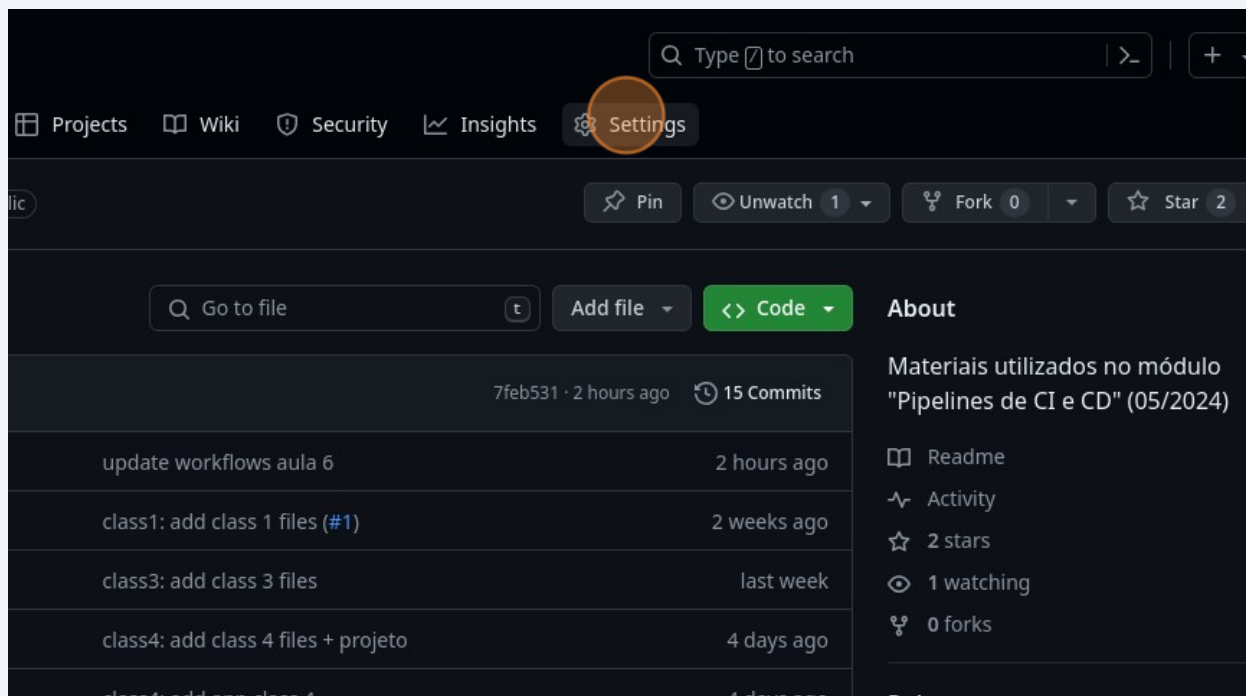


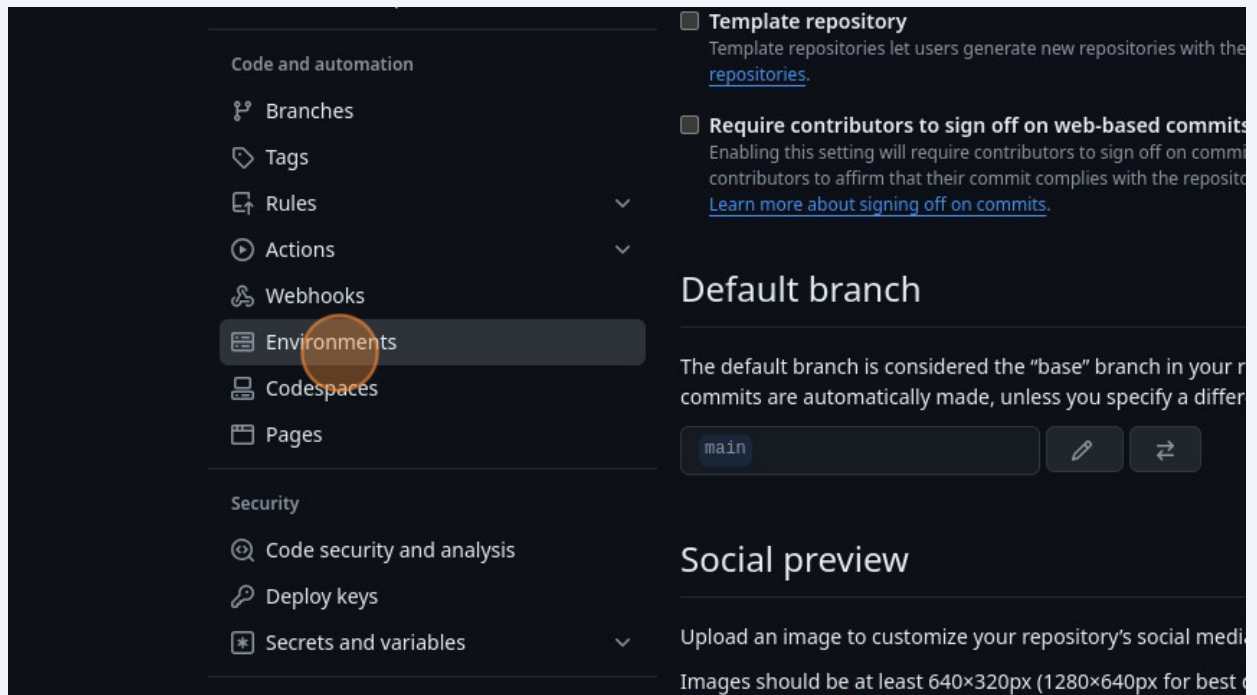
# Set Up Environment with Required Reviewers and Deployment Rules

