OWASP
The Open Web Application Security Project

Cornucopia

${Common_Title}

${Common_T00010}

${Common_T00020}
Colin Watson

${Common_T00030}
Colin Watson and Darío De Filippis

${Common_T00040}
Tom Brennan, Johanna Curiel and Timo Goosen

${Common_T00100}

${Common_T00110}

${Common_T00120}

${Common_T00130}

${Common_T00140}

${Common_T00150} ${Common_T00160} ${Common_T00170}

${Common_T00180}

${Common_T00200}

${Common_T00210} ${Common_T00220}

${Common_T00230} ${Common_T00240}

${Common_T00250} ${Common_T00260}

${Common_T00270}

${Common_T00300}

${Common_T00310} ${Common_T00320}

- ${Common_T00330}
- ${Common_T00340}
- ${Common_T00350}
- ${Common_T00360}
- ${Common_T00370}
- ${Common_T00380}

${Common_T00390} ${Common_T00400}

${Common_T00500}

${Common_T00510} ${Common_T00520} ${Common_T00530}

${Common_T00600}

${Common_T00610}

${Common_T00700}

${Common_T00710}

${Common_T00720} ${Common_T00730} ${Common_T00740} ${Common_T00750} ${Common_T00760} ${Common_T00770}

${Common_T00780} ${Common_T00790}

${Common_T00800} ${Common_T00810} ${Common_T00820} ${Common_T00830} ${Common_T00840} ${Common_T00850}

${Common_T00900}

${Common_T00910} ${Common_T00920}

${Common_T01000}

${Common_T01010} ${Common_T01020}

${Common_T01030}

- ${Common_T01040} https://lists.owasp.org/mailman/listinfo/owasp_cornucopia
- ${Common_T01050} https://www.owasp.org/index.php/OWASP_Cornucopia

${Common_T01060} ${Common_T01070}

${Common_T01100}

${Common_T01110} ${Common_T01120} ${Common_T01130} ${Common_T01140} ${Common_T01150}

${Common_T01160}

${Common_T01170} ${Common_T01180}

${Common_T01190}

https://www.owasp.org/index.php/Cornucopia_-_Ecommerce_Website_Edition_-_Wiki_Deck

${Common_T01200}

- ${Common_T01210} https://www.owasp.org/index.php/File:OWASP_SCP_Quick_Reference_Guide_v2.pdf
- ${Common_T01220} https://www.owasp.org/images/3/33/OWASP_Application_Security_Verification_Standard_3.0.1.pdf
- ${Common_T01230} https://www.owasp.org/index.php/AppSensor_DetectionPoints
- ${Common_T01240} http://capec.mitre.org/data/archive/capec_v2.8.zip
- ${Common_T01250} http://www.safecode.org/publications/SAFECode_Agile_Dev_Security0712.pdf

${Common_T01260} ${Common_T01270} ${Common_T01280} ${Common_T01290}

${Common_T01300} ${Common_T01310}

https://youtu.be/i5Y0akWj31khttps://www.owasp.org/index.php/File:Cornucopia-scoresheet.pdf

${Common_T01900}

${Common_T01910} ${Common_T01920} ${Common_T01930}

${Common_T01940}

${Common_T01950} ${Common_T01960} ${Common_T01970}

${Common_T01980}

${Common_T01990} ${Common_T02000}

${Common_T02010} ${Common_T02020} ${Common_T02030}

${Common_T02040}

${Common_T02100}

${Common_T02110} ${Common_T02120}

${Common_T02130} ${Common_T02140}

${Common_T01400}

${Common_T01410}
${Common_T01420}
${Common_T01430}
${Common_T01440}
${Common_T01450}

${Common_T01500}

${Common_T01510} ${Common_T01520} ${Common_T01530}

${Common_T01540}
${Common_T01550}
${Common_T01560}
${Common_T01570}
${Common_T01580} ${Common_T01590}
${Common_T01600}
${Common_T01610}

${Common_T01700}

${Common_T01710}

${Common_T01720}
${Common_T01730}
${Common_T01740}

${Common_T01800}

${Common_T01810}
${Common_T01820}

${Common_T02200}

${Common_T02210}

${Common_T02220}		
${Common_T02230}	${Common_T02270}	${Common_T02310}
${Common_T02240}	*${Common_T02280}*	*${Common_T02320}*
${Common_T02250}	${Common_T02290}	${Common_T02330}
${Common_T02260}	*${Common_T02300}*	*${Common_T02340}*

${Common_T02400}

${Common_T02410}

${Common_T02420}		
${Common_T02430}	${Common_T02470}	${Common_T02510}
${Common_T02440}	*${Common_T02480}*	*${Common_T02520}*
${Common_T02450}	${Common_T02490}	${Common_T02530}
${Common_T02460}	*${Common_T02500}*	*${Common_T02540}*

