stone

ABRIL, 2021

CONTEÚDO CONFIDENCIAL

Documentação do Processo de Análise dos Códigos Fontes - Dashboard

DEVSEC TEAM

Revisão Abril 2021

Sumário

1. Gandalf

1.1. Definição

Gandalf, software que agrupa diversas ferramentas de análise estática de códigos fonte, em busca de vulnerabilidades.

Sua característica principal é executar análises diretamente nos repositórios, sem a necessidade de implementações específicas e complexas em pipelines.

Esta ferramenta funciona de forma **automatizada (24/7)**, onde todos os repositórios são analisados **continuamente**.

1.2. Objetivo

O Gandalf busca identificar, categorizar e propor tratativas para vulnerabilidades, a fim de aprimorar a segurança dos códigos das empresas envolvidas.

1.3. Fluxo de funcionamento do Gandalf

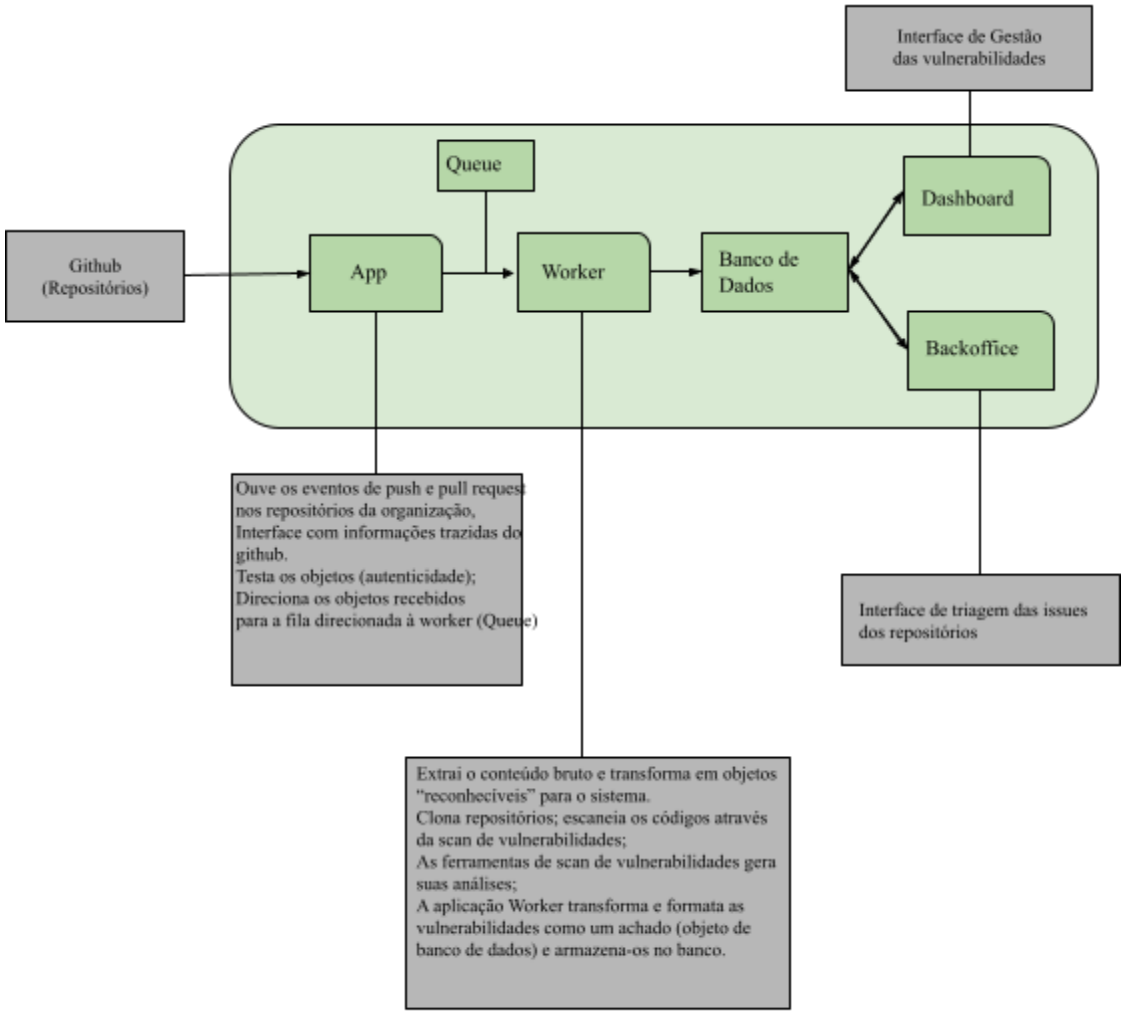

Figura 2 - *Documentação do Processo de Análise dos Códigos Fonte*

2. Dashboard

2.1. Login

A Dashboard é acessível ao usuário através do login do Github (vinculado à alguma das empresas que são monitoradas pelo Gandalf).

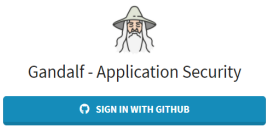