1 Navigate to <https://github.com/<seu-usuario>/<seu-repositorio>>

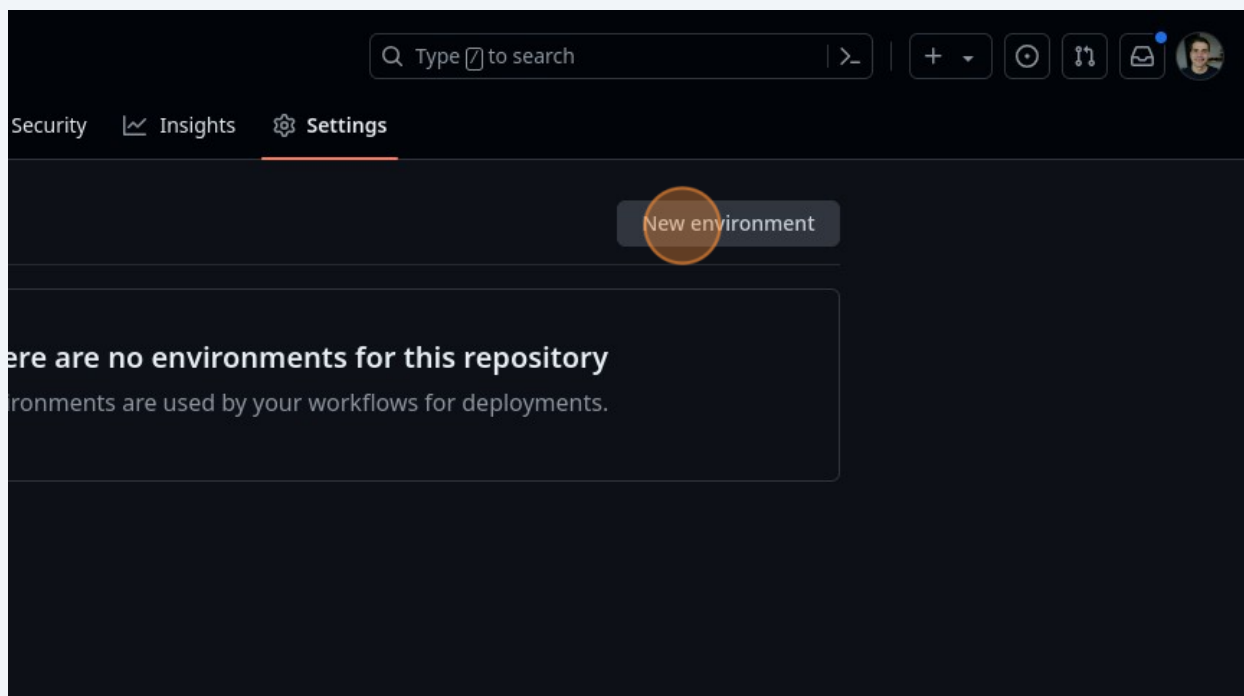
2 Click "Settings"



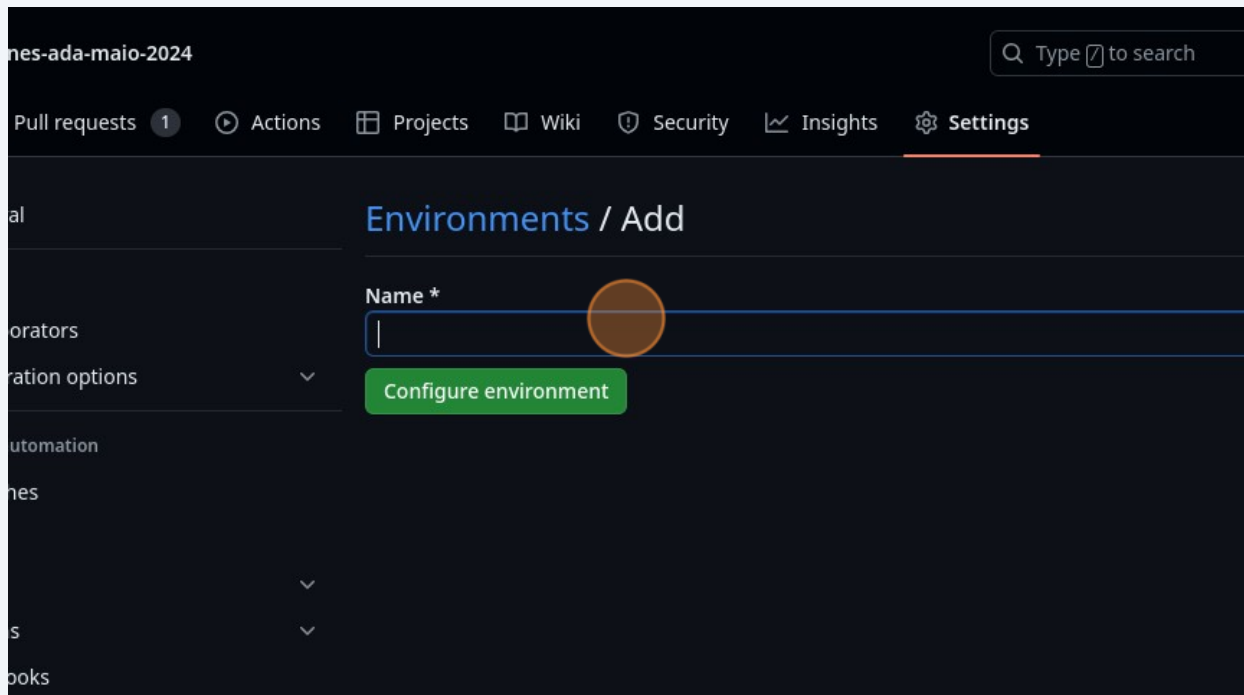
### 3 Click "Environments"



