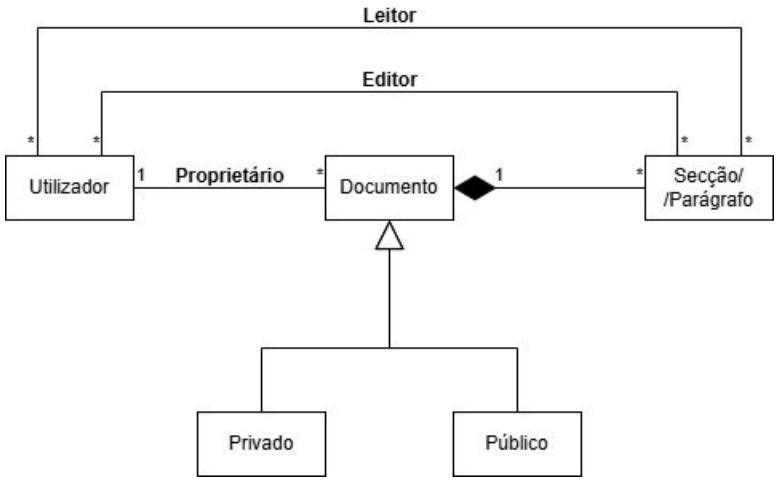
Editor de Documentos Colaborativo Seguro

Segurança em Engenharia de Software

Grupo EMA
up201804979 | André Serra
up202108758 | Eduardo Roçadas
up202108744 | Manuel Neto

