



Cornucopia

Édition d'application site Web v1.30-FR

OWASP® Cornucopia est un mécanisme qui permet aux équipes de développement logiciel d'identifier les exigences sécurité dans les processus de développement Agile, conventionnels et formels

Auteur

Colin Watson

Chefs de Projet

Colin Watson and Grant Ongers

Traducteurs / Relecteurs (version française)

Tom Brennan, Johanna Curiel, Darío De Filippis and Timo Goosen

Remerciements

Adam Shostack et L'Équipe Microsoft SDL pour le "Jeu de Modélisation de Menaces d'Elévation de Privilège", publié sous licence Creative Commons, comme inspiration pour Cornucopia, et à partir duquel bien des idées, en particulier la théorie du jeu, ont été copiées.

Keith Turpin et les contributeurs au « Guide de Référence Rapide - OWASP Secure Coding Practices », à l'origine donné par Boeing à l'OWASP, qui est utilisé comme source principale d'information des exigences sécurité, pour formuler le contenu des cartes.

Les contributeurs, soutiens, sponsors et volontaires aux projets OWASP ASVS, AppSensor et Web Framework Security Matrix, au Common Attack Pattern Enumeration and Classification (CAPEC) du Mitre, et au « Practical Security Stories and Security Tasks for Agile Development Environments » du SAFECode, qui sont tous utilisés dans les références fournies.

Playgen pour avoir réalisé un séminaire d'après-midi d'éclaircissement sur la ludification des tâches, et tartanmaker.com pour l'outil en ligne permettant de créer le graphisme du verso.

Blackfoot UK Limited pour la création et le don des fichiers prêt-à-imprimer, Tom Brennan et la Fondation OWASP pour l'incitation à la création d'une boîte et feuillet portant la marque OWASP, les employés OWASP, en particulier Kate Hartmann, pour la gestion de la commande, du stockage, et de la distribution des jeux de cartes imprimés Oana Cornea et d'autres participants du sommet AppSec EU 2015 project, pour leur aide à la création d'une démo vidéo. Colin Watson en tant qu'auteur et chef de projet avec Grant Ongers, avec d'autres volontaires OWASP qui ont aidé en bien des manières.



3.0

Introduction

L'idée de Cornucopia est d'aider les équipes de développement, en particulier celles qui utilisent des méthodologies Agile, à identifier les exigences sécurité des applications et de développer des scénarii utilisateur basés sur la sécurité. Bien que cette idée fût en gestation depuis longtemps, la motivation finale arriva lorsque SAFECode a publié son Practical Security Stories and Security Tasks for Agile Development Environments en juillet 2012.

L'Équipe Microsoft SDL avait déjà publié son super jeu Elevation of Privilege: The Threat Modeling Game (EoP), mais cela ne semblait pas répondre de manière adéquate aux types de problèmes que les équipes de développement logiciel doivent le plus souvent affronter. EoP est un grand concept de stratégie de jeu, et a été publié sous une licence Creative Commons d'Attribution.

L'Édition d'application web de Cornucopia est basé sur les concepts et les idées de jeu d'EoP, mais ceux-ci ont été modifiés pour être plus en accord avec les types de problèmes que les développeurs de sites web d'e-commerce rencontrent. Elle essaie d'apporter des idées de modélisation de menace au niveau des équipes de développement qui utilisent les méthodologies Agile, ou qui sont plus portées sur les faiblesses des applications web que les autres types de vulnérabilité logicielle, ou ne sont pas familiarisées avec STRIDE et DREAD.

L'Édition d'application web de Cornucopia est référencé comme ressource d'information dans le PCI Security Standard Council's Information Supplement PCI DSS E-commerce Guidelines, v2, janvier 2013.

Le jeu de cartes (paquet)

Au lieu d'utiliser les couleurs de l'EoP STRIDE (jeux de cartes aux designs similaires), les couleurs Cornucopia sont basés sur la structure du OWASP Secure Coding Practices - Quick Reference Guide (SCP), mais avec l'étude additionnelle des sections du OWASP Application Security Verification Standard, du OWASP Testing Guide et des Principles of Secure Development de David Rook. Ceux-ci ont permis de constituer cinq couleurs, et une sixième, appelée « Cornucopia » a été créée pour tout le reste :

- Validation des Données & l'Encodage (VE -EN)
- Authentification (AT -EN)
- Gestion des Sessions (SM -EN)
- Habilitation (AZ -EN)
- Cryptographie (CR -EN)
- Cornucopia (C -EN)

Comme au jeu de cartes de poker, chaque couleur comprend 13 cartes (As, 2-10, Valet, Dame et Roi) mais, contrairement à EoP, il y a aussi 2 cartes Joker. Le contenu provient surtout du SCP.

Correspondances

L'autre moteur de Cornucopia est de lier les attaques aux exigences et aux techniques de vérification. Le but initial était de référencer les identifiants des faiblesses CWE, mais celles-ci étant trop nombreuses, il a été décidé de relier chaque carte à une attaque référencée dans CAPEC, elle-même reliée aux CWE, pour que le but recherché soit atteint. Chaque carte est également liée aux 36 scénarii de sécurité du document SAFECode, de même à l'OWASP SCP v2, ASVS v4.0 et AppSensor (application attack detection and response) pour aider les équipes à créer leurs propres scénarii de sécurité pour utilisation dans les processus Agile.

Stratégie de jeu

A part les différences de contenu, les règles du jeu sont identiques à celles de l'EoP

Imprimer les cartes

La page du projet Cornucopia indique comment obtenir des jeux de cartes brillantes pré-imprimées.

Les cartes peuvent être imprimées à partir de ce document en noir et blanc mais la couleur est davantage conseillée. Les cartes des pages suivantes de ce document ont été mises en page pour sortir sur un modèle de page A4 de cartes business. Ceci semblait être le moyen le plus rapide de créer des cartes à jouer. Les codes produit Avery C32015 & C32030 ont été testés avec succès, mais toute page A4 à 10 cartes 85mm x 54 mm devrait convenir avec un peu d'ajustement. Ces modèles de cartes étant plutôt chères, un soin particulier devra être apporté dans la décision du choix du format et de l'imprimante. Les cartes peuvent bien entendu être imprimées sur tout format de papier ou carton, puis coupées manuellement, ou une imprimante professionnelle sera capable d'imprimer de plus grandes quantités et de couper les cartes à la bonne taille.

Les lignes de coupe sont indiquées à l'avant-dernière page de ce document, mais Avery fournit également un modèle A4 en paysage (A-0017-01_L.doc) qui peut être utilisé comme guide. L'impression et la découpe peuvent prendre environ une heure, une imprimante rapide est conseillée.

Privilégiez une haute qualité d'impression pour gagner en lisibilité. Un style optionnel de dos de carte (tartan OWASP) est fourni dans la dernière page de ce document. Il n'y a pas d'alignement spécial à prendre en compte. L'impression recto-verso doit être faite avec soin. Vous pouvez personnaliser les rectos ou les versos pour coller aux préférences de votre organisation. Vous pouvez personnaliser les faces ou le dos des cartes selon les préférences de votre propre organisation.

Personnalisation

Après avoir joué quelques parties de Cornucopia, vous pourriez penser que certaines cartes sont moins pertinentes pour vos applications, ou que les menaces sont différentes pour votre organisation. Editez vous-même ce document pour ajuster le contenu des cartes à vos équipes, ou créez de nouveaux jeux entiers.

Faites un retour

Si vous avez des idées ou un retour à faire sur l'usage d'OWASP® Cornucopia, merci de les partager. Mieux encore, si vous créez de nouvelles versions des cartes, ou des versions professionnelles imprimables, merci de les partager avec les volontaires qui ont créé cette édition, ainsi que la communauté de la sécurité et du développement d'applications.

Le meilleur endroit pour discuter ou contribuer est dans la liste ou le groupe du projet OWASP:

- Liste/Groupe
https://lists.owasp.org/mailman/listinfo/owasp_cornucopia
- Page d'accueil du projet
https://www.owasp.org/index.php/OWASP_Cornucopia

Tous les documents et outils OWASP sont libres de téléchargement et d'utilisation. OWASP® Cornucopia est publié sous une licence Creative Commons Attribution-ShareAlike 3.0 .

Instructions

Le texte de chaque carte décrit une attaque, sauf que l'attaquant a un nom, qui est unique à chaque carte. Ce nom peut représenter un système informatique (ex : base de données, système de fichiers, une autre application, un service lié, un botnet), un particulier (ex : un citoyen, client, employé, criminel), ou même un groupe de personnes (ex : organisation concurrente, activistes œuvrant pour une cause). L'attaquant peut opérer depuis un autre lieu/équipement, ou avoir un accès local/interne au même équipement, hôte, ou réseau dans lequel l'application fonctionne. L'attaquant est toujours nommé au début de chaque description Par exemple : William a le contrôle sur la génération des identifiants de session.

