VECTOR
CYBERSECURITY.

VECTOR.
ITCGROUP

Seguridad Preventiva

INFORMATION IS THE
NEW SECURITY PERIMETER

Nuestro servicio de Protección Preventiva busca evaluar y detectar vulnerabilidades en los sistemas y en las redes de nuestros clientes, comprobando los accesos a sus diferentes servicios, aplicaciones o datos simulando ataques a los mismos por medio de Pentesting, con el objetivo de anticiparnos y remediar las posibles carencias ante un ataque real.

¿EN QUÉ CONSISTE?

Aplicamos nuestra experiencia y conocimiento en Hacking Ético para asegurar la confidencialidad, autenticidad, integridad y disponibilidad de los sistemas de nuestros clientes.

1. RECOPILACIÓN DE INFORMACIÓN:

a. Identificación de la versión de la aplicación y del tipo de servidor.
b. Análisis de códigos de error.
c. Pruebas del receptor de escucha de la base de datos.
d. Gestión de extensiones de archivo (conocimiento de las tecnologías usadas).

2. ANÁLISIS DE SISTEMAS DE IDENTIFICACIÓN Y AUTENTICACIÓN:

a. Cuentas por defecto o adivinables.
b. Ataques de fuerza bruta.
c. Salto del sistema de autenticación (petición directa de páginas, modificación de parámetros, predicción de IDs de sesión, inyección SQL, etc.).
d. Atravesar directorios/acceso a archivos de la aplicación (atravesar rutas, escalado de directorios de los servidores, etc.).
e. Recordatorio de contraseñas y reseteo de password.
f. Gestión de caché de navegación y de salida de sesión.

3. GESTIÓN DE SESIONES:

a. Gestión del identificador de sesión (integridad en la creación del identificador de sesión, gestión segura de sesiones activas y de los identificadores de sesión).
b. Análisis de las estrategias de gestión de sesiones.
c. Manipulación de cookies (recolección, ingeniería inversa, manipulación, etc.).
d. Variables de sesión expuestas (pruebas de cifrado y vulnerabilidades por reutilización de testigos de sesión).
e. CSRF (Cross-site request forgery – Comprobación de que se puede forzar a un usuario final a ejecutar acciones no deseadas en una aplicación Web en la que ya está autenticado).
f. Tampering HTTP (tratar de explotar debilidades de la aplicación Web o de la forma en que se manejan las peticiones http).

4. PRUEBAS DE VALIDACIÓN DE DATOS DE ENTRADA:

a. Cross-site scripting y Cross-site tracing (manipulación de los parámetros de entrada que recibe una aplicación).
b. Inyección SQL, LDAP y XML (inyección de consultas SQL directamente sobre una base de datos, inyección de consultas LDAP sobre un servidor LDAP e inyección de documentos XML en una aplicación).
c. Inyección Xpath, IMAP/SMTP y de código (inyección de elementos Xpath sobre consultas sobre datos XML, inyección de comandos IMAP/SMTP en los servidores de correo, inyección de código ejecutable como entrada en una página Web).
d. Os Commanding (Inserción de comandos del sistema operativo a través de peticiones http a la aplicación).

La metodología propuesta está alineada con las siguientes normas y estándares:

OWASP
Como referencia para la ejecución de los test de intrusión sobre aplicativos web.

OSSTMM
De ISECOM.

ISSAF
de OISSG.

SANS INSTITUTE

FUNCIONALIDADES CLAVE

- ✓ Identificación de vulnerabilidades y clasificación según riesgo y magnitud.
- ✓ Evaluación de los impactos operacionales de ataques con éxito.
- ✓ Identificación y propuesta de puntos de mejoras.