GitLab Security Scanning & Management

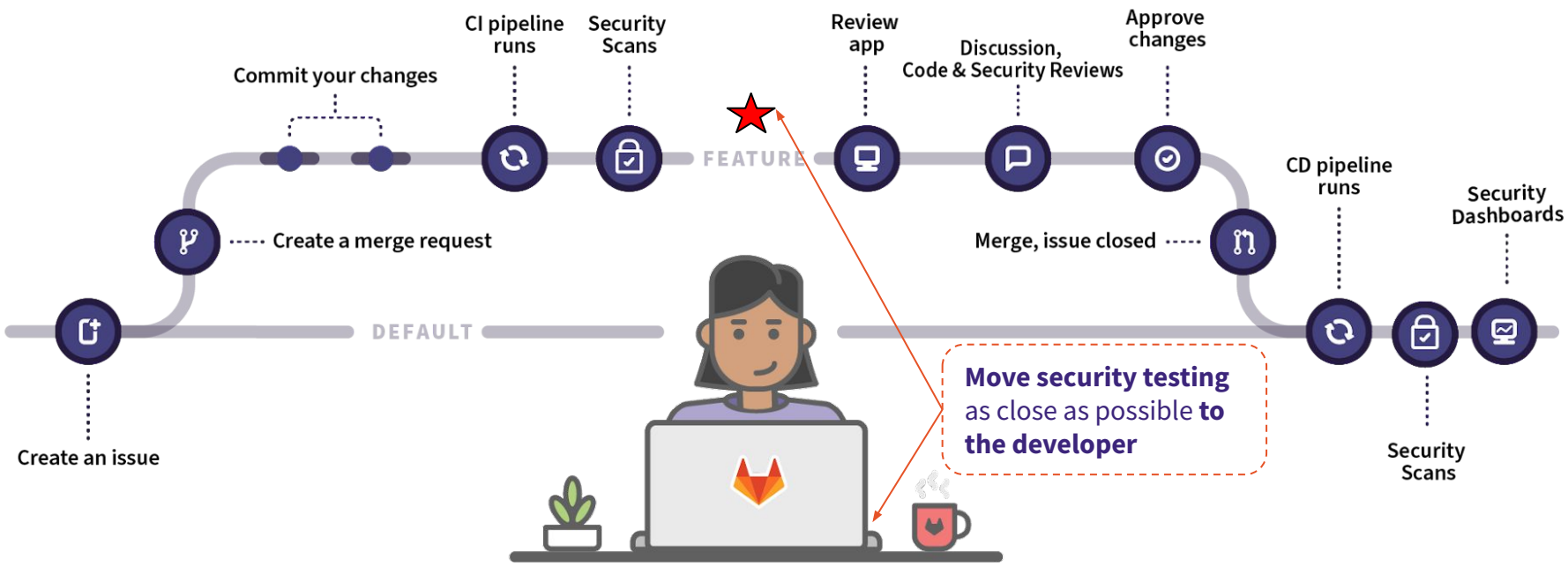
TAM Name, Technical Account Manager
tam@gitlab.com
202x-xx-xx

Agenda

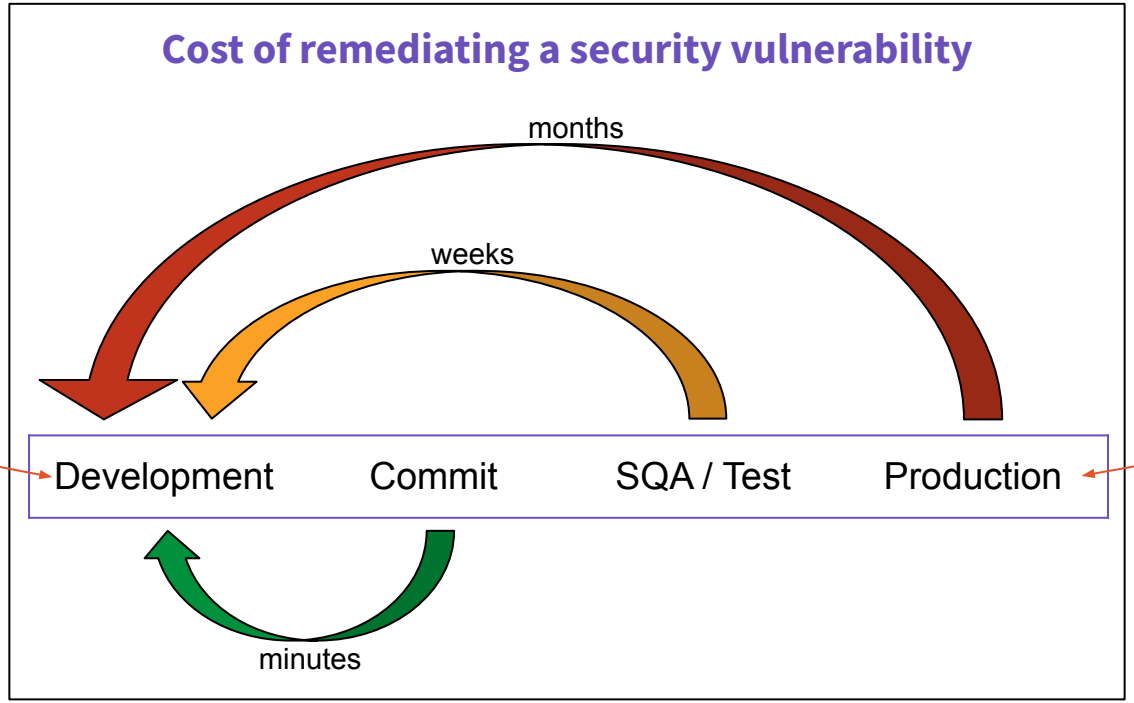
- GitLab as a DevSecOps tool
- What GitLab Offers
  - Available Scanners
  - Dashboard & Vulnerability Management
- Developer Workflow
- Security Workflow
- Q&A

GitLab as a DevSecOps tool

GitLab seamlessly tests for vulnerabilities within the DevOps workflow



Increasing efficiency for both development and security



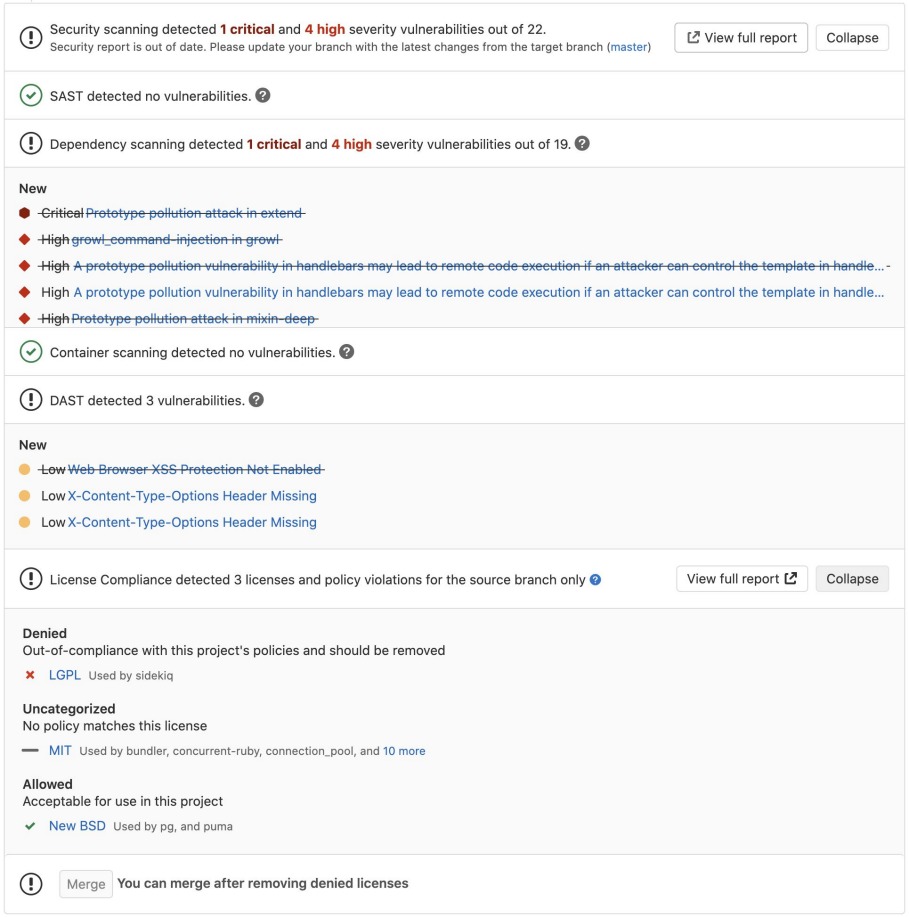
Developers have **no context switching**, receive **immediate feedback**, can be **fix vulnerabilities early** in the SDLC.

Security team has **less vulnerabilities** to assess, manage, and triage **within the apps** deployed **within production**.

DevSecOps in GitLab

- Built into the pipeline & MR
- Robust scanning capabilities:
  - SAST
  - DAST
  - Dependency
  - Secrets Detection
  - Fuzz Testing
  - Container
  - License Compliance
- Pipeline, Project, & Group Security Dashboards
- Vulnerability Management

https://about.gitlab.com/stages-devops-lifecycle/secure/



Available Security Scanners

GitLab Security and Compliance Scanners

SAST	Static Application Security Testing: Detects vulnerabilities in source code. (e.g. SQL Injection, XXS)
Dependency Scanning	Detects **known** vulnerabilities in libraries/components (e.g. CVE 2021-45046 in Apache log4j)
Secret Detection	Detects credentials/secrets/passwords in source code to prevent sensitive information leakage. (e.g. AWS Key)
License Compliance	Searches for approved and disallowed licenses defined by custom policies. (e.g. AGPL License)
Container Scanning	Detects **known** vulnerabilities in container images (e.g. Heartbleed, ShellShock)

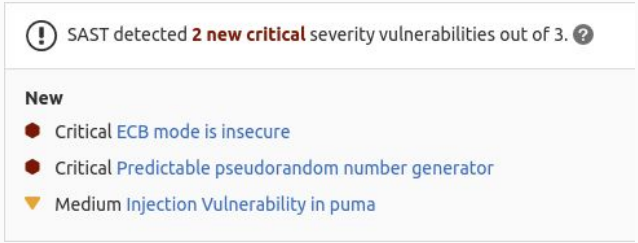
Infrastructure as Code (IaC) Scanning	Scans IaC configuration files (Terraform, Ansible, CloudFormation, Kubernetes) for known vulnerabilities
Coverage Guided Fuzz	Detects unexpected behaviors at program method level by passing arguments as white-box testing. (e.g. ArrayIndexOutOfBoundsException for Java, Heap-Buffer-Overflow for C++)
DAST	Dynamic Application Security Testing: Analyzes your running web application for runtime vulnerabilities leveraging the Review App. (e.g. CSRF, XXS)
Web API Fuzz	Detects unexpected behaviors of running Web applications by generating random requests to the Web APIs. (e.g. 500 INTERNAL SERVER ERROR)

Static Scan **Runtime Scan** **Dynamic Scan**

Static Application Security Testing (SAST)

Language/Framework	Scan Tool
.NET Core, .NET Framework	Security Code Scan
Apex (Salesforce)	PMD
C/C++	Flawfinder
Elixir (Phoenix)	Sobelow
Go	Gosec, Semgrep
Groovy, Java, Scala, & Kotlin (Ant, Gradle, Maven, & SBT)	SpotBugs with the find-sec-bugs plugin
Java (Android), Kotlin (Android), Objective-C (iOS), & Swift (iOS)	MobST (beta)
Helm Charts	Kubesec
JavaScript	ESLint security plugin, Semgrep
Kubernetes Manifests	Kubesec
Node.js	NodeJsScan
PHP	phpcs-security-audit
Python (pip)	bandit
Python	Semgrep
React	ESLint react plugin, Semgrep
Ruby, Ruby on Rails	brakeman
Typescript	ESLint security plugin, Semgrep

- Analyzes source code for known vulnerabilities
- Checks the SAST report and compares the found vulnerabilities between the source and target branches
- Vulnerabilities shown in-line in merge request, sorted by severity



https://docs.gitlab.com/ee/user/application_security/sast/

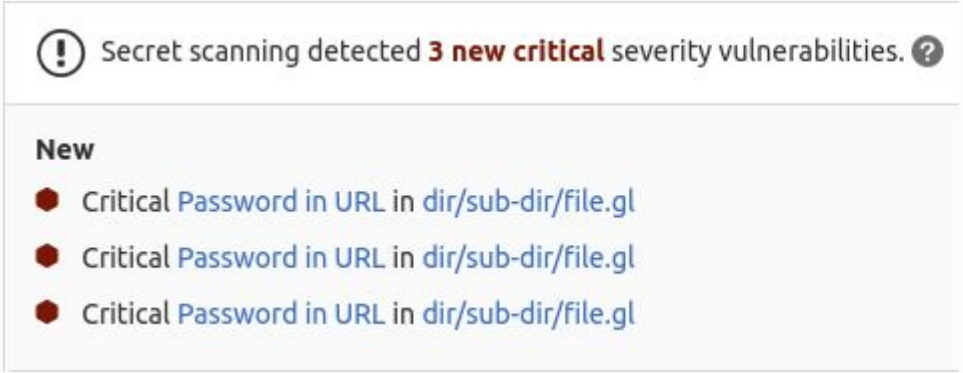
Dynamic Application Security Testing (DAST)

- Analyzes running web application for known runtime vulnerabilities
- Runs passive (ZAP Baseline Scan) and active scans (live attacks against a Review App*)
- Uses open source tool **OWASP ZAProxy**, modified to add authentication capabilities
- Vulnerabilities shown in-line in merge request, sorted by severity

**Dynamically deployed application instances per merge request*

https://docs.gitlab.com/ee/user/application_security/dast/

Secrets Detection



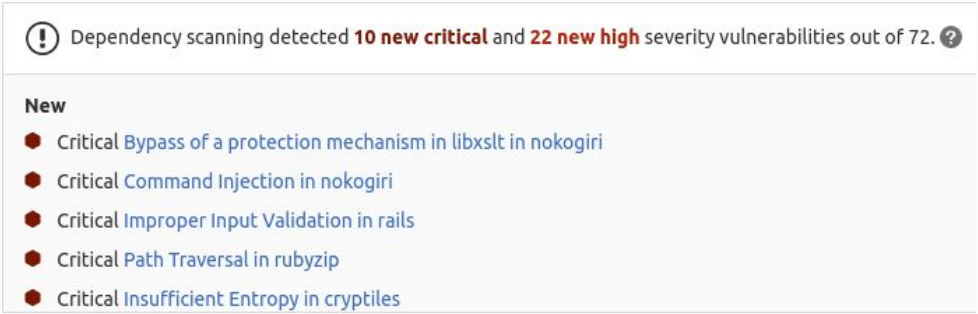

```
[secrets]
  description = 'secrets custom rules configuration'

  [[secrets.passthrough]]
    type  = "raw"
    target = "gitleaks.toml"
    value = """\
title = "gitleaks config"
# add regexes to the regex table
[[rules]]
description = "Test for Raw Custom Rulesets"
regex = '''Custom Raw Ruleset T[est]{3}'''
"""
```

- Scans the contents of a repository to find API keys & other unintended sensitive information
  - Unintentional commit of *secrets* like keys, passwords, and API tokens
- Performs a single or recurring scan of the full history of a repository for secrets
- Includes Gitleaks and TruffleHog checks
- Detects a variety of common secrets by default, but patterns can be customized using rulesets
- Results presented in:
  - Merge Request widget
  - Security Dashboard
  - Pipelines' Security tab

https://docs.gitlab.com/ee/user/application_security/secret_detection/

Dependency Scanning

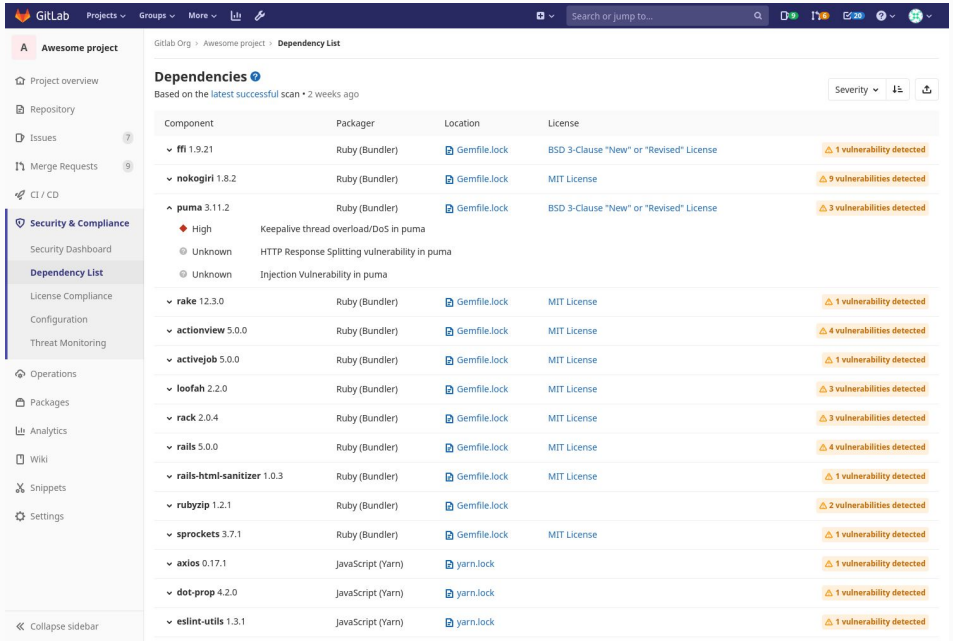
Language (package managers)	Scan Tool
C, C++ (Conan)	gemnasium
C#, .NET (NuGet 4.9+)	gemnasium
Go (Golang)	gemnasium
Java (Gradle, Maven)	gemnasium
JavaScript (npm, yarn 1.x)	gemnasium, Retire.js
PHP (Composer)	gemnasium
Python (setuptools, pip, Pipenv)	gemnasium
Ruby (Bundler)	gemnasium, bundler-audit
Scala (sbt)	gemnasium



- Analyzes external dependencies for known vulnerabilities
- Checks the dependency scanning report and compares the found vulnerabilities between the source and target branches
- Suggested solutions automate remediation
- Uses GitLab Gemnasium technology
- Vulnerabilities shown in-line in merge request, sorted by severity

https://docs.gitlab.com/ee/user/application_security/dependency_scanning/

Dependency List



- The Dependency List provides visibility into a project's dependencies
- This includes key details for each, including their known vulnerabilities
  - Component
  - Packager
  - Location
  - License
- This information is also referred to as a *Software Bill of Materials* or SBoM / BOM
- Uses GitLab Gemnasium technology

https://docs.gitlab.com/ee/user/application_security/dependency_list/

Container Scanning

- Static analysis on Docker images for vulnerabilities in the application environment
- Checks the Container Scanning report, compares vulnerabilities between source and target branch
- Vulnerabilities shown in-line in merge request
- Uses open source tools **Trivy** and **Grype**, able to scan any type of Docker image
- Results available as a single report

https://docs.gitlab.com/ee/user/application_security/container_scanning/

License Compliance

Language	Package Managers	Scan Tool
JavaScript	Bower, npm, yarn (experimental support)	License Finder
Go	Godep, go mod	License Finder
Java	Gradle, Maven	License Finder
.NET	Nuget	License Finder
Python	pip	License Finder
Ruby	gem	License Finder

- Searches project dependencies for respective licenses
- Checks License Compliance report to compare licenses between source and target branch
- Displays information in merge request
- Denied and new Licenses are clearly marked
- Manually allow or deny Licenses in Project Settings
- Additional languages and package managers are supported experimentally
- Results available as a single report

https://docs.gitlab.com/ee/user/application_security/license_management/

Fuzz Testing

Language	Fuzzing Engine	Example
C/C++	libFuzzer	c-cpp-example
GoLang	go-fuzz (libFuzzer support)	go-fuzzing-example
Swift	libFuzzer	swift-fuzzing-example
Rust	cargo-fuzz (libFuzzer support)	rust-fuzzing-example
Java	Javafuzz (recommended), JQF (not preferred)	javafuzz-fuzzing-example, jqf-fuzzing-example
JavaScript	jsfuzz	jsfuzz-fuzzing-example
Python	pythonfuzz	pythonfuzz-fuzzing-example
AFL (any language that works on top of AFL)	AFL	afl-fuzzing-example