William a le contrôle sur la génération des identifiants de session.

Ce qui veut dire que l'attaquant (William) est en mesure de créer de nouveaux identifiants de session que l'application accepte. Ces attaques sont principalement tirées des exigences de sécurité listées dans le SCP v2, mais ont été complétées avec les objectifs de vérification « Application Security Verification Standard for Web Applications » de l'OWASP, les scénarii de sécurité du « Practical Security Stories and Security Tasks for Agile Development Environments » de SAFECode, et une revue des cartes de l'EoP.

De l'aide supplémentaire pour chaque carte est disponible dans la description en ligne du jeu :

https://wiki.owasp.org/index.php/Cornucopia - Ecommerce_Website_Edition - Wiki_Deck

Des renvois entre les attaques et cinq ressources sont fournis sur la plupart des cartes

- Exigences dans “Secure Coding Practices (SCP) - Quick Reference Guide”, v2, OWASP®, novembre 2010 (ref: [OWASP SCP Quick Reference Guide v2.1](#))
- Identifiants de vérification dans “Application Security Verification Standard (ASVS) for Web Applications” (ref: [ASVS v3 and v4 downloads](#))
- Identifiants de points de détection d'attaque dans “AppSensor”, OWASP®, août 2010-2015 (ref: [AppSensor DetectionPoints](#))
- Identifiants dans “Common Attack Pattern Enumeration and Classification (CAPEC)”, v2.8, Mitre Corporation, novembre 2015 (ref: [capec \(31. July 2018\)](#))
- Scénarii de sécurité dans 'Practical Security Stories and Security Tasks for Agile Development Environments', SAFECode, juillet 2012 (ref: [SAFECode Agile Dev Security](#))

Un renvoi signifie que l'attaque est incluse dans l'objet référencé, mais ne comprend pas nécessairement l'ensemble de son objectif. Pour des données structurées comme CAPEC, la référence la plus spécifique est fournie, mais parfois est présente une référence croisée qui a aussi des exemples plus spécifiques (enfants). Il n'y a pas de renvois dans les six As et les deux Jokers. Ces dernières cartes présentent des conseils généraux en italique.

Il y a bien des manières de jouer à Cornucopia. En voici une, en situation dans une vidéo en ligne sur (ref: [ColinWatsonOWASP](#)), qui utilise la nouvelle (mai 2015) feuille de scores disponible ici: (refL [Cornucopia scoresheet](#))

A - Préparations

- A1. Procurez-vous un jeu, ou imprimez votre propre jeu de cartes Cornucopia (voir page 2 de ce document), et séparez/découpez les cartes.
- A2. Identifiez une application ou processus à évaluer, cela peut être un concept, une spécification ou une véritable implémentation.
- A3. Créez un diagramme de flux de données, des cas d'utilisation, ou d'autres supports pour aider à l'évaluation.
- A4. Identifiez et invitez un groupe de 3-6 architectes, développeurs, testeurs et autres participants métier ensemble et asseyez-vous autour d'une table (essayez d'inclure un profil sensibilisé à la sécurité applicative).
- A5. Prévoyez une distribution de prix (étoiles, pizza, bière ou fleurs en fonction de la culture d'entreprise).

B - Jouer

Une couleur – Cornucopia – fait office d'atouts. Les As sont les plus forts (battent les Rois). Le fait d'avoir un participant non-joueur facilite le relevé des questions et des scores.

- B1. Retirez les Jokers et quelques cartes de bas niveau (2, 3, 4) du jeu Cornucopia pour s'assurer que chaque joueur ait le même nombre de cartes.
- B2. Battez les cartes et distribuez-les toutes.
- B3. Pour commencer, choisissez au hasard un joueur qui jouera en premier – qui peut jouer n'importe quelle carte en main sauf un atout – Cornucopia.
- B4. Pour jouer une carte, chaque joueur doit la lire à voix haute, et expliquer (voir la description en ligne du jeu) comment la menace s'appliquerait (le joueur reçoit un point pour les attaques qui pourraient fonctionner, pour lesquelles le groupe s'accorde à dire qu'il s'agit d'un bug exploitable) – ne réfléchissez pas à des contre-mesures à ce stade, et n'écartez pas une menace au motif que celle-ci fait déjà l'objet d'une contre-mesure – quelqu'un note la carte et relève les questions rencontrées.
- B5. Jouez ainsi dans le sens des aiguilles d'une montre, si vous possédez une carte de la même couleur, vous devez la jouer, sinon vous pouvez jouer n'importe quelle couleur. Seule la carte la plus forte de la couleur appelée, ou l'atout Cornucopia le plus fort qui a été joué, gagne la main.
- B6. Le joueur qui gagne la main, commence au tour suivant, donnant une couleur à suivre.
- B7. Continuez jusqu'à ce que toutes les cartes soient jouées.

C - Scores

L'objectif est d'identifier des menaces applicables, et de gagner des mains (des tours):

- C1. +1 point à chaque carte jouée pour laquelle le groupe s'accorde à dire qu'il s'agit d'une menace applicable.
- C2. +1 point si vous gagnez une main.
- C3. Lorsque toutes les cartes sont jouées, le plus grand score remporte la partie.

D - Clôture

- D1. Parcourez toutes les menaces applicables et les exigences de sécurité correspondantes.
- D2. Créez des cas d'utilisation, des spécifications, et des jeux de tests en fonction de votre méthodologie de développement.

Règles alternatives

Si vous jouez pour la première fois, retirez les As et les deux Jokers pour commencer. Rajoutez les Jokers lorsque les participants sont habitués au principe du jeu. A part les règles de comptage « à base d'atouts » décrites ci-dessus et qui sont très similaires à l'EoP, le jeu peut être joué « à la blackjack » (21 points), ce qui réduit habituellement le nombre de cartes jouées à chaque tour.

Entraînez-vous sur une application imaginaire, ou même une application qui est encore en projet, plutôt que d'essayer de trouver des failles sur des applications existantes, jusqu'à ce que les participants soient conscients de l'utilité et du plaisir que procure le jeu.

Vous pourriez ne jouer qu'avec une seule couleur pour raccourcir la partie – mais pensez à couvrir toutes les couleurs pour chaque projet. Mieux encore, jouez un seul tour avec quelques cartes présélectionnées, et ne comptez les points que sur la capacité à identifier les exigences de sécurité. Vous pourriez ne jouer qu'une partie à une seule couleur par jour, pendant une semaine environ, si les participants ne peuvent pas consacrer de créneaux assez longs pour une partie entière.

Certaines équipes ont préféré jouer un tour complet sans interruption, puis seulement après, échanger sur les contenus des cartes jouées (au lieu de le faire après chaque carte).

Une autre suggestion est que si un joueur n'arrive pas à identifier que la carte est applicable, on peut permettre aux autres joueurs de suggérer des idées, et potentiellement les laisser gagner le point correspondant à la carte. Vous pouvez distribuer des points supplémentaires pour des contributions particulièrement bonnes.

Vous pouvez même jouer tout seul. Utilisez les cartes comme point de départ à des raisonnements. Il est néanmoins avantageux d'impliquer des personnes supplémentaires.

L'EoP Microsoft recommande la tricherie en tant que stratégie de jeu.

Jeux de cartes spécifiques aux frameworks de développement

Des contrôles de sécurité peuvent être intégrés dans certains langages et frameworks de développement web et mobile couramment utilisés. Sous certaines conditions, l'utilisation de ces contrôles peut simplifier l'identification d'exigences supplémentaires – à supposer évidemment que ces contrôles soient inclus, actives, et configurés correctement.

Pensez à supprimer des cartes des jeux si vous êtes sûr qu'elles sont prises en compte dans la manière dont vous utilisez le langage / framework. Les éléments entre crochets sont « optionnels ».

Standards et librairies de code internes

Ajoutez votre propre liste de cartes exclues, qui est basée sur les standards de code de votre organisation (à supposer qu'elles soient confirmées par des étapes de vérification appropriées dans le cycle de développement).

Vos standards et librairies de code		
Validation des Données & l'Encodage [votre liste]	Gestion des sessions [votre liste]	Cryptographie [votre liste]
Authentification [votre liste]	Habilitation [votre liste]	Cornucopia [votre liste]

Jeux d'exigences de conformité

Créez un jeu de cartes plus petit en ne prenant en compte que des cartes concernant une exigence particulière de conformité.