${Common_T02600}

${Common_T02610}

${Common_T02620}* *${Common_T02630} *${Common_T02640}*

${Common_T02650}

${Common_T02660}

${Common_T02670}

${Common_T02680}* *${Common_T02690} *${Common_T02700}* *${Common_T02710}*
${Common_T02720}* *${Common_T02730} *${Common_T02740}*

${Common_T02750}

${Common_T02760}* *${Common_T02770} *${Common_T02780}*

${Common_T02790}

${Common_T02800}* *${Common_T02810}

${Common_T02820}

${Common_T02830}* *${Common_T02840}

${Common_T02850}

${Common_T02860}* *${Common_T02870} *${Common_T02880}*

${Common_T02890}

${Common_T02900}* *${Common_T02910} *${Common_T02920}*

${Common_T02930}

${Common_T02940}* *${Common_T02950} *${Common_T02960}* *${Common_T02970}*
${Common_T02980}* *${Common_T02990}

${Common_T03000}

${Common_T03010}* *${Common_T03020}

${Common_T03030}

${Common_T03040}* *${Common_T03050}

https://www.owasp.org/index.php/Cornucopia_-_Ecommerce_Website_Edition_-_Wiki_Deck

${Common_T03060}* *${Common_T03070}

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

DATA VALIDATION & ENCODING

A

Vous avez inventé une nouvelle attaque contre la Validation des Données et l'Encodage

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

DATA VALIDATION & ENCODING

(${Common_NoCard})

DATA VALIDATION & ENCODING

2

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

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

OWASP ASVS
1.10, 4.5, 8.1, 11.5, 19.1, 19.5

OWASP APPSENSOR
HT1-3

CAPEC
54, 541

SAFECODE
4, 23

DATA VALIDATION & ENCODING

3

Robert peut saisir des données malveillantes, car le format attendu n'est pas vérifié, ou des duplicatas sont acceptés, ou la structure n'est pas vérifiée, ou les éléments individuels des données ne sont pas validées : type, plage, longueur, liste blanche de caractères ou de formats autorisés

OWASP SCP
-

OWASP ASVS
5.1, 5.16, 5.17, 5.18, 5.19, 5.20, 11.1, 11.2

OWASP APPSENSOR
RE7-8, AE4-7, IE2-3, CIE1, CIE3-4, HT1-3

CAPEC
28, 48, 126, 165, 213, 220-221, 261-262, 271-272

SAFECODE
3, 16, 24, 35

DATA VALIDATION & ENCODING

4

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

OWASP SCP
8, 10, 183

OWASP ASVS
4.16, 5.16, 5.17, 15.1

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 peut contourner les routines d'encodage centralisées, car celles-ci ne sont pas utilisées partout, ou bien de mauvais encodages sont utilisés

OWASP SCP
3, 15, 18-22, 168

OWASP ASVS
1.7, 5.15, 5.21, 5.22, 5.23

OWASP APPSENSOR
-

CAPEC
28, 31, 152, 160, 468

SAFECODE
2, 17

DATA VALIDATION & ENCODING

6

Jason peut contourner les routines d'encodage centralisées, car celles-ci ne sont pas utilisées à chaque saisie

OWASP SCP
3, 168

OWASP ASVS
1.7, 5.6, 5.19

OWASP APPSENSOR
IE2-3

CAPEC
28

SAFECODE
3, 16, 24

DATA VALIDATION & ENCODING

7

Jan peut générer des messages de sorte à tromper la validation des données, car le jeu de caractères n'est pas spécifié/imposé, ou les données sont encodées plusieurs fois, ou les données ne sont pas pleinement converties dans le format que l'application utilise (par exemple canonicalisation) avant leur validation, ou les variables sont insuffisamment typées

OWASP SCP
4-5, 7, 150

OWASP ASVS
5.6, 11.8

OWASP APPSENSOR
IE2-3, EE1-2

CAPEC
28, 153, 165

SAFECODE
3, 16, 24

DATA VALIDATION & ENCODING

8

Sarah peut contourner les routines de sanitisation centralisées, car celles-ci ne sont pas pleinement utilisées

OWASP SCP
15, 169

OWASP ASVS
1.7, 5.21, 5.23

OWASP APPSENSOR
-

CAPEC
28, 31, 152, 160, 468

SAFECODE
2, 17

DATA VALIDATION & ENCODING

9

Shamun peut contourner la validation des saisies ou la validation des sorties, car les échecs de validation ne sont pas rejetés et/ou sanitisés

