CyberShield: Documentación Parcial

Fecha de actualización: 20 de mayo de 2025

Resumen del Proyecto

CyberShield es una plataforma de ciberseguridad diseñada específicamente para usuarios no técnicos. El objetivo principal es proporcionar herramientas intuitivas y accesibles para proteger la información personal y mejorar la seguridad digital. La aplicación integra tres módulos principales:

1. **Gestor de contraseñas**:

Almacenamiento seguro de credenciales con detección de filtraciones.
2. **Simulador de phishing**: Herramienta educativa para identificar intentos de phishing.
3. **Escáner de red local**: Detección de vulnerabilidades en dispositivos conectados.

Este documento describe el progreso actual del desarrollo, los retos superados y el trabajo pendiente.

Tecnologías Utilizadas

Frontend

- React con TypeScript
- Tailwind CSS para estilos
- Wouter para enrutamiento
- TanStack Query para gestión de estado y peticiones
- ShadCN/UI para componentes de interfaz

Backend

- Node.js con Express
- PostgreSQL como base de datos
- Drizzle ORM para interacción con la base de datos
- Passport.js para autenticación
- SendGrid para envío de correos electrónicos

Funcionalidades Implementadas

Sistema de Autenticación

- **Registro de usuarios**: Implementado con validación de datos mediante Zod
- **Inicio de sesión**: Autenticación basada en sesiones con Passport.js
- **Persistencia de sesiones**: Almacenamiento de sesiones en PostgreSQL
- **Verificación por correo**: Envío de correos de bienvenida mediante SendGrid

Gestor de Contraseñas

- Esquema de base de datos para almacenamiento seguro de contraseñas
- Interfaz para visualización, creación y edición de contraseñas
- Encriptación de datos sensibles
- Verificación de filtraciones (implementación básica)

Simulador de Phishing

- Estructura de datos para ejemplos de phishing
- Interfaz para presentar los ejemplos y evaluar respuestas del usuario
- Sistema de tracking de estadísticas de detección

Escáner de Red

- Modelos de datos para dispositivos y vulnerabilidades
- Interfaz de visualización de dispositivos en la red
- Implementación de escaneo de red real
- Detección de puertos abiertos y vulnerabilidades

- Visualización detallada de dispositivos encontrados
- Sistema de clasificación de dispositivos por tipo

Dashboard Central

- Métricas de seguridad consolidadas
- Registro de actividades recientes
- Acceso rápido a los diferentes módulos

Experiencia de Usuario

- Diseño intuitivo centrado en usuarios no técnicos
- Implementación completa de Modo Oscuro
- Interfaz completamente responsive
- Iconografía y feedback visual para mejor comprensión
- Formularios con validación y retroalimentación instantánea

Retos Superados

1. Implementación del Modo Oscuro

La implementación del Modo Oscuro presentó varios desafíos técnicos:

- **Consistencia visual**: Asegurar que todos los componentes mantuvieran la armonía visual en ambos modos.
- **Manejo de contrastes**: Garantizar que el texto y los elementos interactivos mantengan un contraste adecuado para cumplir con estándares de accesibilidad.
- **Adaptación de iconos**: Rediseño de ciertos elementos visuales para que sean visibles en ambos modos.
- **Persistencia de preferencias**: Implementación de almacenamiento local para recordar la preferencia del usuario.
- **Transiciones suaves**: Creación de transiciones naturales al cambiar entre modos.

2. Desarrollo del Escáner de Red Real

Mejorar el escáner de red para realizar análisis reales implicó:

- **Detección de dispositivos activos**: Implementación de técnicas de ping y escaneo de puertos para identificar dispositivos en la red local.
- **Identificación de tipos de dispositivo**: Algoritmos para clasificar dispositivos según puertos abiertos y características de red.
- **Análisis de vulnerabilidades**: Sistema para identificar configuraciones inseguras en los dispositivos.
- **Optimización del rendimiento**: Técnicas para realizar escaneos eficientes sin saturar la red o el sistema.

3. Integración del Correo Electrónico

Uno de los mayores desafíos fue la integración del servicio de correo electrónico. Los problemas incluyeron:

- **Migración de la base de datos**:

Fue necesario añadir el campo email a la tabla de usuarios existente.
- **Validación de correos**: Implementación de validaciones para asegurar que los correos sean únicos y tengan formato correcto.
- **Configuración de SendGrid**: Resolución de problemas de autenticación y verificación del remitente.
- **Manejo de errores**: Implementación de un sistema robusto que permite continuar con el registro aunque falle el envío del correo.