Exigences de conformité		
Validation des Données & l'Encodage [liste de conformité]	Gestion des sessions [liste de conformité]	Cryptographie [liste de conformité]
Authentification [liste de conformité]	Habilitation [liste de conformité]	Cornucopia [liste de conformité]

Foire aux questions

1. Est-ce que je peux copier ou éditer ce jeu?

Bien entendu. Tous les travaux OWASP sont libres d'utilisation, à condition de se conformer à la licence Creative Commons Attribution-ShareAlike 3.0. Peut-être souhaitez-vous créer une nouvelle version et l'offrir au projet Cornucopia OWASP? 2. Comment m'impliquer?

Envoyez des idées ou des offres d'aide à la liste de diffusion du projet.

3. Comment ont été choisis les noms des attaquants?

EoP démarre chaque description avec des termes comme "Un attaquant peut..." Ceux-ci doivent être présentés comme une attaque, mais je n'étais pas pour cette terminologie anonyme, je voulais quelque chose de plus engageant, et donc, j'ai utilisé des prénoms.

On peut faire l'analogie avec une personne interne ou externe, ou un alias de machine. Mais au lieu de choisir des prénoms au hasard, j'ai réfléchi à comment mettre en avant la communauté OWASP. Du coup, à part "Alice et Bob", j'ai choisi parmi les prénoms des employés et des membres dirigeants d'OWASP, passés et présents (sans notion d'ordre), puis j'ai choisi au hasard les quelques 50 prénoms restants à partir de la liste des particuliers cotisants. Aucun prénom n'a été utilisé plus d'une fois, et dans les cas où deux prénoms coexistaient, j'ai coupé une partie pour m'assurer que personne ne soit facilement reconnu. Les prénoms n'ont pas été délibérément alloués à une attaque, défense ou exigence particulière. Le mélange des cultures et des genres reflète simplement ces sources de prénoms, et n'a pas vocation à être multi culturellement exhaustif. Dans la v1.20, le prénom de la carte VÉ-10 a changé pour refléter le nouveau co-chef de projet – cette carte est aussi la seule à présenter deux prénoms.

4. Pourquoi n'y a-t-il pas d'images sur les cartes?

Il y a pas mal de texte sur les cartes, et les références croisées prennent également beaucoup d'espace. Mais cela serait bien d'ajouter des éléments supplémentaires de design. Un volontaire?

5. Est-ce que les attaques sont classées en fonction de leur valeur faciale

Approximativement. Le risque sera dépendant de l'application et de l'organisation, à cause des exigences de sécurité et de conformité qui sont variables, du coup votre propre échelle de notation peut classer les cartes dans un ordre différent que celui de leur valeur faciale.

6. Combien de temps faut-il pour jouer une main en utilisant le jeu complet?

Cela dépend de la portée de l'application, du niveau de discussion et du degré de connaissance des joueurs vis-à-vis de l'application. Comptez 1 heure et demie à 2 heures pour 4 à 6 joueurs.

7. Quels profils de joueurs peuvent participer?

Essayez toujours de panacher des profils qui peuvent contribuer de manière différente. Mais choisissez une personne qui a une connaissance suffisante de la terminologie des vulnérabilités des applications. Sinon, essayez d'inclure un mélange d'architectes, de développeurs, de testeurs, et un chef de projet ou un responsable métier adéquats.

8. Qui doit prendre des notes et noter les scores?

Il est conseillé qu'une tierce personne, qui ne participe pas au jeu, prenne des notes sur les exigences identifiées et les questions soulevées. Cette activité peut faire office de formation pour un développeur junior, ou bien menée par le chef de projet. Quelques organisations ont enregistré leur partie afin de revenir dessus lorsque les exigences ont été formellement écrites.

9. Doit-on toujours utiliser un jeu complet de cartes?

Non. Un jeu plus petit est plus rapide à jouer. Démarrer votre première partie avec assez de cartes pour deux ou trois tours. Pensez toujours à retirer les cartes qui ne sont pas du tout en rapport avec l'application ou la fonction qui est évaluée. Les joueurs débutants seront généralement plus à l'aise pendant les premières parties, si l'on retire les As et les deux Jokers. De même, les atouts peuvent être écartés jusqu'à ce que les participants soient plus à l'aise avec le concept du jeu.

10. Que doivent faire les joueurs lorsqu'ils possèdent un As qui stipule "Vous avez inventé une nouvelle attaque contre...?"

Le joueur peut imaginer n'importe quelle attaque qu'il juge valide, à condition que le thème de la couleur (ex : Validation des Données & l'Encodage) corresponde. Les joueurs débutants seront plus à l'aise sans ces cartes (voir FAQ 9).

11. Je ne comprends pas la description de l'attaque sur une carte – comment trouver plus d'information?

Le Wiki Deck en ligne a été créé pour aider les joueurs à comprendre les attaques. Voir :

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

12. Mon entreprise souhaite imprimer sa propre version de l'OWASP® Cornucopia – à quelle licence devons-nous nous référer? La réponse complète à cette question se trouve sur les pages web du projet.

https://www.owasp.org/index.php/OWASP_Cornucopia - tab=FAQs

VALIDATION DES DONNÉES & ENCODAGE	VALIDATION DES DONNÉES & ENCODAGE	VALIDATION DES DONNÉES & ENCODAGE	VALIDATION DES DONNÉES & ENCODAGE	VALIDATION DES DONNÉES & ENCODAGE
A	<p>(Pas de Carte)</p> <p>You avez inventé une nouvelle attaque contre la Validation des Données et l'Encodage</p> <p><i>Apprenez-en plus à ce sujet dans les antisèches gratuites OWASP sur la Validation des Entrées, la Prévention des XSS, DOM-XSS, et des Injections SQL, ainsi que sur les Requêtes Paramétrées</i></p>		<p>Brian peut recueillir des informations sur les configurations sous-jacentes, les schémas, la logique, le code, le logiciel, les services et l'infrastructure, de par le contenu des messages d'erreur, ou une mauvaise configuration, ou la présence de fichiers d'installation par défaut, ou des ressources de test, de sauvegarde, de copie, ou l'exposition de code source</p>	<p>Robert peut saisir des données malveillantes, car le format attendu n'est pas vérifié, ou des duplicitas sont acceptés, ou la structure n'est pas vérifiée, ou les éléments individuels des données ne sont pas validées : type, plage, longueur, liste blanche de caractères ou de formats autorisés</p>
4	<p>Dave peut saisir des noms de champs ou des données malveillantes, car ils ne sont pas vérifiés dans le contexte de l'utilisateur ou du processus en cours</p>	<p>Jee peut contourner les routines d'encodage centralisées, car celles-ci ne sont pas utilisées partout, ou bien de mauvais encodages sont utilisés</p>	<p>Jason peut contourner les routines d'encodage centralisées, car celles-ci ne sont pas utilisées à chaque saisie</p>	<p>Jan peut générer des messages de sorte à tromper la validation des données, car le jeu de caractères n'est pas spécifié/posé, ou les données sont encodées plusieurs fois, ou les données ne sont pas pleinement converties dans le format que l'application utilise (par exemple canonicalisation) avant leur validation, ou les variables sont insuffisamment typées</p>
VALIDATION DES DONNÉES & ENCODAGE	<p>OWASP SCP 8, 10, 183</p> <p>OWASP ASVS 4.2.1, 5.1.1, 5.1.2, 11.1.1, 11.1.2</p> <p>OWASP APPSENSOR RE3-6, AE8-11, SE1, SE3-6, IE2-4, HT1-3</p> <p>CAPEC 28, 31, 48, 126, 162, 165, 213, 220-221, 261</p> <p>SAFECODE 24, 35</p> <p>Common_Title_full</p>	<p>OWASP SCP 3, 15, 18-22, 168</p> <p>OWASP ASVS 1.1.6, 1.5.3, 5.1.3, 13.2.2, 13.2.5</p> <p>OWASP APPSENSOR -</p> <p>CAPEC 28, 31, 152, 160, 468</p> <p>SAFECODE 2, 17</p> <p>Common_Title_full</p>	<p>OWASP SCP 3, 168</p> <p>OWASP ASVS 1.1.6, 1.5.3, 5.1.3, 13.2.2, 13.2.5</p> <p>OWASP APPSENSOR IE2, IE3</p> <p>CAPEC 28</p> <p>SAFECODE 3, 16, 24</p> <p>Common_Title_full</p>	<p>OWASP SCP 4-5, 7, 150</p> <p>OWASP ASVS 1.5.3, 13.2.2, 13.2.5</p> <p>OWASP APPSENSOR IE2, IE3, EE1, EE2</p> <p>CAPEC 28, 153, 165</p> <p>SAFECODE 3, 16, 24</p> <p>Common_Title_full</p>