- Discovers bugs and potential security issues that other QA processes may miss
- **Coverage Guided Fuzz Testing** sends random inputs to an instrumented version of your application in an effort to cause unexpected behavior, such as a crash, which indicates a bug that you should address
- **API Fuzz Testing** performs fuzz testing of API operation parameters by setting operation parameters to unexpected values to cause unexpected behavior and errors in API backend

https://docs.gitlab.com/ee/user/application_security/coverage_fuzzing/
https://docs.gitlab.com/ee/user/application_security/api_fuzzing/

Infrastructure as Code Scanning

Query ↑↓	Severity ↑↓	Category ↑↓	Description	Help
ECS Service Admin Role is Present 3206240f-2e87-4e58-8d24-3e19e7c83d7c	High	Access Control	ECS Services must not have Admin roles, which means the attribute 'iam_role' must not be an admin role	Documentat
EFS With Vulnerable Policy fae52418-bb8b-4ac2-b287-0b9082d6a3fd	High	Access Control	EFS (Elastic File System) policy should avoid wildcard in 'Action' and 'Principal'.	Documentat
S3 Bucket Allows WriteACP Action From All Principals 64a222aa-7793-4e40-915f-4b302c76e4d4	High	Access Control	S3 Buckets must not allow Write_ACP Action From All Principals, as to prevent leaking private information to the entire internet or allow unauthorized data tampering / deletion. This means the 'Effect' must not be 'Allow' when the 'Action' is Write_ACP, for all Principals.	Documentat

- Covers Kubernetes, CloudFormation, Ansible, and Terraform
- Scanners will catch:
  - Syntax errors
  - Access control
  - Access control
  - Encryption
  - Insecure configurations
  - Networking and firewall
  - Best practices and more
- Uses open source scanner **Kics**

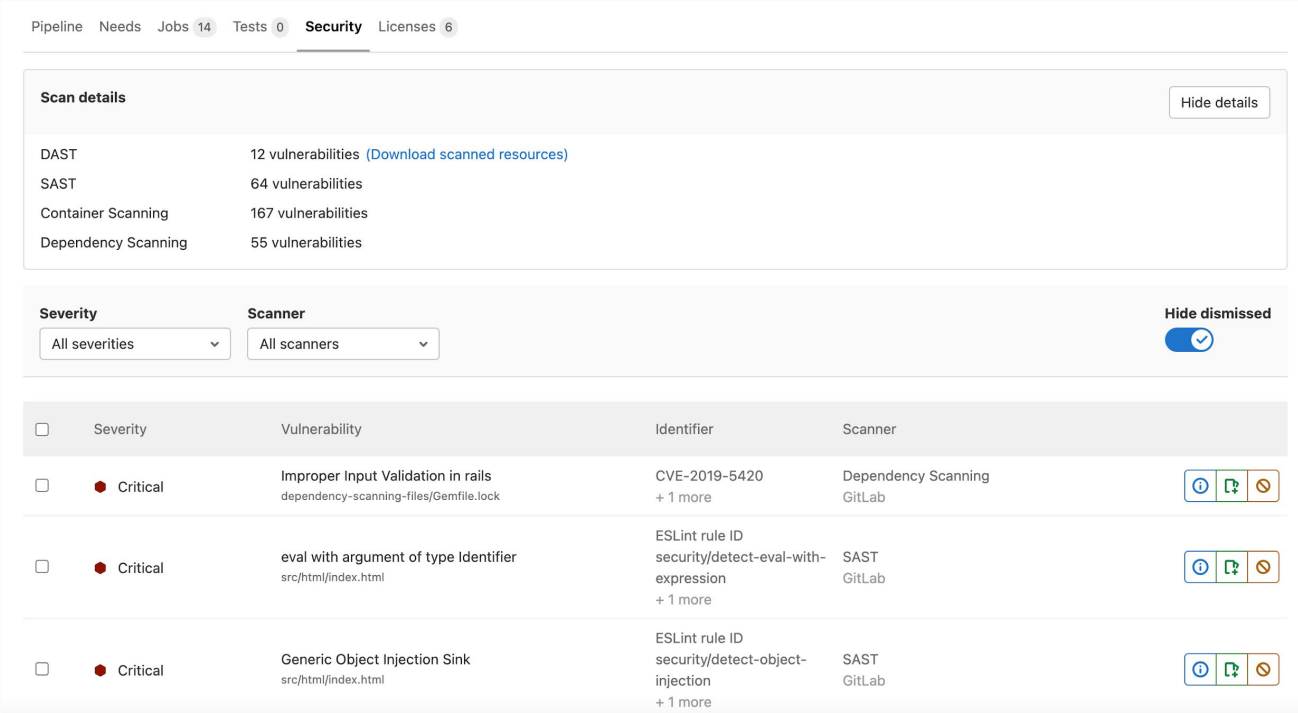
https://docs.gitlab.com/ee/user/application_security/iac_scanning/

GitLab Security Dashboard & Vulnerability Management

Security Dashboards

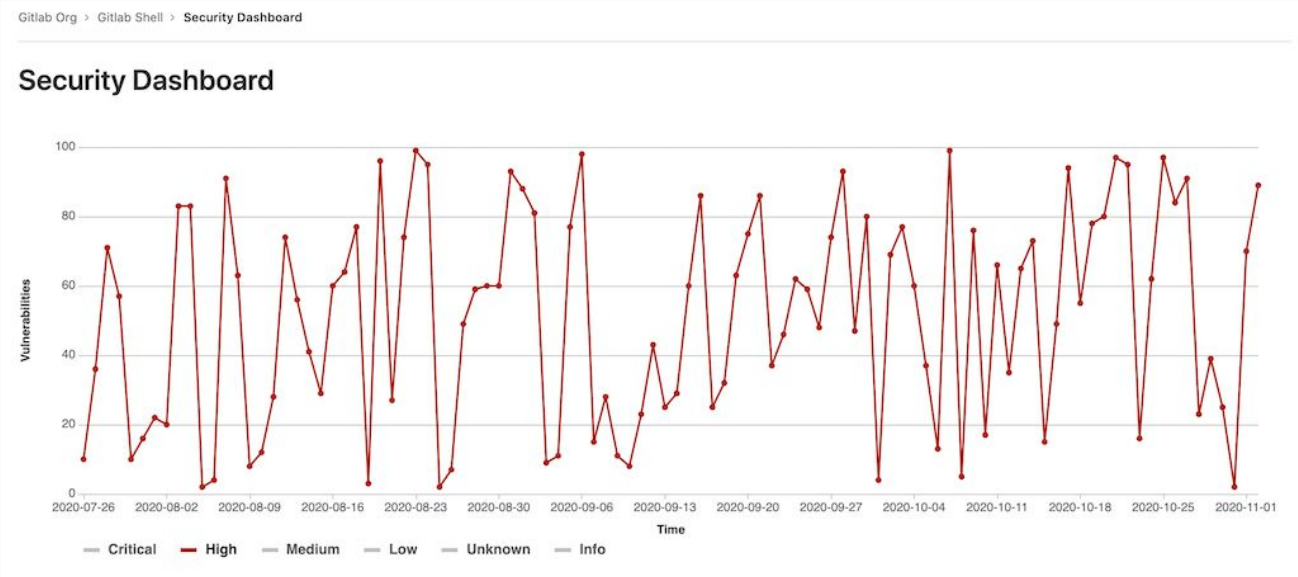
- Security dashboards & reports can be found in:
  - Pipelines ➡️
  - Projects
  - Groups
  - Instance
- Tip: Schedule regular pipelines to ensure updated information

https://docs.gitlab.com/ee/user/application_security/security_dashboard/



Security Dashboards

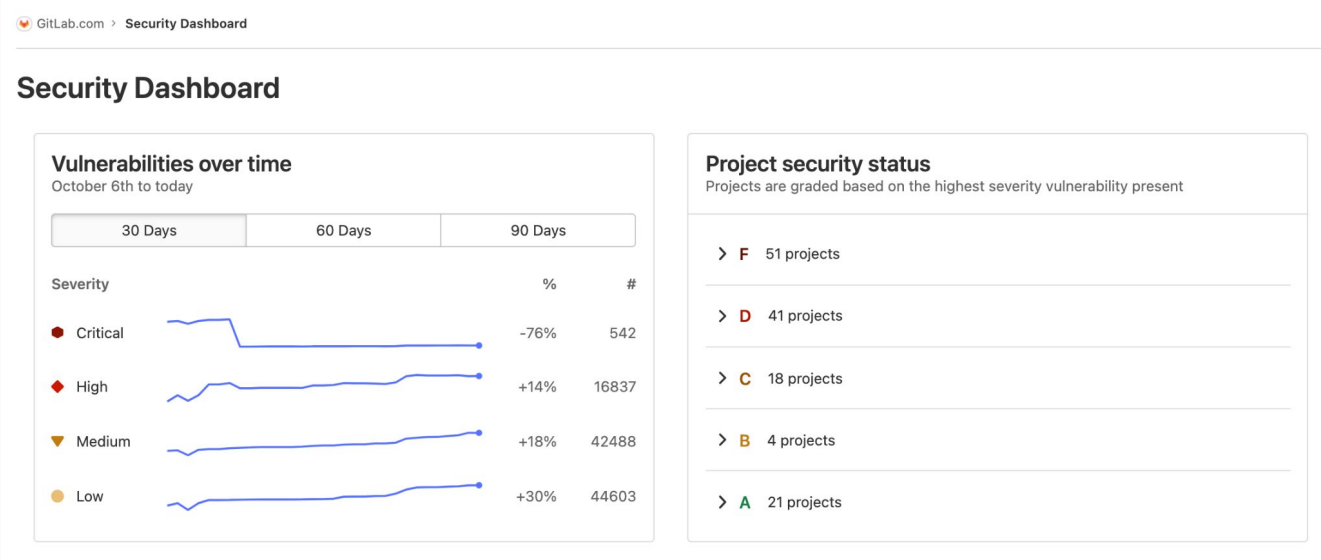
- Security dashboards & reports can be found in:
  - Pipelines
  - Projects ➡️
  - Groups
  - Instance
- Tip: Schedule regular pipelines to ensure updated information



https://docs.gitlab.com/ee/user/application_security/security_dashboard/

Security Dashboards

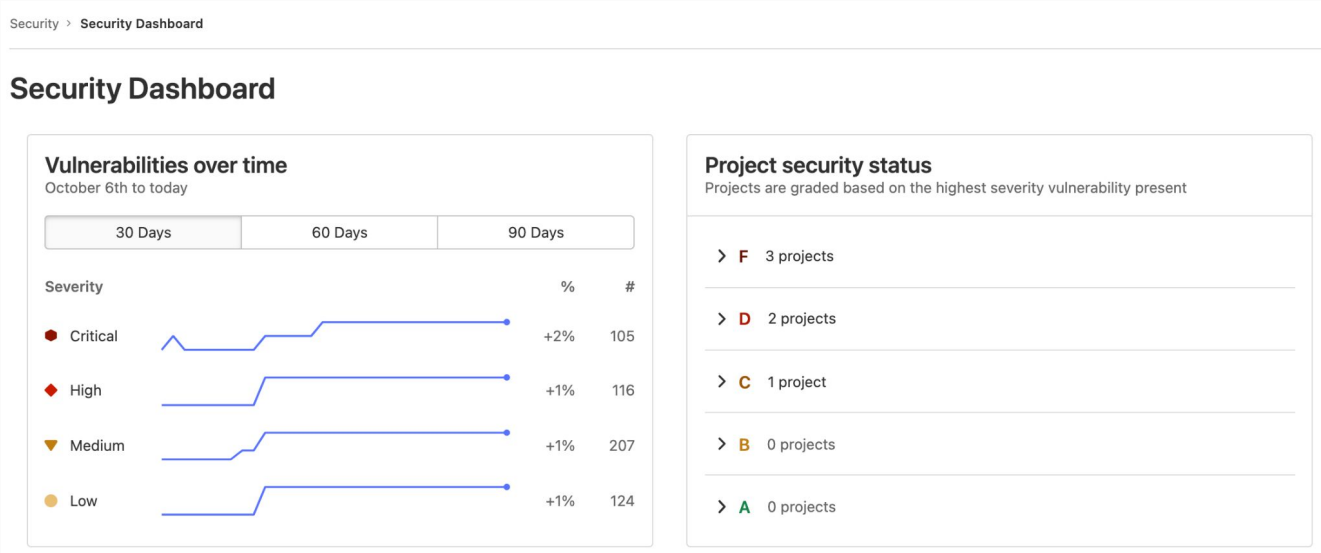
- Security dashboards & reports can be found in:
  - Pipelines
  - Projects
  - Groups ➡️
  - Instance
- Tip: Schedule regular pipelines to ensure updated information



https://docs.gitlab.com/ee/user/application_security/security_dashboard/

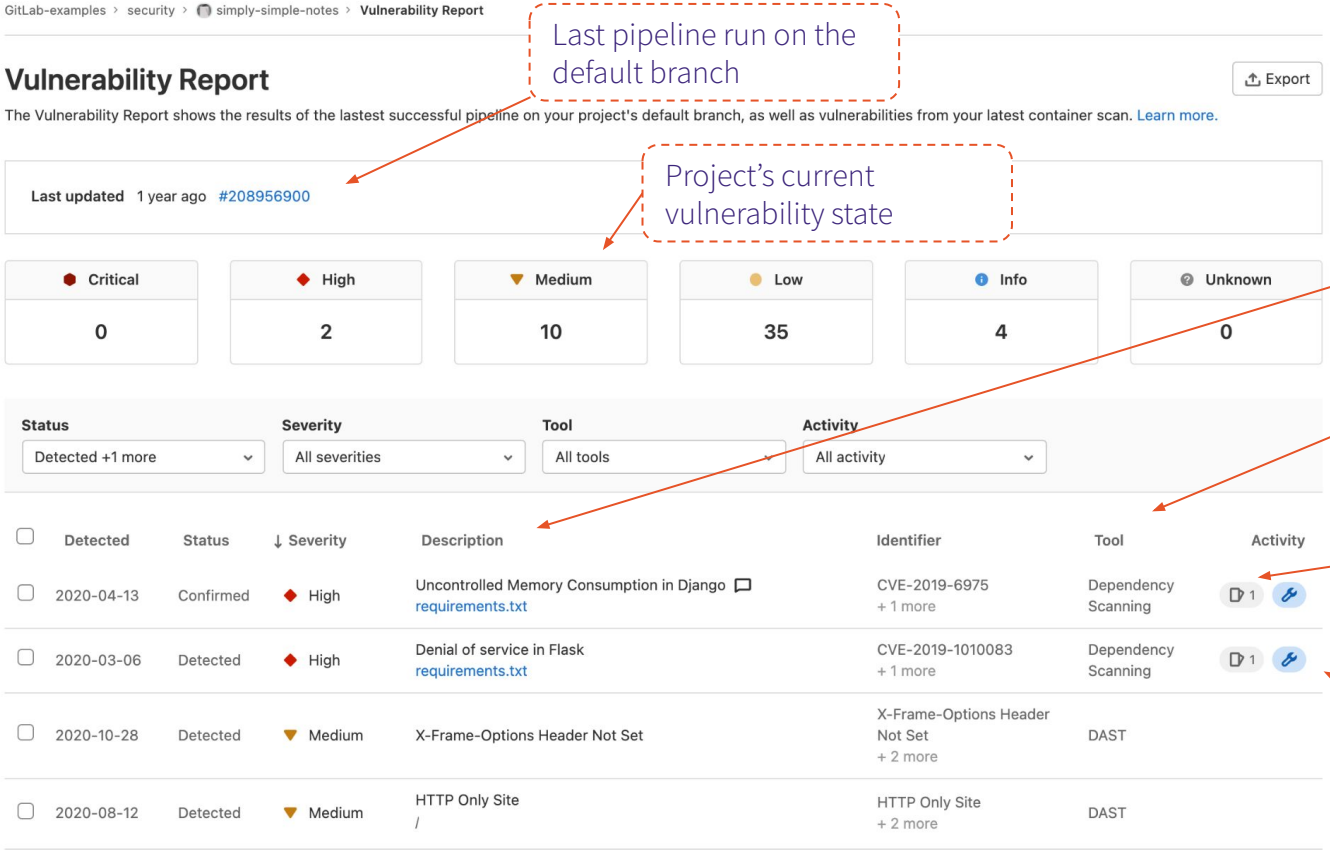
Security Dashboards

- Security dashboards & reports can be found in:
  - Pipelines
  - Projects
  - Groups
  - Instance ➡️
- Tip: Schedule regular pipelines to ensure updated information



https://docs.gitlab.com/ee/user/application_security/security_dashboard/

Vulnerability Reports



Last pipeline run on the default branch

Project's current vulnerability state

Export CSV of vulnerabilities

File and/or line where vulnerability resides

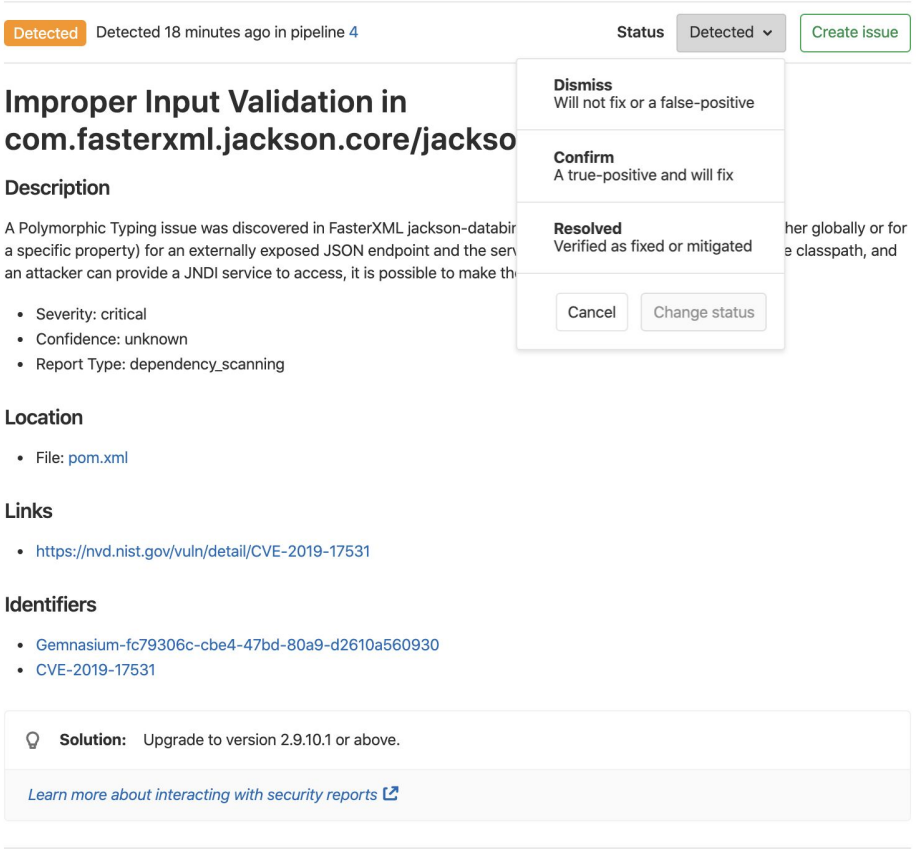
Scanner that identified the vulnerability

