Junta de Andalucía

Consejería de la Presidencia,
Administración Pública e Interior
Dirección General de Estrategia Digital y Gobierno Abierto

Correspondencia entre certificación de seguridad CCC y el ENS

Junta de Andalucía

Hoja de Control del Documento

Información del Documento			
Título	Correspondencia entre certificación de seguridad CCC y el ENS		
Asunto			
Nombre del fichero	DGEDGA_CAL_Correspondencia entre certificación de seguridad CCC y el ENS_v01r02.odt		
Versión	v01r02		
Elaborado por	Centro de Control de Calidad	**Fecha Elaboración**	15/02/2021
Aprobado por		**Fecha Aprobación**	
Confidencialidad			

Control de Versiones			
Versión	**Descripción de los cambios**	**Elaborado por**	**Fecha Elaboración**
v0100	Elaboración inicial del documento	Centro de Control de Calidad	15/02/2019
v0101	Actualización del documento con las aportaciones del Servicio de Producción: inclusión de pautas mp.info.6, mp.s.8, mp.com.2, mp.info.1, mp.info.1 y mp.sw.2	Centro de Control de Calidad	08/03/2019
v01r02	Actualización de plantilla	Centro de Control de Calidad	15/02/2021

Lista de Distribución	
Apellidos, Nombre	**Cargo / Función**
Álvarez Abrio, Juan	Jefe de servicio del Servicio de Producción
Doménech Colomer, Francisco José	Adjunto Servicio de Producción
Rodríguez Sáez, Manuel	Jefe de Servicio Coordinación y Desarrollo de Sistemas Horizontales
Sánchez Martín, Jorge	Jefe de Gabinete Desarrollo Sistemas Gestión
Ochoa Zalduendo, María del Rosario	Gerente de Cuenta Centro de Control de Calidad
Fraile Amodeo, Esther	Jefa de Proyecto Centro de Control de Calidad

Junta de Andalucía

ÍNDICE

1. INTRODUCCIÓN

Se incluye en el presente documento la correspondencia entre las verificaciones del servicio de Certificación de Seguridad que realiza el Centro de Control de Calidad (CCC) y las medidas de seguridad del ENS.

Esta correspondencia se ha realizado a petición del Servicio de Producción, para que los informes que el Centro de Control de Calidad elabora sobre la seguridad de aplicaciones Web puedan aportase como evidencia sólida de actuaciones de seguridad realizadas por iniciativa propia de la Dirección General de Política Digital.

Tal y como se comprobará en próximos apartados, se hace referencia a dos guías concretas del ENS, la correspondiente a la medida 808 y a la 812. Para ambas se ha establecido una relación con las vulnerabilidades correspondientes al servicio de seguridad definido en el servicio de seguridad de aplicaciones que ejecuta el CCC. Dichas vulnerabilidades quedarán descritas en los siguientes apartados.

2. CERTIFICACIÓN DE SEGURIDAD DE APLICACIONES

El Servicio de Certificación de Seguridad tiene como misión detectar posibles vulnerabilidades en los Sistemas de Información con el objeto de minimizar el riesgo de materialización de amenazas y proponer salvaguardas. Este servicio está basado en estándares de seguridad como Open Web Application Security Project (OWASP), el Esquema Nacional de Seguridad (ENS) y el Marco de Desarrollo de Software de la Junta de Andalucía (MADEJA).

La detección de vulnerabilidades se lleva a cabo en base a dos tipos de prueba:

- Pruebas estáticas, que son aquellas que se ejecutan sobre el software sin instalar y que permiten determinar con detalle las líneas de código de las vulnerabilidades encontradas y proporcionar a los equipos de desarrollo el contexto que necesitan para resolver la situación. Este análisis se realiza con la herramienta de HP Fortify.
- Pruebas dinámicas, son aquellas que se ejecutan sobre el software desplegado y en las que se aplica una batería de "exploits" a medida, verificaciones manuales y análisis automáticos que permiten verificar el comportamiento completo de la aplicación.

El Servicio de Certificación de Seguridad tiene como alcance la verificación de aplicaciones web (40 verificaciones) y la verificación de servicios web (14 verificaciones).