VALIDATION DES DONNÉES & ENCODAGE	8	VALIDATION DES DONNÉES & ENCODAGE	9	VALIDATION DES DONNÉES & ENCODAGE	J
VALIDATION DES DONNÉES & ENCODAGE	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 \${Common_Title_full}	OWASP SCP 6, 21-22, 168 OWASP ASVS 7.1.3 OWASP APPSENSOR IE2, IE3 CAPEC 28 SAFECODE 3, 16, 24 \${Common_Title_full}	OWASP SCP 2, 19, 92, 95, 180 OWASP ASVS 1.12.2, 5.1.3, 9.2.3, 12.2.1, 12.3.1-3, 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 \${Common_Title_full}	OWASP SCP 1, 17 OWASP ASVS 1.5.3 OWASP APPSENSOR RE3, RE4 CAPEC 87, 207, 554 SAFECODE 2, 17 \${Common_Title_full}	
VALIDATION DES DONNÉES & ENCODAGE	Q	VALIDATION DES DONNÉES & ENCODAGE	K		

<p>AUTHENTICATION</p>	<p>A</p> <p>Vous avez inventé une nouvelle attaque contre l'Authentification</p> <p><i>Apprenez-en plus à ce sujet dans les antisèches gratuites OWASP sur l'Authentification</i></p>	<p>AUTHENTICATION</p> <p>(Pas de Carte)</p>	<p>AUTHENTICATION</p> <p>James peut entreprendre des fonctions d'authentification sans que l'utilisateur légitime ne s'en aperçoive (par exemple tentative d'authentification, authentification avec des identifiants volés, mise à jour du mot de passe)</p>	<p>AUTHENTICATION</p> <p>2</p> <p>Muhammad peut obtenir le mot de passe d'un utilisateur ou d'autres secrets comme des questions de sécurité, de par l'observation pendant la saisie, ou à partir d'un cache local, de la mémoire, en transit, par lecture d'une ressource non protégée, parce qu'ils sont communément répandus, qu'ils n'expirent jamais, que l'utilisateur ne peut pas changer son propre mot de passe</p>
<p>AUTHENTICATION</p>	<p>4</p> <p>Sebastien peut facilement identifier les noms des utilisateurs ou peut les énumérer</p>	<p>AUTHENTICATION</p> <p>5</p> <p>Javier peut utiliser les identifiants par défaut, de test, ou facilement devinables, ou peut utiliser un ancien compte ou un compte dont l'application n'a pas besoin</p>	<p>AUTHENTICATION</p> <p>6</p> <p>Sven peut réutiliser un mot de passe temporaire car l'utilisateur n'a pas besoin de le changer à la première connexion, ou sa durée de vie est trop longue ou n'expire pas, ou sa communication ne nécessite pas de deuxième canal distinct (par exemple voie postale, application mobile, SMS)</p>	<p>AUTHENTICATION</p> <p>7</p> <p>Cecilia peut réaliser des attaques de type brute force ou de dictionnaire contre un ou plusieurs comptes sans limitation, ou ses attaques sont simplifiées du fait d'une faible politique de mots de passe (faible complexité, longueur, historique, ou durée de vie insuffisante)</p>
<p>AUTHENTICATION</p>	<p>OWASP SCP 33, 53</p> <p>OWASP ASVS 2.2.1, 4.1.5</p> <p>OWASP APPSENSOR AE1</p> <p>CAPEC 383</p> <p>SAFECODE 28</p> <p>Common_Title_full}</p>	<p>AUTHENTICATION</p> <p>OWASP SCP 54, 175, 178</p> <p>OWASP ASVS 4.1.5</p> <p>OWASP APPSENSOR AE12, IT3</p> <p>CAPEC 70</p> <p>SAFECODE 28</p> <p>Common_Title_full}</p>	<p>AUTHENTICATION</p> <p>OWASP SCP 37, 45-46, 178</p> <p>OWASP ASVS 2.5.6</p> <p>OWASP APPSENSOR -</p> <p>CAPEC 50</p> <p>SAFECODE 28</p> <p>Common_Title_full}</p>	<p>AUTHENTICATION</p> <p>OWASP SCP 33, 38-39, 41, 50, 53</p> <p>OWASP ASVS 2.1.2, 2.1.7, 2.1.10, 2.2.1</p> <p>OWASP APPSENSOR AE2, AE3</p> <p>CAPEC 2, 16</p> <p>SAFECODE 27</p> <p>Common_Title_full}</p>

<p>AUTHENTICATION</p>	<p>8</p> <p>Kate peut contourner l'authentification car son échec n'est pas contrôlé (passage en accès non authentifié)</p> <p>OWASP SCP 28</p> <p>OWASP ASVS 4.1.5</p> <p>OWASP APPSENSOR ~</p> <p>CAPEC 115</p> <p>SAFECODE 28</p> <p>{Common_Title_full}</p>	<p>AUTHENTICATION</p>	<p>9</p> <p>Claudia peut effectuer davantage de fonctions critiques car l'authentification est trop faible (ex : pas d'authefntification forte à deux facteurs), ou la réauthentification n'est pas requise pour ces fonctions</p> <p>OWASP SCP 55-56</p> <p>OWASP ASVS 1.4.5, 2.1.6, 2.2.4, 4.1.3, 4.3.3</p> <p>OWASP APPSENSOR ~</p> <p>CAPEC 21</p> <p>SAFECODE 14, 28</p> <p>{Common_Title_full}</p>	<p>AUTHENTICATION</p>	<p>10</p> <p>Pravin peut contourner les contrôles d'authentification car un module/framework/service d'authefntification, qui est centralisé, standardisé, testé, autorisé, et séparé de la ressource requêtée, n'est pas utilisé</p> <p>OWASP SCP 25-27</p> <p>OWASP ASVS 1.1.6, 1.4.4</p> <p>OWASP APPSENSOR ~</p> <p>CAPEC 90, 115</p> <p>SAFECODE 14, 28</p> <p>{Common_Title_full}</p>	<p>AUTHENTICATION</p>	<p>J</p> <p>Mark peut accéder à des ressources ou des services parce qu'il n'y a pas d'authentification, ou il a été pensé à tort que l'authentification était prise en compte par un autre système ou réalisée dans une action précédente</p> <p>OWASP SCP 23, 32, 34</p> <p>OWASP ASVS 1.4.5, 4.3.1</p> <p>OWASP APPSENSOR ~</p> <p>CAPEC 115</p> <p>SAFECODE 14, 28</p> <p>{Common_Title_full}</p>
<p>AUTHENTICATION</p>	<p>Q</p> <p>Johan peut contourner l'authentification car celle-ci n'est pas implémentée avec la même rigueur dans toutes les fonctionnalités (ex : inscription, changement de mot de passe, recouvrement de mot de passe, déconnexion, administration) ou dans toutes les versions/canaux (ex : site web mobile, appli mobile, site web, API, centre d'appel)</p> <p>OWASP SCP 23, 29, 42, 49</p> <p>OWASP ASVS 1.4.5, 2.5.6, 2.5.7, 4.3.1</p> <p>OWASP APPSENSOR ~</p> <p>CAPEC 36, 50, 115, 121, 179</p> <p>SAFECODE 14, 28</p> <p>{Common_Title_full}</p>	<p>AUTHENTICATION</p>	<p>K</p> <p>Olga peut influencer ou modifier du code/routines d'authentification de telle manière que celle-ci soit contournée</p> <p>OWASP SCP 24</p> <p>OWASP ASVS 4.1.1, 10.2.3, 10.2.4-6</p> <p>OWASP APPSENSOR ~</p> <p>CAPEC 115, 207, 554</p> <p>SAFECODE 14, 28</p> <p>{Common_Title_full}</p>	<p>(Pas de Carte)</p>	<p>(Pas de Carte)</p>		

