



Documentação do Processo de Análise dos Códigos Fontes - Dashboard

DEVSEC TEAM

Revisão Abril 2021



Sumário

1.	Gandalf	2
1.1.	Definição	2
1.2.	Objetivo	2
1.3.	Fluxo de funcionamento do Gandalf	3
2.	Dashboard	4
2.1.	Login	4
2.2.	Tela Inicial	5
2.3.	Achados	6
2.3.1.	Lista de Achados	7
2.3.2.	Falso Positivo	8
2.3.3.	Correção	9
2.4.	Treinamentos	10
2.5.	Repositórios	11
2.6.	Usuários	12



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

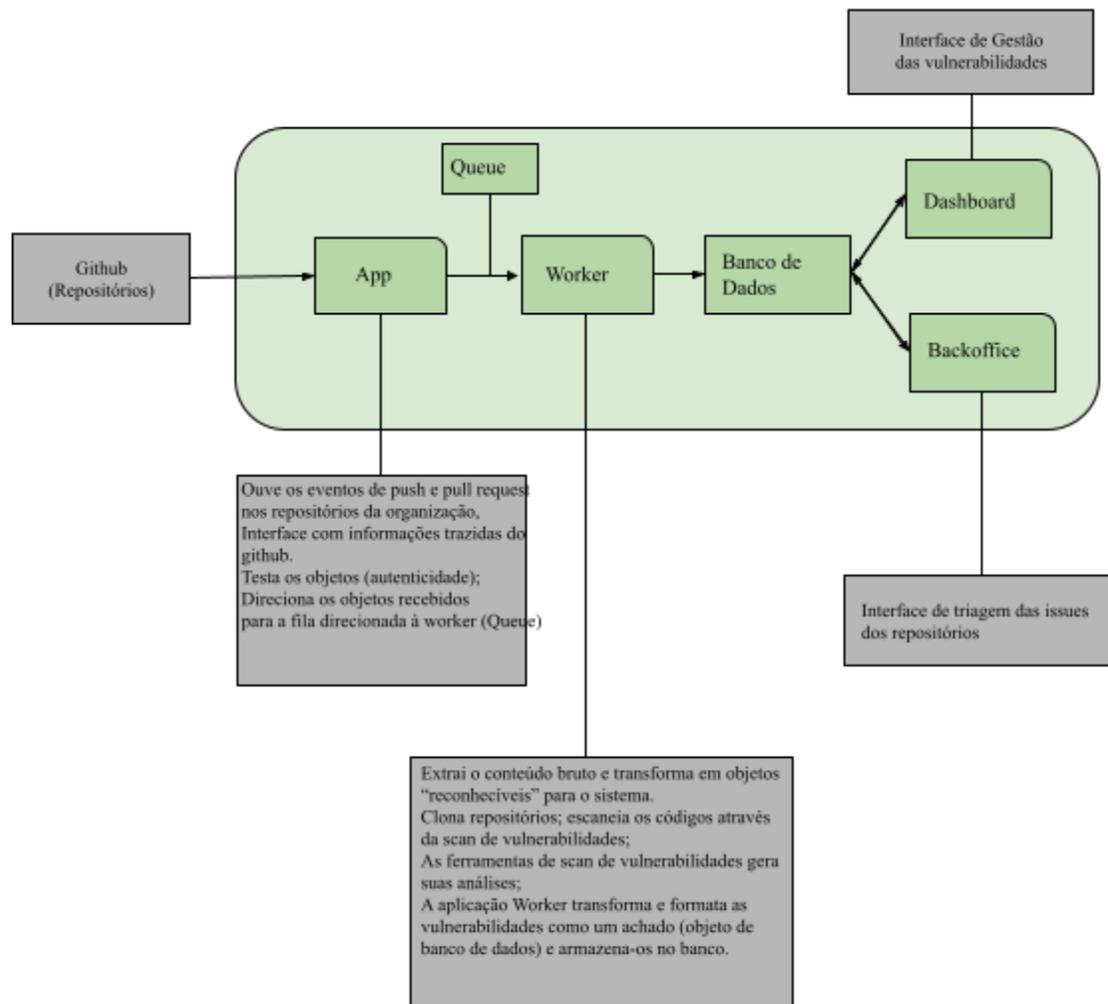


Figura 2 - Documentação do Processo de Análise dos Códigos Fonte



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.

