**Informe Técnico**

**Análisis de Seguridad y Mitigación en un Módulo de Administración – TechData**

**1. Escenario**

La empresa **TechData** desarrolló un panel de administración para gestionar usuarios, reportes y contenido. Durante una auditoría inicial se identificaron **cuatro vulnerabilidades críticas** relacionadas con validación de entradas, control de acceso, uso de dependencias obsoletas y protección insuficiente frente a ataques automatizados. El objetivo del laboratorio fue **analizar los riesgos y proponer medidas de mitigación y prevención**, justificando la prioridad de intervención.

**2. Identificación de Vulnerabilidades y Mitigación**

| **Caso** | **Vulnerabilidad Identificada** | **Técnica de Mitigación** | **Justificación** |
| --- | --- | --- | --- |
| **1** | Falta de validación y escape en formulario de búsqueda → **XSS reflejado** | Validación de entradas + Escape de salida (HTML entities) | Sanitizar y escapar entradas evita que código malicioso inyectado en el campo se ejecute en el navegador, previniendo ataques XSS. |
| **2** | Endpoint /admin/users/export expone datos sin autenticación → **Broken Access Control** | Control de acceso por roles (RBAC) + Autenticación obligatoria | Verificar identidad y rol antes de servir datos sensibles asegura que solo usuarios autorizados accedan a información crítica. |
| **3** | Uso de librería JS obsoleta con CVEs conocidos → **Uso de componente vulnerable** | Actualización de dependencias + Monitoreo con SCA (Snyk, OWASP Dependency-Check) | Mantener librerías actualizadas cierra vulnerabilidades conocidas y reduce superficie de ataque. |
| **4** | Intentos de ejecución automatizada desde dominios externos → **CSRF (Cross-Site Request Forgery)** | Implementación de **tokens CSRF** + Cabecera SameSite en cookies | El uso de tokens únicos y cookies seguras impide que solicitudes externas no autorizadas ejecuten acciones críticas en nombre del usuario. |

**3. Priorización de Mitigación**

La vulnerabilidad más crítica es el **Caso 2 – Broken Access Control en /admin/users/export**, ya que permite acceso directo a todos los datos de usuarios sin ningún control. Este fallo compromete la **confidencialidad, integridad y disponibilidad** de la información y tiene un impacto inmediato en la organización.  
Posteriormente deben abordarse el **XSS (Caso 1)** y el **CSRF (Caso 4)**, ya que exponen a los usuarios a robo de sesiones y manipulación de acciones. Finalmente, aunque importante, la **actualización de la librería (Caso 3)** puede priorizarse en paralelo mediante un ciclo de gestión de dependencias.

**4. Recomendaciones Finales**

1. Implementar un **ciclo de gestión de vulnerabilidades** con parches periódicos.
2. Integrar pruebas **SAST y DAST** en el pipeline de desarrollo.
3. Configurar cabeceras de seguridad HTTP: **CSP, HSTS, X-Frame-Options**.
4. Capacitar a los desarrolladores en **OWASP Top 10 y NIST 800-53**.
5. Aplicar monitoreo continuo y alertas de seguridad en endpoints sensibles.

**5. Conclusión**

El análisis del módulo de administración de TechData evidenció fallas graves en validación de entradas, control de accesos, actualización de librerías y protección frente a ataques CSRF. La aplicación de las mitigaciones propuestas reducirá significativamente la superficie de ataque y mejorará la resiliencia de la aplicación. Este ejercicio refuerza la necesidad de aplicar **seguridad por diseño** y alinear los desarrollos a marcos de referencia como **OWASP Top 10** para minimizar riesgos en entornos empresariales.