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

Has creado un nuevo ataque contra validación de datos y codificación

Lea más sobre este tema en Cheat Sheets de OWASP libre, XSS Prevención, basada en DOM Prevención XSS, SQL Prevención de inyecciones, y Parametrización de consultas

DATA VALIDATION & ENCODING

(${Common_NoCard})

DATA VALIDATION & ENCODING

2

Brian puede reunir información sobre las principales configuraciones: esquemas, lógicas, código, software, servicios e infraestructura debido al contenido de mensajes de error, configuración deficiente, o a la presencia de archivos de instalación predeterminados o antiguos, de prueba, de copia de seguridad o copias de los recursos, o exposición de código fuente

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 puede ingresar datos maliciosos porque el formato de protocolo permitido no está siendo revisado, los duplicados son aceptados, la estructura no está siendo validada, los elementos de datos individuales no están siendo validados por: formato, tipo, rango, longitud y una lista blanca de formatos o caracteres permitidos

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 puede ingresar datos o nombres maliciosos en campos porque actualmente no hay una revisión o monitoreo a nivel de usuario o proceso

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 puede eludir las rutinas de codificación centralizadas, ya que dichas rutinas no son usadas por todos los activos o se están utilizando codificaciones incorrectas

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 puede eludir las rutinas de validación centralizadas, ya que no se utilizan en todas las entradas

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 puede crear cargas especiales para frustrar la validación de entrada, porque el conjunto de caracteres no es especificado/aplicado, o los datos se codifican varias veces, o los datos no están completamente transformados en el mismo formato que la aplicación usa (por ejemplo, canonicalización) antes de ser validados, o las variables no están configuradas de manera robusta

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 puede pasar por alto las rutinas de sanitización centralizadas ya que no están siendo utilizadas exhaustivamente

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 puede pasar por alto los checks de validaciones de entrada o salida porque los fallos en las validaciones no son rechazados y/o sanitizados

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 puede explotar la confianza que la aplicación deposita en una fuente de datos (por ejemplo, datos definibles por el usuario, manipulación de datos almacenados localmente, alteración de los datos del estado en un dispositivo cliente, falta de verificación de identidad durante la validación de datos, como Darío puede pretender ser 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 tiene control sobre la validación de entrada, la validación de salida o código de codificación de salida o rutinas para que puedan ser evitados

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 puede inyectar datos en el lado del cliente o en el dispositivo porque no se está utilizando una interfaz parametrizada, o no ha sido implementada correctamente, o los datos no han sido codificados correctamente, o no hay una política restrictiva en el código o los datos incluidos

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 puede inyectar datos en un intérprete del lado del servidor (por ejemplo, SQL, comandos del sistema operativo, Xpath, servidor JavaScript, SMTP) porque no se está utilizando una interfaz parametrizada fuertemente tipificada o no se ha implementado correctamente

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

Usted tiene inventado un nuevo ataque contra la autenticación

Leer mas sobre este tema en OWASP's free Authentication Cheat Sheet

AUTHENTICATION

(${Common_NoCard})

AUTHENTICATION

2

James puede emprender funciones de autenticación sin que el usuario real se dé cuenta alguna vez de lo ocurrido (por ejemplo, intento de logueo, inicio de sesión con credenciales robadas, restablecimiento de la contraseña)

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

AUTHENTICATION

3

Muhammad puede obtener una contraseña de usuario u otros secretos tales como preguntas de seguridad, por observación durante el ingreso o desde el cache, o desde la memoria, o en tránsito, o leyéndolo de alguna ubicación desprotegida, o porque es ampliamente conocido, o porque nunca caduca, o porque el usuario no puede cambiar su propia contraseña

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 puede fácilmente identificar nombres de usuario o puede enumerarlos

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

AUTHENTICATION

5

Javier puede usar credenciales por defecto, de prueba o fáciles de adivinar para autenticar, o puede usar una cuenta antigua o una cuenta no necesaria para la aplicación

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

AUTHENTICATION

6

Sven puede reutilizar contraseñas temporales porque el usuario no realizó el cambio en el primer logueo. o tiene demasiado tiempo y no tiene vencimiento, o no usa un método correcto de entrega (por ejemplo, publicación, aplicación móvil, SMS)

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

AUTHENTICATION

7

Cecilia puede usar ataques de fuerza bruta y ataques de diccionario sin límites contra uno o muchas cuentas, o estos ataques se simplifican debido a una complejidad insuficiente, longitud, caducidad inadecuada y reutilización de requisitos para las contraseñas