### 4 Click "New environment"

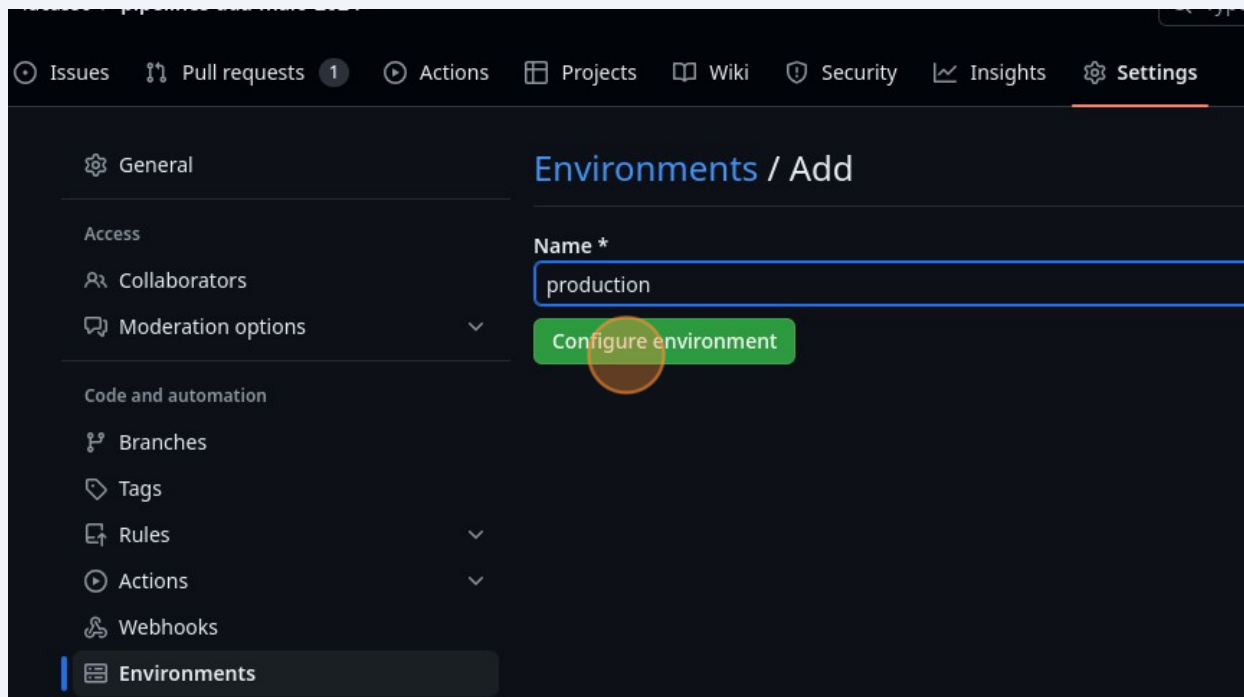


5 Click the "Name" field.

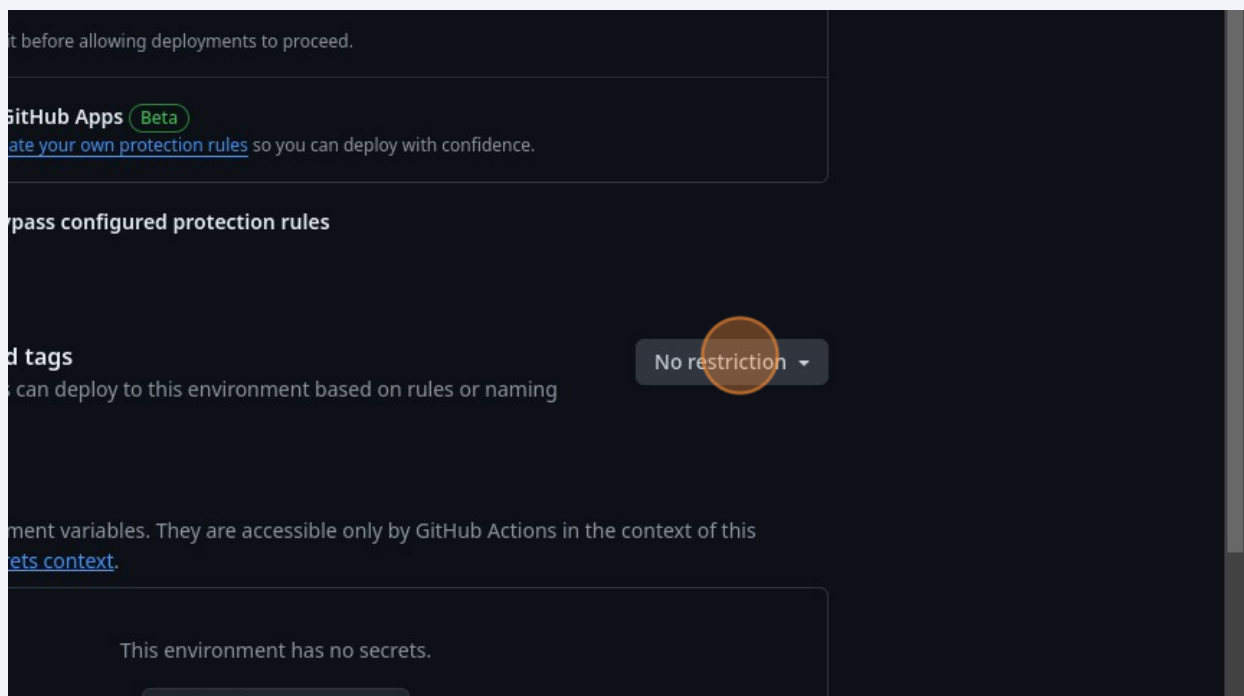


6 Type "production"

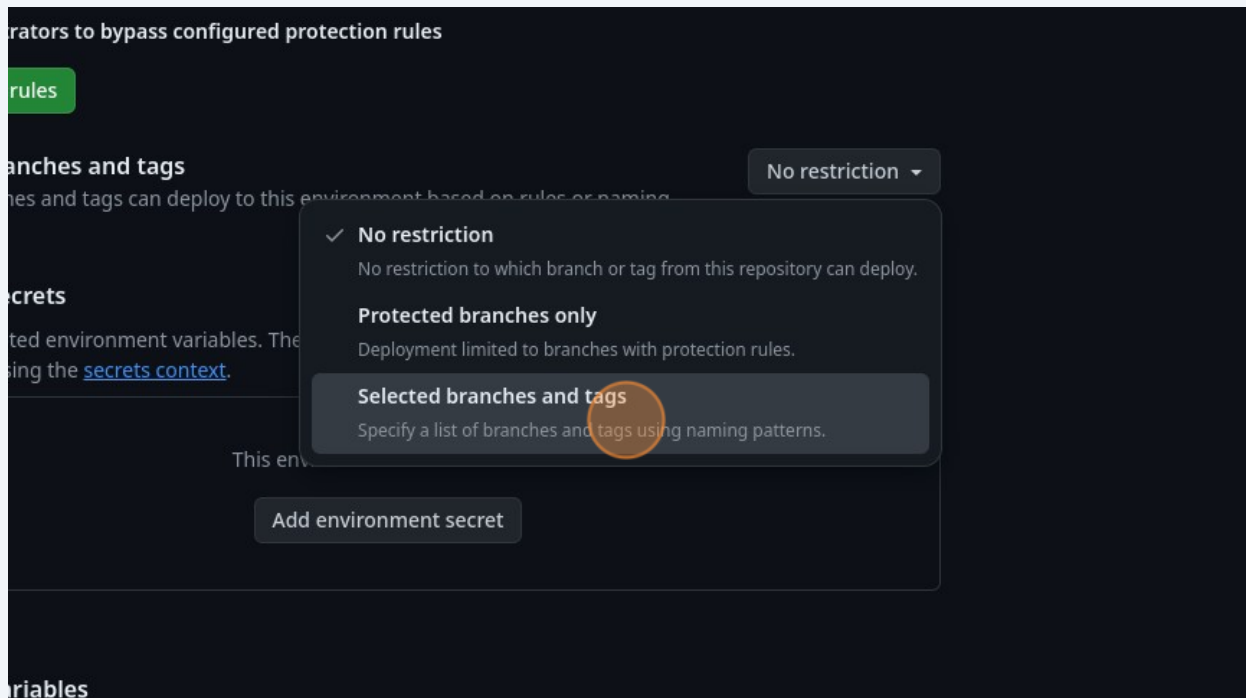
7 Click "Configure environment"