GESTION DES SESSIONS	A			2	3
	<p>(Pas de Carte)</p> <p>Vous avez inventé une nouvelle attaque contre la Gestion des Sessions</p> <p><i>Apprenez-en plus à ce sujet dans les antisèches gratuites OWASP sur la Gestion des Sessions, et sur la prévention des Cross Site Request Forgery (CSRF)</i></p>			William a le contrôle sur la génération des identifiants de session	Ryan peut utiliser le même compte en parallèle, puisque les sessions concurrentes sont autorisées
GESTION DES SESSIONS	4		5	6	7
	<p>Alison peut régler les cookies d'identification de session vers une autre application web, car le chemin et le domaine sont insuffisamment restreints</p> <p>OWASP SCP 59, 61</p> <p>OWASP ASVS 3.4.1-5</p> <p>OWASP APPSENSOR SE2</p> <p>CAPEC 31, 61</p> <p>SAFECODE 28</p> <p>Common_Title_full</p>	<p>John peut prédire ou deviner les identifiants de session car ceux-ci ne sont pas modifiés lorsque le rôle de l'utilisateur change (par exemple pré et post authentification) et lors de la bascule entre communications chiffrées et non chiffrées, ou ne sont pas suffisamment longs et aléatoires, ou ne sont pas changés périodiquement</p> <p>OWASP SCP 60, 62, 66-67, 71-72</p> <p>OWASP ASVS 3.2.1, 3.2.2, 3.2.4, 3.3.1</p> <p>OWASP APPSENSOR SE4-6</p> <p>CAPEC 31</p> <p>SAFECODE 28</p> <p>Common_Title_full</p>	<p>Gary peut prendre la main sur une session d'un utilisateur car le délai d'attente sur l'inactivité est trop long ou inexistant, ou la même session peut être utilisée depuis plus d'un équipement/site</p> <p>OWASP SCP 64-65</p> <p>OWASP ASVS 3.3.2, 3.3.3, 3.3.4</p> <p>OWASP APPSENSOR SE5, SE6</p> <p>CAPEC 21</p> <p>SAFECODE 28</p> <p>Common_Title_full</p>	<p>Graham peut utiliser la session d'Adam après qu'il ait terminé, car il n'existe pas de fonction de déconnexion, ou il ne peut pas se déconnecter facilement, ou la déconnexion ne clôture pas proprement la session</p> <p>OWASP SCP 62-63</p> <p>OWASP ASVS 3.3.1, 3.3.4</p> <p>OWASP APPSENSOR -</p> <p>CAPEC 21</p> <p>SAFECODE 28</p> <p>Common_Title_full</p>	

GESTION DES SESSIONS	8	GESTION DES SESSIONS	9	GESTION DES SESSIONS	10	GESTION DES SESSIONS	J
	Matt peut profiter abusivement de sessions longues car l'application ne réauthentifie pas régulièrement pour vérifier si les priviléges ont changé		Ivan peut voler des identifiants de session car ceux-ci sont transmis via des canaux non sécurisés, ou sont journalisés, ou sont révélés dans les messages d'erreur, ou sont inutilement accessibles par du code que l'attaquant peut influencer ou modifier		Marce peut contrefaire des requêtes car des tokens per-session, ou per-request pour des actions plus critiques (ex : tokens anti-CSRF ou similaires), ne sont pas utilisés lors des actions qui changent l'état d'une session		Jeff peut rejouer une interaction identique (ex : requête HTTP, signal, click sur bouton), celle-ci est acceptée et non rejetée
GESTION DES SESSIONS	OWASP SCP 96	GESTION DES SESSIONS	OWASP SCP 69, 75-76, 119, 138		OWASP SCP 73-74	GESTION DES SESSIONS	OWASP SCP -
	OWASP ASVS 3.3.2, 3.6.1		OWASP ASVS 1.9.1, 3.1.1, 7.1.1, 7.1.2, 7.2.1, 9.1.3, 9.2.2		OWASP ASVS 4.2.2		OWASP ASVS 11.1.1, 11.1.2, 11.1.3
GESTION DES SESSIONS	OWASP APPSENSOR -	GESTION DES SESSIONS	OWASP APPSENSOR SE4-6		OWASP APPSENSOR IE4	GESTION DES SESSIONS	OWASP APPSENSOR IE5
	CAPEC 21		CAPEC 31, 60		CAPEC 62, 111		CAPEC 60
GESTION DES SESSIONS	SAFECODE 28	GESTION DES SESSIONS	SAFECODE 28		SAFECODE 18	GESTION DES SESSIONS	SAFECODE 12, 14
	Common_Title_full}		Common_Title_full}		Common_Title_full}		OWASP Cornucopia Ecommerce Website Edition v1.20-EN
GESTION DES SESSIONS	Q	GESTION DES SESSIONS	K		(Pas de Carte)	GESTION DES SESSIONS	(Pas de Carte)
	Salim peut contourner la gestion de session car celle-ci n'est pas globalement et régulièrement appliquée à travers l'application		Peter peut contourner les contrôles de gestion de session car ceux-ci ont été développés en interne, au lieu d'utiliser un framework standard ou un module approuvé et testé				
GESTION DES SESSIONS	OWASP SCP 58	GESTION DES SESSIONS	OWASP SCP 58, 60		OWASP ASVS 1.1.6	GESTION DES SESSIONS	OWASP APPSENSOR -
	OWASP ASVS 1.1.6, 3.7.1		OWASP ASVS 1.1.6		OWASP APPSENSOR -		OWASP APPSENSOR -
GESTION DES SESSIONS	OWASP APPSENSOR -	GESTION DES SESSIONS	OWASP APPSENSOR -		CAPEC 21	GESTION DES SESSIONS	CAPEC 21
	CAPEC 21		CAPEC 21		SAFE CODE 14, 28		SAFE CODE 14, 28
GESTION DES SESSIONS	SAFE CODE 14, 28		SAFE CODE 14, 28		Common_Title_full}		Common_Title_full}
	Common_Title_full}		Common_Title_full}				

HABILITATION	A <p>Vous avez inventé une nouvelle attaque contre les Habilitations</p> <p><i>Apprenez-en plus à ce sujet dans les guides gratuits OWASP sur le Développement et les Tests</i></p>	HABILITATION <p>(Pas de Carte)</p>	HABILITATION <p>Tim peut modifier l'emplacement où la donnée est envoyée ou renvoyée</p>	HABILITATION <p>2</p>	HABILITATION <p>3</p> <p>Christian peut accéder à des informations auxquelles il n'est pas habilité via un autre canal pour lequel il l'est (ex : résultats de recherche, journaux, reporting) ou parce que celles-ci sont en cache, ou l'information est conservée plus longtemps que nécessaire, ou toute autre fuite de données</p>
			<p>OWASP SCP 44</p> <hr/> <p>OWASP ASVS 4.1.3, 4.2.1, 5.1.5</p> <hr/> <p>OWASP APPSENSOR -</p> <hr/> <p>CAPEC 153</p> <hr/> <p>SAFECODE 8, 10-11</p> <hr/> <p>{Common_Title_full}</p>		<p>OWASP SCP 51, 100, 135, 139-141, 150</p> <hr/> <p>OWASP ASVS 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</p> <hr/> <p>OWASP APPSENSOR -</p> <hr/> <p>CAPEC 69, 213</p> <hr/> <p>SAFECODE 8, 10-11</p> <hr/> <p>{Common_Title_full}</p>
HABILITATION	4 <p>Kelly peut contourner les contrôles d'habilitation car ils n'échouent pas de façon sécurisée (c'est-à-dire qu'en cas d'échec, retour au comportement par défaut qui est un accès autorisé)</p> <p>OWASP SCP 79-80</p> <hr/> <p>OWASP ASVS 4.1.5</p> <hr/> <p>OWASP APPSENSOR -</p> <hr/> <p>CAPEC 122</p> <hr/> <p>SAFECODE 8, 10-11</p> <hr/> <p>{Common_Title_full}</p>	HABILITATION <p>5</p> <p>Chad peut accéder à des ressources (services, processus, AJAX, Flash, vidéo, images, documents, fichiers temporaires, données de session, de configuration, propriétés système, registre, journaux) auxquelles il ne devrait pas à cause d'habilitations défaillantes ou de privilèges excessifs (par exemple en n'appliquant pas le principe de moindre privilège)</p> <p>OWASP SCP 70, 81, 83, 84, 87-9, 99, 117, 131, 132, 142, 154, 170, 179</p> <hr/> <p>OWASP ASVS 1.2.2, 4.1.1, 4.1.3, 4.2.1</p> <hr/> <p>OWASP APPSENSOR ACE1, ACE2, ACE3, ACE4, HT2</p> <hr/> <p>CAPEC 75, 87, 95, 126, 149, 155, 203, 213, 264-265</p> <hr/> <p>SAFECODE 8, 10-11, 15</p> <hr/> <p>{Common_Title_full}</p>	HABILITATION <p>6</p> <p>Eduardo peut avoir accès à des données auxquelles il n'est pas habilité, même s'il a un accès légitime au formulaire/page/ URL/point d'entrée</p> <p>OWASP SCP 81, 88, 131</p> <hr/> <p>OWASP ASVS 4.1.3, 4.2.1</p> <hr/> <p>OWASP APPSENSOR ACE1-4</p> <hr/> <p>CAPEC 122</p> <hr/> <p>SAFECODE 8, 10-11</p> <hr/> <p>{Common_Title_full}</p>		HABILITATION <p>7</p> <p>Yuanjing peut accéder à des fonctions de l'application, des objets ou des propriétés auxquels elle n'est pas habilitée</p> <p>OWASP SCP 81, 85-86, 131</p> <hr/> <p>OWASP ASVS 4.1.3, 4.2.1</p> <hr/> <p>OWASP APPSENSOR ACE1-4</p> <hr/> <p>CAPEC 122</p> <hr/> <p>SAFECODE 8, 10-11</p> <hr/> <p>{Common_Title_full}</p>