OWASP SCP
6, 21-22, 168

OWASP ASVS
5.3

OWASP APPSENSOR
IE2-3

CAPEC
28

SAFECODE
3, 16, 24

DATA VALIDATION & ENCODING

10

Darío peut exploiter la confiance que l'application place dans une source de données (par exemple données définies par l'utilisateur, manipulation de données stockées localement, changement de déclaration des données sur un système client, manque de vérification de l'identité pendant la validation de données de telle manière que Darío peut se faire passer pour Colin)

OWASP SCP
2, 19, 92, 95, 180

OWASP ASVS
5.19, 10.6, 16.2, 16.3, 16.4, 16.5, 16.8

OWASP APPSENSOR
IE4, IE5

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

SAFECODE
14

DATA VALIDATION & ENCODING

J

Dennis a le contrôle sur la validation des saisies, la validation des sorties, ou le code d'encodage des sorties, ou les routines, de telle manière que celles-ci peuvent être contournées

OWASP SCP
1, 17

OWASP ASVS
5.5, 5.18

OWASP APPSENSOR
RE3, RE4

CAPEC
87, 207, 554

SAFECODE
2, 17

DATA VALIDATION & ENCODING

Q

Geoff peut injecter des données dans un client ou un système interpréteur, car une interface paramétrée n'est pas utilisée, ou n'a pas été implémentée correctement, ou les données n'ont pas été encodées correctement dans ce contexte, ou il n'y a pas de politique restrictive sur le code ou les ajouts de données

OWASP SCP
10, 15-16, 19-20

OWASP ASVS
5.15, 5.22, 5.23, 5.24, 5.25

OWASP APPSENSOR
IE1, RP3

CAPEC
28, 31, 152, 160, 468

SAFECODE
2, 17

DATA VALIDATION & ENCODING

K

Gabe peut injecter des données dans un interpréteur côté serveur (ex : SQL, commandes OS, Xpath, Server JavaScript, SMTP), car une interface paramétrée fortement typée n'est pas utilisée ou n'a pas été implémentée correctement

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

OWASP ASVS
5.10, 5.11, 5.12, 5.13, 5.14, 5.16, 5.21

OWASP APPSENSOR
CIE1, CIE2

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

SAFECODE
2, 19-20

(${Common_NoCard})

(${Common_NoCard})

AUTHENTICATION

A

Vous avez inventé une nouvelle attaque contre l'Authentification

Apprenez-en plus à ce sujet dans les antisèches gratuites OWASP sur l'Authentification

AUTHENTICATION

(${Common_NoCard})

AUTHENTICATION

2

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)

OWASP SCP 47, 52
OWASP ASVS 2.12, 8.4, 8.10
OWASP APPSENSOR UT1
CAPEC -
SAFECODE 28

AUTHENTICATION

3

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

OWASP SCP 36-37, 40, 43, 48, 51, 119, 139-140, 146
OWASP ASVS 2.2, 2.17, 2.24, 8.7, 9.1, 9.4, 9.5, 9.9, 9.11
OWASP APPSENSOR -
CAPEC 37, 546
SAFECODE 28

AUTHENTICATION

4

Sebastien peut facilement identifier les noms des utilisateurs ou peut les énumérer

OWASP SCP 33, 53
OWASP ASVS 2.18, 2.28
OWASP APPSENSOR AE1
CAPEC 383
SAFECODE 28

AUTHENTICATION

5

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

OWASP SCP 54, 175, 178
OWASP ASVS 2.19
OWASP APPSENSOR AE12, HT3
CAPEC 70
SAFECODE 28

AUTHENTICATION

6

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)

OWASP SCP 37, 45-46, 178
OWASP ASVS 2.22
OWASP APPSENSOR -
CAPEC 50
SAFECODE 28

AUTHENTICATION

7

Cecilia peut réaliser des attaques de type brute force ou de dictionnaire contre un ou plusieurs comptes sans limitation, ou ses attaques sont simplifiées du fait d'une faible politique de mots de passe (faible complexité, longueur, historique, ou durée de vie insuffisante)

OWASP SCP 33, 38-39, 41, 50, 53
OWASP ASVS 2.7, 2.20, 2.23, 2.25, 2.27
OWASP APPSENSOR AE2, AE3
CAPEC 2, 16
SAFECODE 27

AUTHENTICATION

8

Kate peut contourner l'authentification car son échec n'est pas contrôlé (passage en accès non authentifié)

OWASP SCP 28
OWASP ASVS 2.6
OWASP APPSENSOR -
CAPEC 115
SAFECODE 28

AUTHENTICATION

9

Claudia peut effectuer davantage de fonctions critiques car l'authentification est trop faible (ex : pas d'authentification forte à deux facteurs), ou la réauthentification n'est pas requise pour ces fonctions