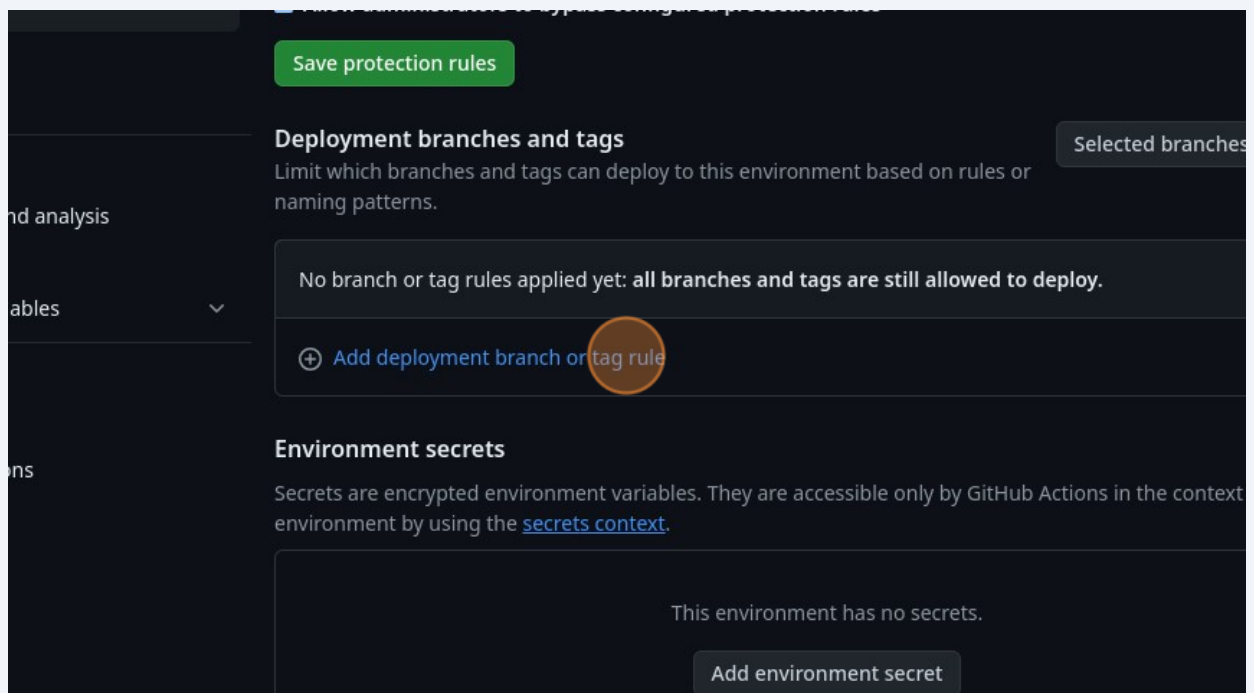
8 Click "No restriction"



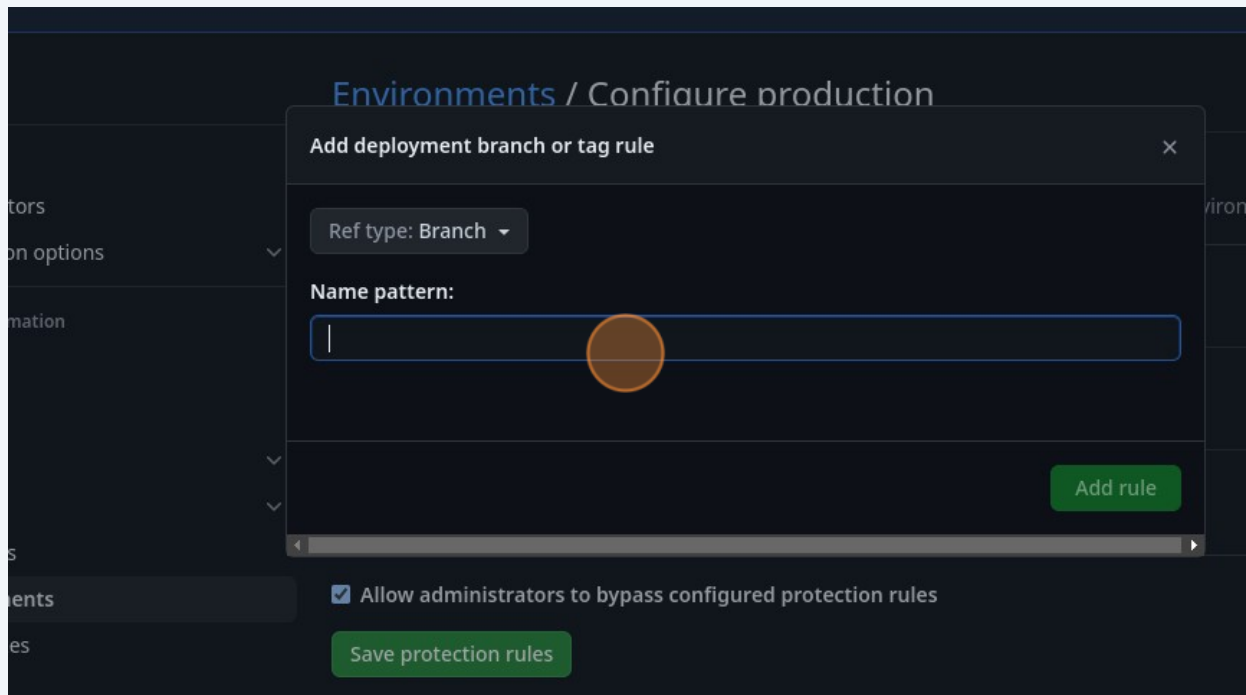
9 Click "Specify a list of branches and tags using naming patterns."



