

INTRODUCCION



El SMT Web Applications es un servicio de evaluaciones de seguridad para aplicaciones WEB 2.0 basado estratégicamente en el cumplimiento del estándar PCI (Payment Card Industry Security Standard Council), el cual es requerido por cualquier organización que guarde, procese o transmita un número de tarjeta de pago (crédito o débito)

En función de los requerimientos del estándar, el servicio Security Modular Test en la modalidad Web Applications nos permite a través de una evaluación de seguridad, verificar cuál es el plan de trabajo necesario para cumplir con las necesidades presentadas por la norma PCI DSS, todo esto representado mes a mes en un reporte que contenga los componentes involucrados, el riesgo asociado a cada componente y el nivel de compromiso que debe tomar la organización para mitigarlos.

De esta forma nuestros servicios profesionales podrán acompañarlo no solo en la revisión y verificación de la situación de seguridad sino también en la aplicación de las soluciones más óptimas para cada uno de los casos.

A continuación enumeramos alguno de los controles necesarios según el estándar PCI y cuales son los procesos de evaluación asociados permiten detectar incumplimientos de la norma, que se traducen en vulnerabilidades que ponen en riesgo el negocio.

Ctrl	Requisito PCI	Proceso de evaluación
2.2.4	Eliminar todas las funcionalidades innecesarias, tales como archivos de comandos (scripts), accionadores, funciones, subsistemas, sistemas de archivo y servidores de Web innecesarios.	Estructura de navegación Revisión de comentarios Directory Listening Path Allows Análisis de Vulnerabilidades
6.5.1	Ingreso de datos sin validar	Web Evaluación de Inyecciones Cross Site Scripting Validación de Variables SQL Injection Exponed Session Data Session Hijacking Autenticaciones persistentes
6.5.3	Interrupción de la autenticación o administración de sesiones (uso de credenciales de cuenta y cookies de sesión)	
6.5.4	Ataques con inyección de códigos en ventanas pertenecientes a diferentes dominios	
6.5.6	Defectos de inyección	
6.5.7	Manejo inapropiado de errores	
6.5.8	Almacenaje de datos sin la debida seguridad	Estructura de navegación Directory Listening
6.5.9	Negación de servicio	Brute Force
6.5.10	Administración no segura de configuraciones	Directory Listening Path Allows Análisis de Vulnerabilidades