Issues related to vulnerability

Remediated vulnerability awaiting review

https://docs.gitlab.com/ee/user/application_security/vulnerability_report/

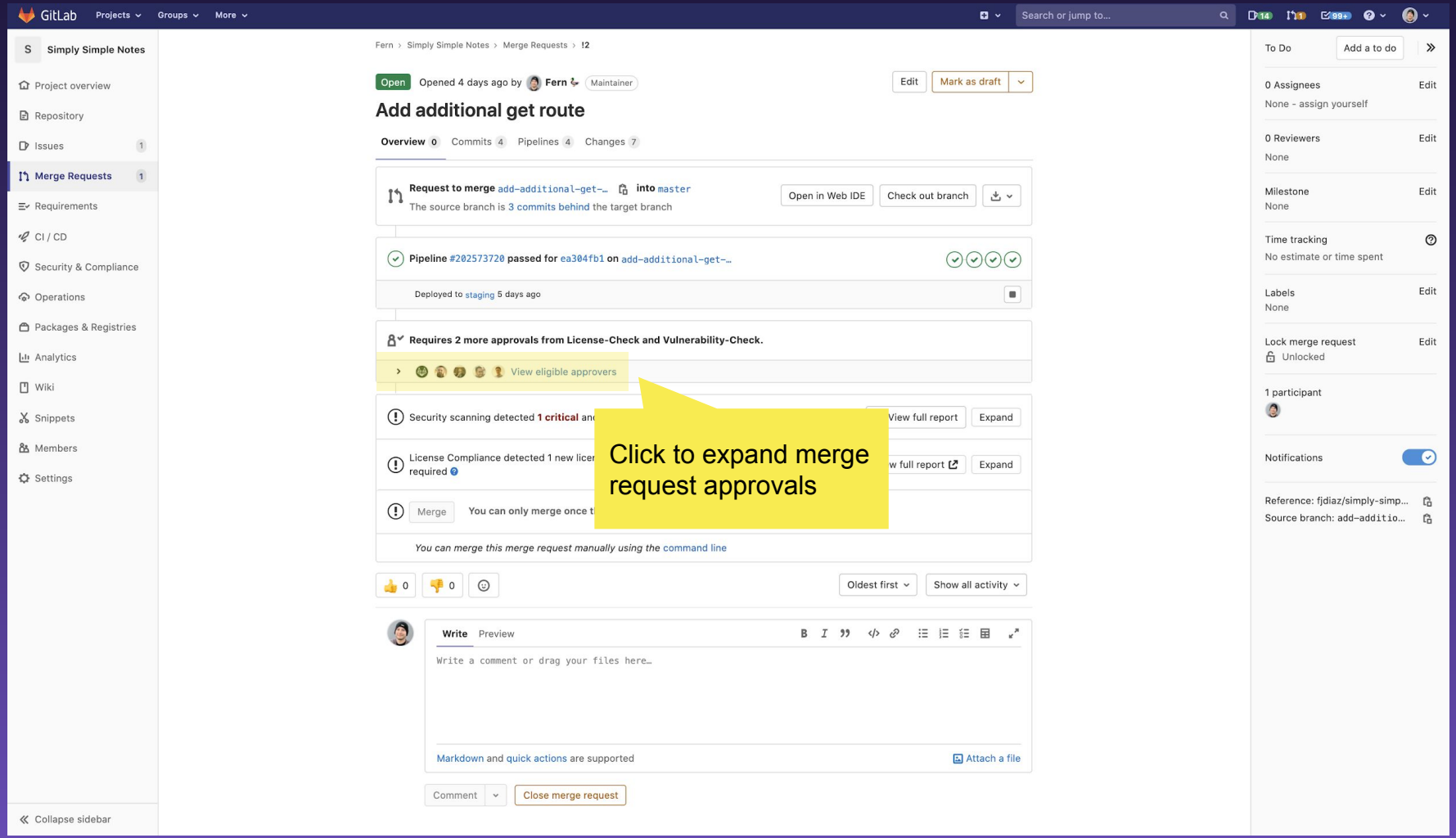
Vulnerability Pages

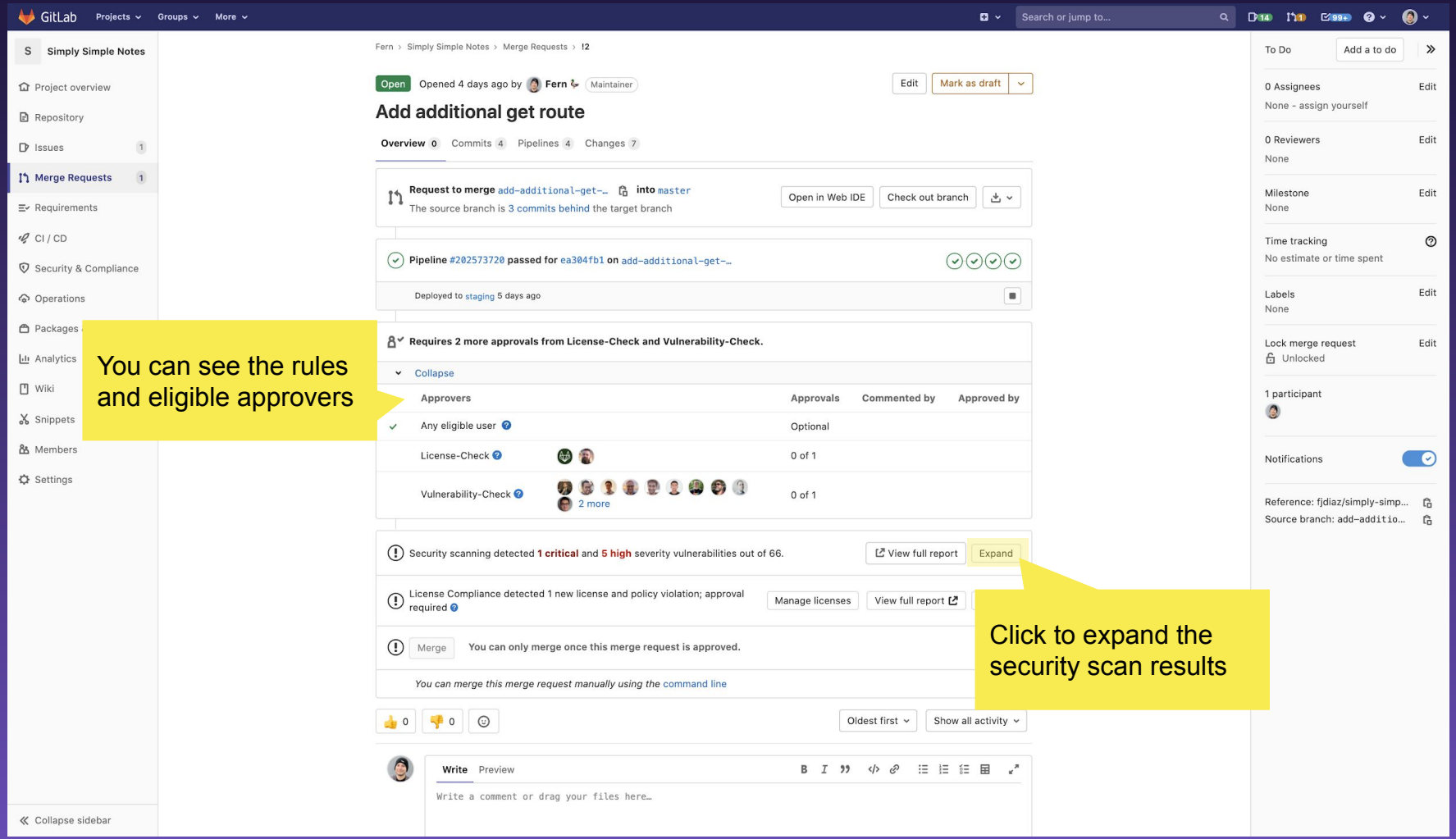


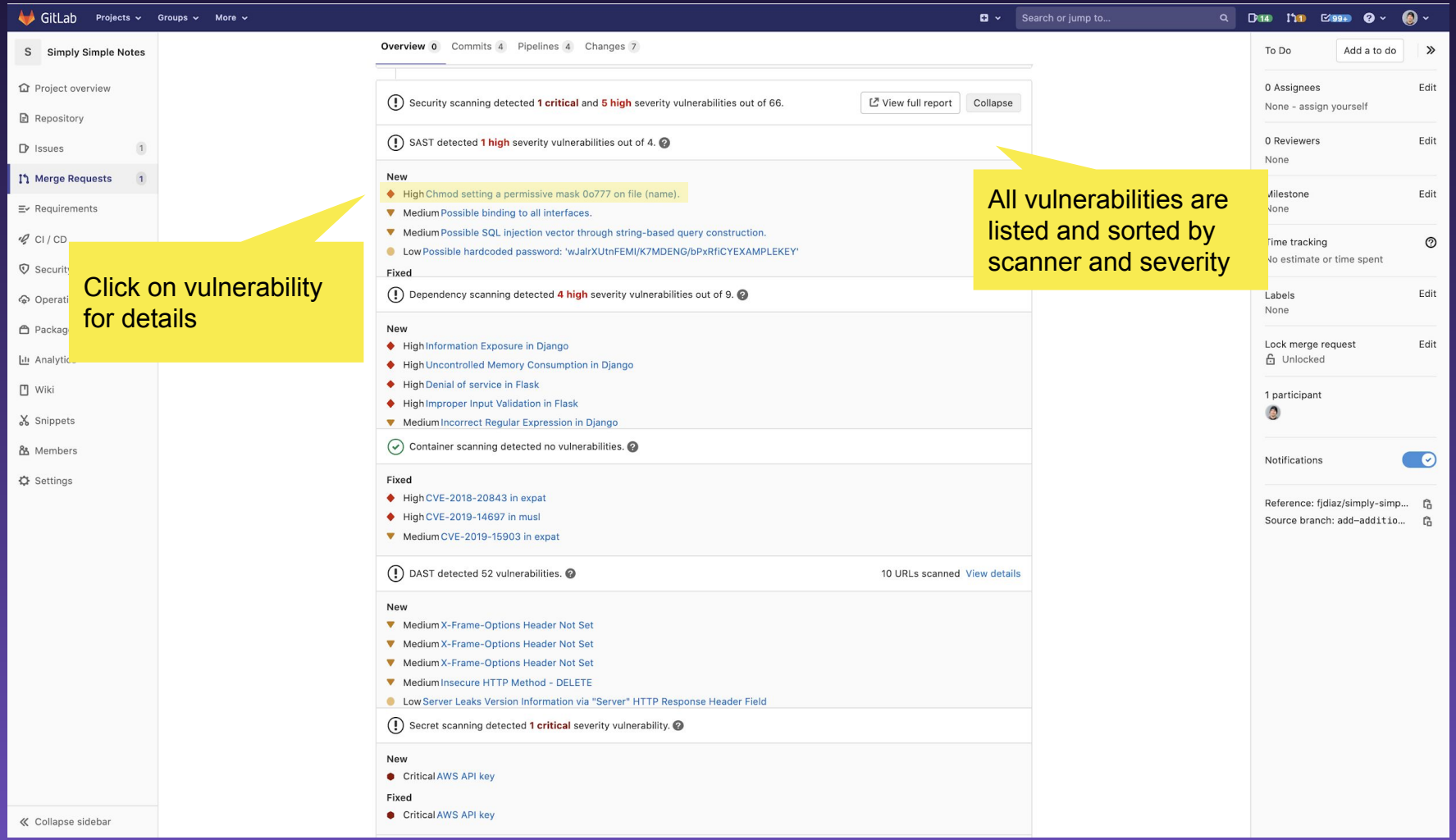
- Each vulnerability in the Dependency List has its own standalone page
- The standalone vulnerability pages can be accessed via the vulnerability report
- On the standalone page, you can:
  - Change the vulnerability status
  - Create a new confidential issue, pre-populated with relevant information
  - Link existing issues to the vulnerability
  - Apply automatically-generated solution

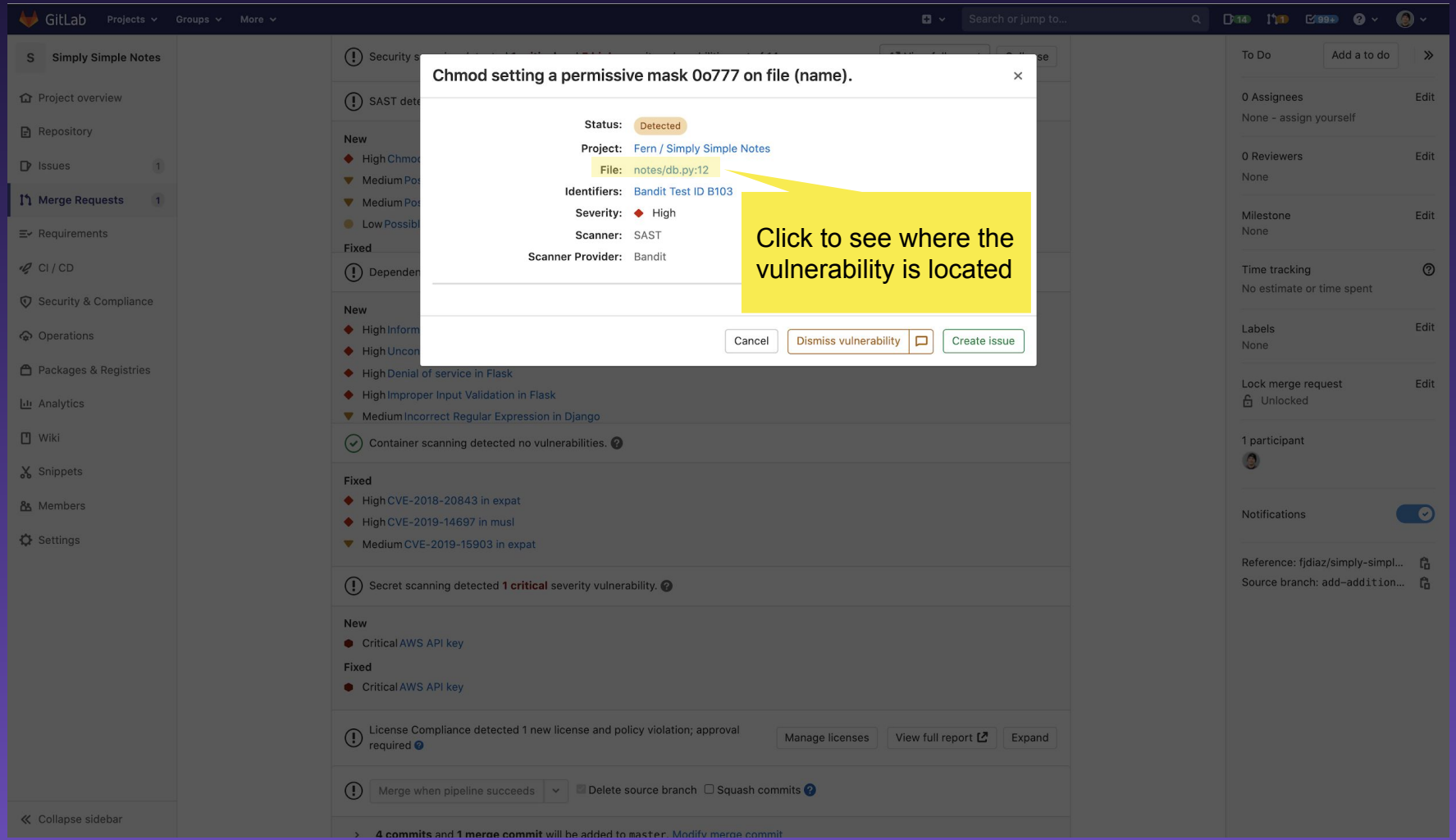
https://docs.gitlab.com/ee/user/application_security/vulnerabilities/

