



GitHub4Women

Domain 6: Privacy, Security, and
Administration



Agenda

- 1 Autenticação - Autenticação de dois Fatores (2FA)
- 2 Administração - Diferentes permissões de acesso e gerenciamento de colaboradores
- 3 Enterprise Managed Users (EMUs)
- 4 Recursos de Segurança
- 5 Insights



Autenticação



Autenticação de usuário



A autenticação de usuário tradicional usa um ID de usuário e senha.

A autenticação de fator único é insegura; é fácil para invasores imitarem um usuário legítimo.

O GitHub tem ferramentas de autenticação que promovem as melhores práticas de segurança.



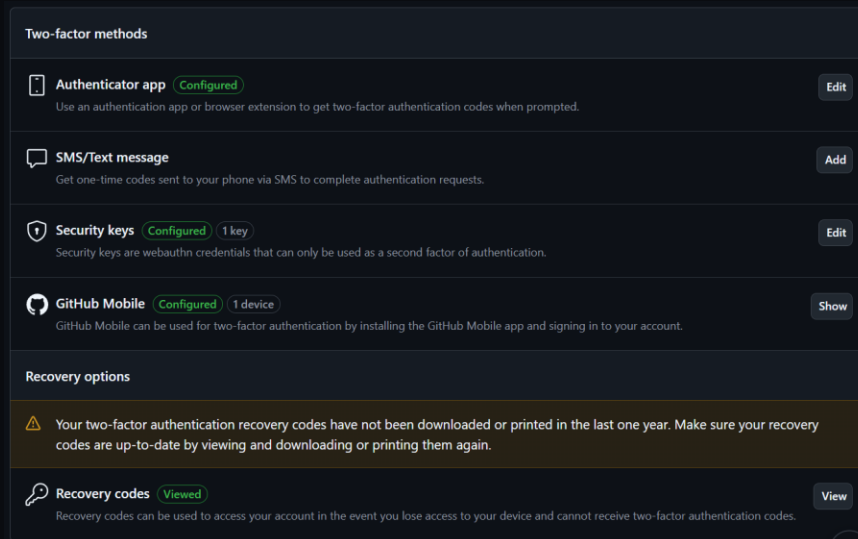
Autenticação de dois Fatores (2FA)

A autenticação de dois fatores (2FA) é uma camada extra de segurança usada ao fazer login em sites ou aplicativos. Com a 2FA, você precisa fazer login com seu nome de usuário e senha e fornecer outra forma de autenticação que somente você conhece ou tem acesso.

✓ TOTP

✓ SMS

✓ Chaves de Segurança




Autenticação de dois Fatores (2FA)

TOTP (Time-based one-time password) – Authenticator App

O GitHub recomenda usar um aplicativo TOTP baseado em nuvem para configurar a 2FA. Os aplicativos TOTP são mais confiáveis do que o SMS. Os aplicativos TOTP dão suporte para o backup seguro de seus códigos de autenticação na nuvem e podem ser restaurados se você perder o acesso ao seu dispositivo.


Two-factor methods

 **Authenticator app** Configured

Authenticator apps and browser extensions like 1Password, Authy, Microsoft used as a second factor to verify your identity when prompted during sign-in.

Scan the QR code

Use an authenticator app or browser extension to scan. [Learn more about authenticator apps](#)



Unable to scan? You can use the [setup key](#) to manually configure your authenticator app.


Verify the code from the app

XXXXXX

Save Cancel

17:32


IDs verificadas







Aceite um ID Verificado para ter mais controle de sua identidade

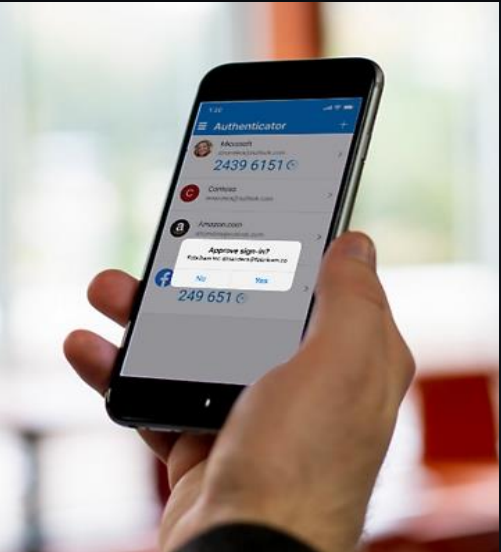
Alguns sites e organizações agora oferecem IDs verificadas. Elas tornam a configuração da conta mais simples e segura, ao mesmo tempo em que oferecem mais visibilidade e controle sobre seus dados pessoais.