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 puede pasar por alto la autenticación porque ésta no falla de forma segura (es decir, por defecto permite acceso no autenticado)

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

AUTHENTICATION

9

Claudia puede utilizar Funciones más críticas porque los requisitos de autenticación son demasiado débiles (por ejemplo, no usa autenticación robusta como el doble factor), o no hay requisitos de re-autenticación para éstos

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 puede omitir el control de autenticación porque no se está utilizando un módulo/framework/servicio de autenticación centralizado, estándar, testeado, probado y aprobado, separado del recurso solicitado

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

AUTHENTICATION

J

Mark puede acceder a los recursos o servicios porque no hay requisitos de autenticación, o fue asumido erróneamente que la autentificación sería realizada por algún otro sistema o realizada en alguna acción previa

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

AUTHENTICATION

Q

Jaime puede omitir la autenticación porque no se aplica con igual rigor para todos los tipos de funcionalidad de autenticación (por ejemplo, registro, cambio de contraseña, recuperación de contraseña, cierre de sesión, administración) o en todas las versiones / canales (por ejemplo, sitio web móvil, aplicación móvil, sitio web completo, API, call center)

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 puede influir o alterar el código o rutina de autenticación o puede evitarlo

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

Has inventado un nuevo ataque contra la gestión de sesión

Read more about this topic in OWASP's free Cheat Sheets on Session Management, and Cross Site Request Forgery (CSRF) Prevention

SESSION MANAGEMENT

(${Common_NoCard})

SESSION MANAGEMENT

2

William tiene el control sobre la generación de identificadores de sesión

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

SESSION MANAGEMENT

3

Ryan puede usar una sola cuenta en paralelo ya que permite sesiones concurrentes

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

SESSION MANAGEMENT

4

Alison puede configurar cookies de identificación de sesión en otra aplicación web porque el dominio y la ruta no están suficientemente restringidos

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

SESSION MANAGEMENT

5

John puede predecir o adivinar los identificadores de sesión porque no se cambian cuando se modifica la función del usuario (por ejemplo, la autenticación previa y posterior) y cuando se cambia entre comunicaciones no cifradas y cifradas, o no son lo suficientemente largas y aleatorias, o no se cambian periódicamente

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 puede hacerse cargo de la sesión de un usuario porque hay un tiempo de espera de inactividad largo o nulo, un límite de tiempo de sesión general largo o nulo, o la misma sesión puede usarse desde más de un dispositivo / ubicación

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 puede utilizar la sesión de Adam después de que haya terminado, porque no hay una función de cierre de sesión, o no puede cerrar sesión fácilmente, o el cierre de sesión no termina la sesión correctamente

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

SESSION MANAGEMENT

8

Matt puede abusar de sesiones largas porque la aplicación no requiere una autenticación periódica para verificar si los privilegios han cambiado

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

SESSION MANAGEMENT

9

Ivan puede robar identificadores de sesión porque se envían a través de canales inseguros, se registran, se revelan en mensajes de error, se incluyen en URL o son accesibles de manera innecesaria mediante el código que el atacante puede influir o modificar

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 puede forjar solicitudes porque las sesiones por sesión o por acciones más críticas, los tokens aleatorios fuertes (es decir, los tokens anti-CSRF) o similares no se utilizan para acciones que cambian de estado

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

SESSION MANAGEMENT

J

Jeff puede reenviar una interacción de repetición idéntica (por ejemplo, solicitud HTTP, señal, pulsación de botón) y se acepta, no se rechaza

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

SESSION MANAGEMENT

Q

Salim puede omitir la administración de sesiones porque no se aplica de manera integral y coherente en toda la aplicación

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

SESSION MANAGEMENT

K

Peter puede omitir los controles de administración de la sesión porque se construyeron por sí mismos y / o son débiles, en lugar de usar un marco estándar o un módulo aprobado aprobado

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

(${Common_NoCard})

(${Common_NoCard})

AUTHORIZATION

A

Has inventado un nuevo ataque contra la Autorización

Read more about this topic in OWASP's Development and Testing Guides

AUTHORIZATION

(${Common_NoCard})

AUTHORIZATION

2

Tim puede influir a donde se envía o reenvía la data

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

AUTHORIZATION

3

Christian puede acceder a información, a la que no debería tener permiso, a través de otro mecanismo al que sí tiene permiso (por ejemplo, indexador de búsqueda, registrador, reporte), o porque está en caché, o guardada por más tiempo del necesario u otro medio de fuga de información

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

4

Kelly puede eludir los controles de autorización porque no fallan de forma segura (es decir, por defecto permiten el acceso)