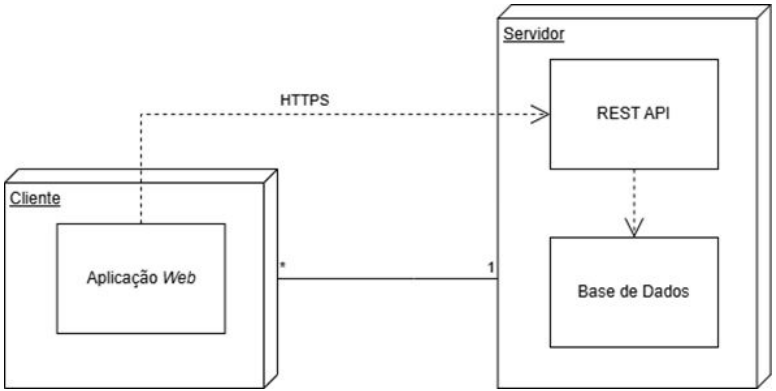
Requisitos

- ➔ Interface
- ➔ Autenticação
- ➔ Controlo de Acessos



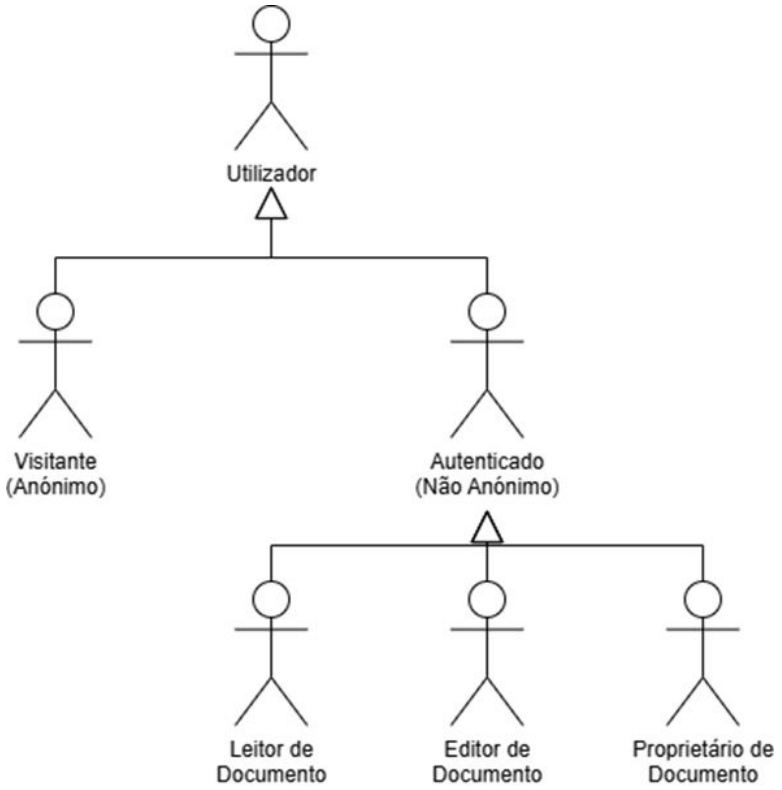
Arquitetura

- ➔ Aplicação Web
- ➔ REST API
- ➔ Base de Dados



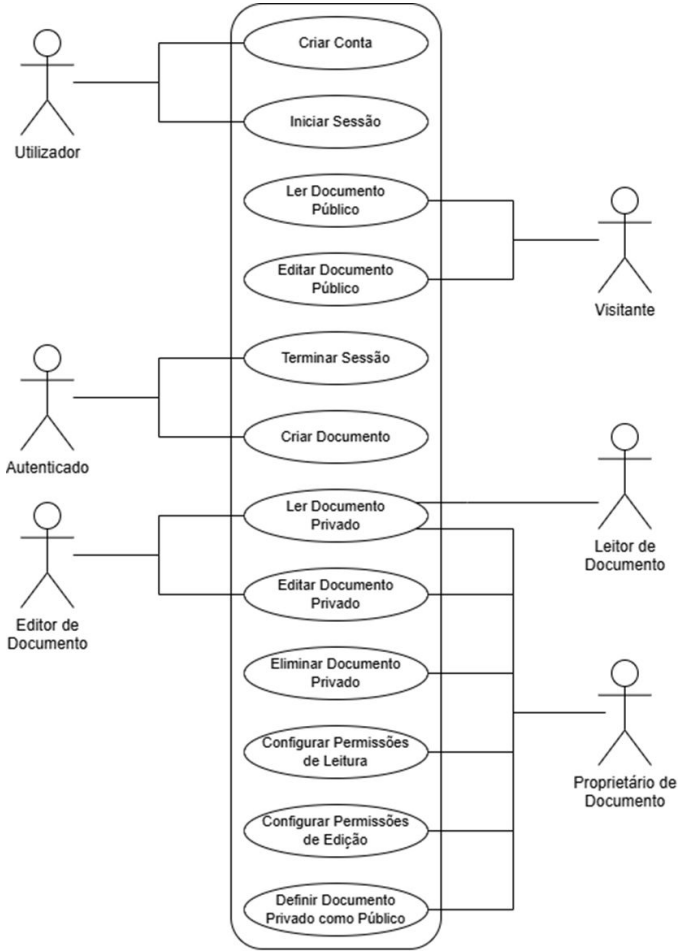
Atores

- ➔ Utilizador
- ➔ Visitante
- ➔ Autenticado
- ➔ Leitor
- ➔ Editor
- ➔ Proprietário



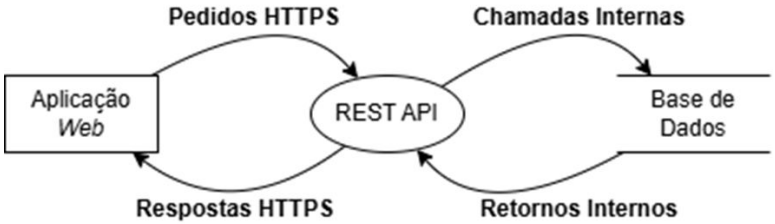
Use Cases

- ➔ Use Cases
- ➔ Misuse Cases
- ➔ Abuse Cases



Modelação de Ameaças

- ➔ **S**poofing
- ➔ **T**ampering
- ➔ **R**epudiation
- ➔ **I**nformation Disclosure
- ➔ **D**enial of Service
- ➔ **E**levation of Privilege



Implementação

- ➔ Etherpad
- ➔ OnlyOffice
- ➔ Collabora
- ➔ **CryptPad**
- ➔ HedgeDoc
- ➔ MUTE
- ➔ PeerPad