Um site normalmente oferece uma ID verificada por meio de um código QR. Digitalize o código para começar.

 Digitalizar código QR


Saiba mais sobre os IDs Verificados





Two-factor authentication



Authentication code ⓘ

XXXXXX

Verify

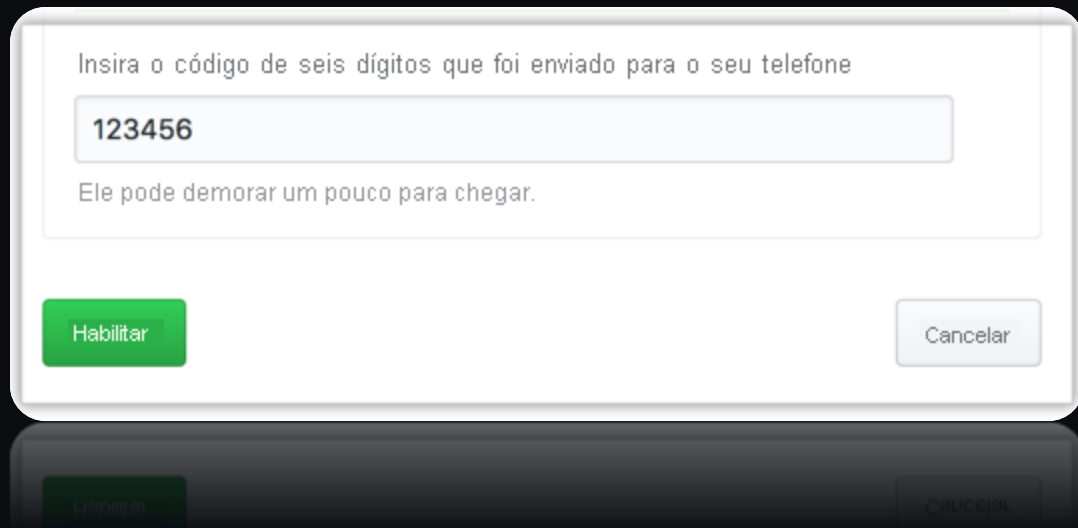
Open your two-factor authenticator (TOTP) app or browser extension to view your authentication code.

Having problems?

- Use your passkey
- Use GitHub Mobile
- Use a recovery code or begin 2FA account recovery

Autenticação de dois Fatores (2FA)

SMS



Insira o código de seis dígitos que foi enviado para o seu telefone

Ele pode demorar um pouco para chegar.

Habilitar Cancelar

Caso os usuários não possam se autenticar usando um aplicativo móvel TOTP, podem usar mensagens SMS. Essa forma de 2FA se baseia na suposição de que o usuário é a única pessoa com acesso ao seu dispositivo móvel.



Autenticação de dois Fatores (2FA)

Chaves de Segurança

As chaves de segurança também são credenciais WebAuthn, mas ao contrário das senhas, elas não exigem validação do usuário. Como as chaves de segurança só **precisam verificar a presença do usuário**, elas contam apenas como segundo fator e devem ser usadas em conjunto com sua senha.

Registrar uma chave de segurança para sua conta está disponível após ativar a autenticação de dois fatores com um aplicativo TOTP ou mensagem de texto. Se você perder sua chave de segurança, ainda poderá usar o código do seu telefone para fazer login.

Se você estiver acessando o GitHub.com de um dispositivo e navegador elegíveis, o GitHub pode solicitar que você registre o dispositivo como uma passkey durante o processo de login.





Unable to

Verify the

XXXXXX

Save

SMS/Text

Get one-time

Security key

Security key

hello

GitHub Mobile

GitHub Mobile

Recovery option

Recovery key

Recovery key

Windows Security
Corporation".



Couldn't recognize you. Please enter your
PIN.



