MUESTRA DE ENTREGABLE / VULNERABILIDADES

Informe de evaluación de vulnerabilidades

Organización DEMO A · Infraestructura ficticia · Versión ilustrativa 1.0

Este documento muestra cómo se presentan hallazgos, prioridades y acciones. Todos los activos, evidencias y responsables son ficticios. No describe pruebas ejecutadas ni resultados de un cliente.

Objetivo y resumen ejecutivo

Identificar exposición y configuraciones que requieren revisión en un portal ficticio. El ejemplo contiene tres observaciones: una exposición administrativa no prevista y dos configuraciones web mejorables. Ninguna observación demuestra por sí sola una intrusión. La prioridad considera exposición, función del activo y controles descritos en este escenario.

Activos, método y límites

Elemento	Condiciones del ejemplo
Activo DEMO-WEB-01	Portal público y panel administrativo del mismo sistema. No se incluye infraestructura de terceros.
Comprobaciones	Exposición desde una red externa autorizada, revisión de respuestas HTTP y comparación con el inventario ficticio.
Exclusiones	Explotación manual exhaustiva, fuerza bruta, denegación de servicio y cambios productivos.
Evidencia y cobertura	Registros E-01 a E-03 sintetizados en la página siguiente. Sin capturas reales, credenciales ni datos personales.

Prioridades para el equipo

ID / prioridad contextual	Acción inicial / responsable ficticio
V-01 / Alta	Confirmar necesidad del panel público y planificar restricción. Infraestructura.
V-02 / Media	Ajustar atributos de la cookie de sesión y verificar compatibilidad. Desarrollo.
V-03 / Baja	Desactivar listado de directorio y revisar los archivos publicados. Desarrollo.

Las prioridades son ilustrativas; no equivalen a una puntuación CVSS. Las fechas de corrección se acuerdan según dependencias y riesgo aceptado por el cliente.

DETALLE TÉCNICO Y SEGUIMIENTO

Hallazgos y criterios de cierre

V-01 / Panel administrativo expuesto / Alta

Evidencia E-01: El panel de DEMO-WEB-01 responde desde la red externa del escenario. El inventario indica que debería utilizarse solo desde la red interna. No se intentó autenticación.

Impacto: Aumenta la superficie administrativa accesible. El ejemplo no demuestra evasión de controles ni acceso no autorizado.

Recomendación: Confirmar la necesidad de publicación y restringir el acceso mediante los controles aprobados por Infraestructura.

Verificación: Comprobar acceso permitido desde la red prevista y rechazo desde la red externa, conservando ambos resultados.

V-02 / Cookie de sesión sin Secure / Media

Evidencia E-02: La respuesta HTTPS ficticia emite la cookie de sesión sin el atributo Secure. El valor está omitido; no se capturó tráfico de usuarios.

Impacto: El navegador podría enviarla por HTTP si se cumplen las condiciones de dominio, ruta y conexión. No se demuestra interceptación de una sesión.

Recomendación: Configurar Secure y mantener HTTPS durante toda la sesión. Revisar los demás atributos según el funcionamiento de la aplicación.

Verificación: Inspeccionar Set-Cookie tras un inicio de sesión de prueba y comprobar que el flujo autorizado conserva su funcionamiento.

V-03 / Listado de directorio habilitado / Baja

Evidencia E-03: Una ruta de archivos de demostración muestra un índice navegable con nombres internos. No se observaron secretos ni documentos confidenciales.

Impacto: Facilita conocer la estructura publicada. La sensibilidad depende del contenido y los accesos realmente permitidos.

Recomendación: Desactivar el índice y revisar qué archivos deben ser públicos, preservando las rutas que utiliza la aplicación.

Verificación: Comprobar que el índice ya no se presenta y que los recursos públicos previstos continúan accesibles.

Entrega y reevaluación

El equipo asigna responsables y fechas y documenta decisiones. Una corrección comunicada no cierra automáticamente un hallazgo: la reevaluación requiere autorización y registra qué se comprobó y qué quedó pendiente. En esta muestra no se ha ejecutado ninguna corrección ni reevaluación.

Referencia técnica para V-02: OWASP Session Management Cheat Sheet, sección Secure Attribute. Consultada el 20/11/2026.