10 Click "Add deployment branch or tag rule"

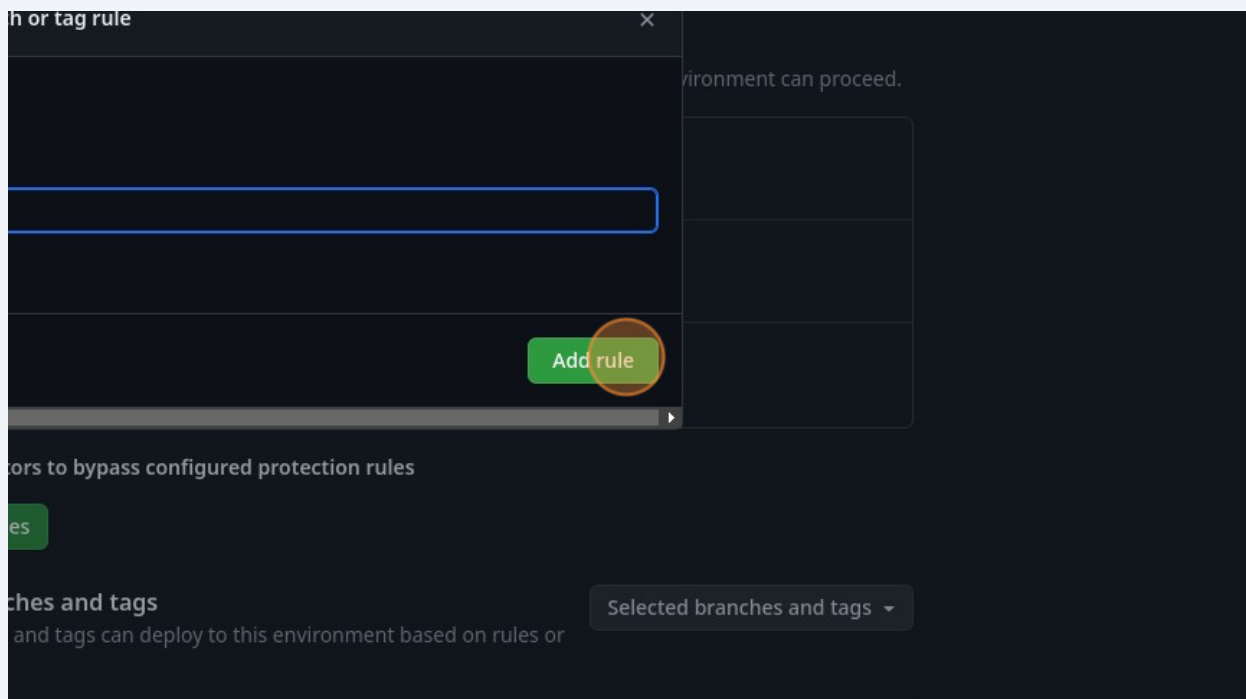


- 11 Click the "Name pattern:" field.

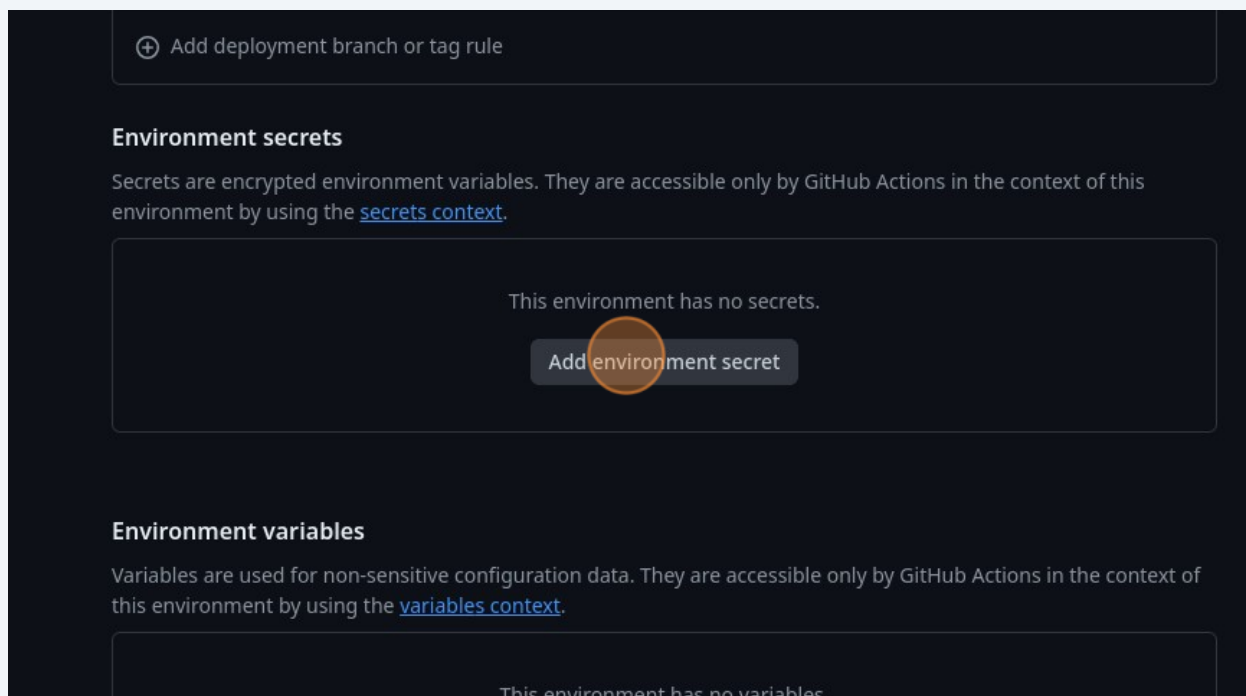


- 12 Type "main"