PIN

PIN

[I forgot my PIN](#)

[More choices](#)



Face



PIN

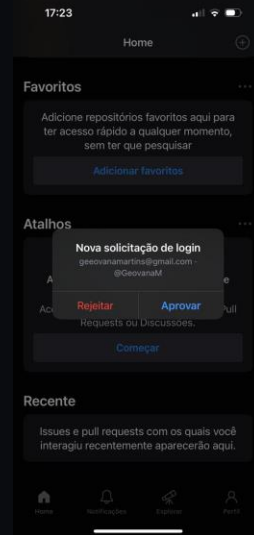
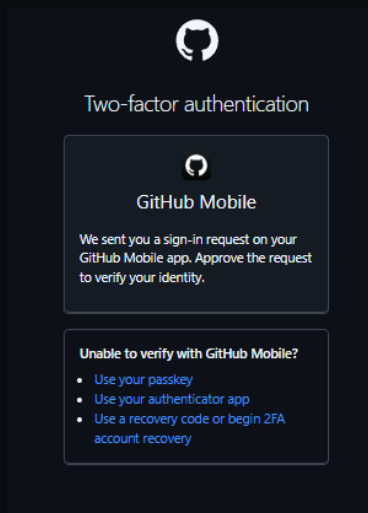
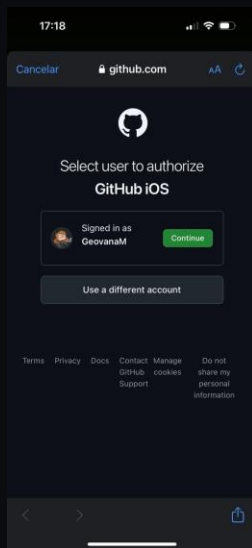
Cancel



Autenticação de dois Fatores (2FA)

GitHub Mobile

- Você pode usar o GitHub Mobile para 2FA ao entrar na sua conta do GitHub em um navegador da web. 2FA com o GitHub Mobile não depende de TOTP e, em vez disso, usa criptografia de chave pública para proteger sua conta.
- Depois de configurar um aplicativo TOTP ou SMS, **você também pode usar o GitHub Mobile para autenticar**. Se, no futuro, você não tiver mais acesso ao GitHub Mobile, ainda poderá usar chaves de segurança ou aplicativos TOTP para entrar.





Demo

Enterprise Managed Users (EMUs)

Quando você usa o Enterprise Managed Users todos os membros são provisionados e gerenciados por meio de seu **IdP**. Os usuários não criam suas próprias contas no GitHub. Você pode gerenciar a organização e a associação à equipe utilizando grupos no seu IdP.

Com EMUs, você gerencia o ciclo de vida e a autenticação de seus usuários no GitHub.com a partir de um sistema externo de gerenciamento de identidade, ou IdP. Isso permite a provisionamento de contas de usuário, controle sobre nomes de usuário, dados de perfil, associação a equipes e acesso a repositórios, além de atribuir funções e auditar ações de usuário dentro de sua empresa.

Provedor de Identidade (IdP): É um serviço que armazena e verifica a identidade digital dos usuários. Ex: Azure Entra ID, Facebook, Microsoft Account



Administração



Diferentes permissões de acesso

- Permissões de repositório (Repo)
- Permissões da equipe (Teams)
- Permissões da organização (Organization)
- Permissões da empresa (Enterprise)



Tipos de Repositórios

Public

Se sua conta não for uma conta de usuário gerenciada, você poderá criar repositórios públicos. Os repositórios públicos são acessíveis a todos na Internet.

Internal

Repositórios internos podem ser acessados por todos os integrantes da empresa, estando disponíveis apenas em contas enterprise.