figura 3 - *Documentação do Processo de Análise dos Códigos Fonte*

2.2. Tela Inicial

A tela inicial da dashboard apresenta a quantidade de achados nos últimos 30 dias, o total de achados abertos pelos analistas de segurança, os resolvidos pelo time de desenvolvedores e os reabertos pelo time de analistas de segurança. Logo abaixo, 4 gráficos categorizam os achados abertos ou reabertos, de acordo com sua criticidade, escopo, categoria OWASP TOP 10 e tipo de teste de vulnerabilidade. Por fim, são apresentadas algumas estatísticas que dizem respeito aos repositórios, usuários e principais linguagens de programação presentes no escopo do usuário logado.

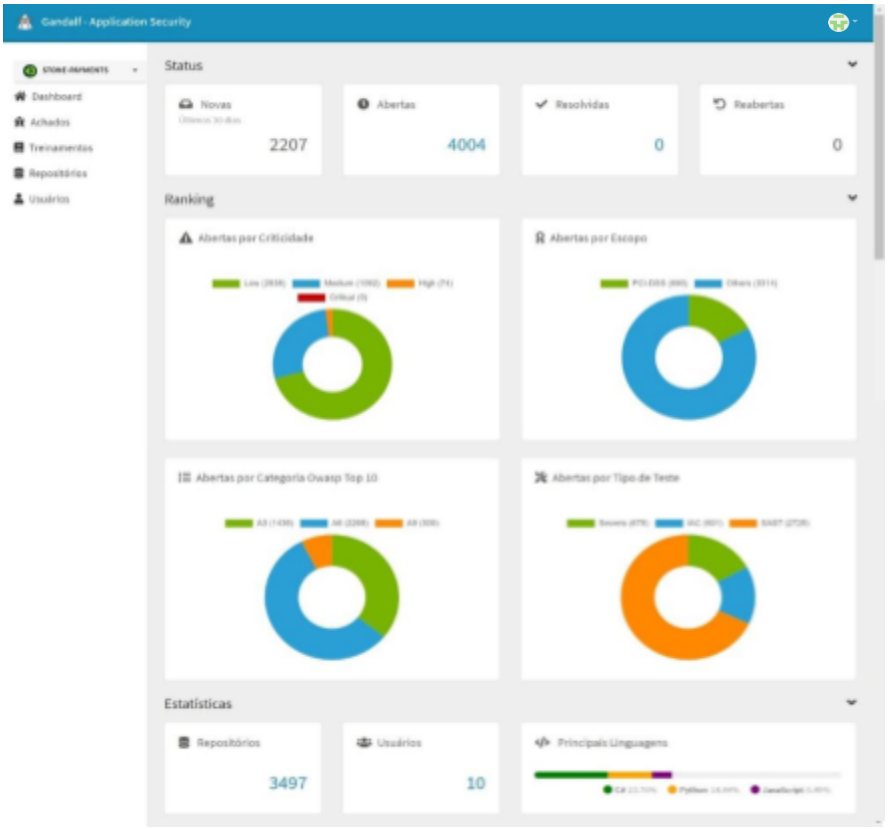

figura 5 - *Documentação do Processo de Análise dos Códigos Fonte*

2.3. Achados

Na tela de achados é possível ver uma lista de acordo com o escopo do usuário, onde um gestor ou desenvolvedor consegue visualizar a descrição/criticidade, o trecho do código que foi indicado com vulnerabilidade, a remediação sugerida e a nota de observação do time de analistas.