CryptPad

Configuração

- ➔ otpSessionExpiration
- ➔ enforceMFA
- ➔ logIP
- ➔ adminKeys

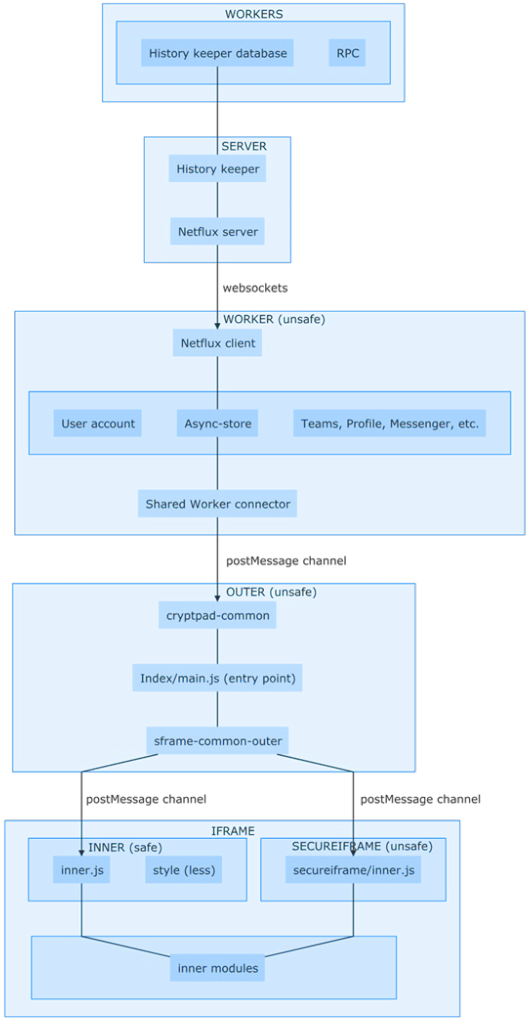
- ➔ availablePadTypes
- ➔ registeredOnlyTypes
- ➔ availableLanguages
- ➔ surveyURL
- ➔ hostDescription
- ➔ enableTemplates
- ➔ enableHistory
- ➔ loginSalt
- ➔ minimumPasswordLength
- ➔ disableAnonymousStore
- ➔ disableAnonymousPadCreation
- ➔ disableFeedback

Linguagem de Programação

- ➔ Same-Origin Policy
- ➔ Content Source Policy
- ➔ Cross-Origin Resource Sharing
- ➔ SubResource Integrity

Design Patterns

- ➔ Sandboxing
- ➔ Sistema de Ficheiros

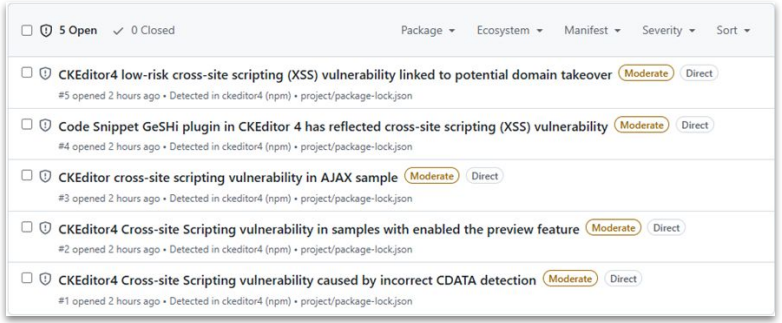


Mitigações para Vulnerabilidades Comuns

- ➔ Broken Access Control
- ➔ Cryptographic Failures
- ➔ Injection
- ➔ Insecure Design
- ➔ Security Misconfiguration

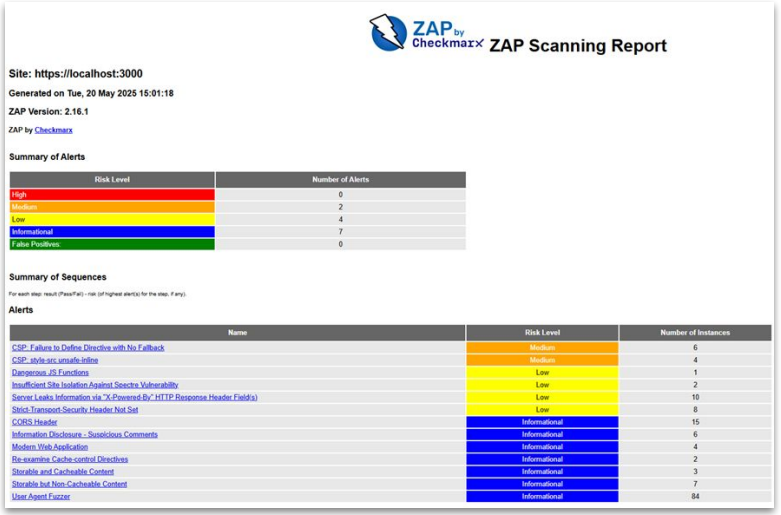
Dependências e Bibliotecas

- ➔ npm audit
- ➔ Snyk
- ➔ Dependabot



Metodologias de Teste de Segurança

- ➔ GitHub Actions
- ➔ OWASP Zap



ZAP by Checkmarx ZAP Scanning Report

Site: https://localhost:3000

Generated on Tue, 20 May 2025 15:01:18

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	4
Informational	7
False Positives:	0