HABILITATION	8 <p>Tom peut contourner les règles métier en altérant la séquence normale du processus ou du flux, ou en réalisant celui-ci dans un ordre incorrect, ou en manipulant la date et l'heure utilisée par l'application, ou en détournant l'usage d'outils légitimes, ou encore en manipulant les données de contrôle.</p> <p>OWASP SCP 10, 32, 93-94, 189</p> <p>OWASP ASVS 4.1.2, 4.2.1, 4.3.3, 7.3.4, 11.1.1, 11.1.2</p> <p>OWASP APPSENSOR ACE3</p> <p>CAPEC 25, 39, 74, 162, 166, 207</p> <p>SAFECODE 8, 10-12</p> <p>{Common_Title_full}</p>	HABILITATION	9 <p>Mike peut altérer le fonctionnement d'une application en utilisant une fonctionnalité légitime trop rapidement ou trop fréquemment, ou d'une façon différente de celle qui est prévue, ou consomme les ressources de l'application, ou cause des situations de compétition (accès concurrent), ou surutilise une fonctionnalité</p> <p>OWASP SCP 94</p> <p>OWASP ASVS 11.1.3, 11.1.4</p> <p>OWASP APPSENSOR AE3, FIO1-2, UT2-4, STE1-3</p> <p>CAPEC 26, 29, 119, 261</p> <p>SAFECODE 1, 35</p> <p>{Common_Title_full}</p>	HABILITATION	10 <p>Richard peut contourner les contrôles d'habilitation centralisés puisqu'ils ne sont pas utilisés de façon exhaustive pour toutes les interactions.</p> <p>OWASP SCP 78, 91</p> <p>OWASP ASVS 1.1.6, 4.1.1</p> <p>OWASP APPSENSOR ACE1-4</p> <p>CAPEC 36, 95, 121, 179</p> <p>SAFECODE 8, 10-11</p> <p>{Common_Title_full}</p>	HABILITATION	J <p>Dinis peut accéder à des informations sur la configuration de sécurité, ou des listes des contrôles d'accès</p> <p>OWASP SCP 89-90</p> <p>OWASP ASVS 4.1.2, 10.2.3-6</p> <p>OWASP APPSENSOR -</p> <p>CAPEC 75, 133, 203</p> <p>SAFECODE 8, 10-11</p> <p>{Common_Title_full}</p>
HABILITATION	Q <p>Christopher peut injecter une commande que l'application exécutera avec un niveau de privilège plus élevé</p> <p>OWASP SCP 209</p> <p>OWASP ASVS 5.3.8</p> <p>OWASP APPSENSOR -</p> <p>CAPEC 17, 30, 69, 234</p> <p>SAFECODE 8, 10-11</p> <p>{Common_Title_full}</p>	HABILITATION	K <p>Ryan peut influencer ou altérer les contrôles d'habilitations et les permissions, et peut ainsi les contourner</p> <p>OWASP SCP 77, 89, 91</p> <p>OWASP ASVS 4.1.1, 4.1.2, 10.2.3-6</p> <p>OWASP APPSENSOR -</p> <p>CAPEC 207, 554</p> <p>SAFECODE 8, 10-11</p> <p>{Common_Title_full}</p>				

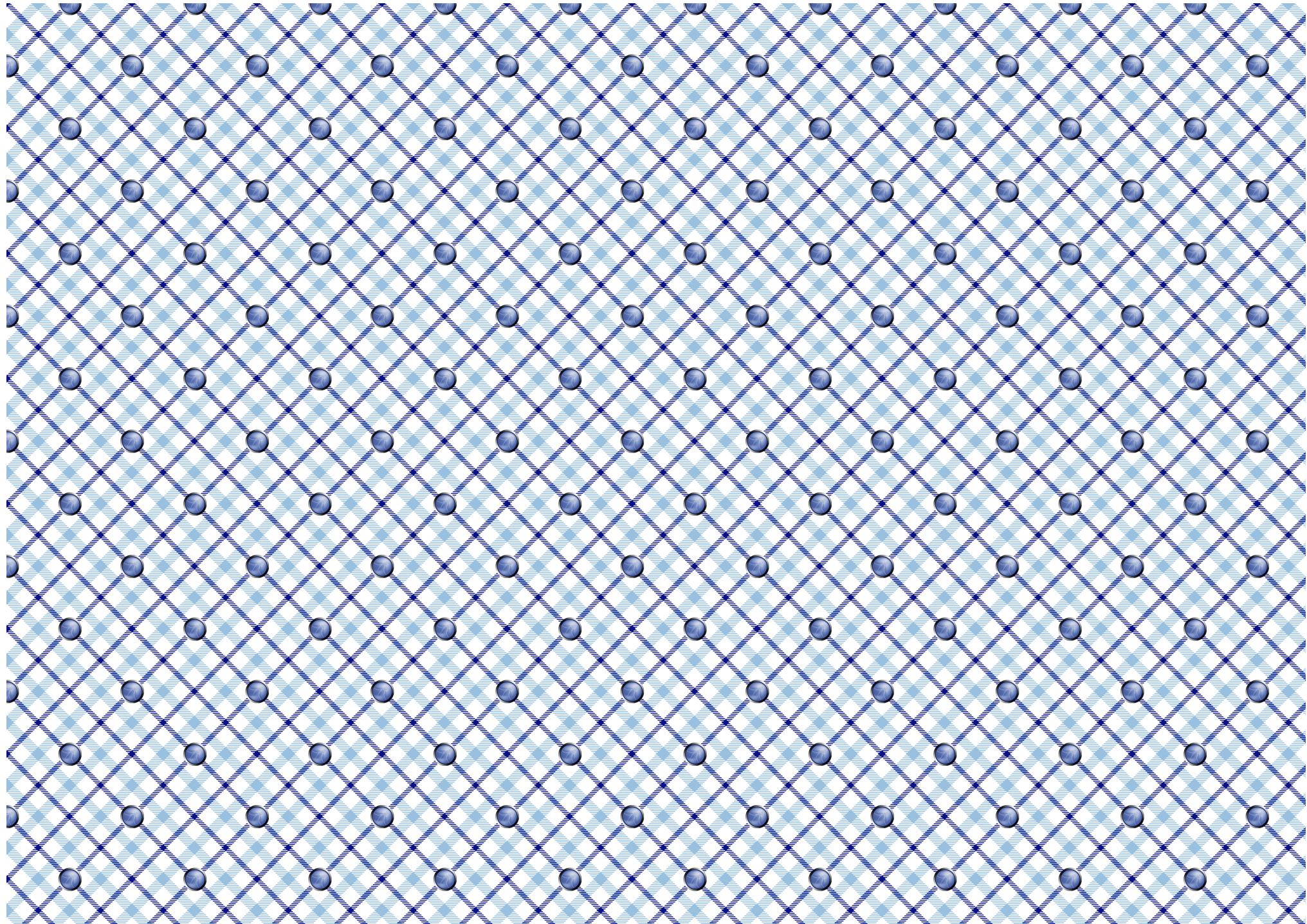
CRYPTOGRAPHIE	<p>A</p> <p>Vous avez inventé une nouvelle attaque contre la Cryptographie</p> <p><i>Apprenez-en plus à ce sujet dans les antisèches gratuites OWASP sur le Stockage Cryptographique et la Protection de la Couche de Transport</i></p>	CRYPTOGRAPHIE	<p>(Pas de Carte)</p>	CRYPTOGRAPHIE	<p>Kyun peut accéder aux données parce qu'elles ont été obfuscées au lieu d'être protégées par une fonction de cryptographie approuvée</p>
	<p>4</p> <p>Paulo peut accéder aux données en transit qui ne sont pas chiffrées, même si le canal de communication est chiffré</p>	CRYPTOGRAPHIE	<p>5</p> <p>Kyle peut contourner les contrôles cryptographiques car ils n'échouent pas de façon sécurisée (c'est-à-dire qu'ils reviennent à leur état non protégé par défaut)</p>	CRYPTOGRAPHIE	<p>6</p> <p>Romain peut lire et modifier des données non chiffrées en mémoire ou en transit (ex. secrets cryptographiques, informations d'identification, identifiants de session, données à caractère personnel et commercialement sensibles), en cours d'utilisation, dans les échanges au sein de l'application, entre l'application et des utilisateurs, entre l'application et des systèmes externes</p>
	<p>7</p> <p>Gunter peut intercepter ou modifier des données chiffrées en transit parce que le protocole est mal déployé, ou faiblement configuré, ou les certificats sont invalides, ou les certificats ne sont pas fiables, ou la connexion peut être dégradée plus faible ou en communication non chiffrée</p>	CRYPTOGRAPHIE	<p>2</p> <p>OWASP SCP 105, 133, 135</p> <p>OWASP ASVS 6.2.2</p> <p>OWASP APPSENSOR ~</p> <p>CAPEC ~</p> <p>SAFECODE 21, 29</p> <p>Common_Title_full}</p>	<p>3</p> <p>Axel peut modifier des données temporaires ou permanentes (stockées ou en transit), ou du code source, ou des mises à jour/patches, ou des données de configuration, parce qu'elles ne sont protégées par aucun contrôle d'intégrité</p>	<p>OWASP SCP 92, 205, 212</p> <p>OWASP ASVS 10.2.3-6, 10.3.1, 10.3.2, 14.1.1, 14.1.4, 14.1.5</p> <p>OWASP APPSENSOR SE1, IE4</p> <p>CAPEC 31, 39, 68, 75, 133, 145, 162, 203, 438-439, 442</p> <p>SAFECODE 12, 14</p> <p>Common_Title_full}</p>