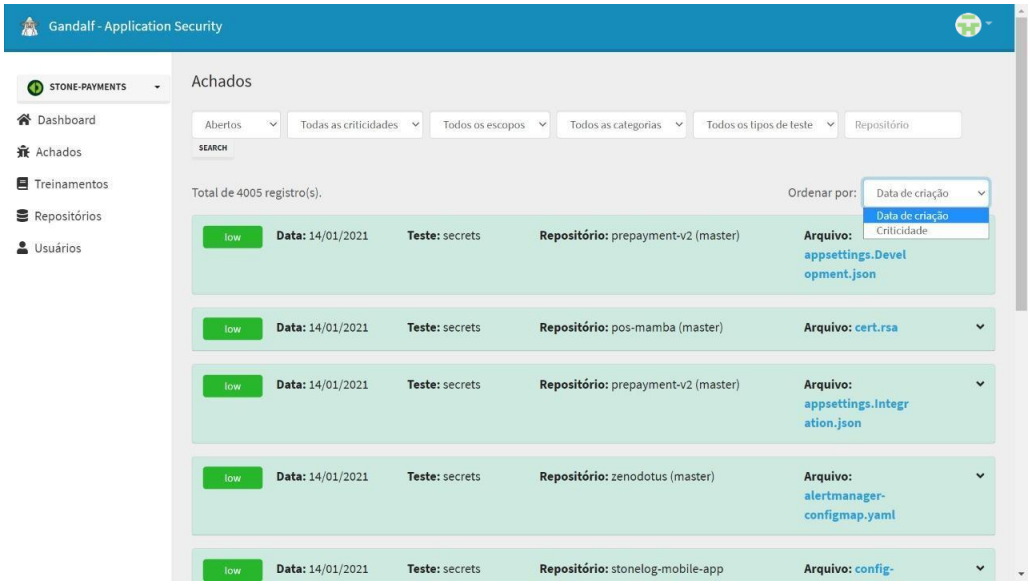

figura 6 - *Documentação do Processo de Análise dos Códigos Fonte*

2.3.1. Lista de Achados

Na lista de achados, clicando em um deles, fica visível a descrição da vulnerabilidade, o trecho do código que ela foi identificada, a remediação sugerida para o problema e possíveis notas feitas pelo analista de segurança com o intuito de auxiliar na mitigação.