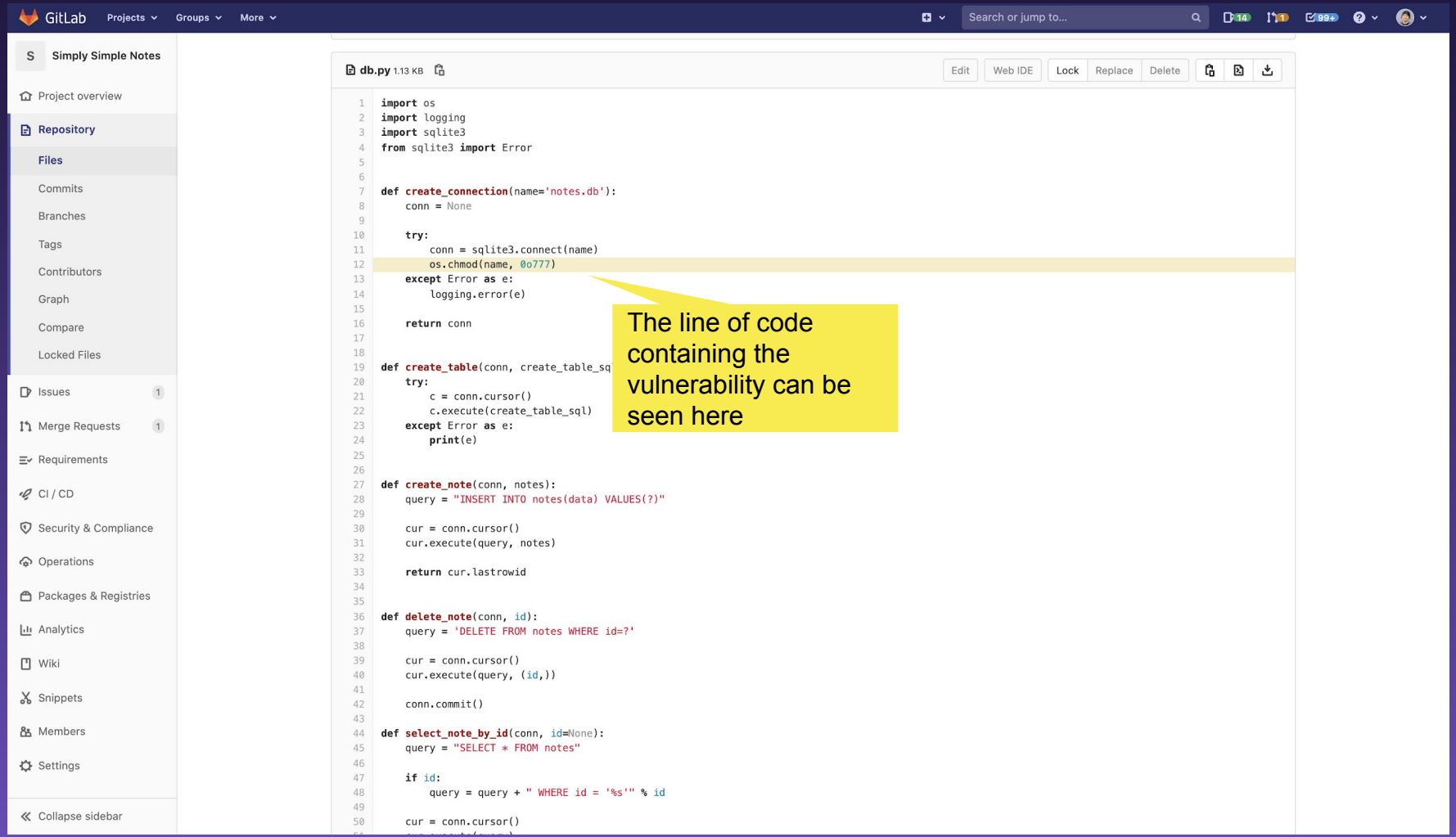
Developer Workflow

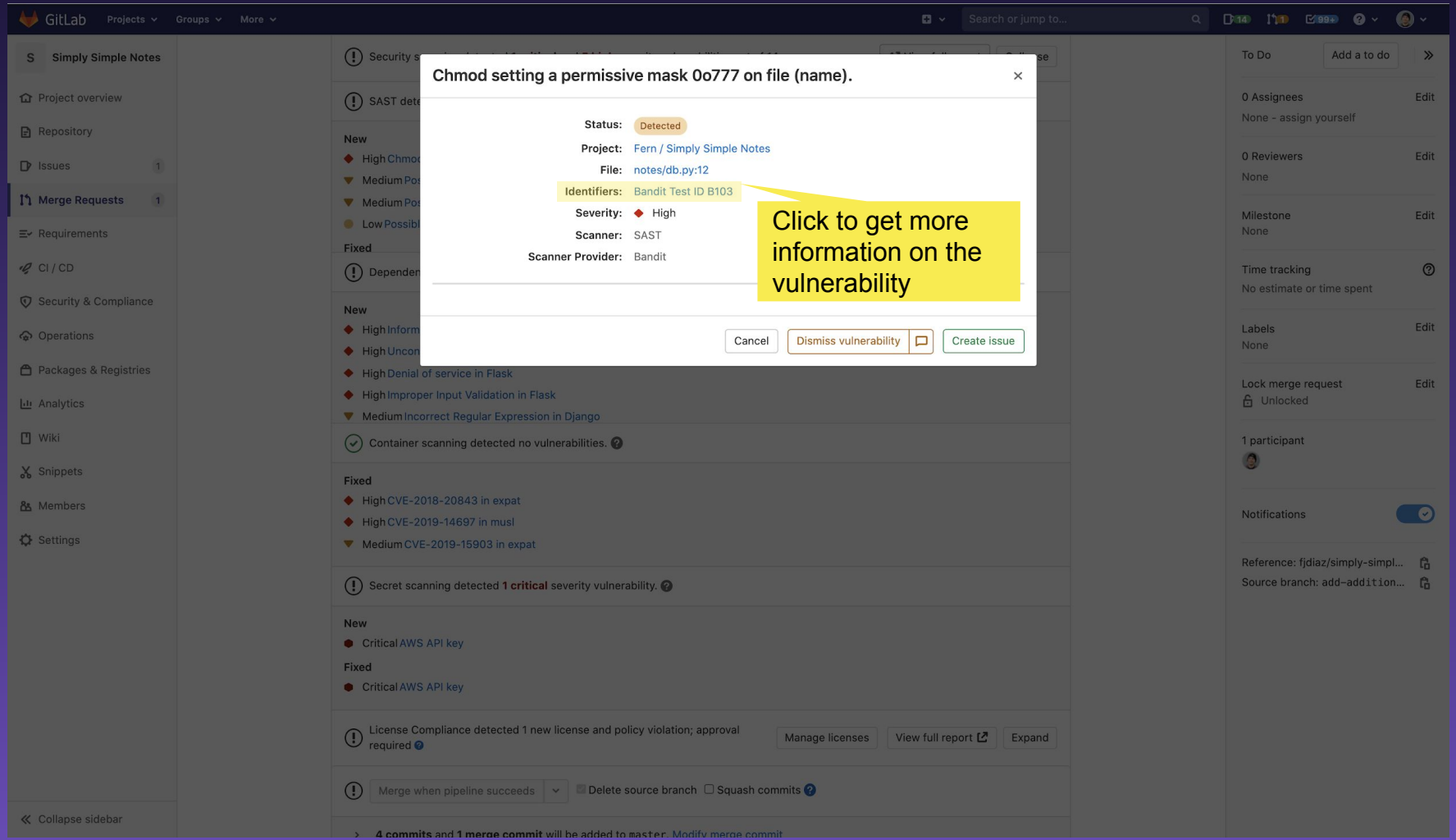

GitLab
Projects
Groups
More
Search or jump to...
Simply Simple Notes
Project overview
Repository
Issues
Merge Requests
Requirements
CI / CD
Security & Compliance
Operations
Packages & Registries
Analytics
Wiki
Snippets
Members
Settings
Collapse sidebar
Fern › Simply Simple Notes › Merge Requests › !2
Open
Opened 4 days ago by Fern
Maintainer
Edit
Mark as draft
Add additional get route
Overview 0
Commits 4
Pipelines 4
Changes 7
Request to merge add-additional-get-… into master
The source branch is 3 commits behind the target branch
Open in Web IDE
Check out branch
Pipeline #202573720 passed for ea304fb1 on add-additional-get-…
Deployed to staging 5 days ago
Requires 2 more approvals from License-Check and Vulnerability-Check.
View eligible approvers
Security scanning detected 1 critical
View full report
Expand
License Compliance detected 1 new
required
Expand
Merge
You can only merge once
You can merge this merge request manually using the command line
Oldest first
Show all activity
Write
Preview
Write a comment or drag your files here…
Markdown and quick actions are supported
Attach a file
Comment
Close merge request
Click to expand merge request approvals
To Do
Add a to do
0 Assignees
Edit
None - assign yourself
0 Reviewers
Edit
None
Milestone
Edit
None
Time tracking
No estimate or time spent
Labels
Edit
None
Lock merge request
Edit
Unlocked
1 participant
Notifications
Reference: fjdiaz/simply-simp…
Source branch: add-additio…


GitLab
Projects
Groups
More
Search or jump to...
Simply Simple Notes
Project overview
Repository
Issues
Merge Requests
Requirements
CI / CD
Security & Compliance
Operations
Packages
Analytics
Wiki
Snippets
Members
Settings
Collapse sidebar
Fern › Simply Simple Notes › Merge Requests › !2
Open
Opened 4 days ago by Fern
Maintainer
Edit
Mark as draft
Add additional get route
Overview 0
Commits 4
Pipelines 4
Changes 7
Request to merge add-additional-get-… into master
The source branch is 3 commits behind the target branch
Open in Web IDE
Check out branch
Pipeline #202573720 passed for ea304fb1 on add-additional-get-…
Deployed to staging 5 days ago
Requires 2 more approvals from License-Check and Vulnerability-Check.
Collapse
Approvers
Approvals
Commented by
Approved by
Any eligible user
Optional
License-Check
0 of 1
Vulnerability-Check
2 more
0 of 1
Security scanning detected 1 critical and 5 high severity vulnerabilities out of 66.
View full report
Expand
License Compliance detected 1 new license and policy violation; approval required
Manage licenses
View full report
Merge
You can only merge once this merge request is approved.
You can merge this merge request manually using the command line
0
0
Oldest first
Show all activity
Write
Preview
Write a comment or drag your files here…
To Do
Add a to do
0 Assignees
Edit
None - assign yourself
0 Reviewers
Edit
None
Milestone
Edit
None
Time tracking
No estimate or time spent
Labels
Edit
None
Lock merge request
Edit
Unlocked
1 participant
Notifications
Reference: fjdiaz/simply-simp…
Source branch: add-additio…
You can see the rules and eligible approvers
Click to expand the security scan results


GitLab
Projects
Groups
More
Search or jump to...
Simply Simple Notes
Project overview
Repository
Issues
Merge Requests
Requirements
CI / CD
Wiki
Snippets
Members
Settings
Collapse sidebar
Overview 0
Commits 4
Pipelines 4
Changes 7
Security scanning detected 1 critical and 5 high severity vulnerabilities out of 66.
View full report
Collapse
SAST detected 1 high severity vulnerabilities out of 4.
New
High Chmod setting a permissive mask 0o777 on file (name).
Medium Possible binding to all interfaces.
Medium Possible SQL injection vector through string-based query construction.
Low Possible hardcoded password: 'wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY'
Fixed
Dependency scanning detected 4 high severity vulnerabilities out of 9.
New
High Information Exposure in Django
High Uncontrolled Memory Consumption in Django
High Denial of service in Flask
High Improper Input Validation in Flask
Medium Incorrect Regular Expression in Django
Container scanning detected no vulnerabilities.
Fixed
High CVE-2018-20843 in expat
High CVE-2019-14697 in musl
Medium CVE-2019-15903 in expat
DAST detected 52 vulnerabilities.
10 URLs scanned View details
New
Medium X-Frame-Options Header Not Set
Medium X-Frame-Options Header Not Set
Medium X-Frame-Options Header Not Set
Medium Insecure HTTP Method - DELETE
Low Server Leaks Version Information via "Server" HTTP Response Header Field
Secret scanning detected 1 critical severity vulnerability.
New
Critical AWS API key
Fixed
Critical AWS API key
To Do
Add a to do
0 Assignees
Edit
None - assign yourself
0 Reviewers
Edit
None
Milestone
Edit
None
Time tracking
No estimate or time spent
Labels
Edit
None
Lock merge request
Edit
Unlocked
1 participant
Notifications
Reference: fjdiaz/simply-simp...
Source branch: add-additio...
Click on vulnerability for details
All vulnerabilities are listed and sorted by scanner and severity


Chmod setting a permissive mask 0o777 on file (name).
Status: Detected
Project: Fern / Simply Simple Notes
File: notes/db.py:12
Identifiers: Bandit Test ID B103
Severity: High
Scanner: SAST
Scanner Provider: Bandit
Click to see where the vulnerability is located
Cancel
Dismiss vulnerability
Create issue


GitLab
Projects
Groups
More
Search or jump to...
Simply Simple Notes
Project overview
Repository
Files
Commits
Branches
Tags
Contributors
Graph
Compare
Locked Files
Issues
Merge Requests
Requirements
CI / CD
Security & Compliance
Operations
Packages & Registries
Analytics
Wiki
Snippets
Members
Settings
Collapse sidebar
db.py 1.13 KB
Edit
Web IDE
Lock
Replace
Delete
import os
import logging
import sqlite3
from sqlite3 import Error
def create_connection(name='notes.db'):
conn = None
try:
conn = sqlite3.connect(name)
os.chmod(name, 0o777)
except Error as e:
logging.error(e)
return conn
def create_table(conn, create_table_sq
try:
c = conn.cursor()
c.execute(create_table_sql)
except Error as e:
print(e)
def create_note(conn, notes):
query = "INSERT INTO notes(data) VALUES(?)"
cur = conn.cursor()
cur.execute(query, notes)
return cur.lastrowid
def delete_note(conn, id):
query = 'DELETE FROM notes WHERE id=?'
cur = conn.cursor()
cur.execute(query, (id,))
conn.commit()
def select_note_by_id(conn, id=None):
query = "SELECT * FROM notes"
if id:
query = query + " WHERE id = '%s'" % id
cur = conn.cursor()
The line of code containing the vulnerability can be seen here


Chmod setting a permissive mask 0o777 on file (name).
Status: Detected
Project: Fern / Simply Simple Notes
File: notes/db.py:12
Identifiers: Bandit Test ID B103
Severity: High
Scanner: SAST
Scanner Provider: Bandit
Click to get more information on the vulnerability
Cancel
Dismiss vulnerability
Create issue

B103: set_bad_file_permissions

B103: Test for setting permissive file permissions

POSIX based operating systems utilize a permissions model to protect access to parts of the file system. This model supports three roles “owner”, “group” and “world” each role may have a combination of “read”, “write” or “execute” flags sets. Python provides `chmod` to manipulate POSIX style permissions.

This plugin test looks for the use of `chmod` and will alert when it is used to set particularly permissive control flags. A MEDIUM warning is generated if a file is set to group executable and a HIGH warning is reported if a file is set world writable. Warnings are given with HIGH confidence.

Example:

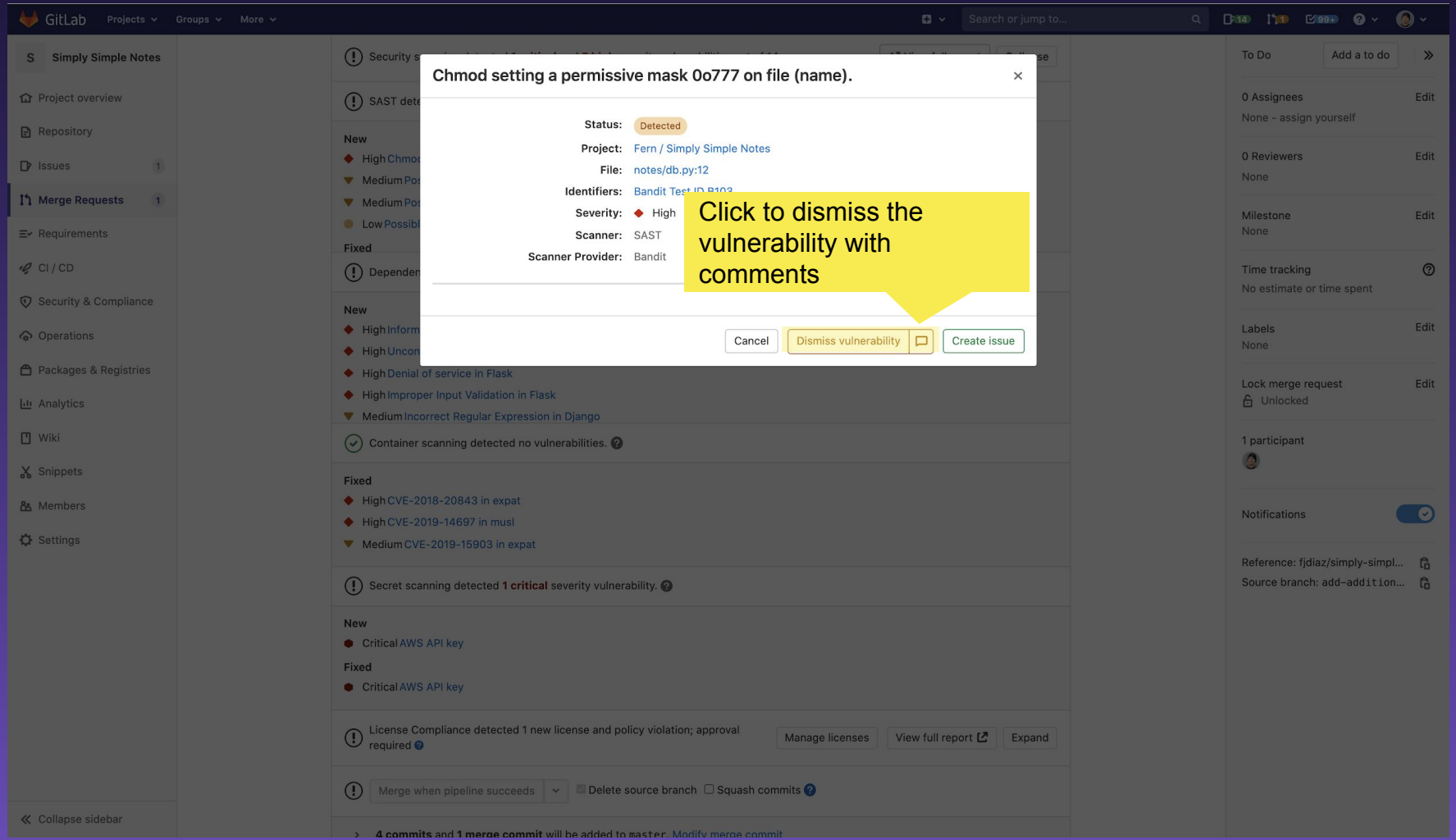
```
>> Issue: Probable insecure usage of temp file/directory.
   Severity: Medium   Confidence: Medium
   Location: ./examples/os-chmod-py2.py:15
14  os.chmod('/etc/hosts', 0o777)
15  os.chmod('/tmp/oh_hai', 0x1ff)
16  os.chmod('/etc/passwd', stat.S_IRWXU)

>> Issue: Chmod setting a permissive mask 0777 on file (key_file).
   Severity: High   Confidence: High
   Location: ./examples/os-chmod-py2.py:17
16  os.chmod('/etc/passwd', stat.S_IRWXU)
17  os.chmod(key_file, 0o777)
18
```

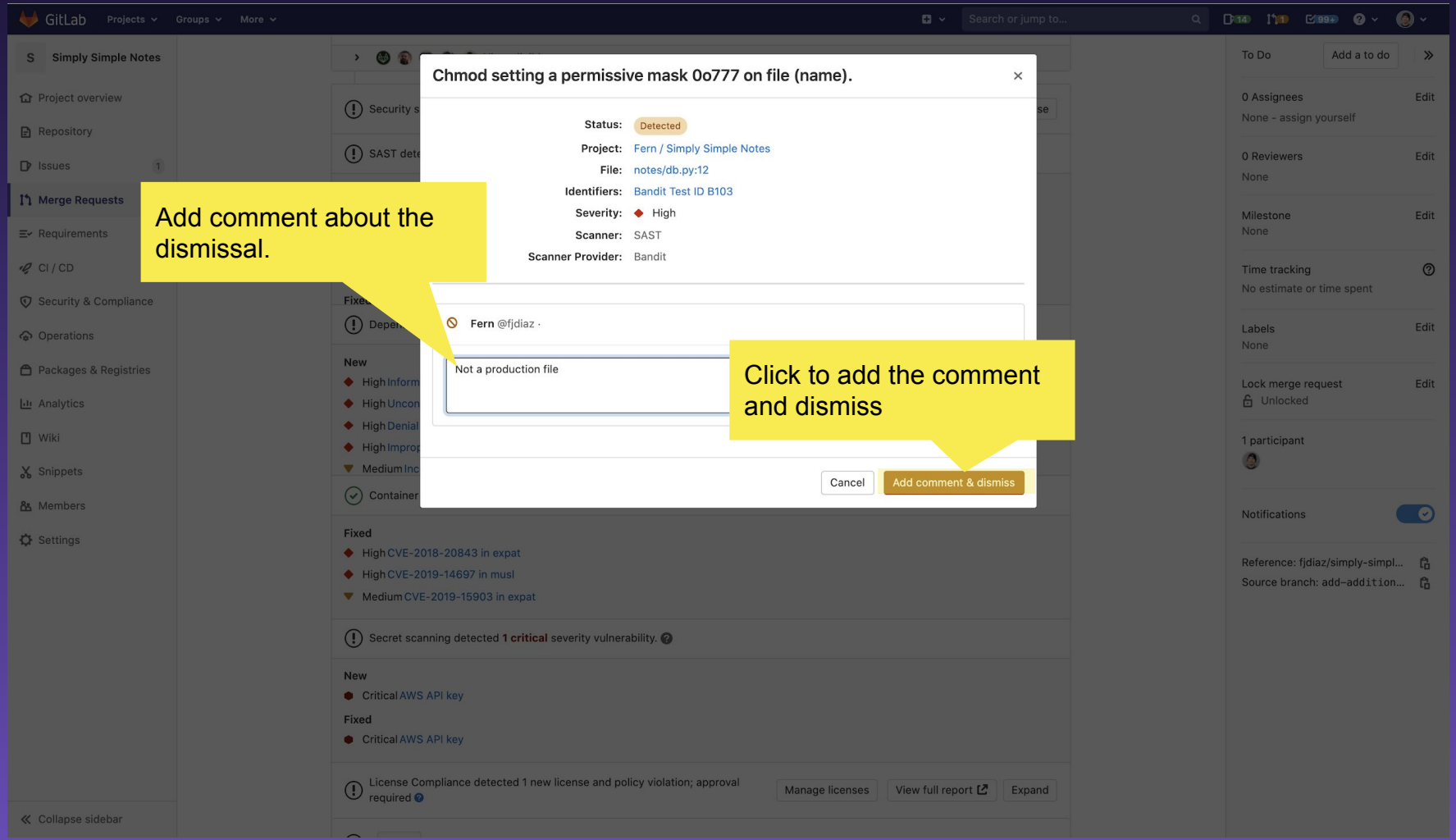
See also

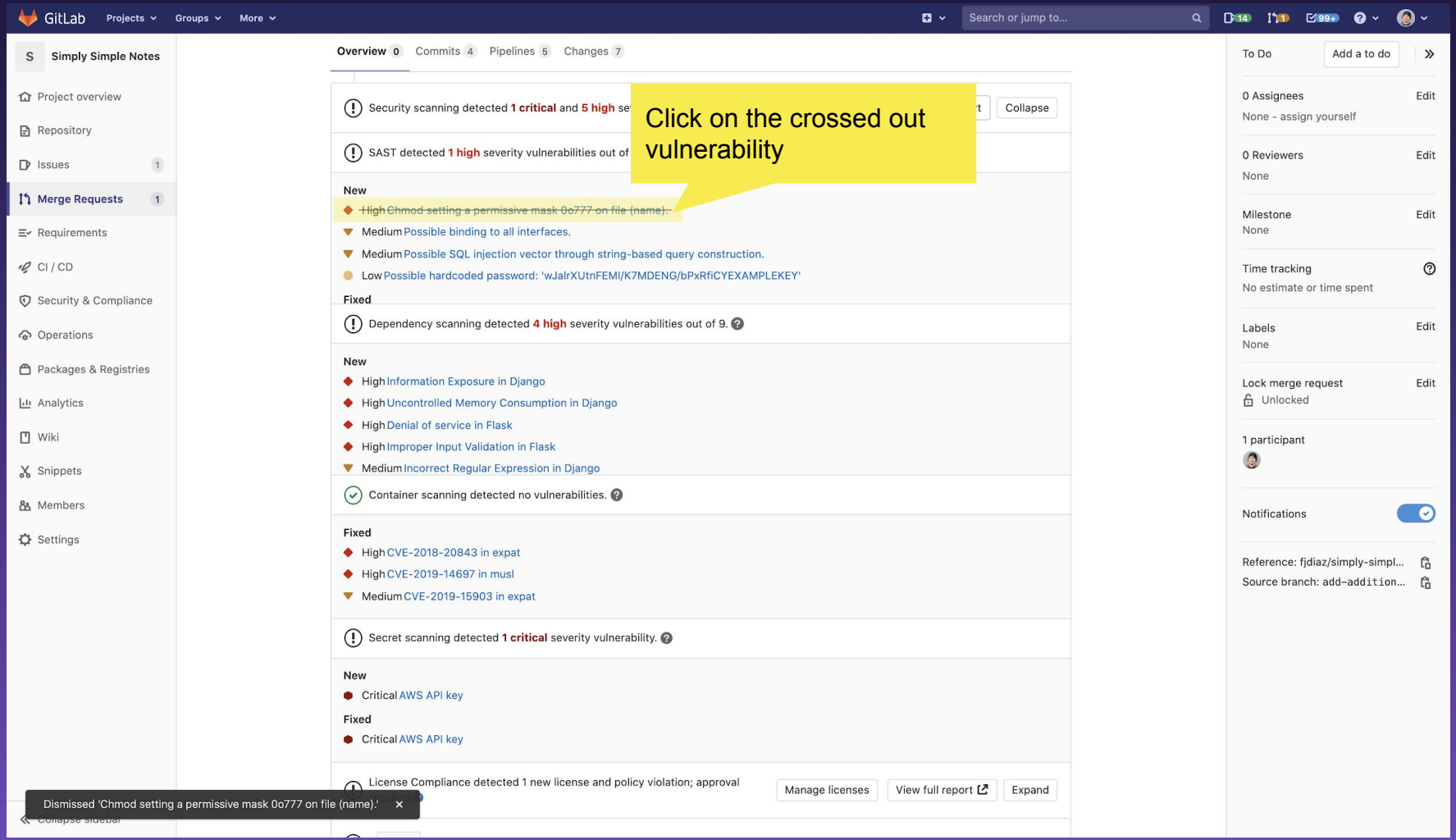
- https://security.openstack.org/guidelines/dg_apply-restrictive-file-permissions.html # noqa
- https://en.wikipedia.org/wiki/File_system_permissions
- https://security.openstack.org