Summary of Sequences

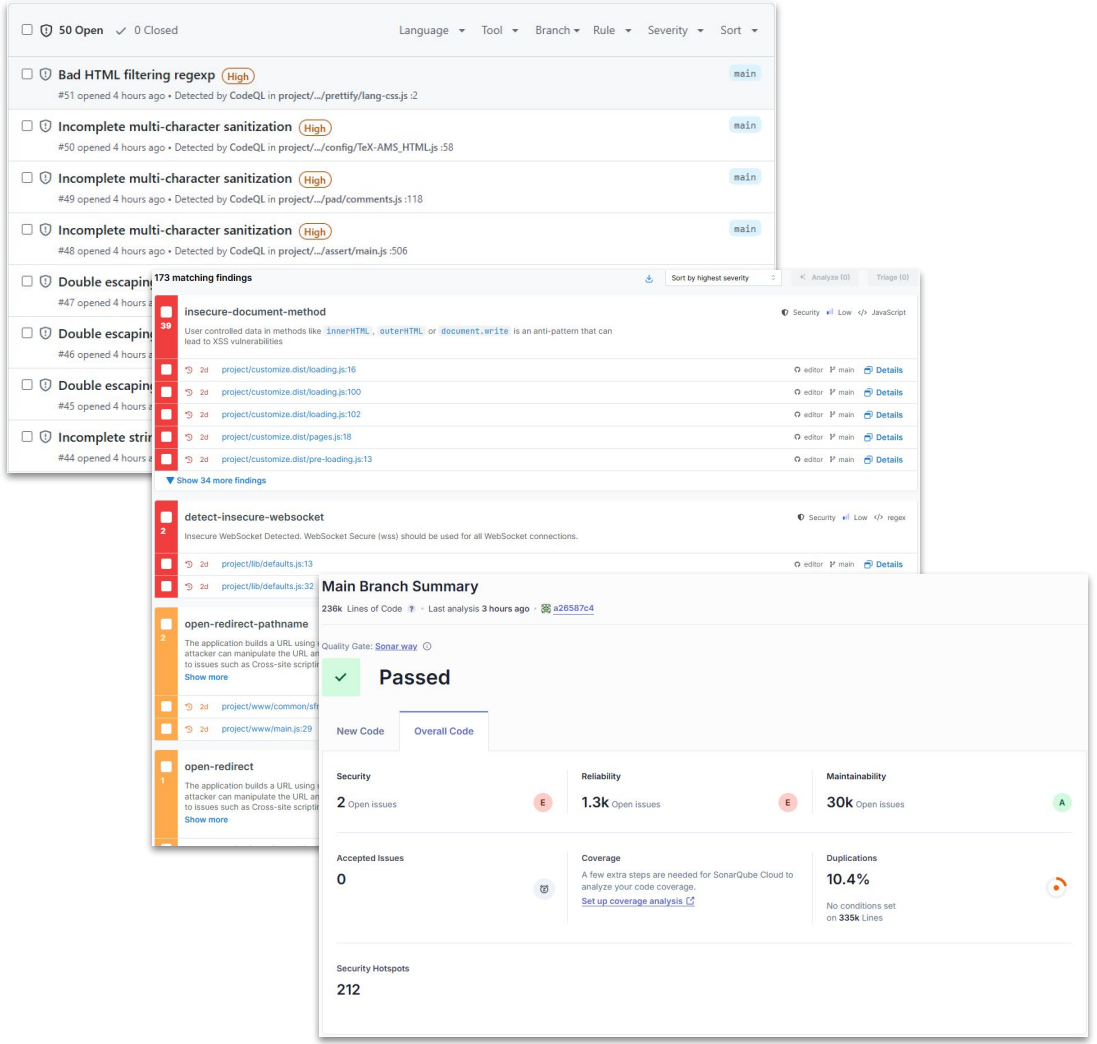
For each step: result (Pass/Fail) - risk (of highest alert(s) for the step, if any).

Alerts

Name	Risk Level	Number of Instances
CSP: Failure to Define Directive with No Fallback	Medium	6
CSP: style-src unsafe-inline	Medium	4
Dangerous JS Functions	Low	1
Insufficient Site Isolation Against Spectre Vulnerability	Low	2
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	10
Strict-Transport-Security Header Not Set	Low	8
CORS Header	Informational	15
Information Disclosure - Suspicious Comments	Informational	6
Modern Web Application	Informational	4
Re-examine Cache-control Directives	Informational	2
Storable and Cacheable Content	Informational	3
Storable but Non-Cacheable Content	Informational	7
User Agent Fuzzer	Informational	84

Ferramentas de Análise de Código

- ➔ CodeQL
- ➔ Semgrep
- ➔ SonarQube Cloud



Conclusão

- ➔ Shift Left Security
- ➔ SecDevOps