OWASP SCP 55-56
OWASP ASVS 2.1, 2.9, 2.26, 2.31, 4.15
OWASP APPSENSOR -
CAPEC 21
SAFECODE 14, 28

AUTHENTICATION

10

Pravin peut contourner les contrôles d'authentification car un module/framework/service d'authentification, qui est centralisé, standardisé, testé, autorisé, et séparé de la ressource requêtée, n'est pas utilisé

OWASP SCP 25-27
OWASP ASVS 1.7, 2.30
OWASP APPSENSOR -
CAPEC 90, 115
SAFECODE 14, 28

AUTHENTICATION

J

Mark peut accéder à des ressources ou des services parce qu'il n'y a pas d'authentification, ou il a été pensé à tort que l'authentification était prise en compte par un autre système ou réalisée dans une action précédente

OWASP SCP 23, 32, 34
OWASP ASVS 2.1
OWASP APPSENSOR -
CAPEC 115
SAFECODE 14, 28

AUTHENTICATION

Q

Jaime peut contourner l'authentification car celle-ci n'est pas implémentée avec la même rigueur dans toutes les fonctionnalités (ex : inscription, changement de mot de passe, recouvrement de mot de passe, déconnexion, administration) ou dans toutes les versions/canaux (ex : site web mobile, appli mobile, site web, API, centre d'appel)

OWASP SCP 23, 29, 42, 49
OWASP ASVS 2.1, 2.8
OWASP APPSENSOR -
CAPEC 36, 50, 115, 121, 179
SAFECODE 14, 28

AUTHENTICATION

K

Olga peut influencer ou modifier du code/routines d'authentification de telle manière que celle-ci soit contournée

OWASP SCP 24
OWASP ASVS 2.4, 13.2
OWASP APPSENSOR -
CAPEC 115, 207, 554
SAFECODE 14, 28

(${Common_NoCard})

(${Common_NoCard})

SESSION MANAGEMENT

A

Vous avez inventé une nouvelle attaque contre la Gestion des Sessions

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)

SESSION MANAGEMENT

(${Common_NoCard})

SESSION MANAGEMENT

2

William a le contrôle sur la génération des identifiants de session

OWASP SCP 58-59
OWASP ASVS 3.10
OWASP APPSENSOR SE2
CAPEC 31, 60-61
SAFECODE 28

SESSION MANAGEMENT

3

Ryan peut utiliser le même compte en parallèle, puisque les sessions concurrentes sont autorisées

OWASP SCP 68
OWASP ASVS 3.16, 3.17, 3.18
OWASP APPSENSOR -
CAPEC -
SAFECODE 28

SESSION MANAGEMENT

4

Alison peut régler les cookies d'identification de session vers une autre application web, car le chemin et le domaine sont insuffisamment restreints

OWASP SCP 59, 61
OWASP ASVS 3.12
OWASP APPSENSOR SE2
CAPEC 31, 61
SAFECODE 28

SESSION MANAGEMENT

5

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

OWASP SCP 60, 62, 66-67, 71-72
OWASP ASVS 3.2, 3.7, 3.11
OWASP APPSENSOR SE4-6
CAPEC 31
SAFECODE 28

SESSION MANAGEMENT

6

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

OWASP SCP 64-65
OWASP ASVS 3.3, 3.4, 3.16, 3.17, 3.18
OWASP APPSENSOR SE5, SE6
CAPEC 21
SAFECODE 28

SESSION MANAGEMENT

7

Casey peut utiliser la session d'Adam après qu'il ait terminé, car il n'existe pas de fonction de déconnexion, ou il ne peut pas se déconnecter facilement, ou la déconnexion ne clôt pas proprement la session

OWASP SCP 62-63
OWASP ASVS 3.2, 3.5
OWASP APPSENSOR -
CAPEC 21
SAFECODE 28

SESSION MANAGEMENT

8

Matt peut profiter abusivement de sessions longues car l'application ne réauthentifie pas régulièrement pour vérifier si les privilèges ont changé

OWASP SCP 96
OWASP ASVS -
OWASP APPSENSOR -
CAPEC 21
SAFECODE 28

SESSION MANAGEMENT

9

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

OWASP SCP 69, 75-76, 119, 138
OWASP ASVS 3.6, 8.7, 10.3
OWASP APPSENSOR SE4-6
CAPEC 31, 60
SAFECODE 28

SESSION MANAGEMENT

10

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

OWASP SCP 73-74
OWASP ASVS 4.13
OWASP APPSENSOR IE4
CAPEC 62, 111
SAFECODE 18

SESSION MANAGEMENT

J

Jeff peut rejouer une interaction identique (ex : requête HTTP, signal, click sur bouton), celle-ci est acceptée et non rejetée