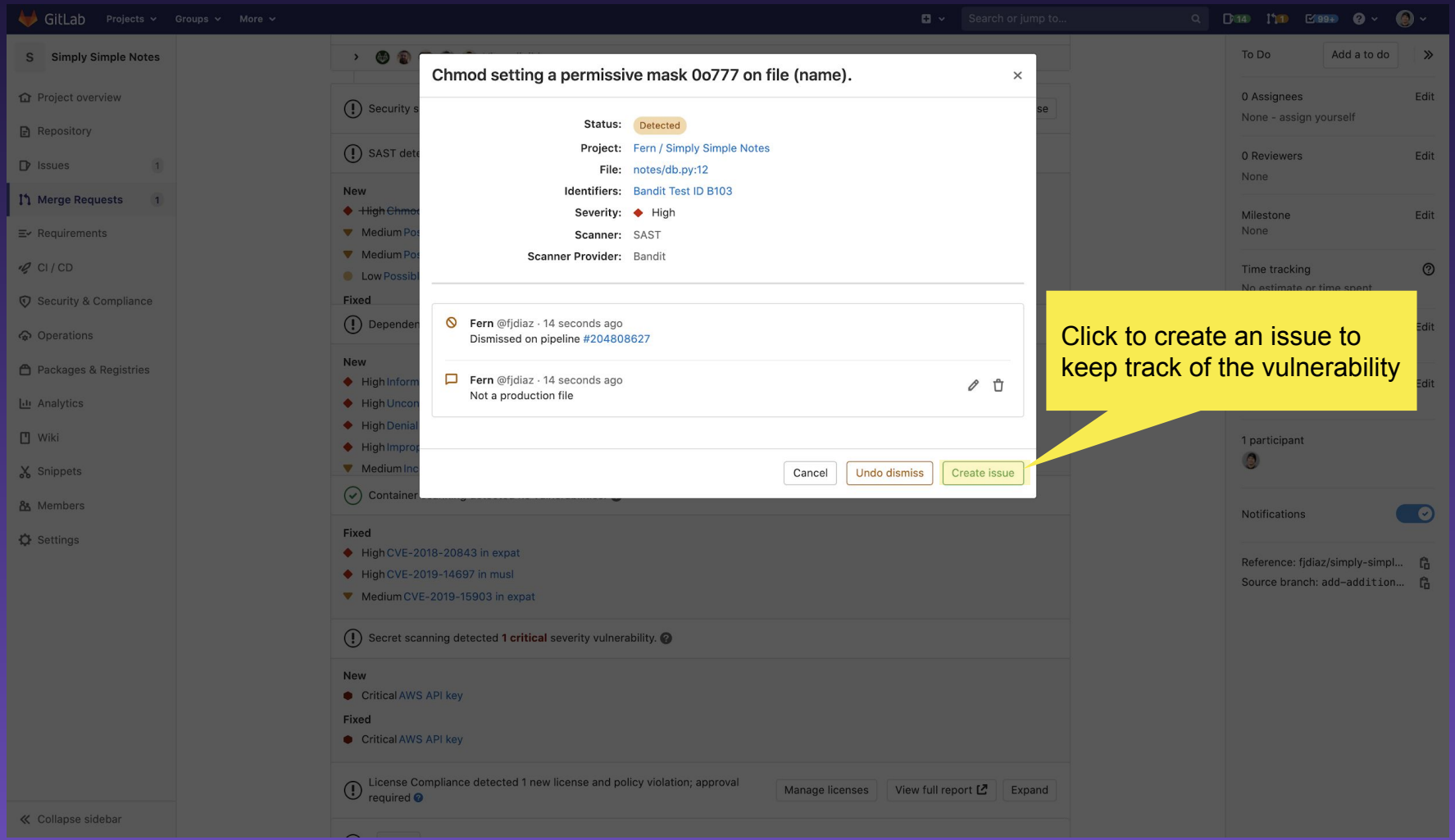
New in version 0.9.0.

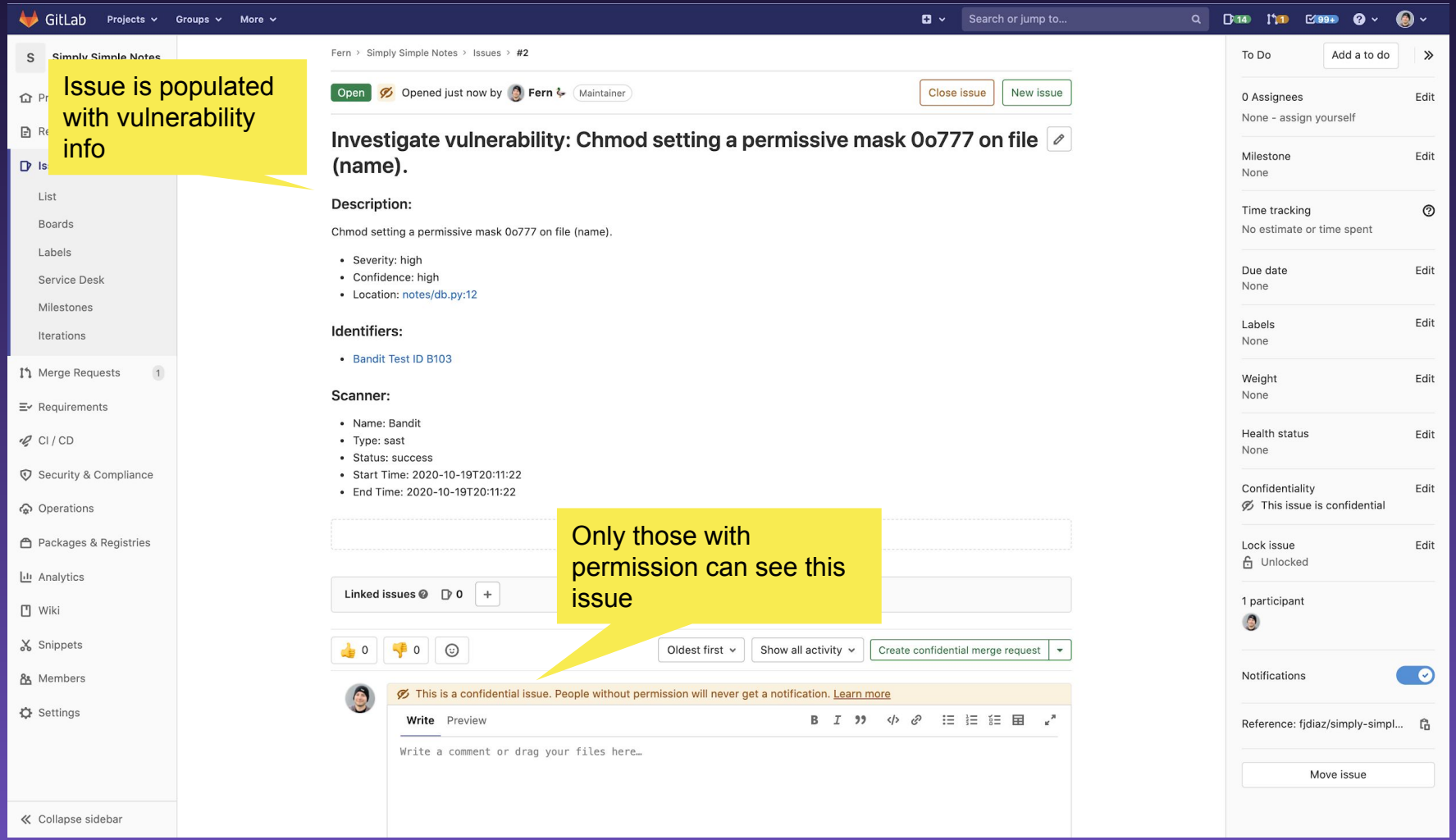
Each vulnerability has detailed information to enhance developer education

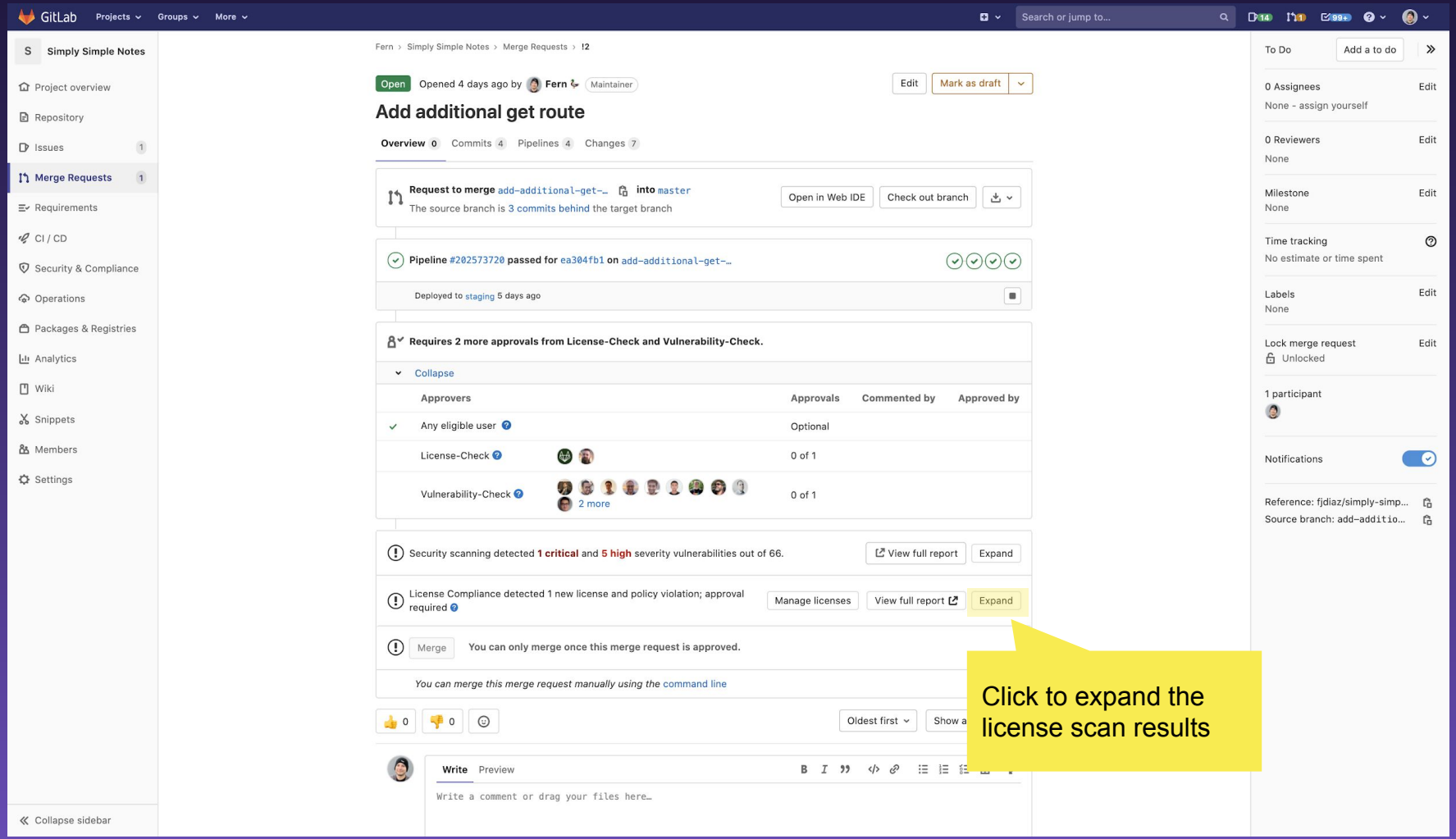

Chmod setting a permissive mask 0o777 on file (name).
Status: Detected
Project: Fern / Simply Simple Notes
File: notes/db.py:12
Identifiers: Bandit Test ID B103
Severity: High
Scanner: SAST
Scanner Provider: Bandit
Click to dismiss the vulnerability with comments
Cancel
Dismiss vulnerability
Create issue

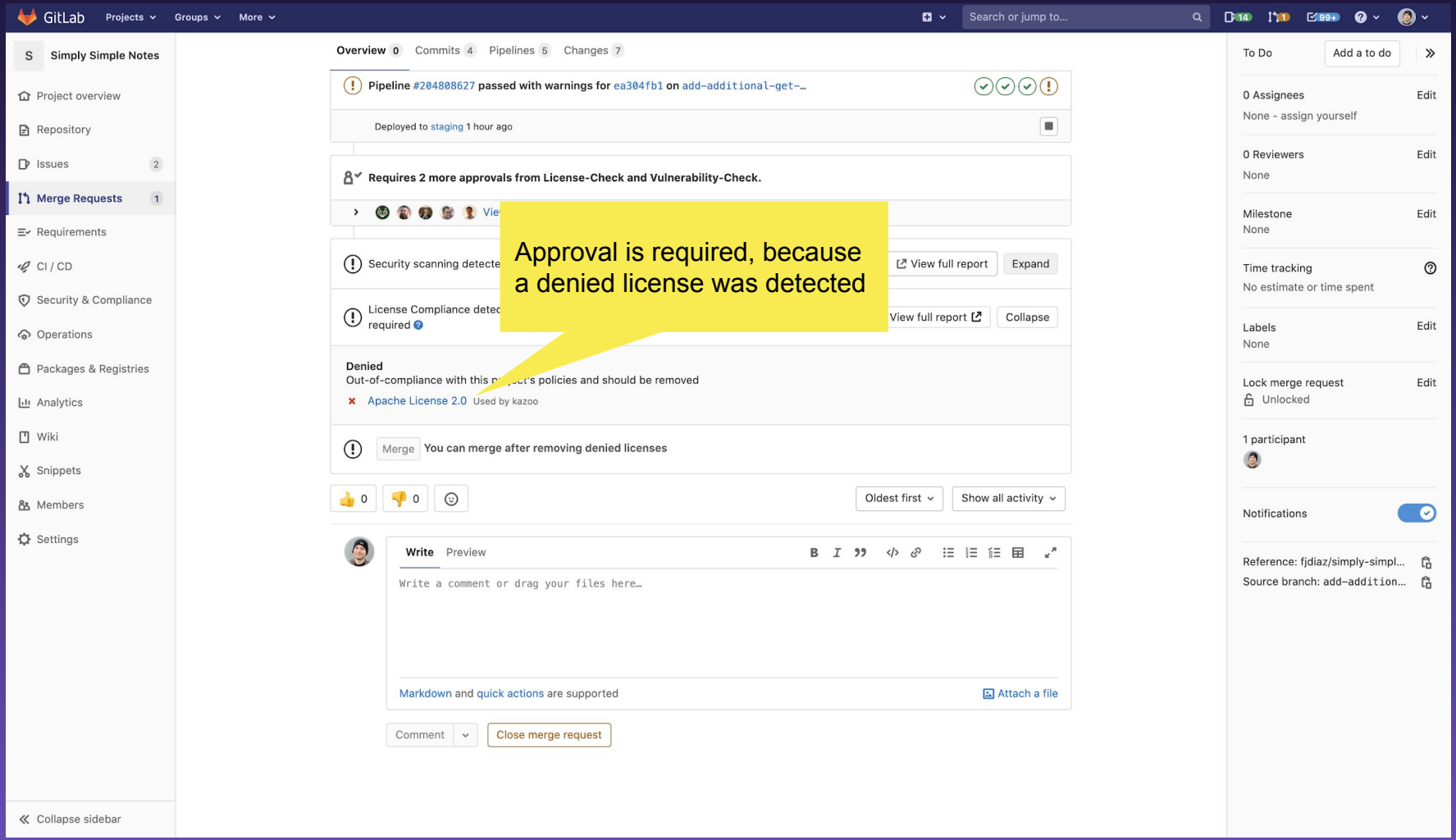

Chmod setting a permissive mask 0o777 on file (name).
Status: Detected
Project: Fern / Simply Simple Notes
File: notes/db.py:12
Identifiers: Bandit Test ID B103
Severity: High
Scanner: SAST
Scanner Provider: Bandit
Fern @fjdiaz ·
Not a production file
Cancel
Add comment & dismiss
Add comment about the dismissal.
Click to add the comment and dismiss


GitLab
Projects
Groups
More
Search or jump to...
Simply Simple Notes
Project overview
Repository
Issues 1
Merge Requests 1
Requirements
CI / CD
Security & Compliance
Operations
Packages & Registries
Analytics
Wiki
Snippets
Members
Settings
Collapse sidebar
Overview 0
Commits 4
Pipelines 5
Changes 7
Security scanning detected 1 critical and 5 high se
Collapse
SAST detected 1 high severity vulnerabilities out of
New
High Chmod setting a permissive mask 0o777 on file (name).
Medium Possible binding to all interfaces.
Medium Possible SQL injection vector through string-based query construction.
Low Possible hardcoded password: 'wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY'
Fixed
Dependency scanning detected 4 high severity vulnerabilities out of 9.
New
High Information Exposure in Django
High Uncontrolled Memory Consumption in Django
High Denial of service in Flask
High Improper Input Validation in Flask
Medium Incorrect Regular Expression in Django
Container scanning detected no vulnerabilities.
Fixed
High CVE-2018-20843 in expat
High CVE-2019-14697 in musl
Medium CVE-2019-15903 in expat
Secret scanning detected 1 critical severity vulnerability.
New
Critical AWS API key
Fixed
Critical AWS API key
License Compliance detected 1 new license and policy violation; approval
Manage licenses
View full report
Expand
Dismissed 'Chmod setting a permissive mask 0o777 on file (name).'
Click on the crossed out vulnerability
To Do
Add a to do
0 Assignees
Edit
None - assign yourself
0 Reviewers
Edit
None
Milestone
Edit
None
Time tracking
No estimate or time spent
Labels
Edit
None
Lock merge request
Edit
Unlocked
1 participant
Notifications
Reference: fjdiaz/simply-simpl...
Source branch: add-addition...