Apenas contas Enterprise

Private

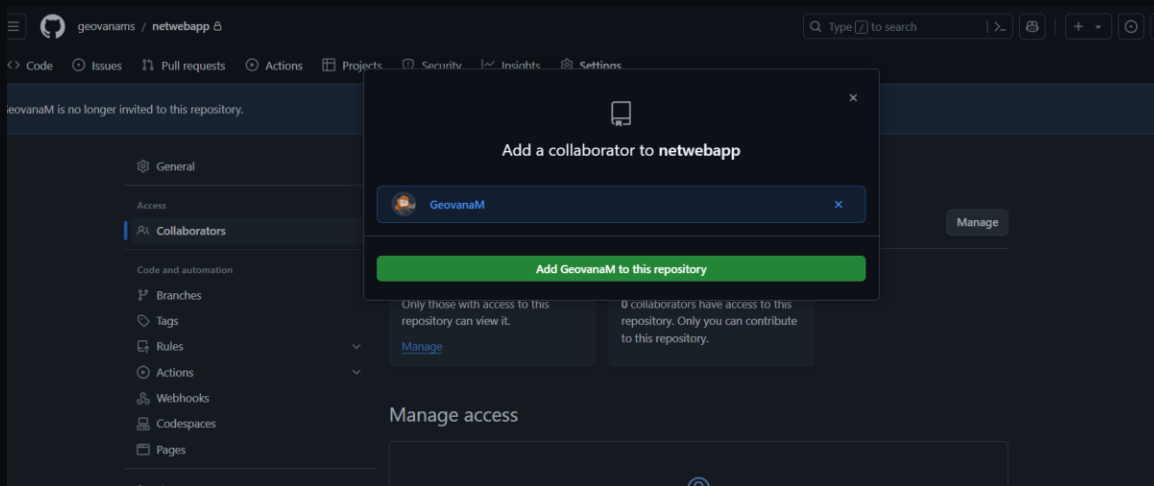
Os repositórios só podem ser acessados por você, pelas pessoas com as quais você compartilha explicitamente o acesso e, para repositórios da organização, por determinados integrantes da organização.



Repositório User Account

Um repositório pertencente a uma conta pessoal tem dois níveis de permissão:

- Owner
- Colaborador



Diferentes permissões de acesso

Permissões de Repositório

Read (Ler) - Recomendada para colaboradores sem código que desejam visualizar ou discutir seu projeto. Esse nível é bom para qualquer pessoa que precise visualizar o conteúdo do repositório, mas não precisa fazer contribuições ou alterações.

Triagem - Recomendado para colaboradores que precisam gerenciar proativamente problemas e pull requests sem acesso de gravação. Esse nível pode ser bom para alguns gerentes de projeto que gerenciam problemas de rastreamento, mas não fazem nenhuma alteração.

Write - Recomendado para colaboradores que fazem push ativamente em seu projeto. Escrever é a permissão padrão para a maioria dos desenvolvedores.

Maintain (Manter) - Recomendado para gerentes de projeto que precisam gerenciar o repositório sem acesso a ações confidenciais ou destrutivas.

Admin - Recomendado para pessoas que precisam de acesso total ao projeto, incluindo ações confidenciais e destrutivas, como gerenciar a segurança ou excluir um repositório. Essas pessoas são proprietários e administradores de repositórios.





General

Access

Collaborators and teams

Moderation options

Code and automation

Branches

Tags

Rules

Actions

Webhooks

Environments

Pages

Custom properties

Security

Code security

Deploy keys

Secrets and variables

Who has access

Add people to templatetotal



GeovanaM

Choose a role

**Read**

Recommended for non-code contributors who want to view or discuss your project.

**Triage**

Recommended for contributors who need to manage issues and pull requests without write access.

**Write**

Recommended for contributors who actively push to your project.

**Maintain**

Recommended for project managers who need to manage the repository without access to sensitive or destructive actions.

**Admin**

Recommended for people who need full access to the project, including sensitive and destructive actions like managing security or deleting a repository.

Cancel

Add GeovanaM

Manage

ORGANIZATION ACCESS

user and 1 team can access this repository through the organization.

[manage](#)

people

Add teams

All

Role: All

Security manager

All-repository triage



geovanams

Diferentes permissões de acesso

Permissões da Equipe

As equipes oferecem uma maneira fácil de atribuir permissões de repositório a vários usuários relacionados de uma só vez. Os membros de uma equipe secundária também herdam as configurações de permissão da equipe principal, o que proporciona uma maneira fácil de distribuir as permissões em cascata com base na estrutura natural de uma empresa.

Nível de permissão	Descrição
Membro	Os membros da equipe têm o mesmo conjunto de habilidades que os membros da organização
Mantenedor	Os mantenedores de equipe podem fazer tudo o que os membros da equipe podem, mais o seguinte: <ul style="list-style-type: none">– Alterar o nome, a descrição e a visibilidade da equipe– Solicitar que a equipe altere as equipes pai e filha– Definir a imagem de perfil da equipe– Editar e excluir as discussões da equipe– Adicionar e remover membros da organização da equipe– Promover os membros da equipe para que também tenham a permissão de mantenedores de equipe– Remover o acesso da equipe aos repositórios– Gerenciar a atribuição da revisão de código da equipe– Gerenciar lembretes agendados para solicitações de pull





eam1

out

is team has no description



© 2024 GitHub, Inc.

my personal information

Find a member...