OWASP SCP -
OWASP ASVS 15.1, 15.2
OWASP APPSENSOR IE5
CAPEC 60
SAFECODE 12, 14

SESSION MANAGEMENT

Q

Salim peut contourner la gestion de session car celle-ci n'est pas globalement et régulièrement appliquée à travers l'application

OWASP SCP 58
OWASP ASVS 3.1
OWASP APPSENSOR -
CAPEC 21
SAFECODE 14, 28

SESSION MANAGEMENT

K

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

OWASP SCP 58, 60
OWASP ASVS 1.7
OWASP APPSENSOR -
CAPEC 21
SAFECODE 14, 28

(${Common_NoCard})

(${Common_NoCard})

AUTHORIZATION

A

Vous avez inventé une nouvelle attaque contre les Habilitations

Apprenez-en plus à ce sujet dans les guides gratuits OWASP sur le Développement et les Tests

AUTHORIZATION

4

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)

OWASP SCP 79-80
OWASP ASVS 4.8
OWASP APPSENSOR -
CAPEC 122
SAFECODE 8, 10-11

AUTHORIZATION

(${Common_NoCard})

AUTHORIZATION

5

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)

OWASP SCP 70, 81, 83-4, 87-9, 99, 117, 131-2, 142, 154, 170, 179
OWASP ASVS 4.1, 4.4, 4.9, 19.3
OWASP APPSENSOR ACE1, ACE2, ACE3, ACE4, HT2
CAPEC 75, 87, 95, 126, 149, 155, 203, 213, 264-265
SAFECODE 8, 10-11, 13

AUTHORIZATION

2

Tim peut modifier l'emplacement où la donnée est envoyée ou renvoyée

OWASP SCP 44
OWASP ASVS 4.1, 4.16, 16.1
OWASP APPSENSOR -
CAPEC 153
SAFECODE 8, 10-11

AUTHORIZATION

6

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

OWASP SCP 81, 88, 131
OWASP ASVS 4.1, 4.4
OWASP APPSENSOR ACE1-4
CAPEC 122
SAFECODE 8, 10-11

AUTHORIZATION

3

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

OWASP SCP 51, 100, 135, 139-141, 150
OWASP ASVS 4.1, 8.2, 9.1-9.6, 9.11, 16.6-16.7
OWASP APPSENSOR -
CAPEC 69, 213
SAFECODE 8, 10-11

AUTHORIZATION

7

Yuanjing peut accéder à des fonctions de l'application, des objets ou des propriétés auxquels elle n'est pas habilitée

OWASP SCP 81, 85-86, 131
OWASP ASVS 4.1, 4.4
OWASP APPSENSOR ACE1-4
CAPEC 122
SAFECODE 8, 10-11

AUTHORIZATION

8

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.

OWASP SCP 10, 32, 93-94, 189
OWASP ASVS 4.10, 4.15, 4.16, 8.13, 15.1
OWASP APPSENSOR ACE3
CAPEC 25, 39, 74, 162, 166, 207
SAFECODE 8, 10-12

AUTHORIZATION

9

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

OWASP SCP 94
OWASP ASVS 4.14, 15.2
OWASP APPSENSOR AE3, FIO1-2, UT2-4, STE1-3
CAPEC 26, 29, 119, 261
SAFECODE 1, 35

AUTHORIZATION

10

Richard peut contourner les contrôles d'habilitation centralisés puisqu'ils ne sont pas utilisés de façon exhaustive pour toutes les interactions.

OWASP SCP 78, 91
OWASP ASVS 1.7, 4.11
OWASP APPSENSOR ACE1-4
CAPEC 36, 95, 121, 179
SAFECODE 8, 10-11

AUTHORIZATION

J

Dinis peut accéder à des informations sur la configuration de sécurité, ou des listes des contrôles d'accès

OWASP SCP 89-90
OWASP ASVS 4.10, 13.2
OWASP APPSENSOR -
CAPEC 75, 133, 203
SAFECODE 8, 10-11

AUTHORIZATION

Q

Christopher peut injecter une commande que l'application exécutera avec un niveau de privilège plus élevé

OWASP SCP 209
OWASP ASVS 5.12
OWASP APPSENSOR -
CAPEC 17, 30, 69, 234
SAFECODE 8, 10-11

AUTHORIZATION

K

Ryan peut influencer ou altérer les contrôles d'habilitations et les permissions, et peut ainsi les contourner

OWASP SCP 77, 89, 91
OWASP ASVS 4.9, 4.10, 13.2
OWASP APPSENSOR -
CAPEC 207, 554
SAFECODE 8, 10-11

(${Common_NoCard})