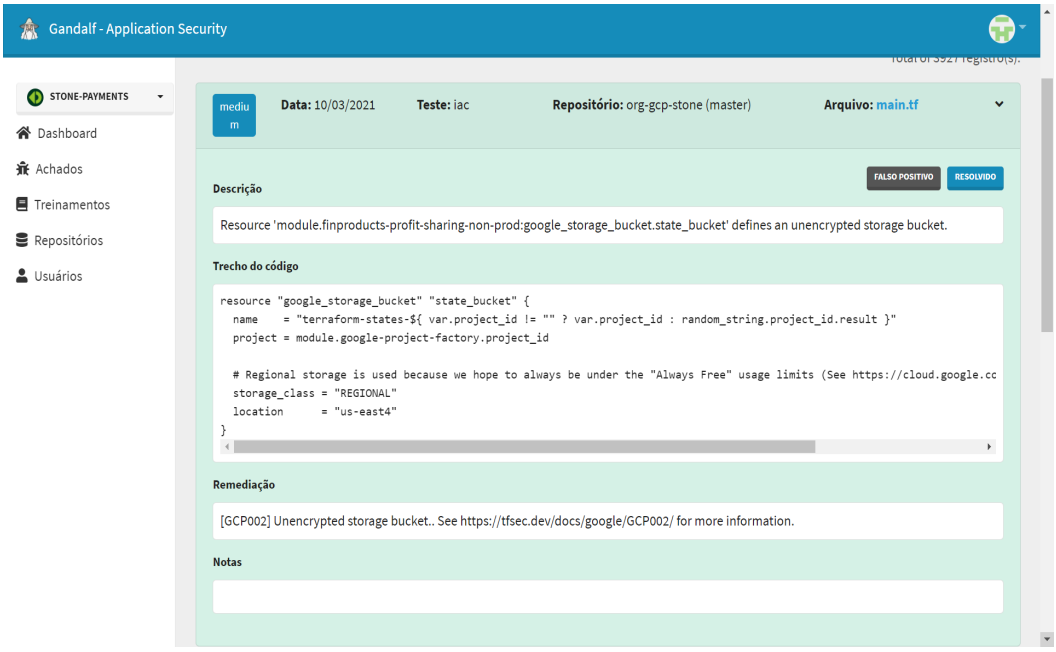

figura 7 - *Documentação do Processo de Análise dos Códigos Fonte*

2.3.2. Falso Positivo

Na opção falso positivo o desenvolvedor, após a análise, pode desconsiderar um achado mediante uma justificativa técnica explicando o porquê se trata de um falso positivo.

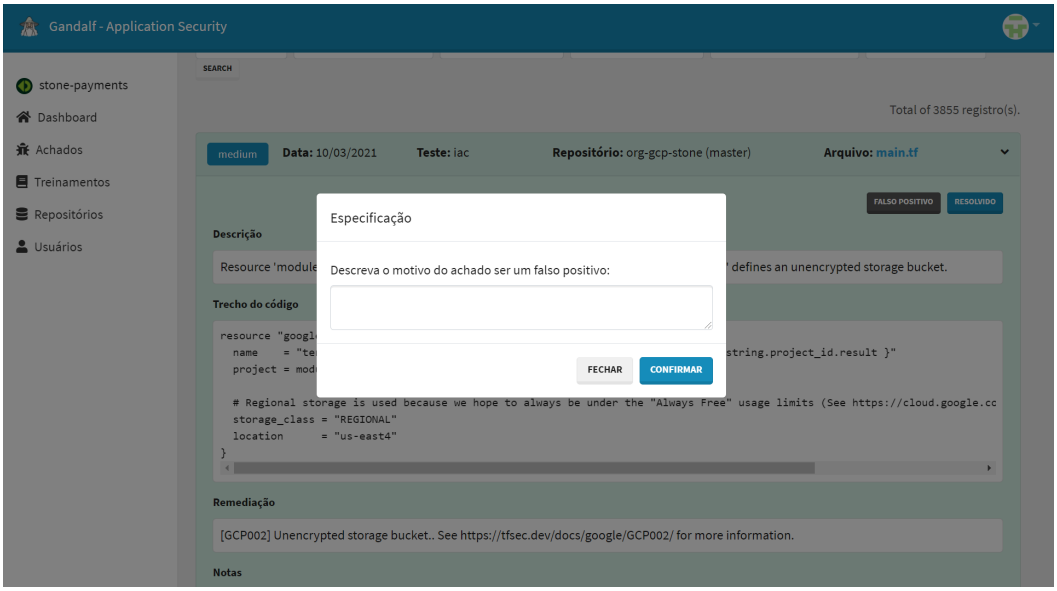

figura 8 - *Documentação do Processo de Análise dos Códigos Fonte*

2.3.3. Correção

Após a correção por parte do desenvolvedor responsável por aquele achado, ele deve ser marcado como resolvido.