2. Diseño de la Arquitectura

Diseñar una arquitectura que permitiera la integración de los tres módulos principales manteniendo el código modular y fácil de mantener:

- **Estructura de carpetas**: Organización clara separando componentes, páginas y lógica.
- **Esquema compartido**: Definición centralizada del modelo de datos para mantener consistencia entre

front y back.
- **Sistema de rutas**: Implementación de rutas protegidas y gestión de estados de autenticación.

3. Experiencia de Usuario

Crear una experiencia de usuario intuitiva para personas no técnicas:

- **Formularios amigables**: Implementación de validación y retroalimentación en tiempo real.
- **Mensajes de error claros**: Traducción de errores técnicos a mensajes comprensibles.
- **Diseño responsive**: Adaptación a diferentes tamaños de pantalla para facilitar el acceso.

Dificultades Encontradas

---

1. Problemas con la Migración de Base de Datos

La adición del campo email a una estructura de datos existente presentó desafíos:

- Error "column email does not exist" al intentar registrar nuevos usuarios
- Necesidad de modificar manualmente la estructura de la tabla
- Actualización de todos los componentes y servicios para manejar el nuevo campo

2. Integración con SendGrid

La configuración de SendGrid requirió resolver varios problemas:

- **Error 403 Forbidden**: Causado por la falta de verificación del correo remitente
- **Tipado de la API**: Resolver problemas de tipado con TypeScript y la librería de SendGrid
- **Manejo asíncrono**: Implementar el envío de correos de forma que no bloqueara el flujo principal

3. Seguridad vs Facilidad de Uso

Encontrar el equilibrio entre seguridad robusta y facilidad de uso para usuarios no técnicos:

- Implementación de validaciones sin intimidar al usuario
- Diseño de interfaces intuitivas que no comprometan la seguridad
- Simplificación de conceptos técnicos sin perder precisión

Trabajo Pendiente

---

1. Mejoras en el Gestor de Contraseñas

- Completar la implementación de generación automática de contraseñas seguras
- Mejorar el algoritmo de detección de filtraciones con APIs externas
- Añadir categorización de contraseñas y función de búsqueda avanzada

- Implementar sincronización segura entre dispositivos

2. Expansión del Simulador de Phishing

- Aumentar la base de datos de ejemplos de phishing con casos recientes
- Incorporar análisis más detallado de los intentos de phishing
- Añadir tutoriales interactivos y recursos educativos personalizados
- Implementar sistema de recomendaciones basado en el desempeño del usuario

3. Optimización del Escáner de Red

- Refinar el proceso de escaneo de red para mejorar la precisión
- Ampliar la detección de vulnerabilidades específicas por tipo de dispositivo
- Desarrollar un sistema de alertas automáticas para nuevos dispositivos

- Añadir recomendaciones específicas y paso a paso para mitigar cada vulnerabilidad

4. Optimizaciones Generales

- Implementar pruebas automatizadas (unitarias y de integración)
- Mejorar la eficiencia de las consultas a la base de datos
- Optimizar el rendimiento en dispositivos móviles
- Implementar un sistema de exportación/importación de datos personales
- Crear documentación detallada para usuarios finales

Conclusiones Actualizadas

El desarrollo de CyberShield continúa avanzando con éxito, habiendo logrado importantes mejoras en las últimas semanas. La implementación del Modo Oscuro completo y la mejora del Escáner

de Red para realizar análisis reales representan avances significativos en términos de usabilidad y funcionalidad.

La plataforma ahora ofrece:

- Un sistema de autenticación robusto con gestión de sesiones
- Un gestor de contraseñas funcional con verificación de filtraciones
- Un simulador de phishing efectivo con análisis detallado
- Un escáner de red que permite la detección real de dispositivos y vulnerabilidades
- Una interfaz adaptativa con modo claro y oscuro

Los desafíos técnicos continúan siendo abordados de manera sistemática, priorizando siempre el equilibrio entre la seguridad y la facilidad de uso. La adaptación visual para diferentes condiciones de iluminación representa un avance importante en la accesibilidad de la plataforma.

Los próximos pasos se centrarán en mejorar cada módulo con funcionalidades más avanzadas,

optimizar el rendimiento general de la aplicación y añadir características que incrementen el valor educativo de la plataforma para usuarios no técnicos.

Fecha de actualización: 20 de mayo de 2025