(${Common_NoCard})

CRYPTOGRAPHY

A

Vous avez inventé une nouvelle attaque contre la Cryptographie

Apprenez-en plus à ce sujet dans les antisèches gratuites OWASP sur le Stockage Cryptographique et la Protection de la Couche de Transport

CRYPTOGRAPHY

4

Paulo peut accéder aux données en transit qui ne sont pas chiffrées, même si le canal de communication est chiffré

OWASP SCP 37, 88, 143, 214
OWASP ASVS 7.12, 9.2
OWASP APPSENSOR -
CAPEC 185-187
SAFECODE 14, 29-30

CRYPTOGRAPHY

({Common_NoCard})

CRYPTOGRAPHY

5

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)

OWASP SCP 103, 145
OWASP ASVS 7.2, 10.3
OWASP APPSENSOR -
CAPEC -
SAFECODE 21, 29

CRYPTOGRAPHY

2

Kyun peut accéder aux données parce qu'elles ont été obfusquées au lieu d'être protégées par une fonction de cryptographie approuvée

OWASP SCP 105, 133, 135
OWASP ASVS -
OWASP APPSENSOR -
CAPEC -
SAFECODE 21, 29

CRYPTOGRAPHY

6

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

OWASP SCP 36-37, 143, 146-147
OWASP ASVS 2.16, 9.2, 9.11, 10.3, 19.2
OWASP APPSENSOR -
CAPEC 31, 57, 102, 157-158, 384, 466, 546
SAFECODE 29

CRYPTOGRAPHY

3

Axel peut modifier des données temporaires ou permanentes (stockées ou en transit), ou du code source, ou des mises à jour/patchs, ou des données de configuration, parce qu'elles ne sont protégées par aucun contrôle d'intégrité

OWASP SCP 92, 205, 212
OWASP ASVS 8.11, 11.7, 13.2, 19.5, 19.6, 19.7, 19.8
OWASP APPSENSOR SE1, IE4
CAPEC 31, 39, 68, 75, 133, 145, 162, 203, 438-439, 442
SAFECODE 12, 14

CRYPTOGRAPHY

7

Gunter peut intercepter ou modifier des données chiffrées en transit parce que le protocole est mal déployé, ou faiblement configuré, ou les certificats sont invalides, or les certificats ne sont pas fiables, ou la connexion peut être dégradée plus faible ou en communication non chiffrée

OWASP SCP 75, 144-145, 148
OWASP ASVS 10.1, 10.5, 10.10, 10.11, 10.12, 10.13, 10.14
OWASP APPSENSOR IE4
CAPEC 31, 216
SAFECODE 14, 29-30

CRYPTOGRAPHY

8

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

OWASP SCP 30-31, 70, 133, 135
OWASP ASVS 2.13, 7.7, 7.8, 9.2
OWASP APPSENSOR -
CAPEC 31, 37, 55
SAFECODE 21, 29, 31

CRYPTOGRAPHY

9

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

OWASP SCP 60, 104-105
OWASP ASVS 7.6, 7.7, 7.8, 7.15
OWASP APPSENSOR -
CAPEC 97
SAFECODE 14, 21, 29, 32-33

CRYPTOGRAPHY

10

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

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

CRYPTOGRAPHY

J

Justin peut lire des informations d'identification pour l'accès à des ressources internes ou externes, des services ou d'autres systèmes parce qu'elles sont stockées dans un format non chiffré, ou intégrées dans le code source

OWASP SCP 35, 90, 171-172
OWASP ASVS 2.29
OWASP APPSENSOR -
CAPEC 116
SAFECODE 21, 29

CRYPTOGRAPHY

Q

Randolph peut accéder ou prédire les secrets cryptographiques maîtres

OWASP SCP 35, 102
OWASP ASVS 7.8, 7.9, 7.11, 7.13, 7.14
OWASP APPSENSOR -
CAPEC 116-117
SAFECODE 21, 29

CRYPTOGRAPHY

K

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

OWASP SCP 31, 101
OWASP ASVS 7.11
OWASP APPSENSOR -
CAPEC 207, 554
SAFECODE 14, 21, 29

(${Common_NoCard})

(${Common_NoCard})

CORNUCOPIA

A

Vous avez inventé une nouvelle attaque de n'importe quel type

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

CORNUCOPIA

(${Common_NoCard})

CORNUCOPIA

2

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

OWASP SCP
194-202, 205-209

OWASP ASVS
5.1

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 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

OWASP SCP
134

OWASP ASVS
19.5

OWASP APPSENSOR
-

CAPEC
189, 207

SAFECODE
-

CORNUCOPIA

4

Keith peut effectuer une action et il n'est pas possible de la lui attribuer.