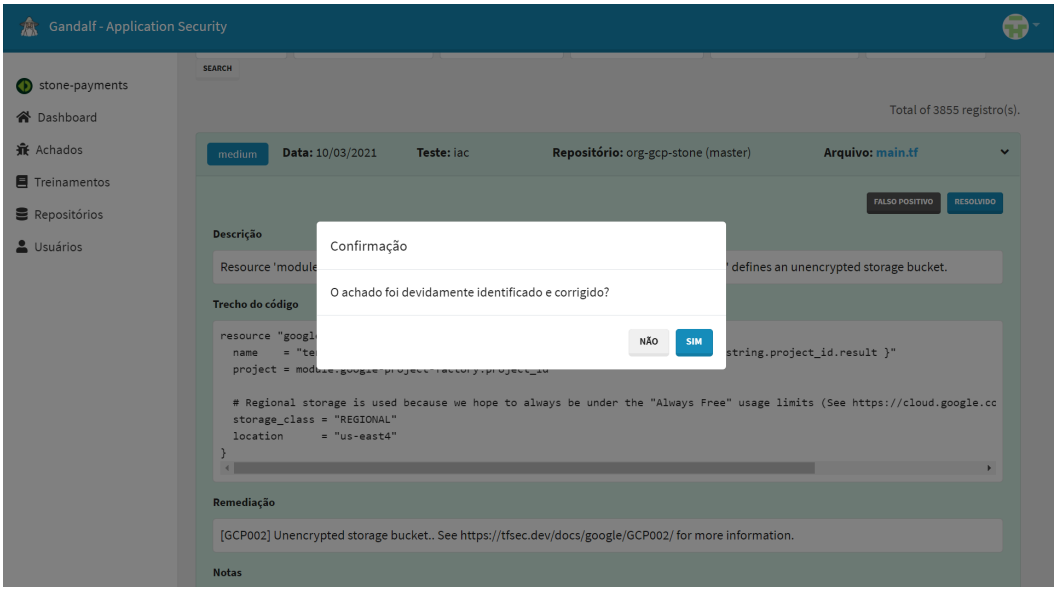

figura 9 - *Documentação do Processo de Análise dos Códigos Fonte*

2.4. Treinamentos

Na tela de treinamentos ficam disponíveis os links que direcionam para a plataforma Studa, onde armazenamos todo o plano de desenvolvimento da cia, incluindo os treinamentos PCI que são obrigatórios para auditoria.

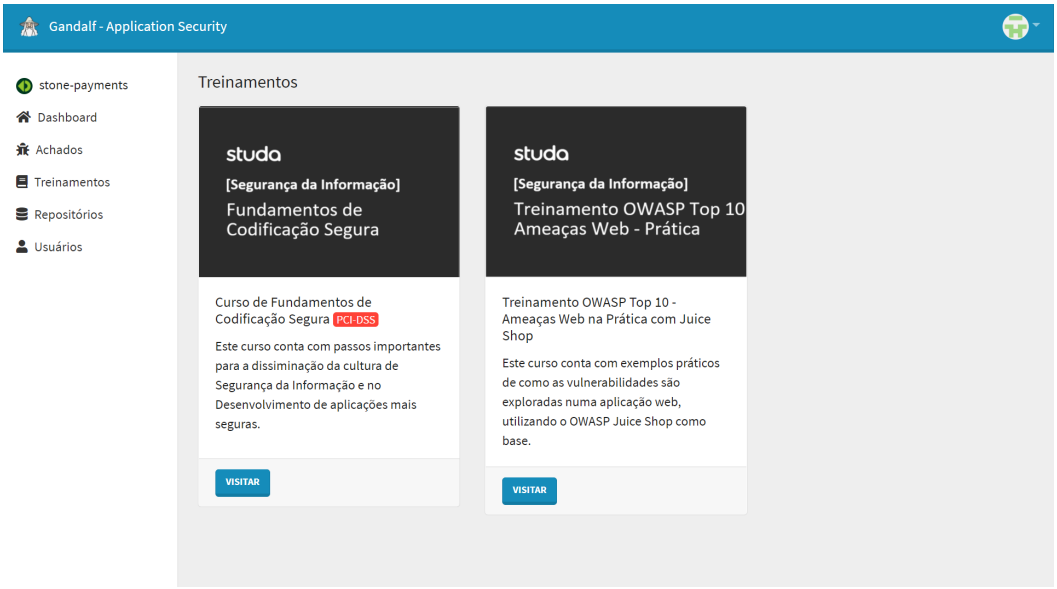

figura 10 - *Documentação do Processo de Análise dos Códigos Fonte*

2.5. Repositórios

Na tela dos repositórios é apresentada a lista de repositórios que tem relação com a organização que está sendo visualizada. As tags indicam o escopo ao qual o repositório está incluído.