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

AUTHORIZATION

5

Chad puede acceder a los recursos (incluidos servicios, procesos, AJAX, Flash, video, imágenes, documentos, archivos temporales, datos de sesión, propiedades del sistema, datos de configuración, registro de configuración, logs) a los que no debería poder acceder debido a la falta de autorización, o debido a privilegios excesivos(por ejemplo, no usar el principio de menor privilegio)

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

6

Eduardo puede acceder a los datos a los que él no tiene permiso, incluso aunque tiene permiso para formulario / página / URL / punto de entrada

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

AUTHORIZATION

7

Yuanjing puede acceder a funciones de la aplicación, objetos o propiedades a las que él no está autorizado para acceder

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 puede omitir las reglas de negocios al alterar la secuencia o flujo de proceso habitual, o realizar el proceso en el orden incorrecto, o manipular los valores de fecha y hora utilizados por la aplicación, o usar características válidas para propósitos no intencionados, o manipulando los datos de control

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 puede hacer uso incorrecto de una aplicación al usar una función válida demasiado rápido, o con demasiada frecuencia, o de otra forma sin intención, o que consuma los recursos de la aplicación, o cause condiciones de carrera, o sobreutilice una función

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 puede eludir los controles de autorización centralizados ya que no están siendo utilizados exhaustivamente en todas las interacciones

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 puede acceder a la información de configuración de seguridad, o listas de control de acceso

OWASP SCP
89-90

OWASP ASVS
4.10, 13.2

OWASP APPSENSOR
-

CAPEC
75, 133, 203

SAFECODE
8, 10-11

AUTHORIZATION

Q

Christopher puede inyectar un comando para que la aplicación se ejecute con un nivel de privilegios más alto

OWASP SCP
209

OWASP ASVS
5.12

OWASP APPSENSOR
-

CAPEC
17, 30, 69, 234

SAFECODE
8, 10-11

AUTHORIZATION

K

Ryan puede influir o alterar controles y permisos de autorización, y por ende puede

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

Has inventado un nuevo ataque contra la Criptografía

Read more about this topic in OWASP's free Cheat Sheets on Cryptographic Storage, and Transport Layer Protection

CRYPTOGRAPHY

(${Common_NoCard})

CRYPTOGRAPHY

2

Kyun puede acceder a los datos porque ha sido ofuscado en lugar de utilizar una función criptográfica aprobada

OWASP SCP
105, 133, 135

OWASP ASVS
-

OWASP APPSENSOR
-

CAPEC
-

SAFECODE
21, 29

CRYPTOGRAPHY

3

Axel puede modificar datos transitorios o permanentes (almacenados o en tránsito), código fuente, actualizaciones / parches o datos de configuración, ya que no están sujetos a verificación de integridad

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

4

Paulo puede acceder a datos en tránsito que no están encriptados, incluso aunque el canal está encriptado

OWASP SCP
37, 88, 143, 214

OWASP ASVS
7.12, 9.2

OWASP APPSENSOR
-

CAPEC
185-187

SAFECODE
14, 29-30

CRYPTOGRAPHY

5

Kyle puede pasar por alto controles criptográficos porque estos no fallan de forma segura (es decir, por defecto no protegen)

OWASP SCP
103, 145

OWASP ASVS
7.2, 10.3

OWASP APPSENSOR
-

CAPEC
-

SAFECODE
21, 29

CRYPTOGRAPHY

6

Romain puede leer y modificar datos sin cifrar en la memoria o en tránsito (por ejemplo, secretos criptográficos, credenciales, identificadores de sesión, datos personales y comerciales), en uso o en comunicaciones dentro de la aplicación, o entre la aplicación y los usuarios, o entre la aplicación y sistemas externos

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

7

Gunter puede interceptar o modificar datos encriptados en tránsito porque el protocolo está mal implementado o configurado de manera débil, o los certificados no son válidos, los certificados no son confiables o la conexión puede degradarse a una comunicación más débil o no encriptada

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 puede acceder a los datos comerciales almacenados (por ejemplo, contraseñas, identificadores de sesión, PII, datos del titular de la tarjeta) porque no está cifrado de forma segura ni hash de forma segura

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 puede omitir la generación de números aleatorios, la generación aleatoria de GUID, el hash y las funciones de cifrado porque han sido construidos por sí mismos y / o son débiles

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 puede romper la criptografía en uso porque no es lo suficientemente fuerte para el grado de protección requerido, o no lo es para la cantidad de esfuerzo que el atacante está dispuesto a hacer

