**⚠️ 5 Amenazas para True Score IA**

1. **Ataques de Inyección SQL:**  
   Intentos maliciosos para manipular consultas hacia la base de datos y obtener acceso a los datos de usuarios y predicciones.
2. **Acceso no autorizado a dashboards premium:**  
   Usuarios no premium o externos pueden intentar explotar vulnerabilidades para acceder a contenido exclusivo sin pagar.
3. **Filtración de modelos de IA o lógica predictiva:**  
   Robo del modelo de IA entrenado que alimenta las predicciones deportivas, comprometiendo el valor diferencial del negocio.
4. **Ataques DDoS (Denegación de servicio):**  
   Saturación de los servidores para volver el servicio inaccesible durante eventos deportivos importantes (cuando más ingresos se generan).
5. **Intercepción de credenciales en redes inseguras (Man-in-the-middle):**  
   Usuarios que inician sesión desde redes públicas podrían tener sus credenciales interceptadas si la conexión HTTPS no está bien implementada.

**🛠️ 5 Vulnerabilidades encontradas o posibles en el sistema**

1. **Falta de validación en el backend (input de formularios):**  
   Si los formularios de login o registro no filtran correctamente los datos ingresados, es susceptible a XSS o inyección SQL.
2. **Mala gestión de tokens de autenticación o sesiones:**  
   No invalidar sesiones tras logout, uso de JWT inseguros o no expirar tokens puede permitir accesos prolongados no autorizados.
3. **Dependencias sin actualizar (librerías de IA o frontend):**  
   Usar bibliotecas desactualizadas puede abrir puertas a exploits conocidos.
4. **Permisos excesivos en la base de datos:**  
   Un solo punto de acceso (usuario root del backend) con permisos totales puede exponer todo si se compromete.
5. **Falta de segmentación en la infraestructura cloud:**  
   Si el frontend, backend, IA y base de datos están en la misma red, un atacante que entre por una puerta podría moverse lateralmente por todo.

**🔥 Riesgo crítico del sistema:**

**"Exposición y pérdida de integridad de la base de datos de usuarios y predicciones inteligentes."**

**Descripción del riesgo:**  
Si un atacante accede a la base de datos principal, puede no solo obtener información sensible (nombres, correos, países y métodos de pago de usuarios), sino también alterar o robar los resultados de la IA. Esto afectaría directamente la confianza en las predicciones, daría lugar a pérdidas económicas y comprometería la reputación del sistema como una plataforma confiable.

|  |  |
| --- | --- |
| **Pregunta** | **Detalle** |
| **What (¿Qué?)** | Proteger la base de datos de usuarios y los modelos/resultados predictivos de la IA para evitar filtraciones, manipulaciones o pérdida de información crítica. |
| **Why (¿Por qué?)** | Porque es el activo más valioso del sistema. Su exposición comprometería la privacidad de los usuarios, la confiabilidad de la plataforma y la continuidad del negocio. Además, implica violaciones a normativas como GDPR o Habeas Data. |
| **Where (¿Dónde?)** | En el servidor de base de datos (cloud o local), en los contenedores del backend y en los entornos donde reside o se ejecuta la IA (modelos y resultados). También en las comunicaciones entre frontend y backend. |
| **When (¿Cuándo?)** | Inmediatamente. Es una acción **prioritaria** que debe implementarse desde la fase de despliegue inicial y mantenerse continuamente (con revisiones mensuales). |
| **Who (¿Quién?)** | Equipo de Seguridad de la Información (o DevSecOps), junto con los encargados de infraestructura y backend. El auditor valida la implementación periódicamente. |
| **How (¿Cómo?)** | Aplicando: • Cifrado AES-256 de base de datos y backups • HTTPS + TLS 1.3 en toda la plataforma • Autenticación multifactor • Control de accesos y roles • Firewalls y segmentación de red • Monitorización y registros (logs) seguros • Validación de integridad de modelos IA |
| **How much (¿Cuánto cuesta?)** | Inicialmente puede costar tiempo de desarrollo e inversión en herramientas (certificados, infraestructura segura, autenticación fuerte), pero comparado con el costo de una filtración (multas, pérdida de reputación y clientes), es insignificante. |