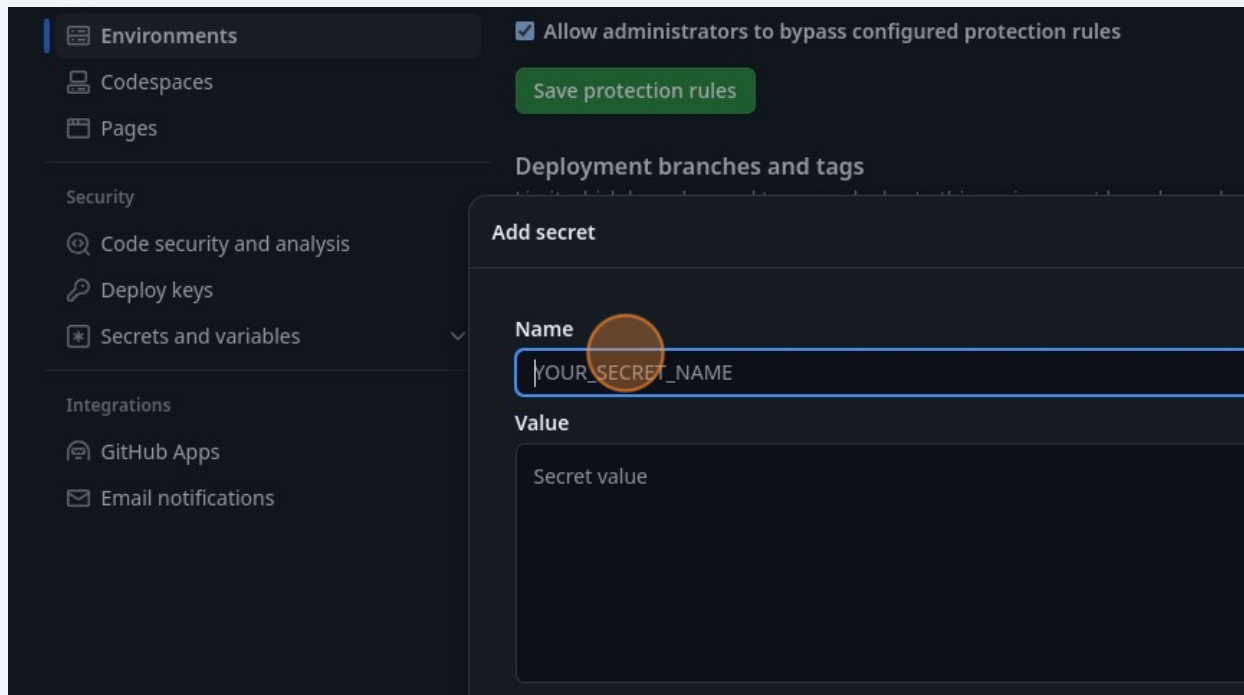
### 13 Click "Add rule"



### 14 Click "Add environment secret"



15 Click the "Name" field.

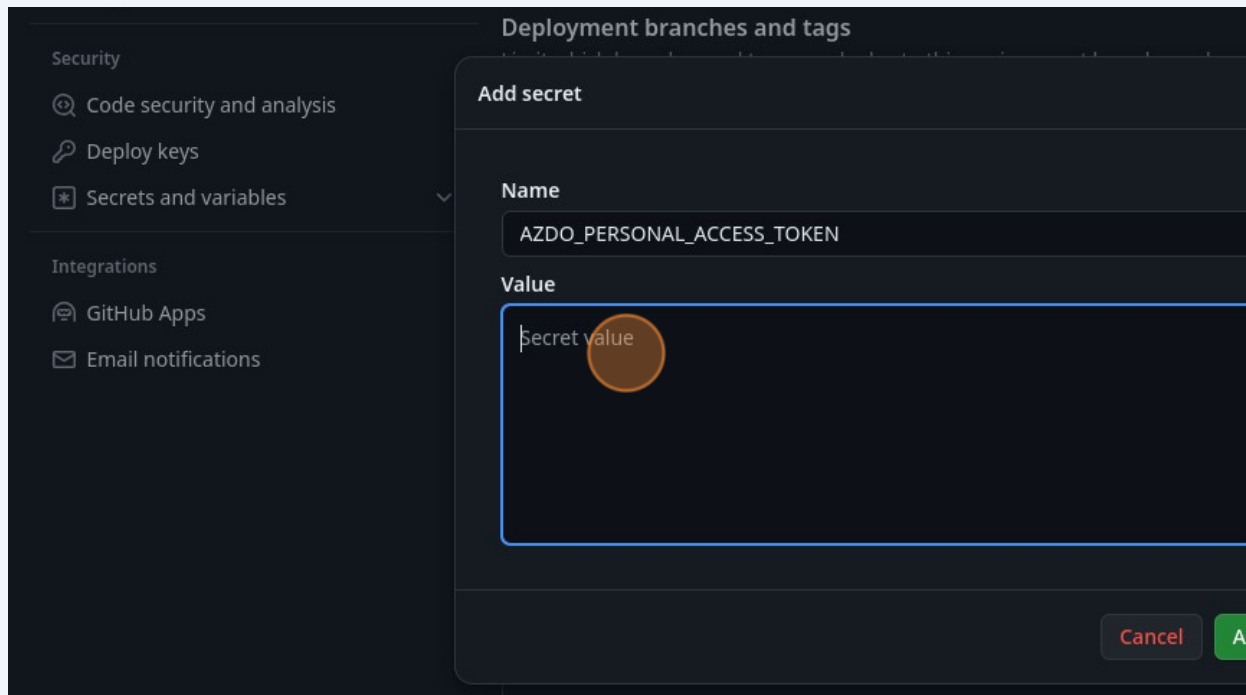


The screenshot shows the GitHub 'Add secret' dialog. On the left is a sidebar with navigation options: Environments, Codespaces, Pages, Security (with sub-items: Code security and analysis, Deploy keys, Secrets and variables), and Integrations (with sub-items: GitHub Apps, Email notifications). The 'Secrets and variables' option is expanded. The main area has a checkbox 'Allow administrators to bypass configured protection rules' which is checked, and a green 'Save protection rules' button. Below this is the 'Deployment branches and tags' section. The 'Add secret' dialog is open, showing a 'Name' field with the placeholder text 'YOUR\_SECRET\_NAME' and a 'Value' field with the placeholder text 'Secret value'. An orange circle highlights the 'Name' field.