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

OWASP ASVS
8.10

OWASP APPSENSOR
-

CAPEC
-

SAFECODE
-

CORNUCOPIA

5

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).

OWASP SCP
-

OWASP ASVS
-

OWASP APPSENSOR
-

CAPEC
89, 103, 181, 459

SAFECODE
-

CORNUCOPIA

6

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.

OWASP SCP
109-112, 155

OWASP ASVS
8.2, 8.4

OWASP APPSENSOR
-

CAPEC
54, 98, 164

SAFECODE
4, 11, 23

CORNUCOPIA

7

Les actions de Mwengu ne peuvent pas être étudiées parce qu'il n'y a pas d'enregistrement des événements de sécurité correctement horodaté, parce qu'il n'y a pas de piste d'audit complète, ou parce que ceux-ci peuvent être modifiées ou supprimées par Mwengu, ou parce qu'il n'y a pas de service de centralisation des traces

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

OWASP ASVS
2.12, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 8.11, 8.12, 9.10, 10.4

OWASP APPSENSOR
-

CAPEC
93

SAFECODE
4

CORNUCOPIA

8

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

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

OWASP ASVS
19.1, 19.4, 19.6, 19.7, 19.8

OWASP APPSENSOR
RE1, RE2

CAPEC
37, 220, 310, 436, 536

SAFECODE
-

CORNUCOPIA

9

Michael peut contourner l'application pour accéder aux données car les outils ou les interfaces d'administration ne sont pas sécurisés de manière adéquate

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

OWASP ASVS
2.1, 2.32

OWASP APPSENSOR
-

CAPEC
122, 233

SAFECODE
-

CORNUCOPIA

10

Xavier peut contourner les contrôles de l'application car les frameworks, les bibliothèques et les composants applicatifs contiennent du code malveillant ou des vulnérabilités (par exemple: interne, sur étagère, externalisé, open source, externe)

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

OWASP ASVS
1.11

OWASP APPSENSOR
-

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

SAFECODE
15

CORNUCOPIA

J

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

OWASP ASVS
19.5, 19.9

OWASP APPSENSOR
-

CAPEC
-

SAFECODE
4

CORNUCOPIA

Q

Jim peut entreprendre des actions malveillantes, non légitimes, sans détection et réponse en temps réel par l'application

OWASP SCP
-

OWASP ASVS
4.14, 9.8, 15.1, 15.2

OWASP APPSENSOR
(All)

CAPEC
-

SAFECODE
1, 27

CORNUCOPIA

K

Gareth peut utiliser l'application pour refuser le service à certains ou à tous ses utilisateurs

OWASP SCP
41, 55

OWASP ASVS
-

OWASP APPSENSOR
UT1-4, STE3

CAPEC
2, 25, 119, 125

SAFECODE
1

JOKER

Joker

Alice peut utiliser l'application pour attaquer les systèmes et les données des utilisateurs