CRYPTOGRAPHIE	8	CRYPTOGRAPHIE	9	CRYPTOGRAPHIE	10	CRYPTOGRAPHIE	J
	Eoin peut accéder à des données métier stockées (par exemple des mots de passe, des identifiants de session, des informations à caractère personnel, des données de titulaires de cartes bancaires) parce qu'elles ne sont pas chiffrées ou hachées de façon sécurisée		Andy peut contourner les fonctions de génération de nombres aléatoires, de génération de GUID aléatoires, de hachage ou de chiffrement parce qu'elles ont été construites par lui-même, ou sont faibles		Susanna peut casser la cryptographie utilisée parce qu'elle n'est pas suffisamment robuste vis-à-vis du niveau de protection requis, ou elle n'est pas suffisamment robuste vis-à-vis de la quantité d'effort que l'attaquant est prêt à faire		Justin peut lire des informations d'identification pour l'accès à des ressources internes ou externes, des services ou d'autres systèmes parce qu'elles sont stockées dans un format non chiffré, ou intégrées dans le code source
CRYPTOGRAPHIE	OWASP SCP 30-31, 70, 133, 135	CRYPTOGRAPHIE	OWASP SCP 60, 104-105	CRYPTOGRAPHIE	OWASP SCP 104-105	CRYPTOGRAPHIE	OWASP SCP 35, 90, 171-172
	OWASP ASVS 2.4.1, 6.2.2, 6.2.3, 8.3.4		OWASP ASVS 6.2.2, 6.2.3, 6.3.1, 6.3.3		OWASP ASVS 6.3.3		OWASP ASVS 1.6.1, 1.6.2, 1.6.4, 2.10.4, 6.4.1, 6.4.2
CRYPTOGRAPHIE	OWASP APPSENSOR -	CRYPTOGRAPHIE	OWASP APPSENSOR -	CRYPTOGRAPHIE	OWASP APPSENSOR -	CRYPTOGRAPHIE	OWASP APPSENSOR -
	CAPEC 31, 37, 55		CAPEC 97		CAPEC 97, 463		CAPEC 116
CRYPTOGRAPHIE	SAFECODE 21, 29, 31	CRYPTOGRAPHIE	SAFE CODE 14, 21, 29, 32-33	CRYPTOGRAPHIE	SAFE CODE 14, 21, 29, 31-33	CRYPTOGRAPHIE	SAFE CODE 21, 29
	\$(Common_Title_full}		\$(Common_Title_full}		\$(Common_Title_full}		\$(Common_Title_full}
CRYPTOGRAPHIE	Q	CRYPTOGRAPHIE	K		(Pas de Carte)		(Pas de Carte)
	Artim peut accéder ou prédire les secrets cryptographiques maîtres		Dan peut influencer ou altérer le code/les routines de cryptographie (chiffrement, hachage, signatures numériques, nombre aléatoire et génération de GUID) et peut ainsi les contourner				
CRYPTOGRAPHIE	OWASP SCP 35, 102	CRYPTOGRAPHIE	OWASP SCP 31, 101				
	OWASP ASVS 1.6.1-3, 6.2.3, 8.3.6		OWASP ASVS 1.6.2, 6.2.5-8				
CRYPTOGRAPHIE	OWASP APPSENSOR -	CRYPTOGRAPHIE	OWASP APPSENSOR -				
	CAPEC 116-117		CAPEC 207, 554				
CRYPTOGRAPHIE	SAFE CODE 21, 29	CRYPTOGRAPHIE	SAFE CODE 14, 21, 29				
	\$(Common_Title_full}		\$(Common_Title_full}				

CORNUCOPIA	A			2	3
	<p>Vous avez inventé une nouvelle attaque de n'importe quel type</p> <p><i>Apprenez-en plus à propos de la sécurité applicative dans les guides gratuits OWASP : Exigences, Développement, Revue de Code et Tests, antisèches, et framework Open Software Assurance Maturity Model</i></p>	(Pas de Carte)		<p>Lee peut contourner les contrôles applicatifs car des fonctions à risque ont été utilisées à la place d'alternatives plus sûres, ou il y a des erreurs de conversion de type, ou car l'application n'est pas fiable lorsqu'une ressource externe est indisponible, ou il y a des situations d'accès concurrent, des problèmes d'initialisation ou d'allocation de ressources, ou des débordements peuvent survenir</p>	<p>Andrew peut accéder au code source, ou décompiler, ou accéder à la logique métier pour comprendre le fonctionnement de l'application et les secrets qu'elle contient</p>
CORNUCOPIA	4		5	6	7
	<p>Keith peut effectuer une action et il n'est pas possible de la lui attribuer.</p>	Larry peut influencer la confiance que les autres parties, y compris les utilisateurs, ont dans l'application, ou abuser de cette confiance ailleurs (par exemple dans une autre application).		<p>Aaron peut contourner les contrôles parce que la gestion des erreurs/exceptions est absente, ou est implémentée de manière incohérente ou partielle, ou ne refuse pas l'accès par défaut (c'est-à-dire que les erreurs doivent mettre fin à l'accès/à l'exécution), ou dépend de la gestion par un autre service ou système.</p>	<p>Les actions de Mwengu ne peuvent pas être étudiées parce qu'il n'y a pas d'enregistrement des événements de sécurité correctement horodaté, parce qu'il n'y a pas de piste d'audit complète, ou parce que ceux-ci peuvent être modifiées ou supprimées par Mwengu, ou parce qu'il n'y a pas de service de centralisation des traces</p>
CORNUCOPIA					
	<p>OWASP SCP 23, 32, 34, 42, 51, 181</p> <p>OWASP ASVS 7.2.1, 7.2.2</p> <p>OWASP APPSENSOR ~</p> <p>CAPEC ~</p> <p>SAFECODE ~</p> <p>Common_Title_full</p>	<p>OWASP SCP ~</p> <p>OWASP ASVS 1.9.2, 9.1.1, 5.1.5, 9.2.1, 9.2.4</p> <p>OWASP APPSENSOR ~</p> <p>CAPEC 89, 103, 181, 459</p> <p>SAFECODE ~</p> <p>Common_Title_full</p>	<p>OWASP SCP 109-112, 155</p> <p>OWASP ASVS 4.1.5, 7.1.4</p> <p>OWASP APPSENSOR ~</p> <p>CAPEC 54, 98, 164</p> <p>SAFECODE 4, 11, 23</p> <p>Common_Title_full</p>	<p>OWASP SCP 113, 114, 115, 117, 118, 121-130</p> <p>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</p> <p>OWASP APPSENSOR ~</p> <p>CAPEC 93</p> <p>SAFECODE 4</p> <p>Common_Title_full</p>	

