCOPIA

Q

Jim pode realizar ações mal-intencionadas, não normais, sem detecção e resposta em tempo real pela aplicação

OWASP SCP
-

OWASP ASVS
8.1.4, 11.1.1-11.1.4

OWASP APPSENSOR
(All)

CAPEC
-

SAFECODE
1, 27

CORNUCOPIA

K

Gareth pode utilizar o aplicativo para negar o serviço a alguns ou a todos os usuários

OWASP SCP
41, 55

OWASP ASVS
2.2.1, 11.1.3, 11.1.4

OWASP APPSENSOR
UT1-4, STE3

CAPEC
2, 25, 119, 125

SAFECODE
1

JOKER

Joker

Alice consegue utilizar a aplicação para realizar ataques a dados e usuários do sistema

Você pensou em se tornar membro individual da OWASP? Todas as ferramentas, guias e reuniões locais são gratuitas para todos, mas ser um membro individual apoia o trabalho da OWASP

JOKER

Joker

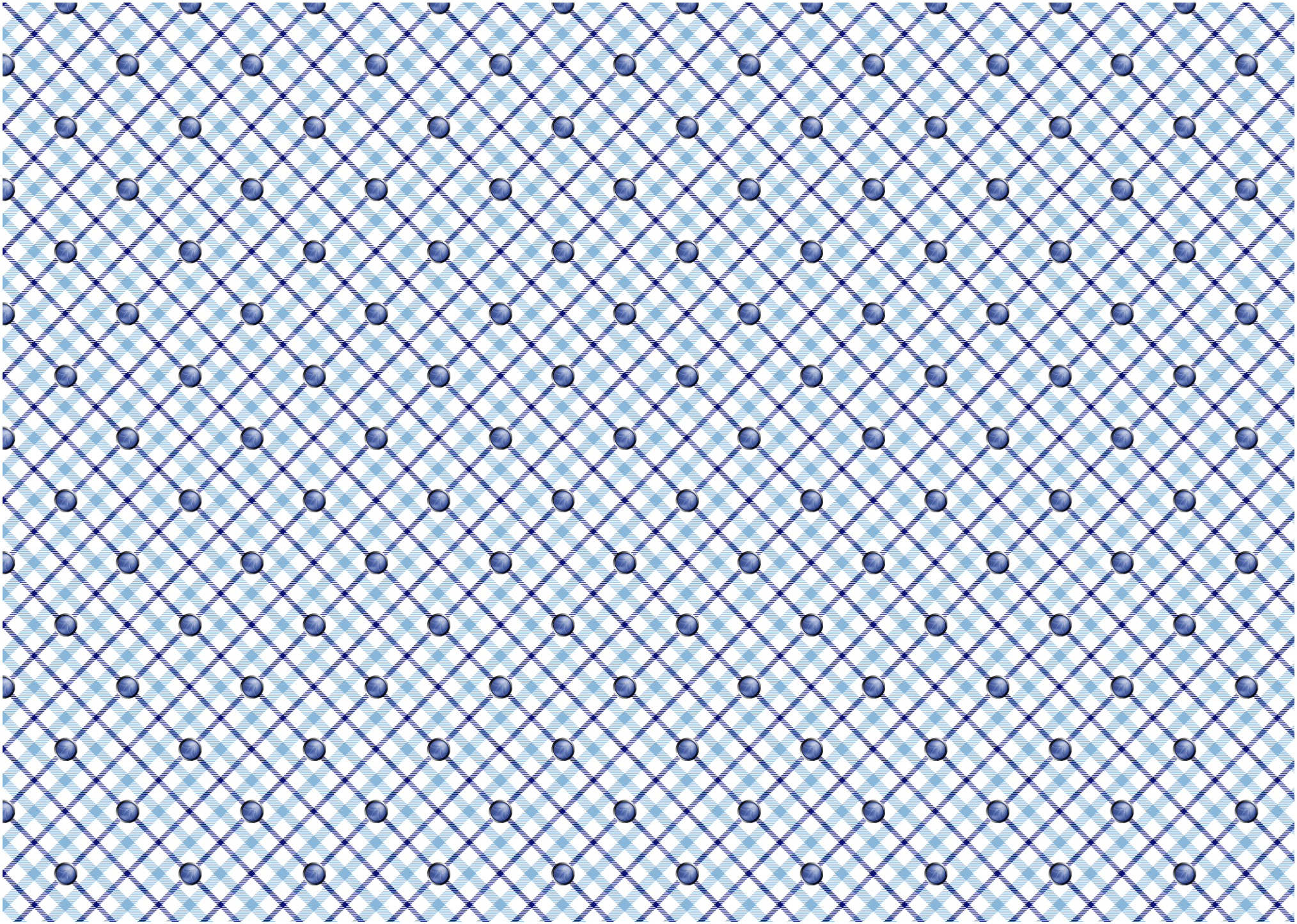
Bob pode influenciar, alterar ou mudar a aplicação para que ela não cumpra os propósitos legais, regulamentadores, contratuais ou outras diretrizes organizacionais

Examine as vulnerabilidades e descubra como elas podem ser solucionadas através do aplicativo de treinamento OWASP Broken Web Applications VM, ou usando o desafio online Hacking Lab. Ambos são gratuitos

© 2012-2024 OWASP Foundation

Cut here

© 2012-2024 OWASP Foundation



© 2012-2024 OWASP Foundation

Change Log

Version / Date		Comments
0.1	30 Jul 2012	Original Draft
0.2	10 Aug 2012	Draft reviewed and updated
0.3	15 Aug 2012	Draft announced OWASP SCP mailing list for comment.
0.4	25 Feb 2013	Play rules updated based on feedback during workshops. Added reference to PCI SSC Information Supplement: PCI DSS E-commerce Guidelines. Descriptive text extended and updated. Added contributors section, page numbering, FAQs and change log.
1	25 Feb 2013	Release.
1.01	03 Jun 2013	Framework-specific card deck discussion added Additional FAQs created. Descriptive text updated. New cover image, and previous cover image moved to back. Cut lines added. FAQs 5 and 6 added. Attack descriptions on cards with tinted backgrounds changed to black (from dark grey). Project contributors added.
1.02	14 Aug 2013	Warning about time to print added. Additional alternative game rules added (twenty-one, play a deck over a week, play full hand and then discuss). Compliance deck concept added. FAQs 5 and 6 added. Attack descriptions on cards with tinted backgrounds changed to black (from dark grey). Project contributors added.
1.03	18 Sep 2013	Minor attack wording changes on two cards. OWASP SCP and ASVS cross-references checked and updated. Code letters added for suits. All remaining attack descriptions on cards changed to black (from dark grey) and background colours amended to provide more contrast and increase readability.
1.04	01 Feb 2014	Text "password change, password change," corrected to "password change, password recovery," on Queen of Authentication card.
1.05	21 Mar 2014	Updates to alternative game rules. Additional FAQs created. Contributors updated. Podcast and video links added.
1.1	04 Mar 2015	Change log date corrected for v1.05. Cross-references updated for 2014 version of ASVS. Contributors updated. Minor text changes to cards to improve readability.
1.2	29 Jun 2016	Video mentioned/linked Separate score sheet mentioned/linked. Previous embedded score sheet pages deleted Correction (identified by Tom Brennan) and addition to text on card 8 Authentication. Oana Cornea and other participants at the AppSec EU 2015 project summit added to list of contributors. 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.
1.3	01 Jan 2024	Cross-references updated from ASVS v3.0.1 to ASVS v4.0 by Johan Sydseter.

© 2012-2024 OWASP Foundation

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
- Johan Sydseter

- 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.