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

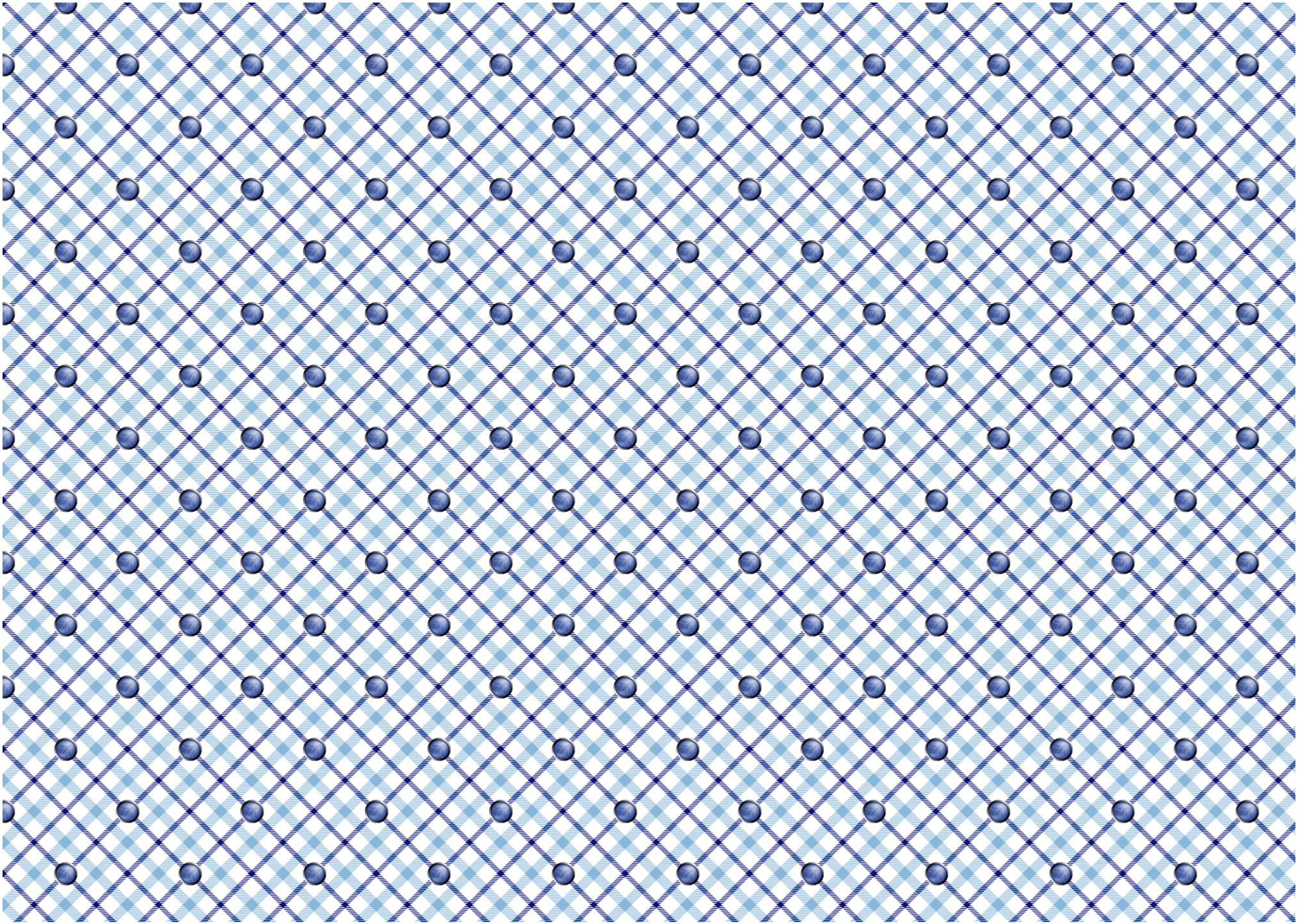
JOKER

Joker

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

Découvrez comment les vulnérabilités peuvent être corrigées dans les applications de formation de la VM gratuite OWASP Broken Web Applications, ou en utilisant les défis en ligne du Hacking Lab gratuit

Cut here



${Common_T03100}

${Common_T03110}		${Common_T03120}
${Common_T03130}	30 Jul 2012	${Common_T03140}
${Common_T03150}	10 Aug 2012	${Common_T03160}
${Common_T03170}	15 Aug 2012	${Common_T03180}
${Common_T03190}	25 Feb 2013	${Common_T03200} ${Common_T03210} ${Common_T03220} ${Common_T03230}
${Common_T03240}	25 Feb 2013	${Common_T03250}
${Common_T03260}	03 Jun 2013	${Common_T03270} ${Common_T03280} ${Common_T03290} ${Common_T03300} ${Common_T03310} ${Common_T03320} ${Common_T03330} ${Common_T03340}
${Common_T03350}	14 Aug 2013	${Common_T03360} ${Common_T03370} ${Common_T03380} ${Common_T03390} ${Common_T03400} ${Common_T03410}
${Common_T03420}	18 Sep 2013	${Common_T03430} ${Common_T03440} ${Common_T03450} ${Common_T03460}
${Common_T03470}	01 Feb 2014	${Common_T03480}
${Common_T03490}	21 Mar 2014	${Common_T03500} ${Common_T03510} ${Common_T03520} ${Common_T03530}
${Common_T03540}	04 Mar 2015	${Common_T03550} ${Common_T03560} ${Common_T03570}
${Common_T03580}	29 Jun 2016	${Common_T03590} ${Common_T03600} ${Common_T03610} ${Common_T03620} ${Common_T03630} ${Common_T03640} ${Common_T03650} ${Common_T03660} ${Common_T03670} ${Common_T03680} ${Common_T03690} ${Common_T03700}

${Common_T03800}

${Common_T03810}

${Common_T03820}

${Common_T03830}

${Common_T03840}

- 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

- ${Common_T03850}
- ${Common_T03860}
- ${Common_T03870}
- ${Common_T03880}

${Common_T03900}

${Common_T03910}

- ${Common_T03920}
  https://www.youtube.com/watch?v=i5Y0akWj31k
- ${Common_T03930}
  http://trustedsoftwarealliance.com/2014/03/21/the-owasp-cornucopia-project-with-colin-watson/
- ${Common_T03940}
  https://www.youtube.com/watch?v=Q_LE-8xNXVk

${Common_T03950}