**Informe Técnico**

**Análisis y Propuesta de Mitigación y Prevención ante Incidentes de Seguridad – SecureWeb Ltd.**

**1. Escenario**

En la empresa ficticia **SecureWeb Ltd.**, el equipo de monitoreo detectó cinco incidentes de seguridad en las últimas 48 horas. El objetivo de este análisis es **clasificar los incidentes, proponer medidas de mitigación y prevención** y **priorizar las acciones** según riesgo, impacto y facilidad de explotación.

**2. Clasificación de Incidentes**

| **Nº** | **Incidente** | **Clasificación** |
| --- | --- | --- |
| 1 | Intentos fallidos de login desde misma IP | 🟡 Mitigación y Prevención |
| 2 | Inyección de JavaScript en comentarios (XSS almacenado) | 🟡 Mitigación y Prevención |
| 3 | Acceso no autorizado a /admin/export sin validación de rol | 🔵 Mitigación inmediata |
| 4 | Uso de librería JS con vulnerabilidad conocida sin parchear | 🟢 Prevención |
| 5 | Backend expone mensajes de error con estructura de BD | 🟡 Mitigación y Prevención |

**3. Propuesta Técnica**

**1. Intentos fallidos de login (Brute Force)**

* **Mitigación:** habilitar **bloqueo temporal** de la cuenta tras múltiples intentos fallidos; alertar al SOC.
* **Prevención:** implementar **MFA** y limitar intentos por IP con reglas en WAF o firewall.

**2. Inyección de JavaScript (XSS)**

* **Mitigación:** sanitizar inmediatamente los comentarios existentes y limpiar entradas ya almacenadas.
* **Prevención:** aplicar **escape de salida en HTML**, validación de entradas y políticas **CSP**.

**3. Acceso a /admin/export sin validación de rol**

* **Mitigación:** cerrar temporalmente el endpoint en el firewall y restringir acceso solo desde red interna.
* **Prevención:** implementar **RBAC** (control de acceso basado en roles) y validación en servidor.

**4. Librería JavaScript vulnerable**

* **Mitigación:** aplicar actualización urgente de la librería afectada.
* **Prevención:** establecer un **ciclo de gestión de dependencias** con herramientas SCA (Software Composition Analysis).

**5. Mensajes de error con datos de BD**

* **Mitigación:** deshabilitar errores detallados en producción, habilitar logs internos solo para administradores.
* **Prevención:** configurar **manejadores globales de excepciones**, mostrar mensajes genéricos y aplicar pruebas SAST/DAST.

**4. Priorización de Incidentes**

1. **Acceso sin validación de rol (/admin/export)** → riesgo crítico, compromete datos sensibles de inmediato.
2. **XSS almacenado en comentarios** → afecta a todos los usuarios y facilita robo de sesiones.
3. **Intentos masivos de login (Brute Force)** → riesgo alto de acceso indebido, mitigable con MFA y bloqueo.
4. **Exposición de mensajes de error** → filtra información útil para futuros ataques.
5. **Uso de librería vulnerable** → riesgo latente, requiere parcheo pero menor inmediatez que los anteriores.

**5. Conclusión**

El análisis mostró que SecureWeb Ltd. enfrenta vulnerabilidades críticas de **Broken Access Control** y **XSS**, que deben ser mitigadas de forma prioritaria. Otros incidentes, como errores de backend y librerías sin actualizar, refuerzan la necesidad de una **gestión integral de seguridad basada en OWASP y NIST**. La aplicación de medidas preventivas y reactivas propuestas garantizará una reducción significativa del riesgo y la mejora continua en la postura de ciberseguridad de la empresa.