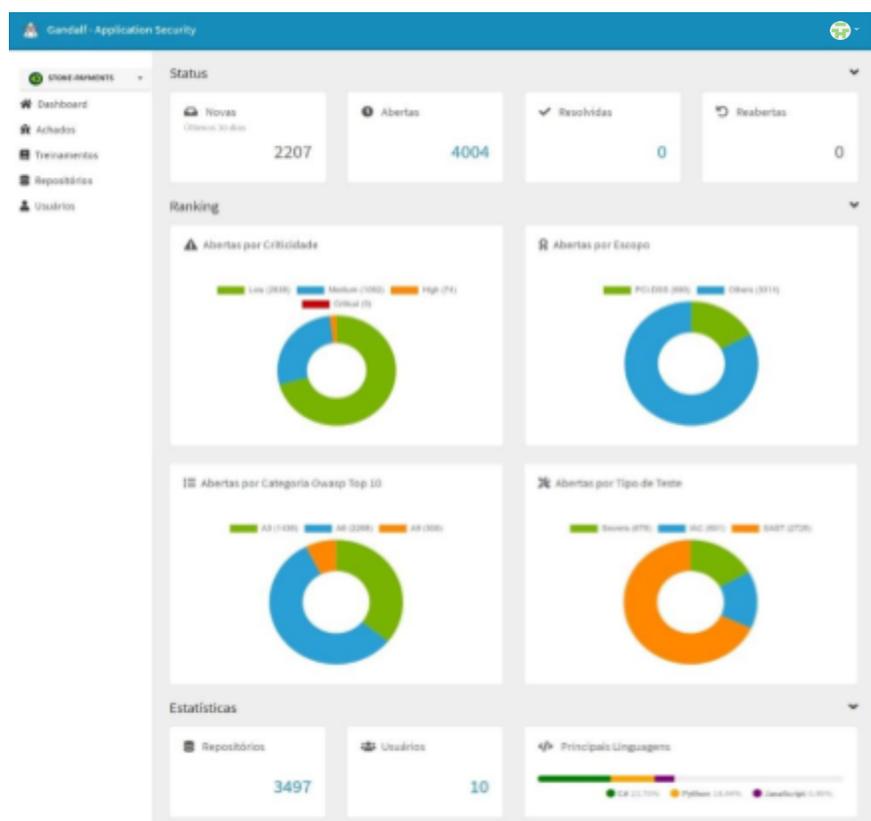


figura 5 - Documentação do Processo de Análise dos Códigos Fonte



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.

low	Data: 14/01/2021	Teste: secrets	Repositório: prepayment-v2 (master)	Arquivo: appsettings.Development.json
low	Data: 14/01/2021	Teste: secrets	Repositório: pos-mamba (master)	Arquivo: cert.rsa
low	Data: 14/01/2021	Teste: secrets	Repositório: prepayment-v2 (master)	Arquivo: appsettings.Integration.json
low	Data: 14/01/2021	Teste: secrets	Repositório: zenodotus (master)	Arquivo: alertmanager-configmap.yaml
low	Data: 14/01/2021	Teste: secrets	Repositório: stonelog-mobile-app	Arquivo: config-

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.

The screenshot displays the Gandalf - Application Security interface. The top navigation bar includes the application name and a user profile icon. A sidebar on the left lists navigation options: Dashboard, Achados, Treinamentos, Repositórios, and Usuários. The main content area shows a vulnerability report for a 'medium' severity issue. The report includes the following details:

- Data:** 10/03/2021
- Teste:** iac
- Repositório:** org-gcp-stone (master)
- Arquivo:** main.tf
- Descrição:** Resource 'module.finproducts-profit-sharing-non-prod:google_storage_bucket.state_bucket' defines an unencrypted storage bucket. Buttons for 'FALSO POSITIVO' and 'RESOLVIDO' are visible.
- Trecho do código:**

```
resource "google_storage_bucket" "state_bucket" {
  name = "terraform-states-${ var.project_id != "" ? var.project_id : random_string.project_id.result }"
  project = module.google-project-factory.project_id

  # Regional storage is used because we hope to always be under the "Always Free" usage limits (See https://cloud.google.cc
  storage_class = "REGIONAL"
  location      = "us-east4"
}
```
- Remediação:** [GCP002] Unencrypted storage bucket.. See <https://tfsec.dev/docs/google/GCP002/> for more information.
- Notas:** A text input field for notes is present but empty.