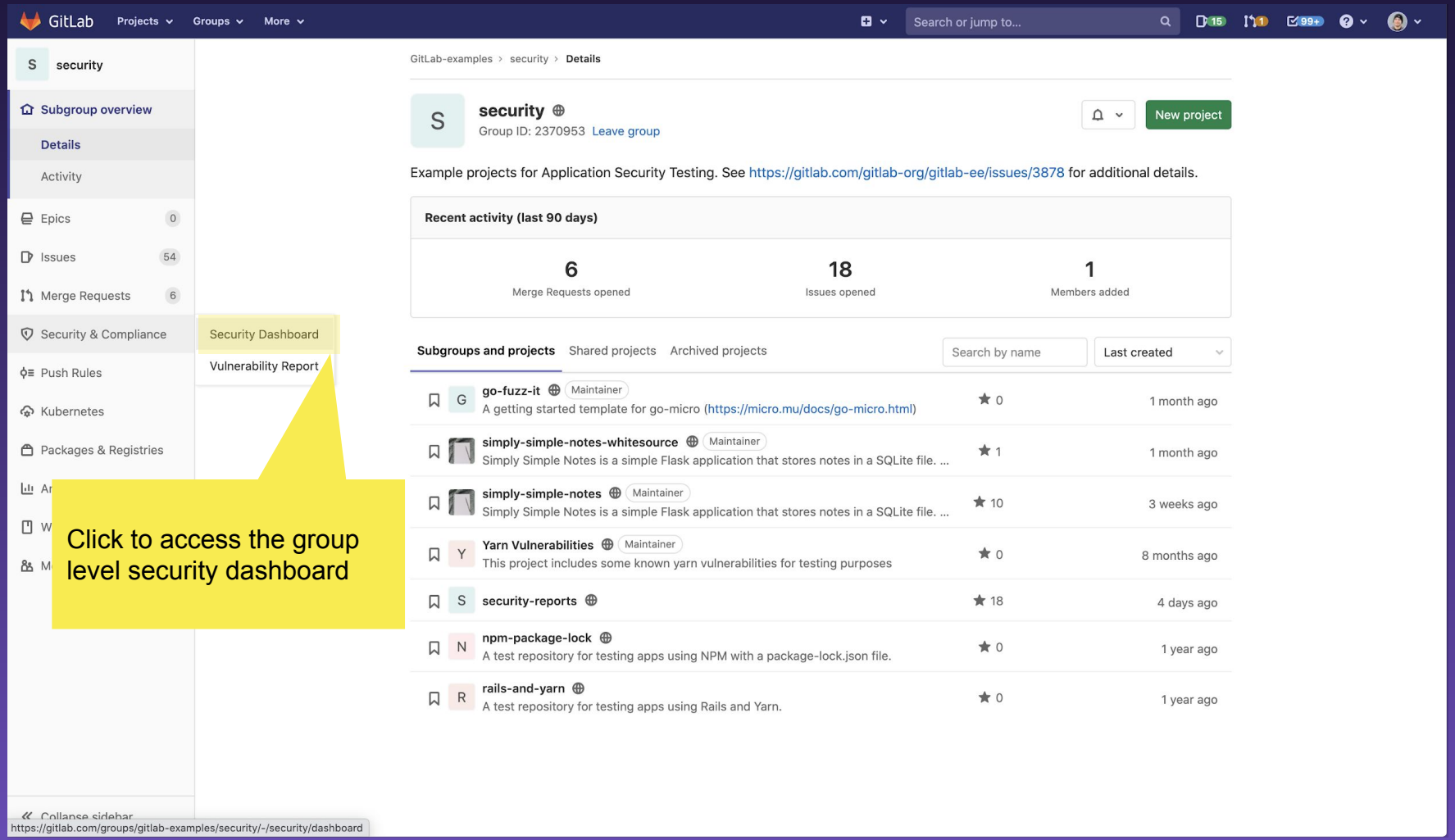

Chmod setting a permissive mask 0o777 on file (name).
Status: Detected
Project: Fern / Simply Simple Notes
File: notes/db.py:12
Identifiers: Bandit Test ID B103
Severity: High
Scanner: SAST
Scanner Provider: Bandit
Fern @fjdiaz · 14 seconds ago
Dismissed on pipeline #204808627
Fern @fjdiaz · 14 seconds ago
Not a production file
Cancel
Undo dismiss
Create issue
Click to create an issue to keep track of the vulnerability

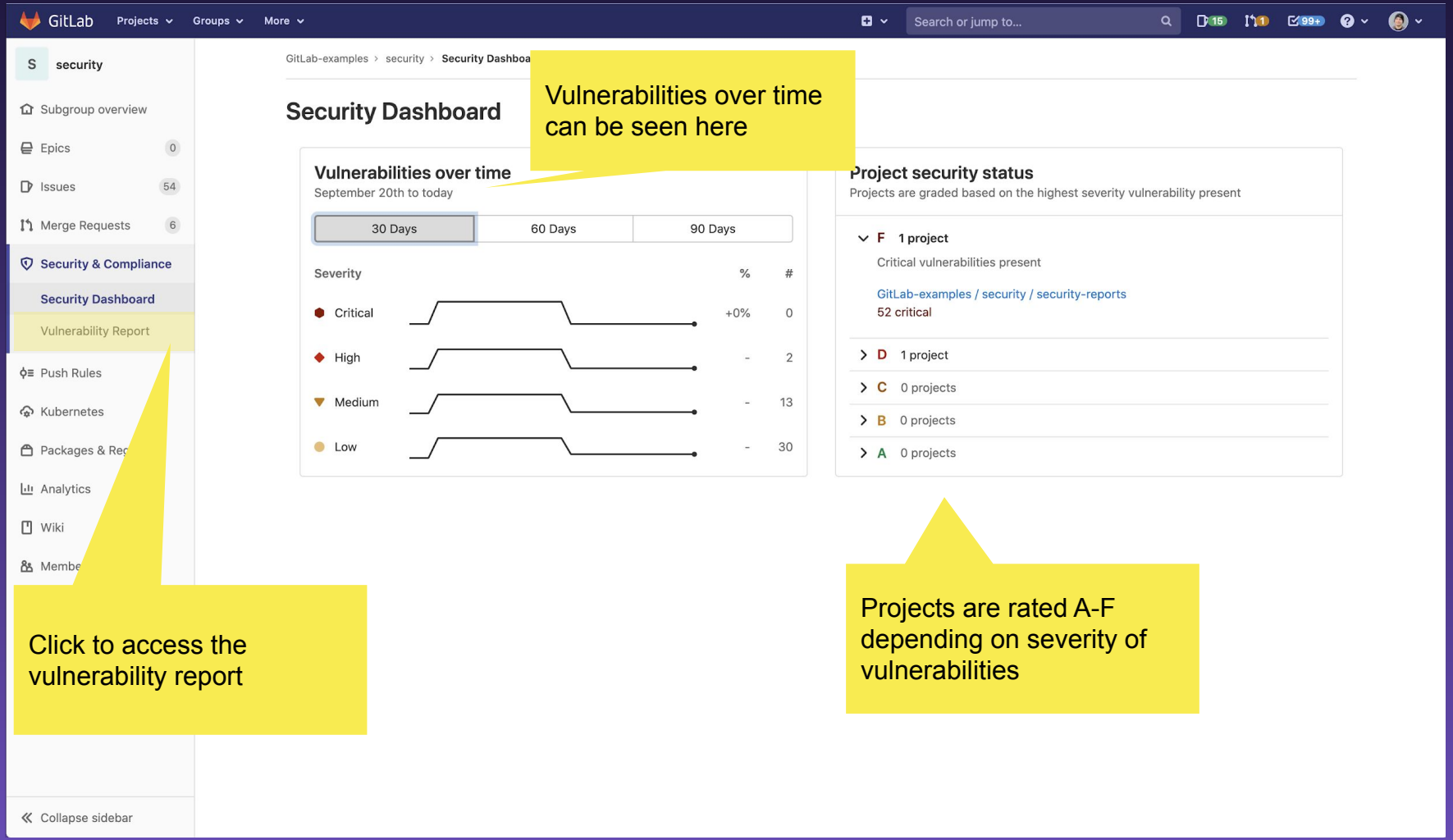

GitLab
Projects
Groups
More
Search or jump to...
Simply Simple Notes
List
Boards
Labels
Service Desk
Milestones
Iterations
Merge Requests
Requirements
CI / CD
Security & Compliance
Operations
Packages & Registries
Analytics
Wiki
Snippets
Members
Settings
Collapse sidebar
Issue is populated with vulnerability info
Fern › Simply Simple Notes › Issues › #2
Open
Opened just now by Fern
Maintainer
Close issue
New issue
Investigate vulnerability: Chmod setting a permissive mask 0o777 on file (name).
Description:
Chmod setting a permissive mask 0o777 on file (name).
Severity: high
Confidence: high
Location: notes/db.py:12
Identifiers:
Bandit Test ID B103
Scanner:
Name: Bandit
Type: sast
Status: success
Start Time: 2020-10-19T20:11:22
End Time: 2020-10-19T20:11:22
Only those with permission can see this issue
Linked issues 0
Oldest first
Show all activity
Create confidential merge request
This is a confidential issue. People without permission will never get a notification. Learn more
Write
Preview
Write a comment or drag your files here…
To Do
Add a to do
0 Assignees
Edit
None - assign yourself
Milestone
None
Time tracking
No estimate or time spent
Due date
None
Labels
None
Weight
None
Health status
None
Confidentiality
This issue is confidential
Lock issue
Unlocked
1 participant
Notifications
Reference: fjdiaz/simply-simpl...
Move issue

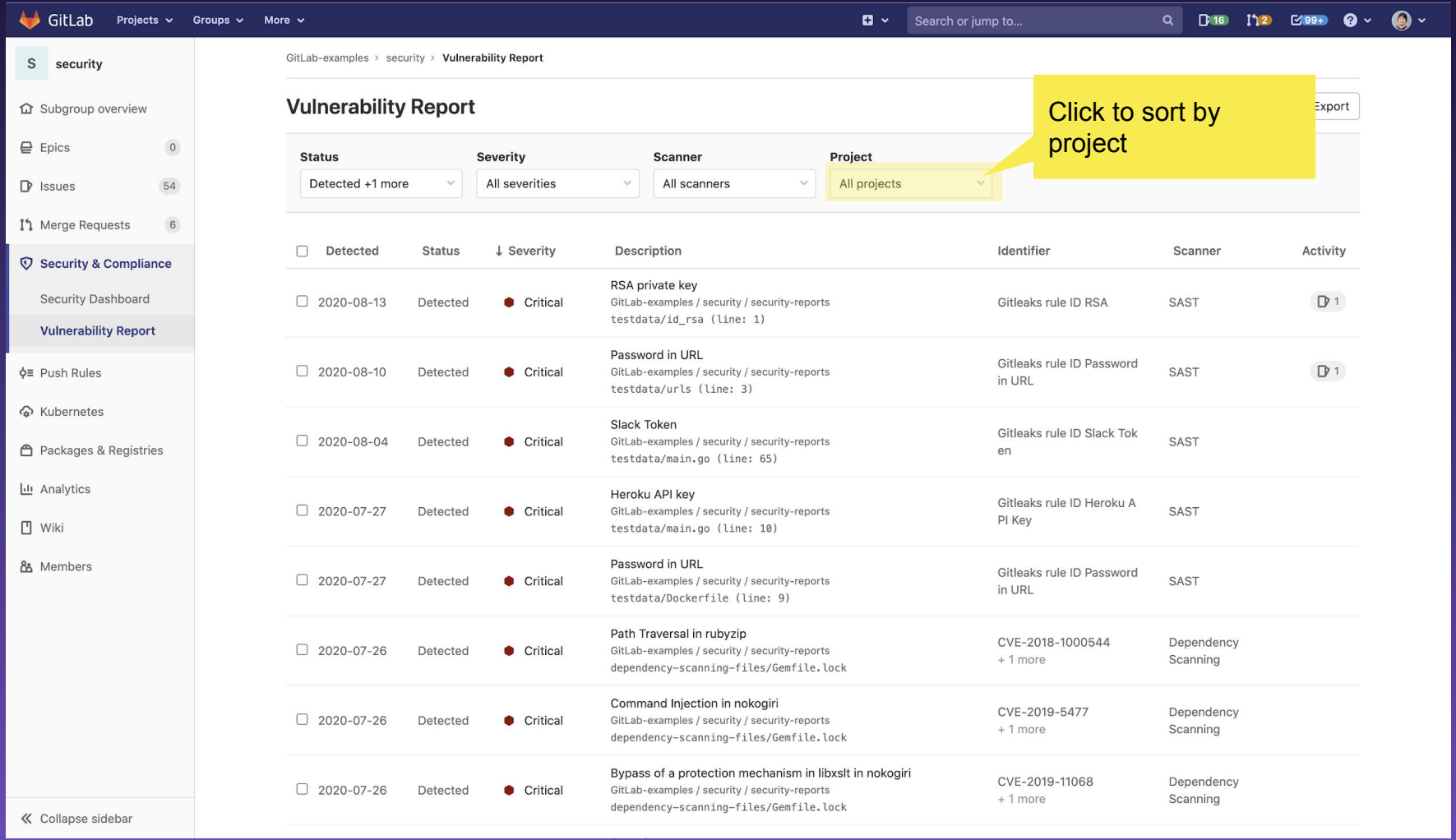

GitLab
Projects
Groups
More
Search or jump to...
Simply Simple Notes
Project overview
Repository
Issues
Merge Requests
Requirements
CI / CD
Security & Compliance
Operations
Packages & Registries
Analytics
Wiki
Snippets
Members
Settings
Collapse sidebar
Fern › Simply Simple Notes › Merge Requests › !2
Open
Opened 4 days ago by Fern
Maintainer
Edit
Mark as draft
Add additional get route
Overview 0
Commits 4
Pipelines 4
Changes 7
Request to merge add-additional-get-… into master
The source branch is 3 commits behind the target branch
Open in Web IDE
Check out branch
Pipeline #202573720 passed for ea304fb1 on add-additional-get-…
Deployed to staging 5 days ago
Requires 2 more approvals from License-Check and Vulnerability-Check.
Collapse
Approvers
Approvals
Commented by
Approved by
Any eligible user
Optional
License-Check
0 of 1
Vulnerability-Check
2 more
0 of 1
Security scanning detected 1 critical and 5 high severity vulnerabilities out of 66.
View full report
Expand
License Compliance detected 1 new license and policy violation; approval required
Manage licenses
View full report
Expand
Merge
You can only merge once this merge request is approved.
You can merge this merge request manually using the command line
0
0
Oldest first
Write
Preview
Write a comment or drag your files here…
To Do
Add a to do
0 Assignees
Edit
None - assign yourself
0 Reviewers
Edit
None
Milestone
Edit
None
Time tracking
No estimate or time spent
Labels
Edit
None
Lock merge request
Edit
Unlocked
1 participant
Notifications
Reference: fjdiaz/simply-simp…
Source branch: add-additio…
Click to expand the license scan results

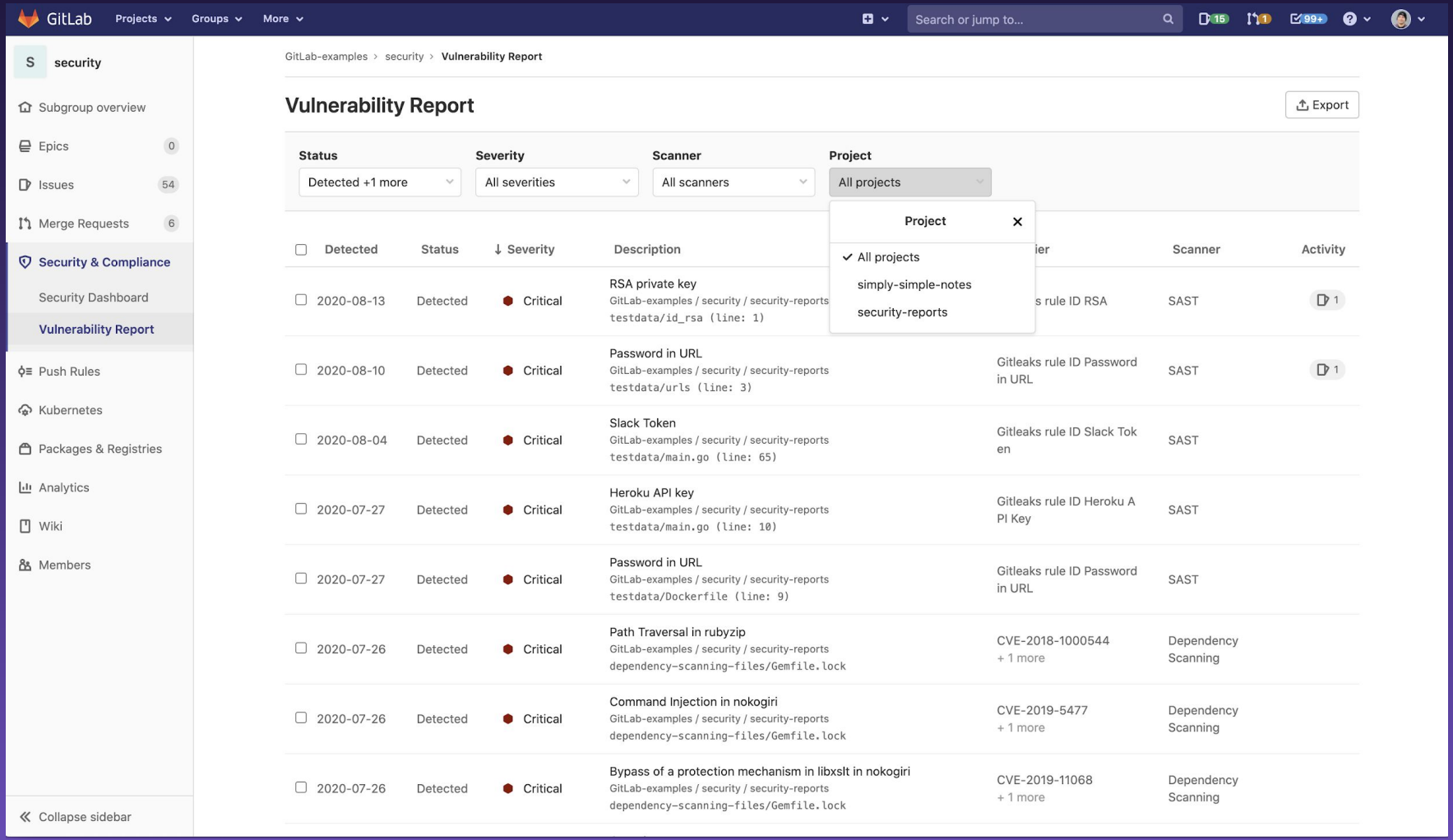

GitLab
Projects
Groups
More
Search or jump to...
Simply Simple Notes
Project overview
Repository
Issues 2
Merge Requests 1
Requirements
CI / CD
Security & Compliance
Operations
Packages & Registries
Analytics
Wiki
Snippets
Members
Settings
Collapse sidebar
Overview 0
Commits 4
Pipelines 5
Changes 7
Pipeline #204808627 passed with warnings for ea304fb1 on add-additional-get-...
Deployed to staging 1 hour ago
Requires 2 more approvals from License-Check and Vulnerability-Check.
Security scanning detecte
View full report
Expand
License Compliance detec
required
View full report
Collapse
Denied
Out-of-compliance with this project's policies and should be removed
Apache License 2.0 Used by kazoo
Merge You can merge after removing denied licenses
Approval is required, because a denied license was detected
0
0
Oldest first
Show all activity
Write
Preview
Write a comment or drag your files here...
Markdown and quick actions are supported
Attach a file
Comment
Close merge request
To Do
Add a to do
0 Assignees
Edit
None - assign yourself
0 Reviewers
Edit
None
Milestone
Edit
None
Time tracking
No estimate or time spent
Labels
Edit
None
Lock merge request
Edit
Unlocked
1 participant
Notifications
Reference: fjdiaz/simply-simpl...
Source branch: add-addition...