1 member selected ▾

Change the team role of geovanams?



This action has no effect on Organization owners.

Select a new role:

☒ **Maintainer**

Can add and remove team members and create child teams.

☐ **Member**

Has no administrative permissions on the team.

Change role

Diferentes permissões de acesso

Permissões da Organização

Nível de permissão	Descrição
Proprietário	Os proprietários corporativos têm controle total sobre a empresa e podem executar todas as ações, incluindo: <ul style="list-style-type: none">– Gerenciamento de administradores– Adição/remoção de organizações a/de uma empresa– Gerenciamento de configurações da empresa– Importar políticas a todas as organizações– Gerenciamento de configurações de cobrança
Membro	Os membros da empresa têm o mesmo conjunto de habilidades que os membros da organização
Gerente de cobrança	Os gerentes de cobrança da empresa só podem ver e editar as informações de cobrança dela e adicionar ou remover outros gerentes de cobrança



Invite GeovanaM to geovanaorg

Give them an appropriate role in the organization and add them to some teams to give access to repositories.

Role in the organization

☒ **Member**

Members can see all other members, and can be granted access to repositories. They can also create new teams and repositories.

☐ **Owner**

Owners have full administrative rights to the organization and have complete access to all repositories and teams.

Teams — Optional

🔍 Find a team...

☐ **team1**

1 member 0 repositories

Send invitation



Contas Enterprise

Lembre-se de que contas corporativas são coleções de organizações. Por extensão, cada conta de usuário individual que é membro de uma organização também é membro da enterprise. Você pode controlar várias configurações relacionadas à autenticação a partir deste nível mais alto.

Existem três níveis de permissão no nível corporativo:

Permission level	Description
Owner	Os proprietários da empresa têm controle total sobre a empresa e podem tomar todas as medidas, incluindo: <ul style="list-style-type: none">- Gerenciar administradores.- Adicionar e remover organizações da empresa.- Gerenciar configurações da empresa.- Aplicar políticas em todas as organizações.- Gerenciar configurações de cobrança.
Member	Os membros da empresa têm o mesmo conjunto de habilidades que os membros da organização.
Billing manager	Os gerentes de cobrança empresarial só podem visualizar e editar as informações de cobrança da sua empresa e adicionar ou remover outros gerentes de cobrança.



Recursos de Segurança



prado-org / dotnetcore-webapp

Q Type to search

>_

+

> Code

Issues 11

Pull requests 9

Discussions

Actions

Projects

Wiki

Security 154

Insights

Settings

Overview

Reporting

Policy

Vulnerability alerts

Dependabot 3

Code scanning 138

Secret scanning 9

Default 9

Experimental 4

Security overview

Security policy • Enabled
View how to securely report security vulnerabilities for this repository
[View security policy](#)

Dependabot alerts • Enabled
Get notified when one of your dependencies has a vulnerability
[View Dependabot alerts](#)

Code scanning alerts • Enabled
Automatically detect common vulnerability and coding errors
[View alerts](#)

Secret scanning alerts • Enabled
Get notified when a secret is pushed to this repository
[View detected secrets](#)

?

Did you know? You can see a [security overview](#) for all repositories in the organization.

GitHub coleta algumas informações e disponibiliza por padrão, como gráfico de dependências, mas para receber alertas e obter outros recursos de segurança podemos configurar o GitHub Advanced Security.



GitHub Advanced Security

Code Scanning

Análise de
vulnerabilidade de
código

Dependabot

Detecta
vulnerabilidade em
suas dependências

Secret Scanning

Secret Scanning para
detectar secrets
expostas



Code Scanning

- Encontre vulnerabilidades antes que elas sejam incorporadas à base de código com varreduras automatizadas de CodeQL
- Integre os resultados diretamente no fluxo de trabalho do desenvolvedor
- Execute consultas personalizadas e o conjunto de consultas do GitHub com tecnologia da comunidade
- Extensível, com suporte para outras ferramentas SAST

The screenshot shows the GitHub Code Scanning interface for the repository `prado-org / dotnetcore-webapp`. The left sidebar contains navigation links: Overview, Reporting, Policy, Vulnerability alerts, Dependabot (3), Code scanning (138), Secret scanning, Default (9), and Experimental (4). The main panel is titled "Code scanning" and shows a status "All tools are working as expected". Below this, a search bar is set to "iscopen branch:main". A list of vulnerabilities is displayed, including:

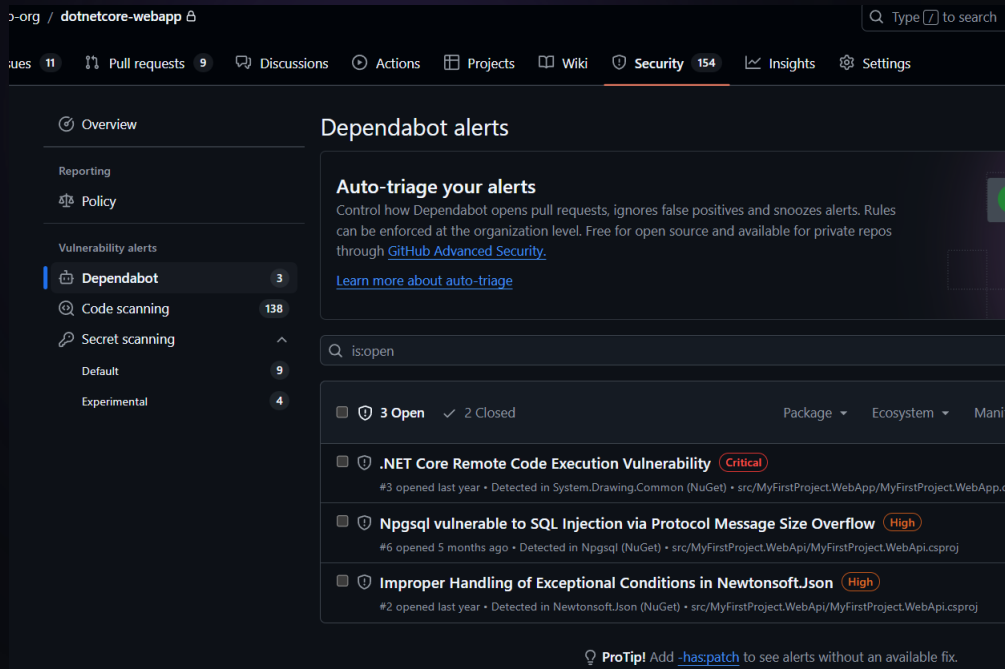
- dotnet: Remote Code Execution Vulnerability** (Critical) - #36 opened 3 months ago - Detected by Trivy in `app/MyfirstProject.WebApp.de...:42`
- zlib: integer overflow and resultant heap-based buffer overflow in zipOpenNewFileInZip4_6** (Critical) - #55 opened 3 months ago - Detected by Trivy in `myfirstproject.webapp :1`
- sqlite: heap out-of-bound read in function rtreeNode()** (Critical) - #43 opened 3 months ago - Detected by Trivy in `myfirstproject.webapp :1`
- perl: CPAN.pm does not verify TLS certificates when downloading distributions over HTTPS** (High) - #54 opened 3 months ago - Detected by Trivy in `myfirstproject.webapp :1`
- perl-CPAN: Bypass of verification of signatures in CHECKSUMS files** (High) - #53 opened 3 months ago - Detected by Trivy in `myfirstproject.webapp :1`
- e2fsprogs: out-of-bounds read/write via crafted filesystem** (High) - #52 opened 3 months ago - Detected by Trivy in `myfirstproject.webapp :1`
- zstd: mysql: buffer overrun in util.c** (High) - #51 opened 3 months ago - Detected by Trivy in `myfirstproject.webapp :1`



Dependabot

Atualizar automaticamente dependências vulneráveis e desatualizadas

- Pull requests automatizadas para atualizações de segurança e versão
- Mantenha seus projetos seguros e atualizados monitorando-os para componentes vulneráveis e desatualizados. Se uma atualização sugerida for encontrada, abriremos automaticamente uma solicitação de pull com correções sugeridas.
- Integrado com o fluxo de trabalho do desenvolvedor
- O Dependabot é integrado diretamente ao fluxo de trabalho do desenvolvedor para uma experiência sem atrito e correções mais rápidas.
- Dados ricos sobre vulnerabilidades
- O GitHub rastreia vulnerabilidades em pacotes de gerenciadores de pacotes suportados usando dados de pesquisadores de segurança, mantenedores e do National Vulnerability Database, todos detectáveis no GitHub Advisory Database.