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.

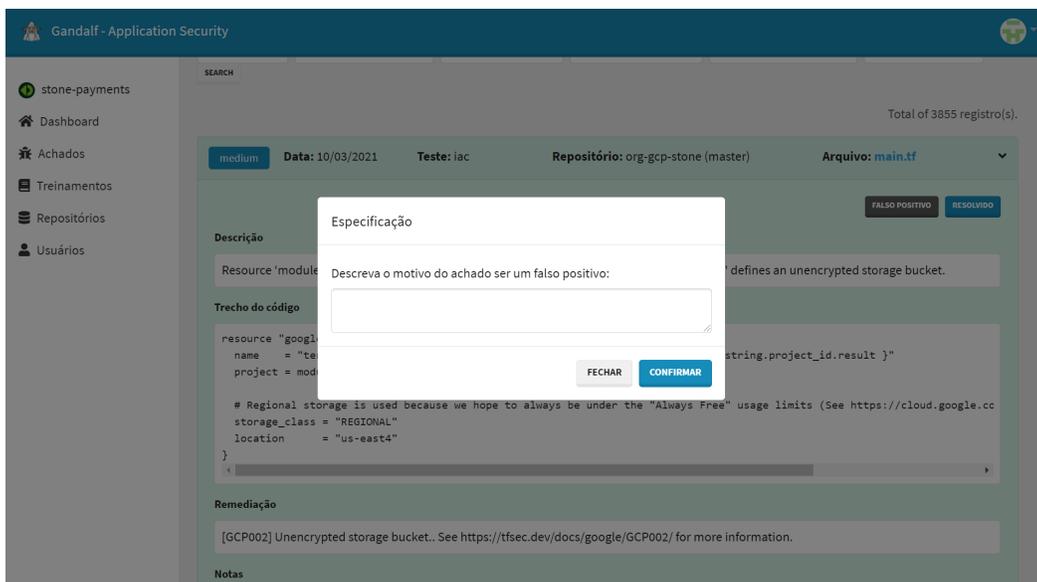


figura 8 - Documentação do Processo de Análise dos Códigos Fonte



2.3.3. Correção

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

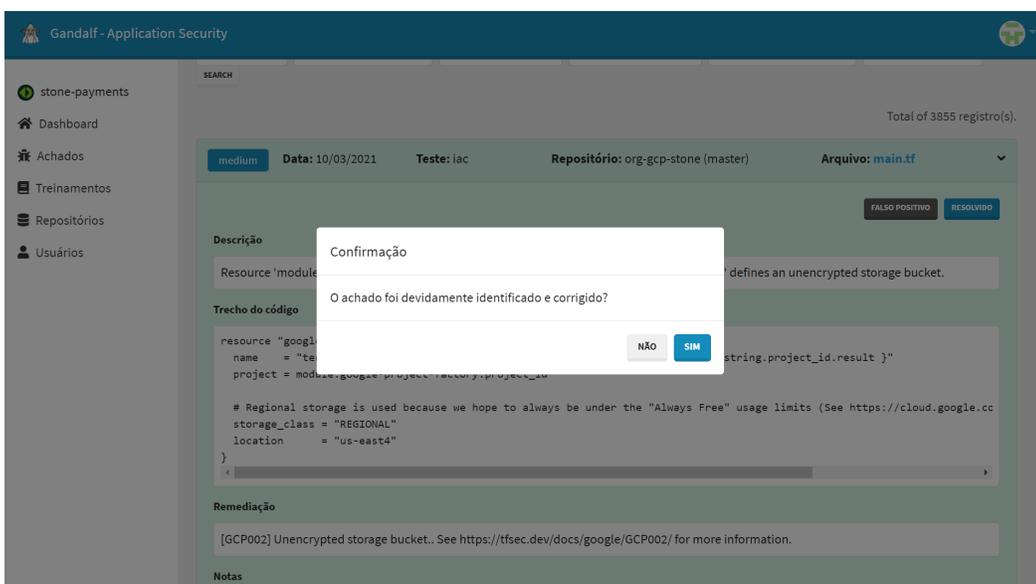


figura 9 - Documentação do Processo de Análise dos Códigos Fonte



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.