A continuación se verán los detalles de cada una de estas verificaciones, relacionadas con las medidas ENS:

Código	Descripción	Medidas ENS
SEG-1	La aplicación es vulnerable a ataques de fuerza bruta.	[mp.s.2] Protección de servicios y aplicaciones web
SEG-2	Existe un control en la aplicación para evitar el acceso tras un tiempo inactivo.	[mp.s.2] Protección de servicios y aplicaciones web
SEG-3	La desconexión de la sesión debe ser controlada desde la aplicación tras un tiempo de inactividad.	[mp.s.2] Protección de servicios y aplicaciones web

Código	Descripción	Medidas ENS
SEG-4	La aplicación tiene implementado funcionalidad para salir de la misma y evitar robo de identidad.	[mp.s.2] Protección de servicios y aplicaciones web
SEG-5	Identificación de escenarios de denegación de servicio por bloqueo de cuentas de usuarios tras un número determinado de intentos de acceso fallidos.	[mp.s.2] Protección de servicios y aplicaciones web [mp.s.8] Protección frente a la denegación de servicio
SEG-6	La aplicación es vulnerable a ataques de Cross-Site Scripting (XSS).	[mp.s.2] Protección de servicios y aplicaciones web
SEG-7	La aplicación es vulnerable a ataques de inyección SQL.	[mp.s.2] Protección de servicios y aplicaciones web
SEG-8	La inyección LDAP es evitada por la aplicación.	[mp.s.2] Protección de servicios y aplicaciones web
SEG-9	La inyección XML es evitada por la aplicación.	[mp.s.2] Protección de servicios y aplicaciones web
SEG-10	Verificar que la aplicación no permite inyección de comandos en el sistema operativo.	[mp.s.2] Protección de servicios y aplicaciones web
SEG-11	La aplicación permite establecer contraseñas de longitud inapropiada.	[mp.s.2] Protección de servicios y aplicaciones web
SEG-12	Verificar que la aplicación genera automáticamente contraseñas de autenticación fuertes	[mp.s.2] Protección de servicios y aplicaciones web
SEG-13	Verificar que en la operación de cambio de contraseña se solicita el valor antiguo del mismo	[mp.s.2] Protección de servicios y aplicaciones web
SEG-14	La aplicación no utiliza un protocolo seguro para enviar la información crítica	[mp.s.2] Protección de servicios y aplicaciones web [mp.com.2] Protección de la confidencialidad
SEG-15	Comprobar que los datos sensibles se almacenan en el sistema encriptados	[mp.s.2] Protección de servicios y aplicaciones web [mp.info.1] Datos de carácter personal
SEG-16	Comprobar que la información sensible es tratada sin cifrar solo en las ocasiones en la que es imprescindible desencriptarla	[mp.s.2] Protección de servicios y aplicaciones web [mp.info.1] Datos de carácter personal

Código	Descripción	Medidas ENS
SEG-17	Protección insuficiente de la capa de transporte	[mp.s.2] Protección de servicios y aplicaciones web
SEG-18	La aplicación contiene información inapropiada en la url	[mp.s.2] Protección de servicios y aplicaciones web
SEG-19	No deben mostrarse en la URL parámetros cuyo nombre pueda indicar la información que contienen.	[mp.s.2] Protección de servicios y aplicaciones web
SEG-20	Las referencias cruzadas de páginas no deben contener información de direcciones IP físicas	[mp.s.2] Protección de servicios y aplicaciones web
SEG-21	Comprobar que no se pueden realizar ataques por fijación de sesión, ni se revela el o los parámetros que identifican la sesión en la URL	[mp.s.2] Protección de servicios y aplicaciones web
SEG-22	Comprobar que el o los parámetros que identifican la sesión no se generan mediante algoritmos predecibles	[mp.s.2] Protección de servicios y aplicaciones web
SEG-23	Verificar que no existe un inapropiado manejo de la información y de errores que puedan ayudar a aumentar el riesgo de otras vulnerabilidades	[mp.s.2] Protección de servicios y aplicaciones web
SEG-24	Verificar que no se utilizan cuentas y usuarios predeterminados o predecibles	[mp.s.2] Protección de servicios y aplicaciones web
SEG-25	La aplicación permite el escalado de privilegios en partes concretas	[mp.s.2] Protección de servicios y aplicaciones web [mp.sw.2] Aceptación y puesta en servicio
SEG-26	Verificar que se registra los accesos de los usuarios al sistema	[mp.s.2] Protección de servicios y aplicaciones web
SEG-27	Comprobar que no se puede realizar una ejecución maliciosa de archivos en el lado del servidor pudiéndose perder el control total sobre la máquina	[mp.s.2] Protección de servicios y aplicaciones web
SEG-28	Comprobar que no existen referencias a objetos inseguras, ni que se pueden realizar ataques por transversal path	[mp.s.2] Protección de servicios y aplicaciones web
SEG-29	La aplicación carece de token por lo que es vulnerable a ataques de CSRF	[mp.s.2] Protección de servicios y aplicaciones web