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

CRYPTOGRAPHY

J

Justin puede leer las credenciales para acceder a recursos, servicios y otros sistemas internos o externos porque se almacenan en un formato no cifrado o se guardan en el código fuente

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

CRYPTOGRAPHY

Q

Randolph puede acceder o predecir los algoritmos o llaves de los secretos criptográficos

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 puede influir o alterar el código / las rutinas criptográficas (cifrado, hash, firmas digitales, números aleatorios y generación de GUID) y, por lo tanto, puede omitirlos

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

(${Common_NoCard})

(${Common_NoCard})

CORNUCOPIA

A

Has inventado un nuevo ataque de cualquier tipo

Read more about application security in OWASP's free Guides on Requirements, Development, Code Review and Testing, the Cheat Sheet series, and the Open Software Assurance Maturity Model

CORNUCOPIA

(${Common_NoCard})

CORNUCOPIA

2

Lee puede omitir los controles de la aplicación porque se han usado funciones de lenguaje de programación peligrosas/riesgosas en lugar de alternativas más seguras, o hay errores de conversión de tipo, o porque la aplicación no es confiable cuando un recurso externo no está disponible, o hay race conditions, o hay problemas en la inicialización/asignación de recursos, o pueden ocurrir

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 puede acceder al código fuente, o descompilar, o de otro modo acceder a la lógica de negocio para entender cómo la aplicación y cualquier secreto contenido funciona

OWASP SCP
134

OWASP ASVS
19.5

OWASP APPSENSOR
-

CAPEC
189, 207

SAFECODE
-

CORNUCOPIA

4

Keith puede realizar una acción y no es posible atribuirla a él

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

OWASP ASVS
8.10

OWASP APPSENSOR
-

CAPEC
-

SAFECODE
-

CORNUCOPIA

5

Larry puede influir en la confianza que otras partes, incluidos los usuarios tienen en la aplicación, o abusar de esa confianza en otra parte (por ejemplo, en otra aplicación)

OWASP SCP
-

OWASP ASVS
-

OWASP APPSENSOR
-

CAPEC
89, 103, 181, 459

SAFECODE
-

CORNUCOPIA

6

Aaron puede omitir los controles porque falta el manejo de errores/excepciones, o se implementa de manera inconsistente o parcial, o no niega el acceso por defecto (es decir, los errores deben terminar el acceso / ejecución), o se basan en el manejo por parte de otro servicio o sistema

OWASP SCP
109-112, 155

OWASP ASVS
8.2, 8.4

OWASP APPSENSOR
-

CAPEC
54, 98, 164

SAFECODE
4, 11, 23

CORNUCOPIA

7

Las acciones de Mwengu no se pueden investigar porque no hay un registro adecuado de los eventos de seguridad con una marca de tiempo adecuada, o no hay un registro de auditoría completo, o Mwengu puede modificarlas o eliminarlas, o no existe un servicio de registro centralizado

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 puede omitir la aplicación para obtener acceso a los datos debido a que la red y la infraestructura del host, y los servicios/aplicaciones compatibles, no se han configurado de manera segura, la configuración no se verificó periódicamente ni se aplicaron parches de seguridad, o los datos se almacenaron localmente, o los datos no se guardaron protegidos físicamente

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 puede pasar por alto la aplicación para acceder a los datos porque las herramientas administrativas o las interfaces administrativas no están aseguradas adecuadamente

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

OWASP ASVS
2.1, 2.32

OWASP APPSENSOR
-

CAPEC
122, 233

SAFECODE
-

CORNUCOPIA

10

Xavier puede eludir los controles de la aplicación porque los frameworks de código, librerías y componentes contienen código malicioso o vulnerabilidades (por ejemplo, inhouse, software comercial, servicio tercerizado, de código abierto, ubicado externamente)

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 puede explotar la aplicación porque fue compilada utilizando herramientas obsoletas, o su configuración no es segura por defecto, o la seguridad de la información no fue documentada y pasada a equipos operacionales

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 puede emprender acciones maliciosas, no normales sin detección y respuesta por la aplicación en tiempo real

OWASP SCP
-

OWASP ASVS
4.14, 9.8, 15.1, 15.2

OWASP APPSENSOR
(All)

CAPEC
-

SAFECODE
1, 27

CORNUCOPIA

K

Gareth puede utilizar la aplicación para negar el servicio a algunos o todos sus usuarios

OWASP SCP
41, 55

OWASP ASVS
-

OWASP APPSENSOR
UT1-4, STE3

CAPEC
2, 25, 119, 125

SAFECODE
1

JOKER

Joker

Alice puede utilizar la aplicación para atacar los sistemas y datos de los usuarios.