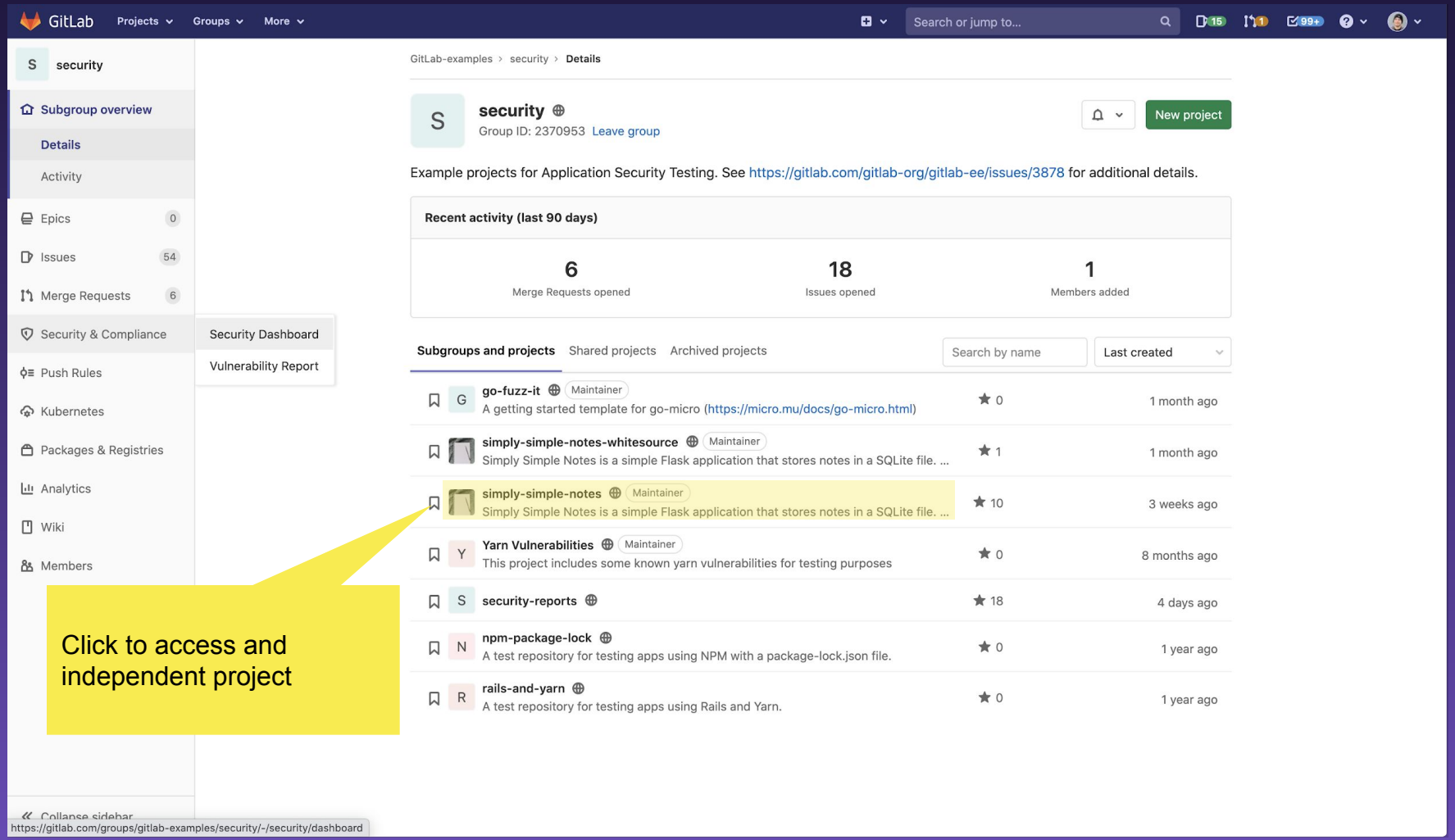
Security Team Workflow

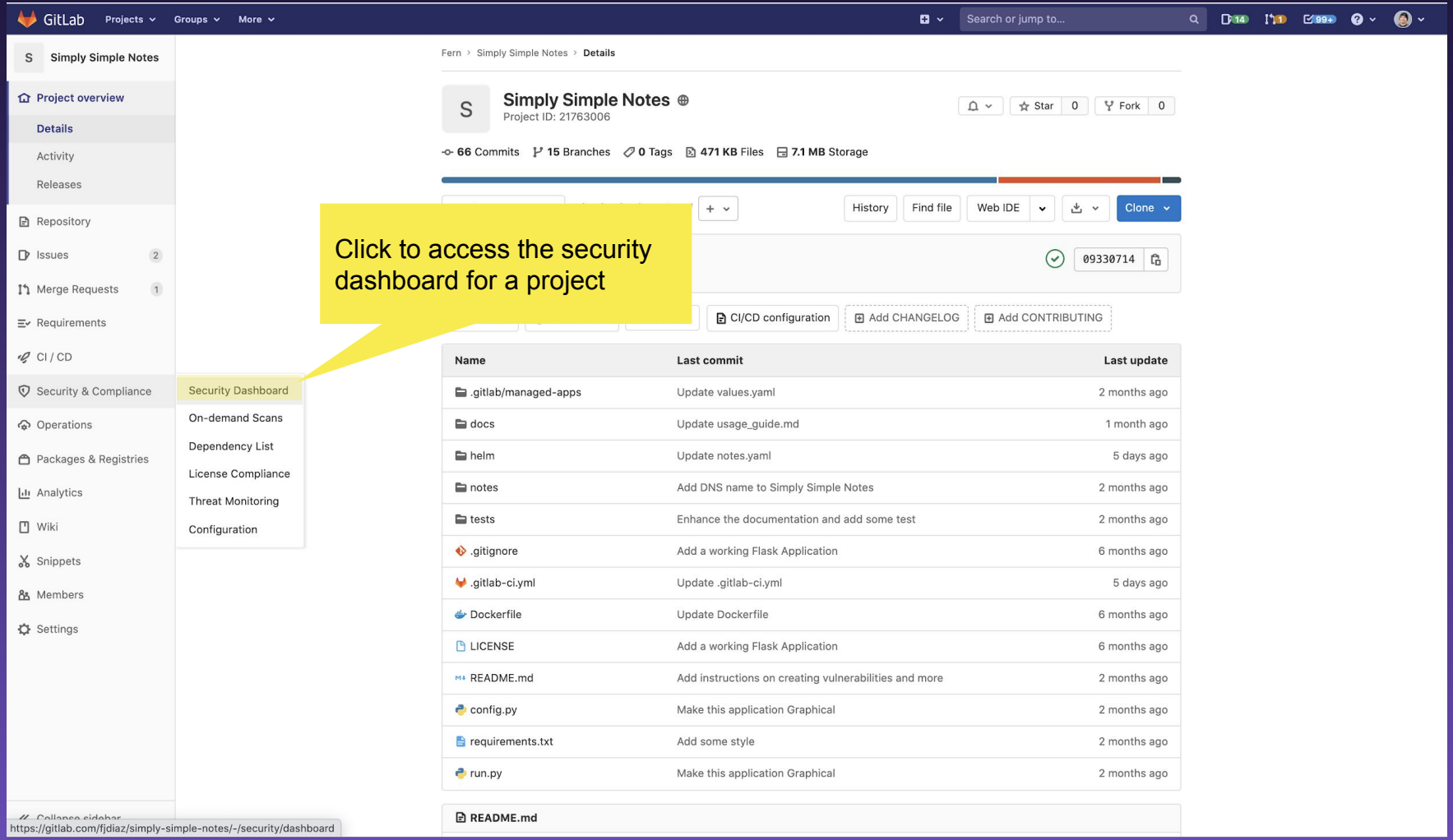

GitLab
Projects
Groups
More
Search or jump to...
S
security
Subgroup overview
Details
Activity
Epics 0
Issues 54
Merge Requests 6
Security & Compliance
Push Rules
Kubernetes
Packages & Registries
Security Dashboard
Vulnerability Report
Click to access the group level security dashboard
GitLab-examples › security › Details
S
security
Group ID: 2370953 Leave group
New project
Example projects for Application Security Testing. See https://gitlab.com/gitlab-org/gitlab-ee/issues/3878 for additional details.
Recent activity (last 90 days)
6
Merge Requests opened
18
Issues opened
1
Members added
Subgroups and projects
Shared projects
Archived projects
Search by name
Last created
go-fuzz-it Maintainer
A getting started template for go-micro (https://micro.mu/docs/go-micro.html)
0
1 month ago
simply-simple-notes-whitesource Maintainer
Simply Simple Notes is a simple Flask application that stores notes in a SQLite file. ...
1
1 month ago
simply-simple-notes Maintainer
Simply Simple Notes is a simple Flask application that stores notes in a SQLite file. ...
10
3 weeks ago
Yarn Vulnerabilities Maintainer
This project includes some known yarn vulnerabilities for testing purposes
0
8 months ago
security-reports
18
4 days ago
npm-package-lock
A test repository for testing apps using NPM with a package-lock.json file.
0
1 year ago
rails-and-yarn
A test repository for testing apps using Rails and Yarn.
0
1 year ago
https://gitlab.com/groups/gitlab-examples/security/-/security/dashboard


GitLab
Projects
Groups
More
Search or jump to...
S
security
Subgroup overview
Epics 0
Issues 54
Merge Requests 6
Security & Compliance
Security Dashboard
Vulnerability Report
Push Rules
Kubernetes
Packages & Rec
Analytics
Wiki
Membe
Collapse sidebar
GitLab-examples › security › Security Dashboa
Security Dashboard
Vulnerabilities over time can be seen here
Vulnerabilities over time
September 20th to today
30 Days
60 Days
90 Days
Severity
%
#
Critical +0% 0
High - 2
Medium - 13
Low - 30
Project security status
Projects are graded based on the highest severity vulnerability present
F 1 project
Critical vulnerabilities present
GitLab-examples / security / security-reports
52 critical
D 1 project
C 0 projects
B 0 projects
A 0 projects
Click to access the vulnerability report
Projects are rated A-F depending on severity of vulnerabilities

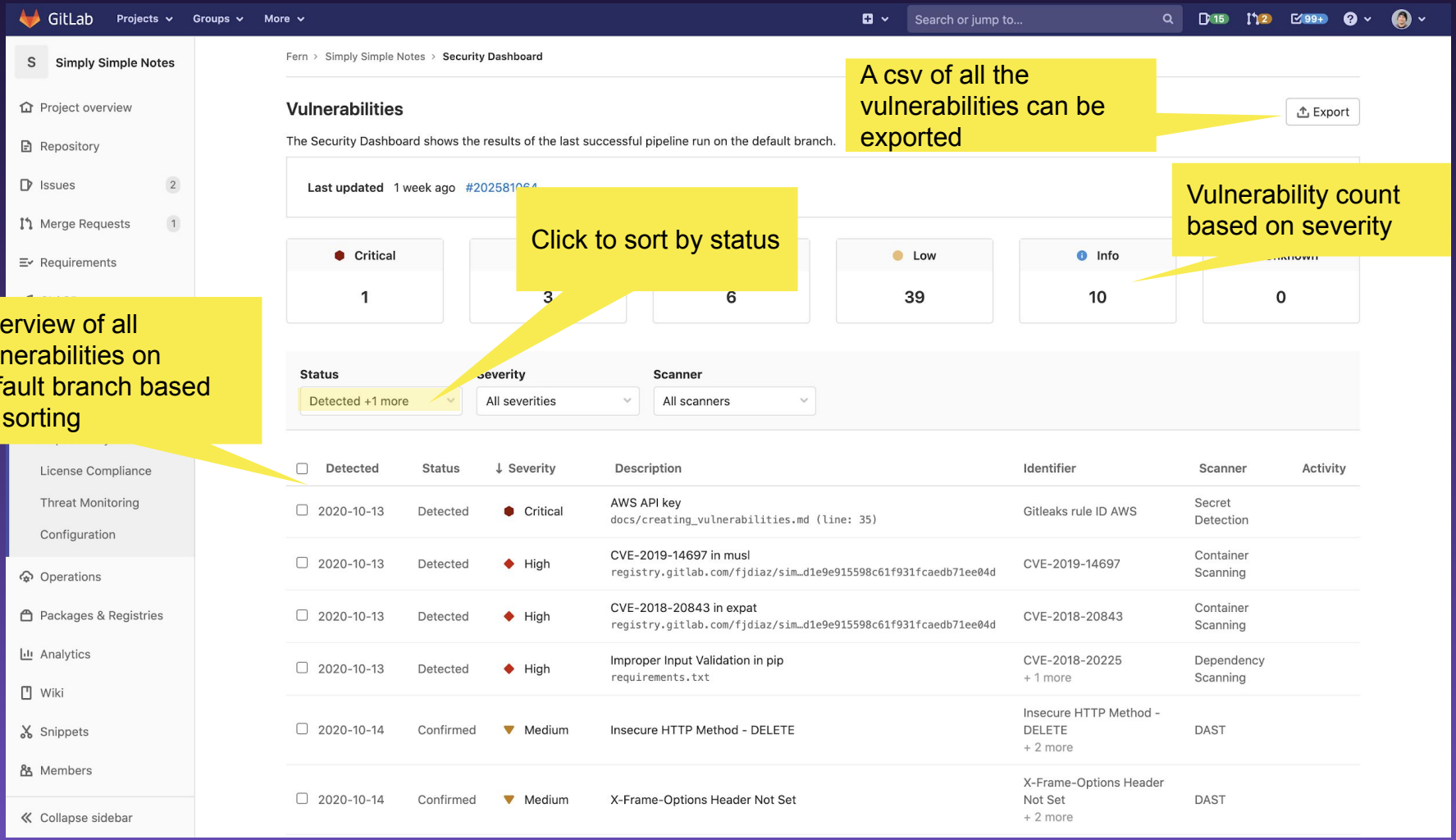

GitLab
Projects
Groups
More
Search or jump to...
16
2
99+
S
security
Subgroup overview
Epics 0
Issues 54
Merge Requests 6
Security & Compliance
Security Dashboard
Vulnerability Report
Push Rules
Kubernetes
Packages & Registries
Analytics
Wiki
Members
Collapse sidebar
GitLab-examples › security › Vulnerability Report
Vulnerability Report
Export
Click to sort by project
Status
Detected +1 more
Severity
All severities
Scanner
All scanners
Project
All projects
Detected
Status
↓ Severity
Description
Identifier
Scanner
Activity
2020-08-13 Detected Critical RSA private key GitLab-examples / security / security-reports testdata/id_rsa (line: 1) Gitleaks rule ID RSA SAST 1
2020-08-10 Detected Critical Password in URL GitLab-examples / security / security-reports testdata/urls (line: 3) Gitleaks rule ID Password in URL SAST 1
2020-08-04 Detected Critical Slack Token GitLab-examples / security / security-reports testdata/main.go (line: 65) Gitleaks rule ID Slack Token SAST
2020-07-27 Detected Critical Heroku API key GitLab-examples / security / security-reports testdata/main.go (line: 10) Gitleaks rule ID Heroku API Key SAST
2020-07-27 Detected Critical Password in URL GitLab-examples / security / security-reports testdata/Dockerfile (line: 9) Gitleaks rule ID Password in URL SAST
2020-07-26 Detected Critical Path Traversal in rubyzip GitLab-examples / security / security-reports dependency-scanning-files/Gemfile.lock CVE-2018-1000544 + 1 more Dependency Scanning
2020-07-26 Detected Critical Command Injection in nokogiri GitLab-examples / security / security-reports dependency-scanning-files/Gemfile.lock CVE-2019-5477 + 1 more Dependency Scanning
2020-07-26 Detected Critical Bypass of a protection mechanism in libxslt in nokogiri GitLab-examples / security / security-reports dependency-scanning-files/Gemfile.lock CVE-2019-11068 + 1 more Dependency Scanning

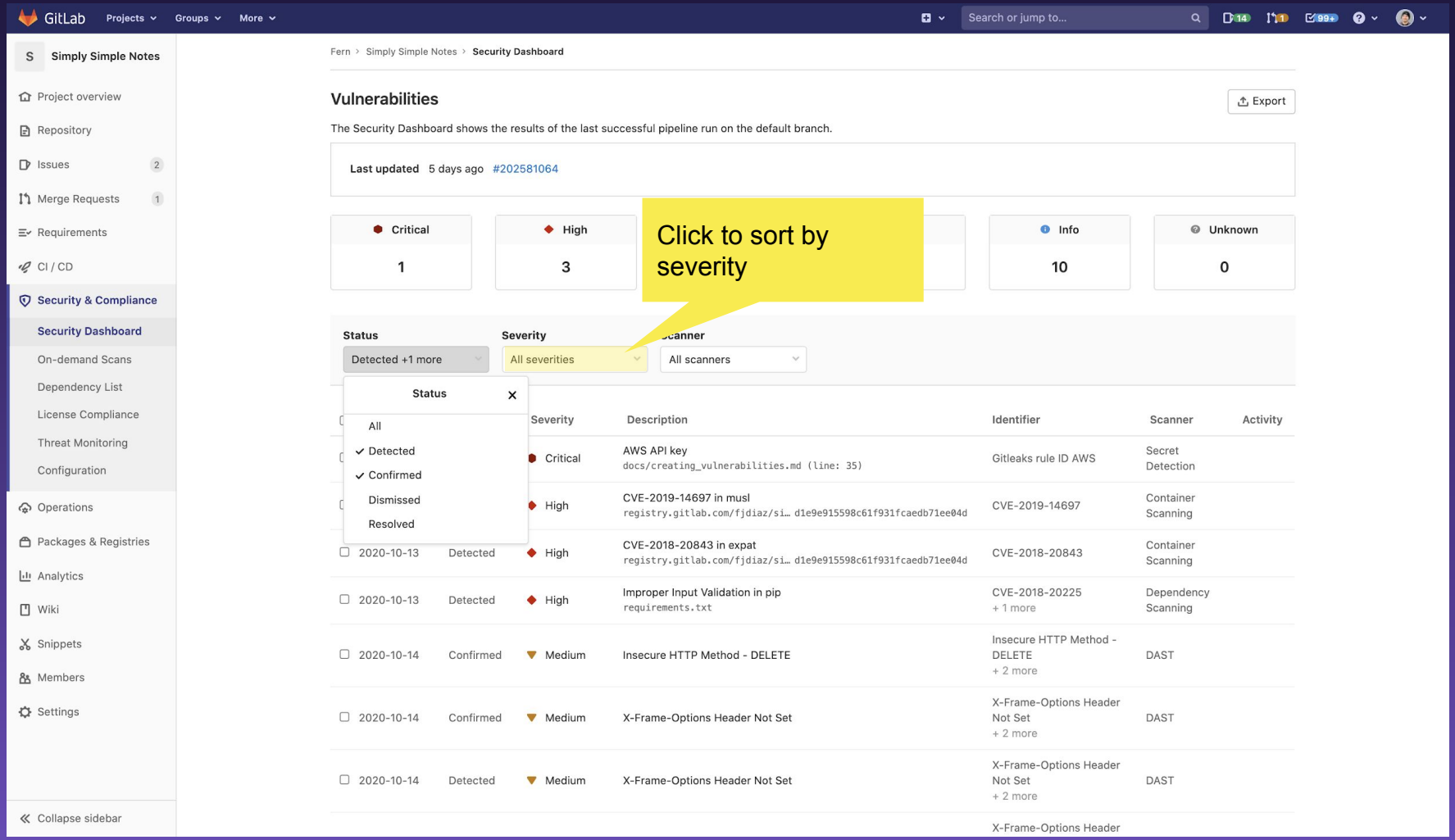

GitLab
Projects
Groups
More
Search or jump to...
15
1
99+
S
security
Subgroup overview
Epics 0
Issues 54
Merge Requests 6
Security & Compliance
Security Dashboard
Vulnerability Report
Push Rules
Kubernetes
Packages & Registries
Analytics
Wiki
Members
Collapse sidebar
GitLab-examples › security › Vulnerability Report
Vulnerability Report
Export
Status
Detected +1 more
Severity
All severities
Scanner
All scanners
Project
All projects
Project
All projects
simply-simple-notes
security-reports
Detected
Status
Severity
Description
Scanner
Activity
2020-08-13 Detected Critical RSA private key GitLab-examples / security / security-reports testdata/id_rsa (line: 1) s rule ID RSA SAST 1
2020-08-10 Detected Critical Password in URL GitLab-examples / security / security-reports testdata/urls (line: 3) Gitleaks rule ID Password in URL SAST 1
2020-08-04 Detected Critical Slack Token GitLab-examples / security / security-reports testdata/main.go (line: 65) Gitleaks rule ID Slack Token SAST
2020-07-27 Detected Critical Heroku API key GitLab-examples / security / security-reports testdata/main.go (line: 10) Gitleaks rule ID Heroku API Key SAST
2020-07-27 Detected Critical Password in URL GitLab-examples / security / security-reports testdata/Dockerfile (line: 9) Gitleaks rule ID Password in URL SAST
2020-07-26 Detected Critical Path Traversal in rubyzip GitLab-examples / security / security-reports dependency-scanning-files/Gemfile.lock CVE-2018-1000544 + 1 more Dependency Scanning
2020-07-26 Detected Critical Command Injection in nokogiri GitLab-examples / security / security-reports dependency-scanning-files/Gemfile.lock CVE-2019-5477 + 1 more Dependency Scanning
2020-07-26 Detected Critical Bypass of a protection mechanism in libxslt in nokogiri GitLab-examples / security / security-reports dependency-scanning-files/Gemfile.lock CVE-2019-11068 + 1 more Dependency Scanning