16 Type "AZDO\_PERSONAL\_ACCESS\_TOKEN"

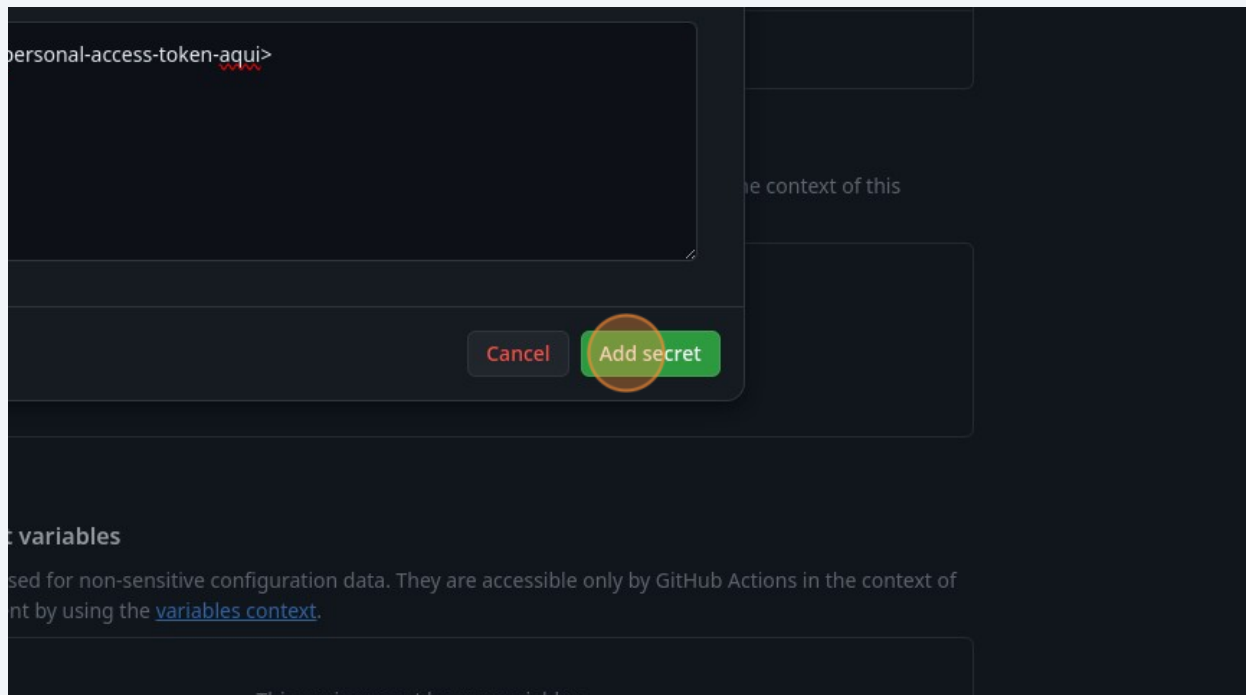


**17** Click the "Value" field.

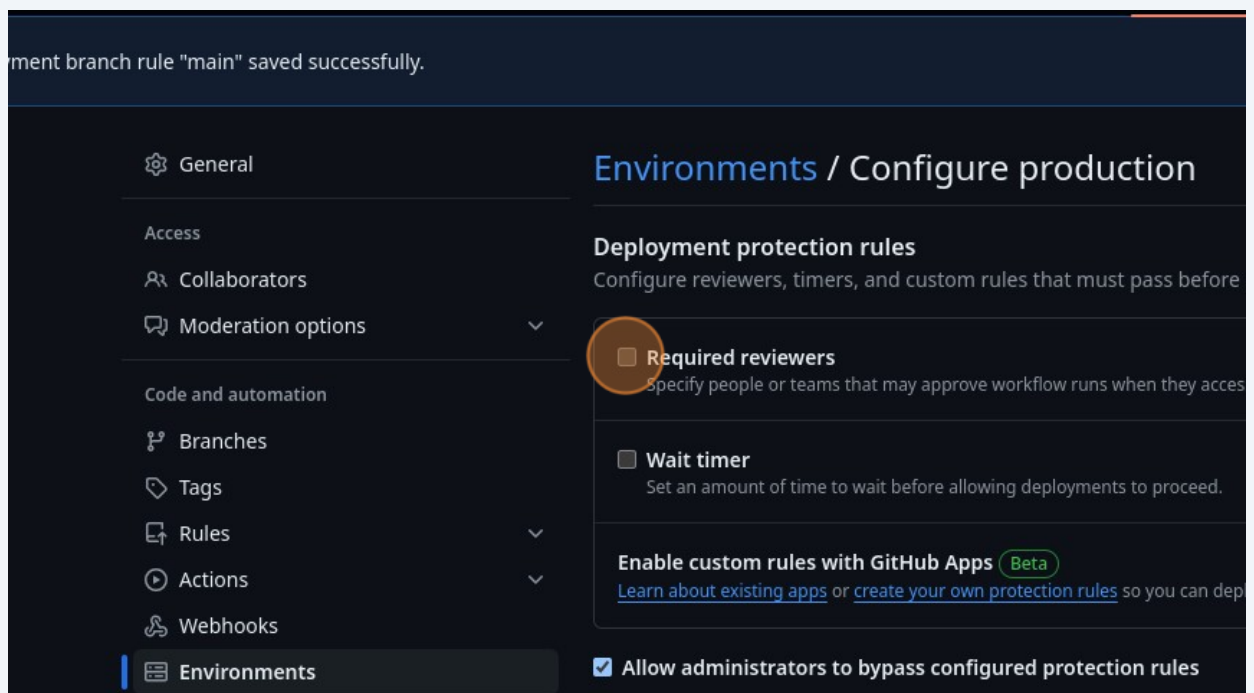


**18** Type "<cole-o-seu-personal-access-token-aqui>"

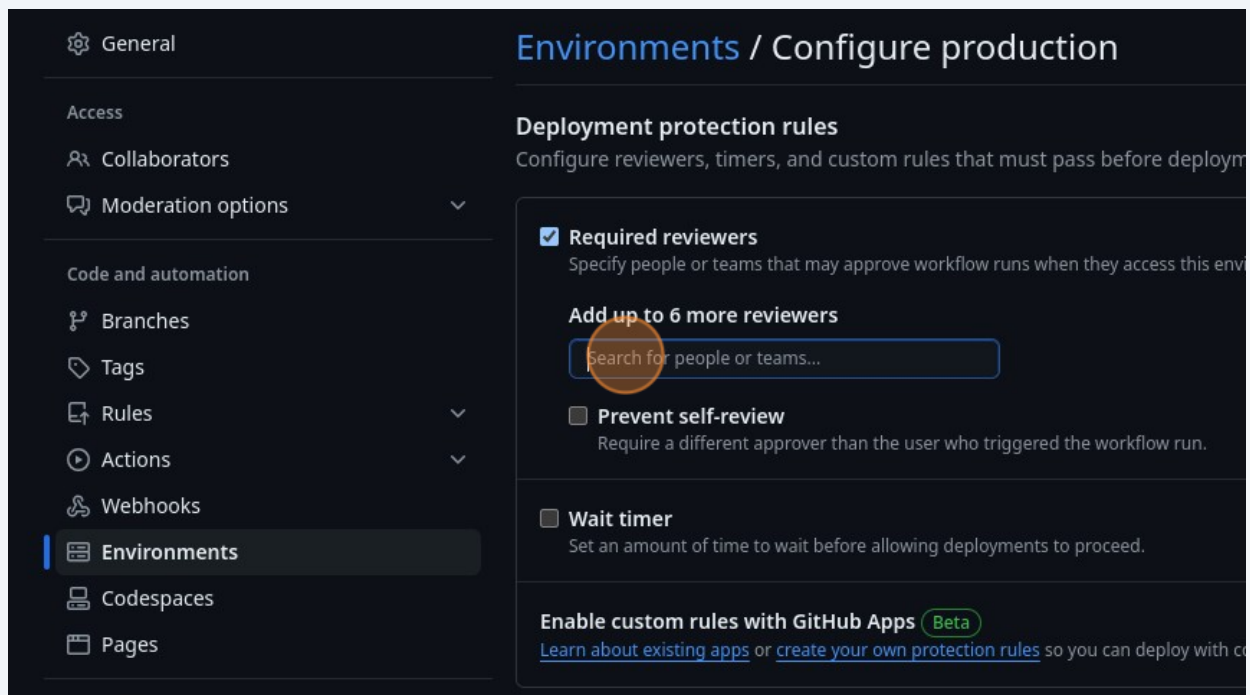