Has pensado convertirte en un individuo Miembro de OWASP? Todas las herramientas, orientación y reuniones locales son gratis para todos, pero la membresía individual ayuda Apoyar el trabajo de OWASP.

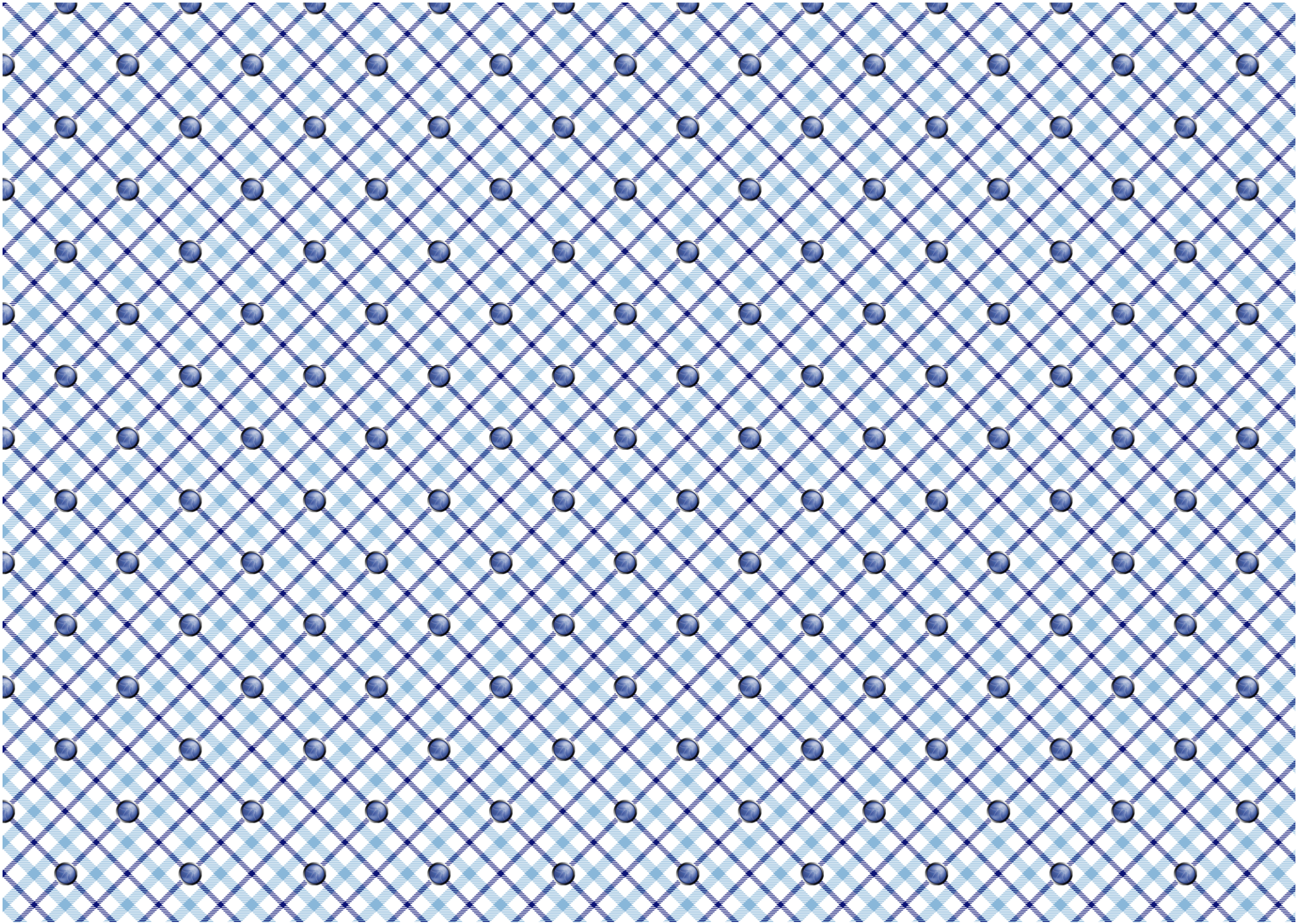
JOKER

Joker

Bob puede influir, alterar o afectar la aplicación para que ya no cumpla con mandatos legales, regulatorios, contractuales u otros mandatos organizacionales

Examine las vulnerabilidades y descubre cómo se pueden arreglar usando aplicaciones de entrenamiento en OWASP Broken Web Applications VM gratis, o utilizando los desafíos en línea en el laboratorio de hacking gratis

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}