CORNUCOPIA	8	CORNUCOPIA	9	CORNUCOPIA	10	CORNUCOPIA	J
	David peut contourner l'application pour accéder aux données car l'infrastructure réseau et hôte et les services / applications de support n'ont pas été configurés de manière sécurisée, ni la configuration périodiquement vérifiée, ni les correctifs de sécurité appliqués, ou les données sont stockées localement, ou les données ne sont pas physiquement protégées		Michael peut contourner l'application pour accéder aux données car les outils ou les interfaces d'administration ne sont pas sécurisés de manière adéquate		Spyros peut contourner les contrôles de l'application car les frameworks, les bibliothèques et les composants applicatifs contiennent du code malveillant ou des vulnérabilités (par exemple: interne, sur étagère, externalisé, open source, externe)		Roman peut exploiter l'application car elle a été compilée à l'aide d'outils obsolètes ou sa configuration n'est pas sécurisée par défaut, ou les informations de sécurité n'ont pas été documentées et transmises aux équipes opérationnelles
	OWASP SCP 151, 152, 156, 160, 161, 173-177		OWASP SCP 23, 29, 56, 81, 82, 84-90		OWASP SCP 57, 151-152, 204-205, 213-214		OWASP SCP 90, 137, 148, 151-154, 175-179, 186, 192
	OWASP ASVS 1.4.5, 10.3.1, 10.3.2, 14.1.4, 14.1.5, 14.2.1, 14.2.2		OWASP ASVS 1.4.5, 4.3.1		OWASP ASVS 1.14.3, 10.1.1, 10.2.3-6, 14.2.1		OWASP ASVS 1.14.3, 14.1.1-5, 14.2.1
	OWASP APPSENSOR RF1, RF2		OWASP APPSENSOR		OWASP APPSENSOR		OWASP APPSENSOR
	CAPEC 37, 220, 310, 436, 536		CAPEC 122, 233		CAPEC 68, 438-439, 442, 524, 538		CAPEC -
	SAFECODE -		SAFECODE -		SAFECODE 15		SAFECODE 4
	\$Common_Title_full]		\$Common_Title_full}		\$Common_Title_full}		\$Common_Title_full]
CORNUCOPIA	Q	CORNUCOPIA	K	JOKER	Joker	JOKER	Joker
	Jim peut entreprendre des actions malveillantes, non légitimes, sans détection et réponse en temps réel par l'application		Grant peut utiliser l'application pour refuser le service à certains ou à tous ses utilisateurs		Alice peut utiliser l'application pour attaquer les systèmes et les données des utilisateurs		Bob peut influencer, altérer ou affecter l'application de façon à ce qu'elle ne soit plus conforme aux exigences légales, réglementaires, contractuelles ou autres exigences de l'organisation
	OWASP SCP -		OWASP SCP 41, 55		Avez-vous déjà songé à devenir membre OWASP? Tous les outils, conseils et réunions locales sont gratuits pour tous, mais l'adhésion individuelle aide à soutenir le travail de l'OWASP		Découvrez comment les vulnérabilités peuvent être corrigées dans la OWASP Jnive Shop, Security Shepherd, ou en utilisant les défis en ligne du OWASP Hacking-lab gratuit
	OWASP ASVS 8.1.4, 11.1.1-4		OWASP ASVS 2.2.1, 11.1.3, 11.1.4				
	OWASP APPSENSOR (All)		OWASP APPSENSOR UT1-4, STE3				
	CAPEC -		CAPEC 2, 25, 119, 125				
	SAFECODE 1, 27		SAFECODE 1				
	\$Common_Title_full]		\$Common_Title_full}				

Cut
here



Changelog

Version / Date		Comments
0.1	30 Jul 2012	Draft original.
0.2	10 Aug 2012	Draft revu et mis à jour.
0.3	15 Aug 2012	Draft annoncé à la liste de diffusion de l'OWASP SCP pour commentaire.
0.4	25 Feb 2013	Mise à jour des règles du jeu suite aux commentaires reçus pendant des ateliers. Ajout d'une référence au PCI SSC Information Supplement: PCI DSS E-commerce Guidelines. Texte descriptif étendu et mis à jour. Ajout de la section des contributeurs, de la numérotation des pages, des FAQs et du changelog.
1	25 Feb 2013	Version initiale.
1.01	03 Jun 2013	Ajout d'une discussion relative au jeu de cartes spécifique à un framework. FAQs additionnelles créées. Texte descriptif mis à jour. Nouvelle image de couverture et image de couverture précédente déplacée vers l'arrière. Lignes de coupe ajoutées. Ajout de règles alternatives et de descriptions de sous-ensemble de cartes. Ajout du site web et de la liste de diffusion du projet. Mise à jour de la référence croisée à AppSensor de la carte Roi Cornucopia.
1.02	14 Aug 2013	Ajout d'un avertissement concernant la durée d'impression. Ajout de règles du jeu alternatives additionnelles (« à la blackjack », jouer un jeu sur une semaine, jouer sans interruption et ensuite discuter). Ajout du concept de jeu d'exigences de conformité. Aout des FAQ 5 et 6. Modification des descriptions d'attaque sur les cartes à fond coloré (du gris foncé au noir). Contributeurs au projet ajoutés.
1.03	18 Sep 2013	Modifications mineures du libellé de l'attaque des cartes 2. Vérification et mise à jour des références croisées OWASP SCP et ASVS. Ajout des lettres de code pour les couleurs. Modification (gris foncé vers noir) de toutes les descriptions d'attaque restantes sur les cartes et des couleurs de fond pour offrir plus de contraste et améliorer la lisibilité.
1.04	01 Feb 2014	Texte “changement de mot de passe, changement de mot de passe,” corrigé par “changement de mot de passe, recouvrement de mot de passe,” pour la carte Reine Authentification.
1.05	21 Mar 2014	Mises à jour des règles du jeu alternatives. FAQs additionnelles créées. Contributeurs mis à jour. Ajout des liens podcast et vidéo.
1.1	04 Mar 2015	Date corrigée pour la v1.05 du changelog. Références croisées mises à jour en fonction de la version 2014 d'ASVS. Mise à jour des contributeurs.
1.2	29 Jun 2016	Vidéo mentionnée et indiquée en lien. Feuille de scores séparée mentionnée et indiquée en lien. Suppression des précédentes pages intégrées de la feuille de score. Correction (identifié par Tom Brennan) et ajout dans le texte de la carte 8 Authentification. Ajout d'Oana Cornea et d'autres participants du sommet AppSec EU 2015 project à la liste des contributeurs. Ajout de Dario De Filippis en tant que co-leader du projet. Ajout du lien Wiki Deck. Mise à jour des références croisées en fonction de la v3.0.1 d'ASVS et de la v2.8 de CAPEC. Modifications mineures de texte pour un petit nombre de cartes. Ajout de “-EN” au numéro de version en préparation de la version “-ES”. Ajout de Susana Romaniz en tant que contributeur à la traduction espagnole. Modifications mineures de texte dans les instructions et les FAQs.
1.3	01 Jan 2023	Références croisées mises à jour d'ASVS v3.0.1 vers ASVS v4.0 par Johan Sydseter.

Contributeurs du projet

Tous les projets de l'OWASP reposent sur les contributions volontaires de personnes dans les secteurs du développement de logiciels et de la sécurité de l'information.

Ils ont consacré leurs temps et leur énergie à faire des suggestions, donner des avis, rédiger, reviser et modifier la documentation, encourager, essayer le jeu, et promouvoir le concept.

Sans tous leurs efforts, le projet n'aurait pas progressé jusqu'à ce point.

Veuillez contacter la liste de diffusion ou les chefs du projet directement, s'il manque quelqu'un dans les listes ci-dessous.

- Simon Bennetts
- Sebastien Gioria
- Mark Miller
- Tom Brennan
- Tobias Gondrom
- Cam Morris
- Fabio Cerullo
- Timo Goosen
- Susana Romaniz
- Oana Cornea
- Anthony Harrison
- Ravishankar Sahadevan
- Johanna Curiel
- John Herrlin
- Tao Sauvage
- Todd Dahl
- Jerry Hoff
- Stephen de Vries
- Luis Enriquez
- Marios Kourtesis
- Colin Watson
- Ken Ferris
- Antonis Manaras
- Johan Sydseter
- Dario De Filippis
- Jim Manico

- Les employés de l'OWASP travaillant dur.
- Les participants aux réunions des branches de l'OWASP Londres, de l'OWASP Manchester, de l'OWASP Pays-Bas et de l'OWASP Écosse, ainsi qu'au London Gamification meetup, qui ont fait des suggestions utiles et posé des questions pertinentes
- Blackfoot UK Limited pour le don des fichiers prêt-à-imprimer et des centaines de jeux de cartes imprimées professionnellement pour distribution par la Poste et dans les réunions de branche de l'OWASP
- OWASP NYC pour la création d'un design de boîte OWASP et la distribution de packs à AppSec USA 2014.

Podcasts et vidéos

Les ressources suivantes de l'OWASP® Cornucopia sont disponibles en ligne:

- Vidéo - Using the cards, créée lors du sommet AppSec EU 2015 project, 20 mai 2015
<https://www.youtube.com/watch?v=i5Y0akWj31k>
- Interview Podcast, OWASP 24/7 Podcast channel, 21 mars 2014
<http://trustedsoftwarealliance.com/2014/03/21/the-owasp-cornucopia-project-with-colin-watson/>
- Vidéo de présentation, lors de l'OWASP EU Tour 2013 London, 3 juin 2013
https://www.youtube.com/watch?v=Q_LE-8xNXVk

Visitez le site web du projet pour de plus amples informations et des documents de présentation.