Código	Descripción	Medidas ENS
SEG-30	Verificar que no se pueden realizar ataques de manipulación de “proxys” o “caches” (por ejemplo mediante http response splitting)	[mp.s.2] Protección de servicios y aplicaciones web
SEG-31	La aplicación no restringe el acceso a ciertas URL's	[mp.s.2] Protección de servicios y aplicaciones web
SEG-32	Verificar que no se puede acceder a la información mediante protocolos con niveles de seguridad diferentes (por ejemplo http y https)	[mp.s.2] Protección de servicios y aplicaciones web
SEG-33	Verificar que no es posible acceder sin permisos a los ficheros de configuración del entorno web	[mp.s.2] Protección de servicios y aplicaciones web
SEG-34	Verificar que no se almacenan archivos obsoletos en directorios de la aplicación dentro del servidor de aplicaciones	[mp.s.2] Protección de servicios y aplicaciones web
SEG-35	Verificar que los documentos publicados no contienen metadatos relevantes	[mp.s.2] Protección de servicios y aplicaciones web [mp.info.6] Limpieza de documentos
SEG-36	Verificar que no se utilizan campos HTML ocultos que almacenan información sensible sin establecer mecanismos de seguridad	[mp.s.2] Protección de servicios y aplicaciones web
SEG-37	Verificar que no es posible evitar los controles de seguridad que evalúan si el usuario no es un proceso automático (captcha, etc)	[mp.s.2] Protección de servicios y aplicaciones web
SEG-38	Verificar que existen controles de seguridad efectivos que evitan ataques por desbordamiento de buffers.	[mp.s.2] Protección de servicios y aplicaciones web
SEG-39	Verificación de las vulnerabilidades públicas existentes para los productos utilizados o integrados en la aplicación	[mp.s.2] Protección de servicios y aplicaciones web
SEG-40	Verificación de vulnerabilidades especificas del aplicativo auditado, como puede ser por ejemplo en un servicio de webmail, no poder enviar mensajes suplantando la identidad de otro usuario	[mp.s.2] Protección de servicios y aplicaciones web
SEG-41	El servicio web tiene una robustez suficiente contra ataques de fuerza bruta o de diccionario	[mp.s.2] Protección de servicios y aplicaciones web

Código	Descripción	Medidas ENS
SEG-42	El servicio web tiene implementado una petición específica para cerrar la sesión y evitar robo de identidad	[mp.s.2] Protección de servicios y aplicaciones web
SEG-43	Existe un control en el servicio web para evitar el envío de peticiones tras un tiempo inactivo	[mp.s.2] Protección de servicios y aplicaciones web
SEG-44	Verificar en el servicio web que no existe un inapropiado manejo de la información y de errores que puedan ayudar a aumentar el riesgo de otras vulnerabilidades	[mp.s.2] Protección de servicios y aplicaciones web
SEG-45	Verificar en el servicio web que no se produce un comportamiento inesperado al realizar peticiones con elementos duplicados	[mp.s.2] Protección de servicios y aplicaciones web
SEG-46	Verificar en el servicio web que no se produce un comportamiento inesperado al omitir elementos en las peticiones	[mp.s.2] Protección de servicios y aplicaciones web
SEG-47	Verificar en el servicio web que no se produce un comportamiento inesperado al realizar peticiones con elementos mal formados	[mp.s.2] Protección de servicios y aplicaciones web
SEG-48	Verificar en el servicio web que no se produce un comportamiento inesperado al sobrecargar los elementos en las peticiones	[mp.s.2] Protección de servicios y aplicaciones web
SEG-49	La inyección XPath es evitada por el servicio web	[mp.s.2] Protección de servicios y aplicaciones web
SEG-50	La inyección SQL es evitada por el servicio web	[mp.s.2] Protección de servicios y aplicaciones web
SEG-51	Verificar en el servicio web que no se produce un comportamiento inesperado al realizar peticiones con inyección de valores aleatorios en los campos	[mp.s.2] Protección de servicios y aplicaciones web
SEG-52	Verificar en los servicios web que no es posible obtener información útil del sistema al violar la restricción de tipos de datos	[mp.s.2] Protección de servicios y aplicaciones web
SEG-53	Verificar en los servicios web que no es posible obtener información útil del sistema al violar los valores límites de los campos	[mp.s.2] Protección de servicios y aplicaciones web