## 19 Click "Add secret"



## 20 Click the "Required reviewers" field.

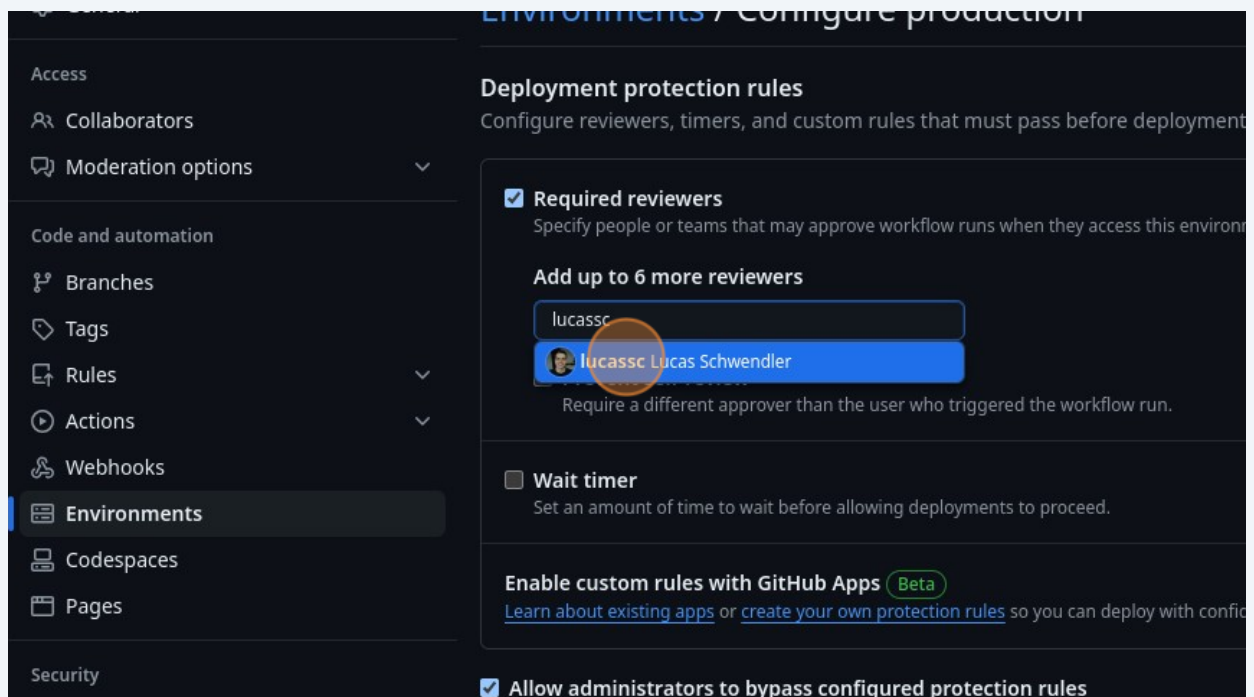


- 21 Click the "Add up to 6 more reviewers" field.



- 22 Type "<seu-usuario>"

## 23 Click "<seu-usuario>"



## 24 Click "Save protection rules"