The screenshot displays the GitHub web interface for the repository `dotnetcore-webapp`. The top navigation bar includes links for Issues (11), Pull requests (9), Discussions, Actions, Projects, Wiki, Security (154), Insights, and Settings. The left sidebar shows the repository's structure with sections for Overview, Reporting, Policy, Vulnerability alerts, and Dependabot (3 alerts). The main content area is titled "Dependabot alerts" and features a section for "Auto-triage your alerts" with instructions on how to control alert behavior. Below this, a list of open alerts is shown, including a critical vulnerability in .NET Core Remote Code Execution and two high-severity issues related to Npgsql and Newtonsoft.Json. A footer note suggests adding `-has:patch` to filter alerts with available fixes.

dotnetcore-webapp

Issues 11 Pull requests 9 Discussions Actions Projects Wiki Security 154 Insights Settings

Overview

Reporting

Policy

Vulnerability alerts

Dependabot 3

Code scanning 138

Secret scanning

Default 9

Experimental 4

Dependabot alerts

Auto-triage your alerts

Control how Dependabot opens pull requests, ignores false positives and snoozes alerts. Rules can be enforced at the organization level. Free for open source and available for private repos through [GitHub Advanced Security](#).

[Learn more about auto-triage](#)

is:open

3 Open 2 Closed Package Ecosystem Mani

- .NET Core Remote Code Execution Vulnerability** Critical
#3 opened last year • Detected in System.Drawing.Common (NuGet) • src/MyFirstProject.WebApp/MyFirstProject.WebApp.csproj
- Npgsql vulnerable to SQL Injection via Protocol Message Size Overflow** High
#6 opened 5 months ago • Detected in Npgsql (NuGet) • src/MyFirstProject.WebApi/MyFirstProject.WebApi.csproj
- Improper Handling of Exceptional Conditions in Newtonsoft.Json** High
#2 opened last year • Detected in Newtonsoft.Json (NuGet) • src/MyFirstProject.WebApi/MyFirstProject.WebApi.csproj

ProTip! Add `-has:patch` to see alerts without an available fix.



Secret scanning

Encontre e gerencie segredos codificados

- Identifica segredos o mais cedo possível
- Encontra segredos (incluindo segredos do Azure) no momento em que são enviados ao GitHub e notifica imediatamente os desenvolvedores quando são encontrados.
- Comunidade de parceiros secretos de digitalização
- Para cada commit feito no seu repositório e seu histórico completo no git, procuraremos formatos secretos de parceiros de varredura secreta.
- Define custom patterns
- Definir padrões personalizados
- Suporta repositórios públicos e privados
- A varredura secreta monitora repositórios públicos e privados em busca de possíveis vulnerabilidades secretas.

The screenshot shows the GitHub interface for repository 'anams / GHASbra'. The top navigation bar includes links for Issues, Pull requests (5), Actions, Projects, Wiki, Security (9), Insights, and Settings. The left sidebar shows the 'Secret scanning' section with a list of items: Overview, Reporting, Policy, Advisories, Vulnerability alerts, Dependabot (6), Code scanning (2), and Secret scanning (2). The main content area is titled 'Secret scanning alerts' and features a search bar with the text 'is:open'. Below the search bar, there are two alert cards. The first card shows '2 Open' alerts and '0 Closed' alerts. The second card shows a 'GitHub Personal Access Token' alert, detected in the file 'albums-api/Controllers/AlbumController.cs:16'. The alert text is: '#2 opened 7 seconds ago • Detected secret in albums-api/Controllers/AlbumController.cs:16'. The third card shows another 'GitHub Personal Access Token' alert, detected in the file 'albums-api/Controllers/AlbumController.cs:15'. The alert text is: '#1 opened 30 minutes ago • Detected secret in albums-api/Controllers/AlbumController.cs:15'.





Demo

Insights



Pulse

Contributors

Community

Traffic

Commits

Code frequency

Dependency graph

Network

Forks

Actions Usage Metrics

Actions Performance Metrics

April 26, 2025 – May 3, 2025

Period: 1 week

Overview

0 Active pull requests

0 Active issues

0

Merged pull requests

0

Open pull requests

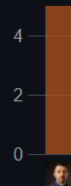
0

Closed issues

0

New issues

Excluding merges, **1 author** has pushed **5 commits** to main and **5 commits** to all branches. On main, **5 files** have changed and there have been **253 additions** and **252 deletions**.





Demo



Hora de praticar!

Atividade Módulo 6