Código	Descripción	Medidas ENS
SEG-54	Los servicios web controlan la reflexión inmediata y los ataques almacenados. Protegiendo de la inyección del tipo "Cross-Site Scripting"	[mp.s.2] Protección de servicios y aplicaciones web

Tabla 1 – Verificaciones relacionadas con medidas ENS

3. CCN-STIC-808 V1.1 - VERIFICACIÓN DEL CUMPLIMIENTO DE LAS MEDIDAS EN EL ENS

3.1. Protección de servicios y aplicaciones web

Referencia	Medida de seguridad	Verificación
mp.s.2- 1	¿Se encuentran protegidos los subsistemas dedicados a la publicación de información frente a las amenazas que les son propias?	
mp.s.2- 2	Cuando la información tenga algún tipo de control de acceso ¿se garantiza la imposibilidad de acceder a la información obviando la autenticación?	SEG-01, SEG-02, SEG-03, SEG-04, SEG-06, SEG-07, SEG-08, SEG-10, SEG-11, SEG-12, SEG-17, SEG-21, SEG-22, SEG-24, SEG-27, SEG-31
mp.s.2- 2.1	¿Se evita que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado?	SEG-32
mp.s.2- 2.2	¿Se previenen ataques de manipulación de URL?	SEG-31
mp.s.2- 2.3	¿Se previenen ataques de manipulación de las cookies de los usuarios?	SEG-21, SEG-22SEG-07, SEG-08, SEG-09, SEG-10
mp.s.2- 2.4	¿Se previenen ataques de inyección de código?	SEG-07, SEG-08, SEG-09, SEG-10 SEG-25
mp.s.2- 3	¿Se previenen intentos de escalado de privilegios?	SEG-25
mp.s.2- 4	¿Se previenen ataques de “cross site scripting” ?	SEG-06
mp.s.2- 5	¿Se previenen ataques de manipulación de “proxys” o “cachés” ?	SEG-30

mp.s.2- 6	¿Se limpian los documentos publicados?	SEG-35
mp.s.2- 7	¿Se realizan auditorias de seguridad y pruebas de penetración?	

Tabla 2 – Correspondencia con 808

Comentar que el servicio se definió haciendo uso de la norma 808 anterior a junio de 2017 y que posteriormente se llevó a cabo una actualización de dicha guía. Se han revisado los cambios y se ha cmprobado que solo afecta de la siguiente forma:

- La mp.s.2.6 de la tabla anterior se elimina y se sustituye por la mp.s.2.7.
- Se crea una nueva mp.s.2.7 bajo el epígrafe "¿Se emplean certificados de autenticación de sitio webacordes a la normativa europea en la materia?" , para la que no se tiene correspondencia.

