Checklist Consolidado de Correes

Data: 26 de Junho de 2025

Versão: 1.0

Componentes Avaliados: API ML, API Principal, Frontend

Pontos Fortes Identificados

API ML

Autenticação com uso de API Key

Usuário de banco com privilégios mínimos

API Principal

Proteção contra SQL Injection

Uso de JWT para autenticação

Vulnerabilidades Críticas (Correção Imediata)

API Principal

CORS sem restrições

Ausência de Rate Limiting

JWT Secret fraco

Falta de Headers de Segurança

Uso do usuário root no banco

Exposição via /static

Frontend

JWT no AsyncStorage

Logs contendo senhas

Recuperação de senha frágil

Vulnerabilidades Críticas (Correção Imediata)

Validação apenas no frontend

Vulnerabilidades de Alta Severidade (Corrigir em até 1 semana)

API Principal

Falta de revogação de tokens

Falta de verificação de privilégios

Stack traces visíveis

Frontend

Falta de verificação de expiração do token

Headers de autorização globais

Reset de senha inseguro

Vulnerabilidades de Severidade Média (Corrigir em até 1 mês)

API ML

Falta de Rate Limiting e validações rigorosas

Logs de auditoria ausentes

API Principal

Tokens de longa duração sem refresh

Banco sem SSL

Falta de variáveis dev/prod

Frontend

Debug em produção

Sem certificate pinning

Vulnerabilidades de Severidade Média (Corrigir em até 1 mês)

Falta de sanitização de dados

Política de senha fraca

Vulnerabilidades de Baixa Severidade (Planejar para o futuro)

API ML

Sanitização e rotação de logs

Monitoramento de segurança

Frontend

Falta de obfuscação de código

Sem MFA

Sem detecção de root

Sem CSRF

Dependências não auditadas

Checklist Consolidado de Correções

[ ] CORS restritivo - Crítico

[ ] Rate limiting - Crítico

[ ] JWT seguro (Keychain) - Crítico

[ ] Headers de segurança - Crítico

[ ] Verificação de privilégios - Alta

[ ] Logging e tratamento de erros - Alta

[ ] Validação/sanitização server-side - Média

[ ] Certificate pinning - Média

[ ] Segregação de ambientes - Média

[ ] MFA e senha forte - Baixa

Checklist Consolidado de Correções

[ ] Obfuscação de código - Baixa