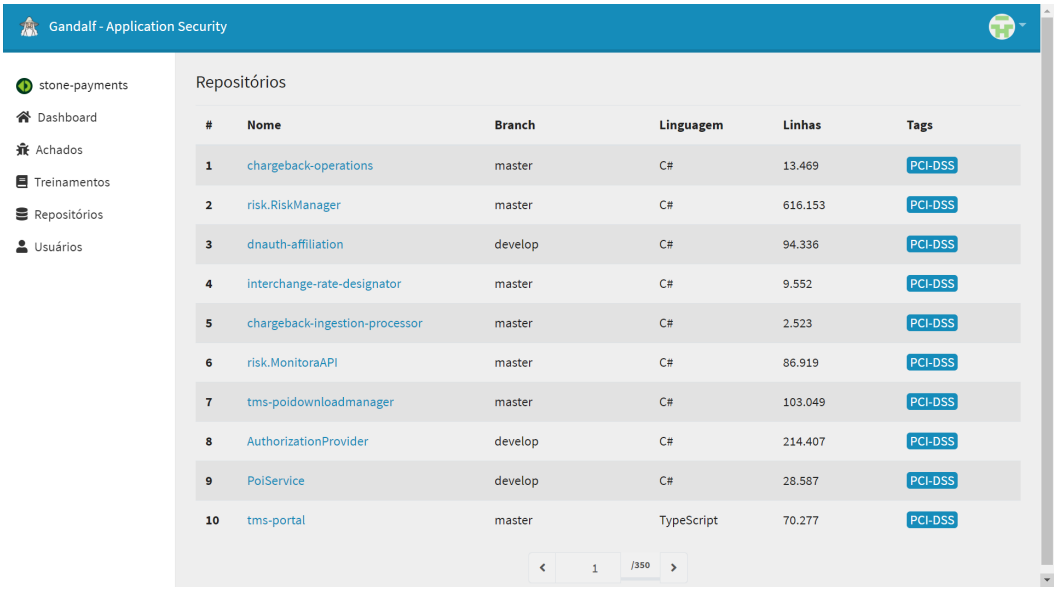

figura 11 - *Documentação do Processo de Análise dos Códigos Fonte*

2.6. Usuários

Na tela de usuários é apresentada a lista das pessoas que fazem parte da organização que está sendo visualizada.

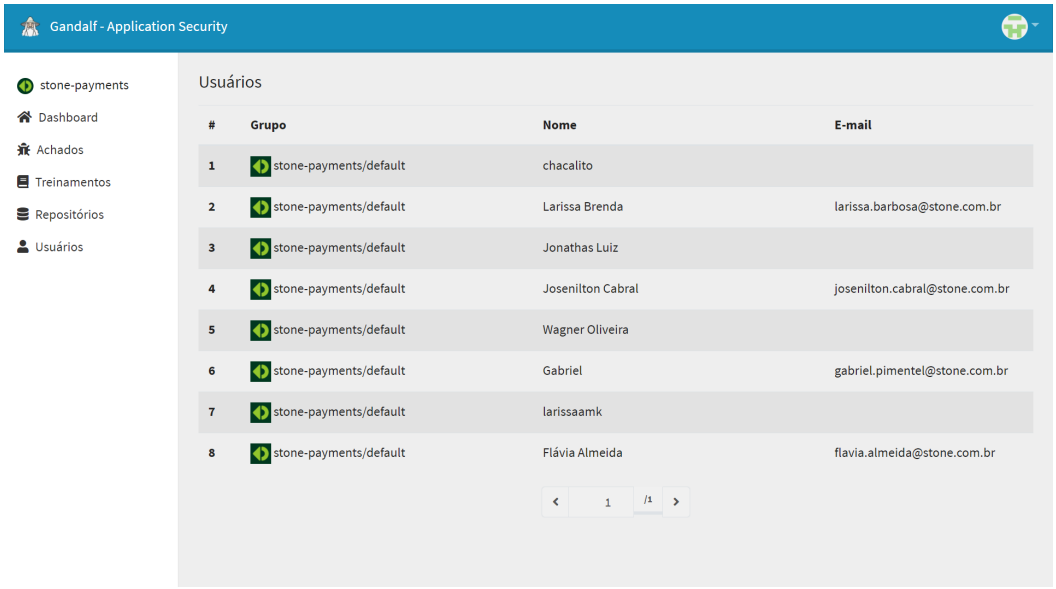

figura 12 - *Documentação do Processo de Análise dos Códigos Fonte*