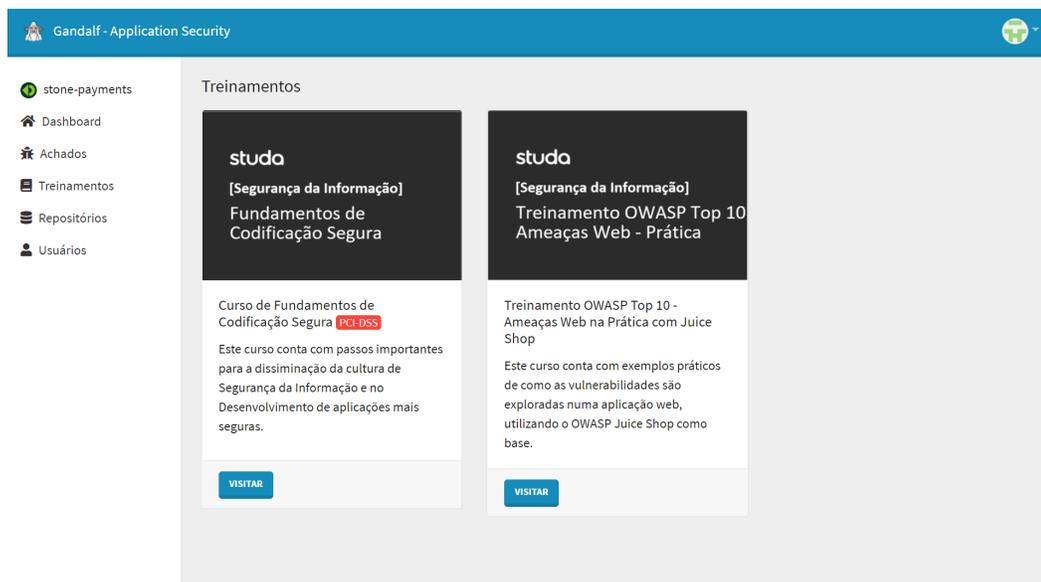


figura 10 - Documentação do Processo de Análise dos Códigos Fonte



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.

The screenshot shows the Gandalf - Application Security interface. On the left is a navigation menu with items: stone-payments, Dashboard, Achados, Treinamentos, Repositórios, and Usuários. The main area is titled 'Repositórios' and contains a table with 10 rows of repository information. Each row includes a number, the repository name, the branch, the language, the number of lines, and a tag (PCI-DSS). A pagination bar at the bottom shows page 1 of 350.

#	Nome	Branch	Linguagem	Linhas	Tags
1	chargeback-operations	master	C#	13.469	PCI-DSS
2	risk.RiskManager	master	C#	616.153	PCI-DSS
3	dnauth-affiliation	develop	C#	94.336	PCI-DSS
4	interchange-rate-designator	master	C#	9.552	PCI-DSS
5	chargeback-ingestion-processor	master	C#	2.523	PCI-DSS
6	risk.MonitoraAPI	master	C#	86.919	PCI-DSS
7	tms-poidownloadmanager	master	C#	103.049	PCI-DSS
8	AuthorizationProvider	develop	C#	214.407	PCI-DSS
9	PoiService	develop	C#	28.587	PCI-DSS
10	tms-portal	master	TypeScript	70.277	PCI-DSS

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.

#	Grupo	Nome	E-mail
1	stone-payments/default	chacalito	
2	stone-payments/default	Larissa Brenda	larissa.barbosa@stone.com.br
3	stone-payments/default	Jonathas Luiz	
4	stone-payments/default	Josenilton Cabral	josenilton.cabral@stone.com.br
5	stone-payments/default	Wagner Oliveira	
6	stone-payments/default	Gabriel	gabriel.pimentel@stone.com.br
7	stone-payments/default	larissaamk	
8	stone-payments/default	Flávia Almeida	flavia.almeida@stone.com.br

figura 12 - Documentação do Processo de Análise dos Códigos Fonte