4. CCN-STIC-812 V1.2 – SEGURIDAD EN ENTORNOS Y APLICACIONES WEB

4.1. Análisis de vulnerabilidades

Referencia	Medida de seguridad	Verificación
5.4.1 - 163	Inyección SQL	SEG-07
5.4.1 - 163	Inyección SQL ciega, incluyendo análisis de las diferencias en los tiempos de respuesta	
5.4.1 - 163	Inyección LDAP y XPath	SEG-08, SEG-09
5.4.1 - 163	XSS, reflejado y persistente	SEG-06
5.4.1 - 163	CSRF	SEG-29
5.4.1 - 163	HTTP Response Splitting	SEG-30
5.4.1 - 163	Inyección de comandos en el sistema operativo	SEG-27, SEG-10
5.4.1 - 163	Desplazamiento por directorios	SEG-28
5.4.1 - 163	Referencias directas a ficheros	SEG-28
5.4.1 - 163	Parámetros y contenidos reflejados en la respuesta del servidor Web	SEG-06, SEG-27
5.4.1 - 163	Métodos para evitar comprobaciones de tipo CAPTCHA	SEG-37
5.4.1 - 163	Desbordamiento de buffers	SEG-38
5.4.1 - 165	Transporte de credenciales sobre canales de comunicación seguros	SEG-17
5.4.1 - 165	Determinación de los elementos de protección frente a ataques de enumeración y adivinación de credenciales: número máximo de intentos de acceso fallidos, limitaciones por tiempo, etc	SEG-01, SEG-11, SEG-12, SEG-22, SEG-24
5.4.1 - 165	Identificación de escenarios de denegación	SEG-05

Referencia	Medida de seguridad	Verificación
	de servicio por bloqueo de cuentas de usuarios tras un número determinado de intentos de acceso fallidos	
5.4.1 - 165	Análisis de la fortaleza de las claves y de los mecanismos de generación de claves por defecto	SEG-12
5.4.1 - 165	En el caso de emplearse certificados de cliente, análisis de los certificados digitales, y de los procedimientos de gestión de los certificados (alta, verificación, revocación de certificados, etc)	
5.4.1 - 165	Ataques de diccionario y fuerza bruta sobre las credenciales de acceso	SEG-01, SEG-11, SEG-22, SEG-23, SEG-24
5.4.1 - 165	Determinación de métodos para evitar el sistema de autentificación	SEG-01, SEG-02, SEG-03, SEG-04, SEG-11, SEG-22, SEG-23, SEG-24
5.4.1 - 165	Determinación de los mecanismos de renovación de claves e identificación de vulnerabilidades en los mismos	SEG-13
5.4.1 - 166	Determinación de la duración y ámbito de las sesiones	SEG-02, SEG-03, SEG-04
5.4.1 - 166	Determinación de los elementos empleados para implementar el mantenimiento de sesiones	SEG-03, SEG-21, SEG-22
5.4.1 - 166	Determinación del formato y contenido del identificador o token de las sesiones	SEG-22
5.4.1 - 166	Identificación y análisis de seguridad del uso de tokens (cookies, variables, cabeceras HTTP, etc) por parte de la aplicación Web	SEG-22
5.4.1 - 166	Determinación de mecanismos de manipulación del token de sesión	SEG-21, SEG-22

Referencia	Medida de seguridad	Verificación
5.4.1 - 166	Identificación de ataques de fijación de sesión	SEG-21
5.4.1 - 166	Identificación y análisis de seguridad de escenarios Single Sign On (SSO)	
5.4.1 - 166	Determinación del mecanismo de cierre de sesiones y gestión de la información de sesión cacheada en los clientes Web	SEG-03
5.4.1 - 167	Acceso a contenidos de usuarios conocidos o típicos (existentes por defecto)	SEG-24
5.4.1 - 167	Acceso a ficheros de configuración del entorno Web	SEG-33
5.4.1 - 167	Acceso a versiones renombradas (bakups) de archivos en producción	SEG-34
5.4.1 - 167	Acceso a la información de otros usuarios con credenciales	SEG-01, SEG-02, SEG-03, SEG-04, SEG-11, SEG-12, SEG-14, SEG-15, SEG-16, SEG-17, SEG-21, SEG-22, SEG-24, SEG-28, SEG-31
5.4.1 - 167	Trazabilidad de los accesos de usuario	SEG-26
5.4.1 - 167	Determinación de métodos para evitar el sistema de autorización	SEG-01, SEG-02, SEG-03, SEG-04, SEG-11, SEG-12, SEG-14, SEG-15, SEG-16, SEG-17, SEG-21, SEG-22, SEG-24, SEG-28, SEG-31
5.4.1 - 167	Escalada de privilegios	SEG-25

Tabla 3 – Correspondencia con 812