Relatório Técnico – Projeto de Login e Registro Seguro com Firebase

Disciplina: Segurança da Informação
Tema: Desenvolvimento Seguro de Tela de Login e Registro
Data de Entrega: 24/04/2025

Tecnologias Utilizadas

- **Linguagens:** HTML5, CSS3 (Material Design 3), JavaScript puro
- **Plataforma de Autenticação:** Firebase Authentication
- **Segurança Antibot:** Google reCAPTCHA v2
- **Simulação de Backend:** Arquivo `firebase-config.private.js`
- **Hospedagem:** Ambiente local (localhost)

As tecnologias foram escolhidas por permitirem o foco na segurança do frontend, com uma estrutura leve, responsiva e compatível com projetos educacionais.

Implementações de Segurança

1. Cadastro de Usuário

- **Validação de senha forte:**
  - Mínimo de 8 caracteres
  - Uma letra maiúscula e uma minúscula
  - Um número e um caractere especial
- **Validação de e-mail** pelo padrão Firebase
- **Verificação obrigatória de e-mail** antes do login
- **Google reCAPTCHA** na tela de registro

2. Login de Usuário

- **Mensagens de erro genéricas**, sem indicar qual campo está errado
- **Senha apagada automaticamente** do campo após tentativa
- **Redirecionamento seguro** com função `safeRedirect()` para prevenir ataques de Open Redirect

3. Proteções Avançadas

- **Content-Security-Policy (CSP):**
  - Restringe scripts e estilos apenas às origens confiáveis (Firebase, Google Fonts)
- **X-Frame-Options: DENY**
  - Bloqueia renderização em `<iframe>` (proteção contra clickjacking)
- **X-Content-Type-Options: nosniff**
  - Impede tentativa de "adivinhar" tipos de arquivo e executá-los incorretamente

4. Proteção de Credenciais Firebase

- **Uso de pseudo-backend local**:
  - Arquivo `firebase-config.private.js` mantido fora do diretório público
  - Não enviado ao GitHub
  - Simula um backend real ao carregar o `firebaseConfig` via variável global segura

Dificuldades Enfrentadas

- Ajustar a **Content-Security-Policy** para funcionar corretamente com Firebase + reCAPTCHA
- Garantir que o `firebaseConfig` não estivesse acessível via inspeção
- Corrigir interações entre o tema escuro e os estilos herdados do Material 3
- Resolver erro de acesso ao Firebase antes da inicialização da config segura

Conclusão

O sistema implementa todas as boas práticas de segurança recomendadas para ambientes web: validação, autenticação com verificação, controle de redirecionamento e headers de proteção.

Mesmo sendo local, o projeto é estruturado como um sistema real, demonstrando preparo para aplicações futuras com publicação em ambientes seguros como Firebase Hosting.

"Segurança não é um recurso opcional — é a base de qualquer sistema web."

Desenvolvedor: kayky J.C. montes,Everton Miranda de Souza
Data: 24/04/2025