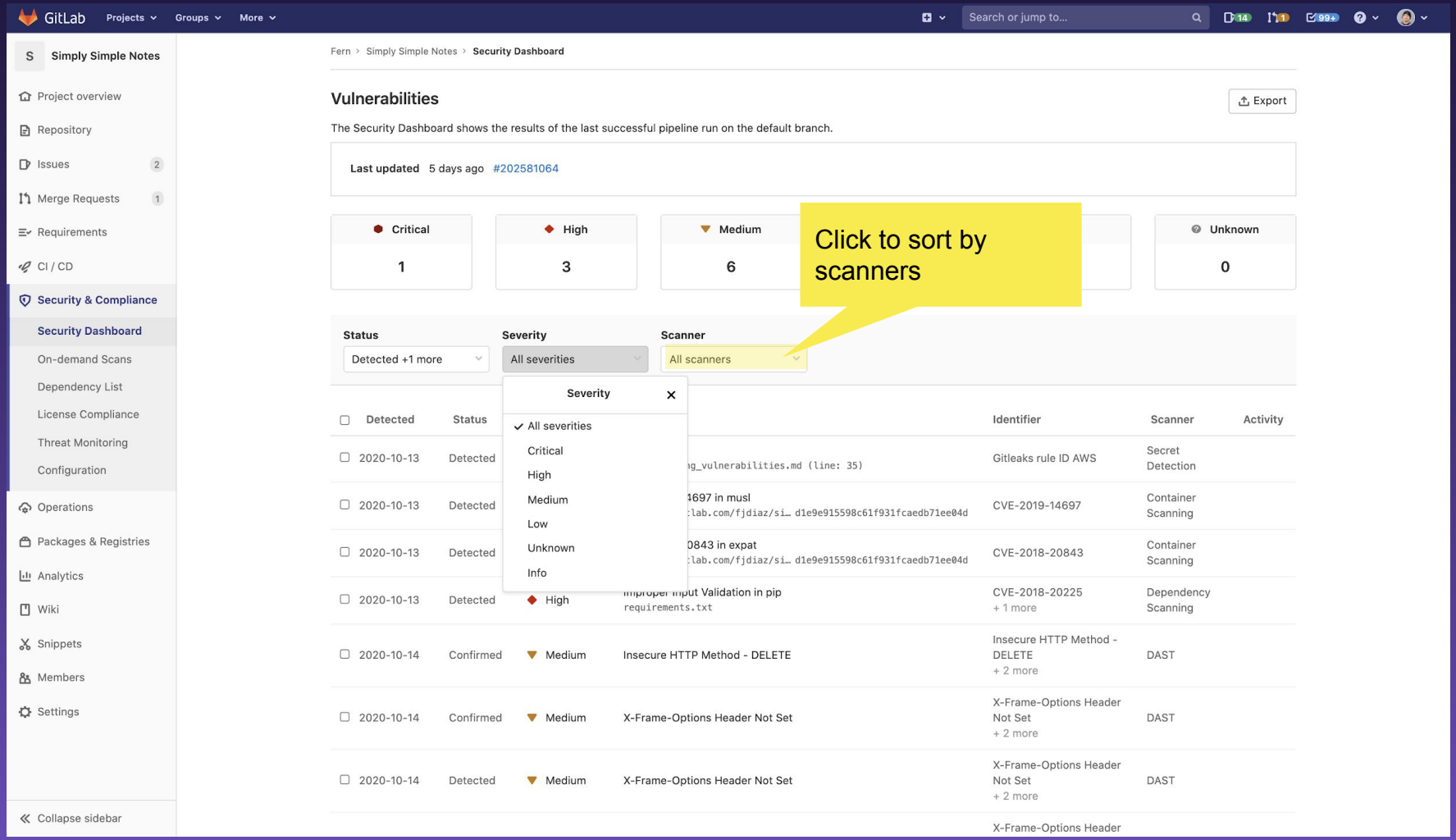

GitLab
Projects
Groups
More
Search or jump to...
S
security
Subgroup overview
Details
Activity
Epics 0
Issues 54
Merge Requests 6
Security & Compliance
Security Dashboard
Vulnerability Report
Push Rules
Kubernetes
Packages & Registries
Analytics
Wiki
Members
Collapse sidebar
https://gitlab.com/groups/gitlab-examples/security/-/security/dashboard
GitLab-examples › security › Details
S
security
Group ID: 2370953 Leave group
New project
Example projects for Application Security Testing. See https://gitlab.com/gitlab-org/gitlab-ee/issues/3878 for additional details.
Recent activity (last 90 days)
6
Merge Requests opened
18
Issues opened
1
Members added
Subgroups and projects
Shared projects
Archived projects
Search by name
Last created
G
go-fuzz-it
Maintainer
A getting started template for go-micro (https://micro.mu/docs/go-micro.html)
0
1 month ago
simply-simple-notes-whitesource
Maintainer
Simply Simple Notes is a simple Flask application that stores notes in a SQLite file. ...
1
1 month ago
simply-simple-notes
Maintainer
Simply Simple Notes is a simple Flask application that stores notes in a SQLite file. ...
10
3 weeks ago
Y
Yarn Vulnerabilities
Maintainer
This project includes some known yarn vulnerabilities for testing purposes
0
8 months ago
S
security-reports
18
4 days ago
N
npm-package-lock
A test repository for testing apps using NPM with a package-lock.json file.
0
1 year ago
R
rails-and-yarn
A test repository for testing apps using Rails and Yarn.
0
1 year ago
Click to access and independent project

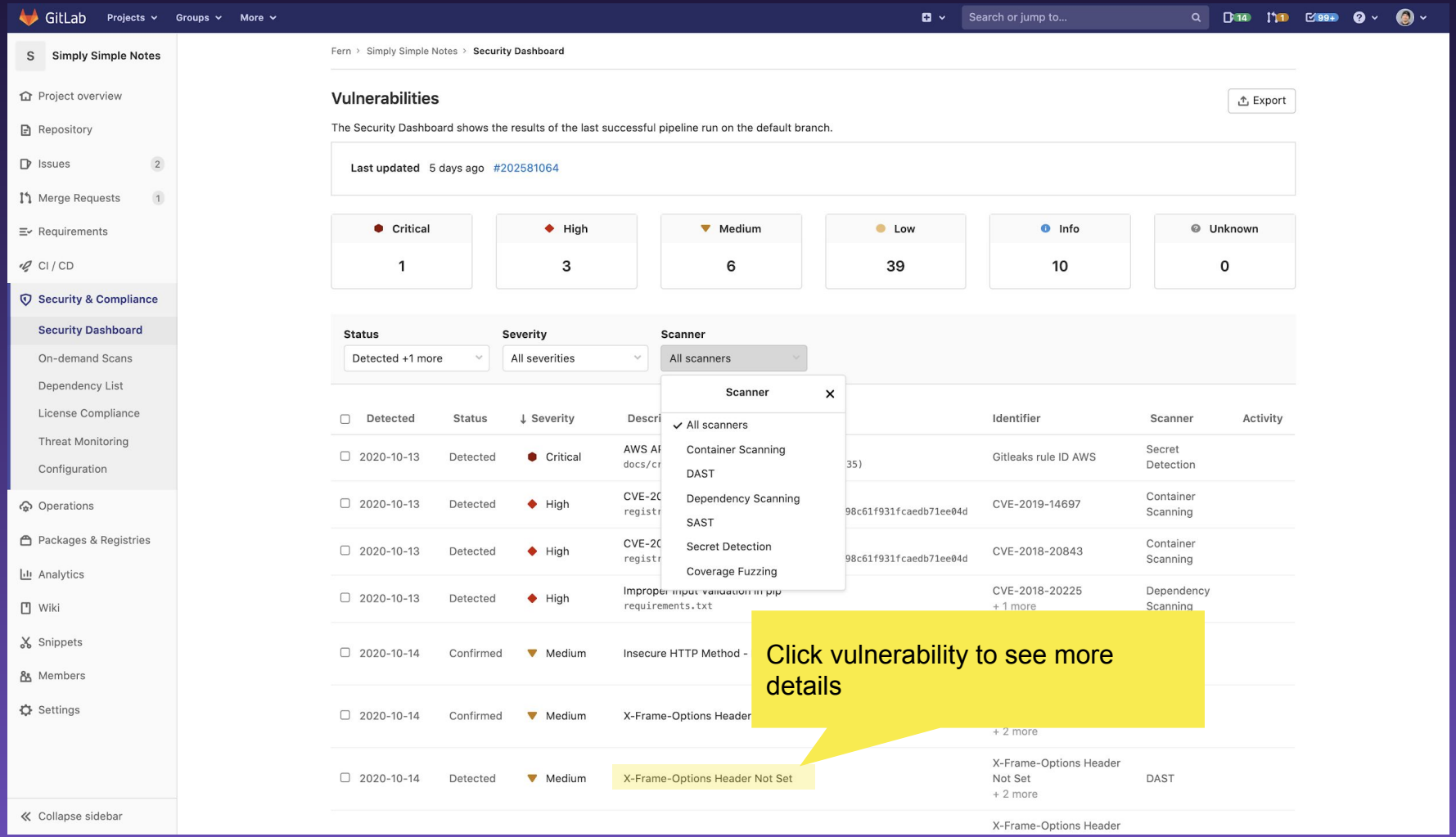


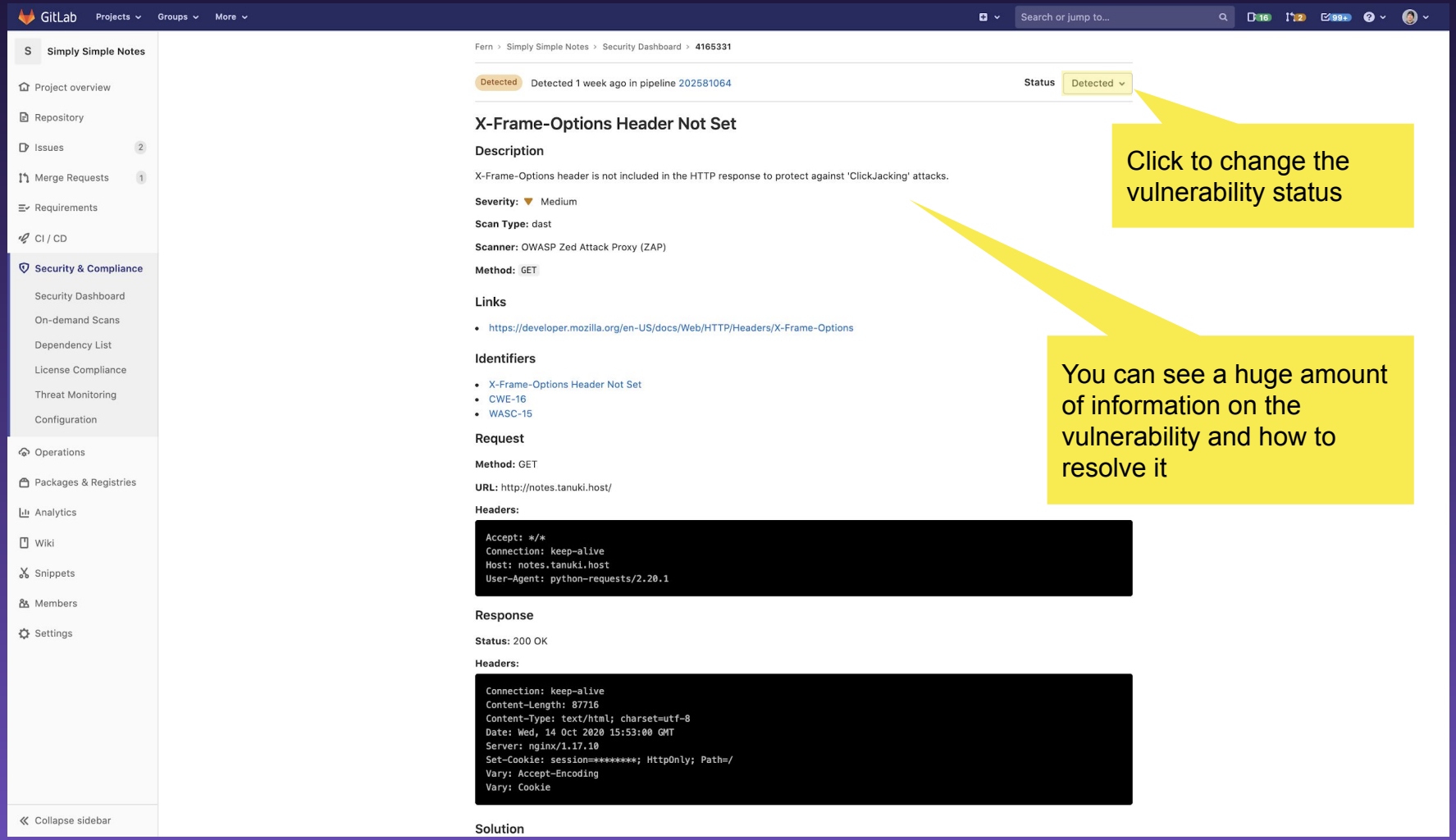
Click to access the security dashboard for a project

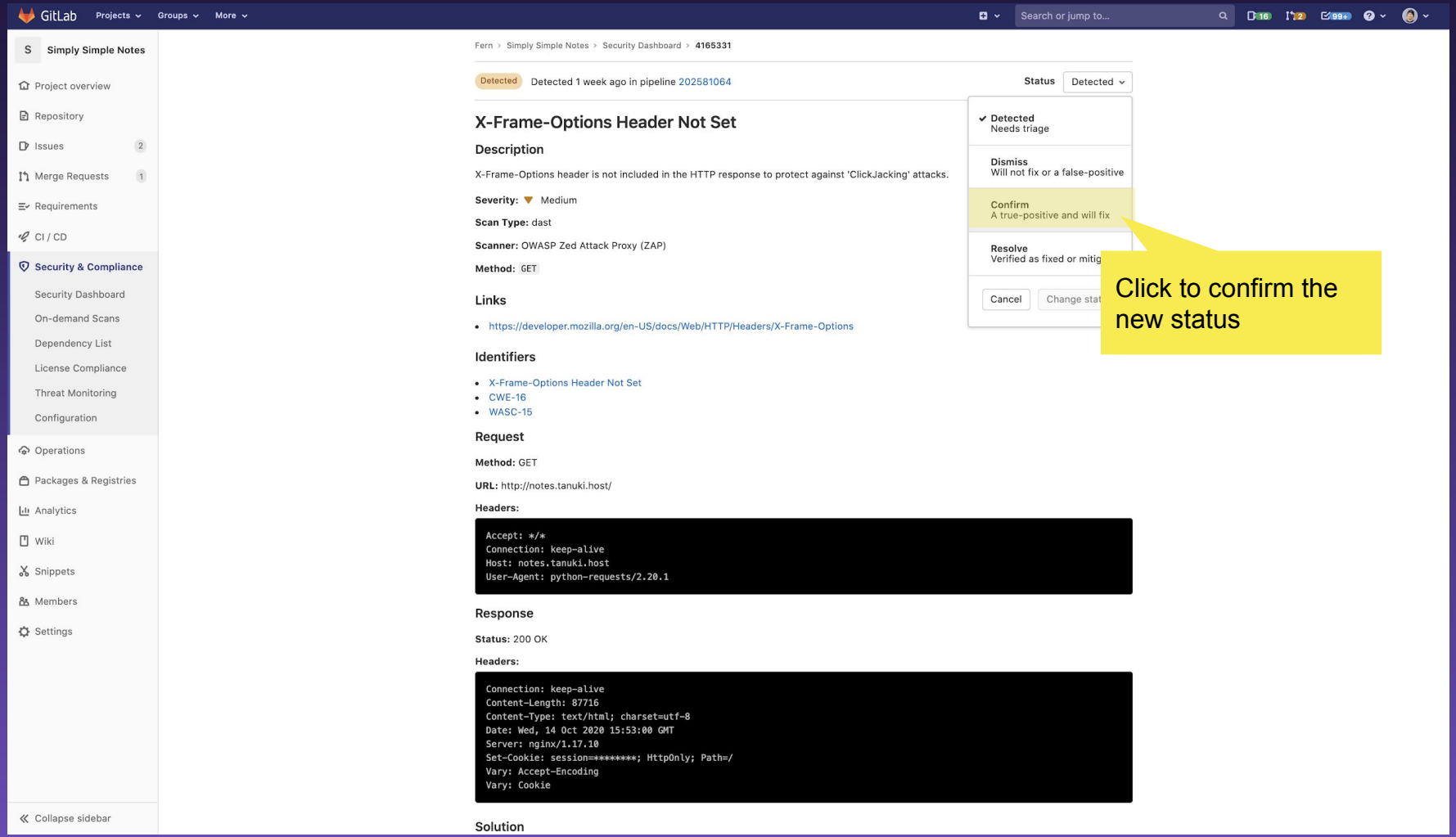

GitLab
Projects
Groups
More
Search or jump to...
Simply Simple Notes
Project overview
Repository
Issues
Merge Requests
Requirements
License Compliance
Threat Monitoring
Configuration
Operations
Packages & Registries
Analytics
Wiki
Snippets
Members
Collapse sidebar
Fern › Simply Simple Notes › Security Dashboard
Vulnerabilities
The Security Dashboard shows the results of the last successful pipeline run on the default branch.
Export
A csv of all the vulnerabilities can be exported
Last updated 1 week ago
Click to sort by status
Vulnerability count based on severity
Critical 1
3
6
Low 39
Info 10
0
Overview of all vulnerabilities on default branch based on sorting
Status
Detected +1 more
Severity
All severities
Scanner
All scanners
Detected
Status
Severity
Description
Identifier
Scanner
Activity
2020-10-13 Detected Critical AWS API key docs/creating_vulnerabilities.md (line: 35) Gitleaks rule ID AWS Secret Detection
2020-10-13 Detected High CVE-2019-14697 in musl registry.gitlab.com/fjdiaz/sim…d1e9e915598c61f931fcaedb71ee04d CVE-2019-14697 Container Scanning
2020-10-13 Detected High CVE-2018-20843 in expat registry.gitlab.com/fjdiaz/sim…d1e9e915598c61f931fcaedb71ee04d CVE-2018-20843 Container Scanning
2020-10-13 Detected High Improper Input Validation in pip requirements.txt CVE-2018-20225 + 1 more Dependency Scanning
2020-10-14 Confirmed Medium Insecure HTTP Method - DELETE Insecure HTTP Method - DELETE + 2 more DAST
2020-10-14 Confirmed Medium X-Frame-Options Header Not Set X-Frame-Options Header Not Set + 2 more DAST

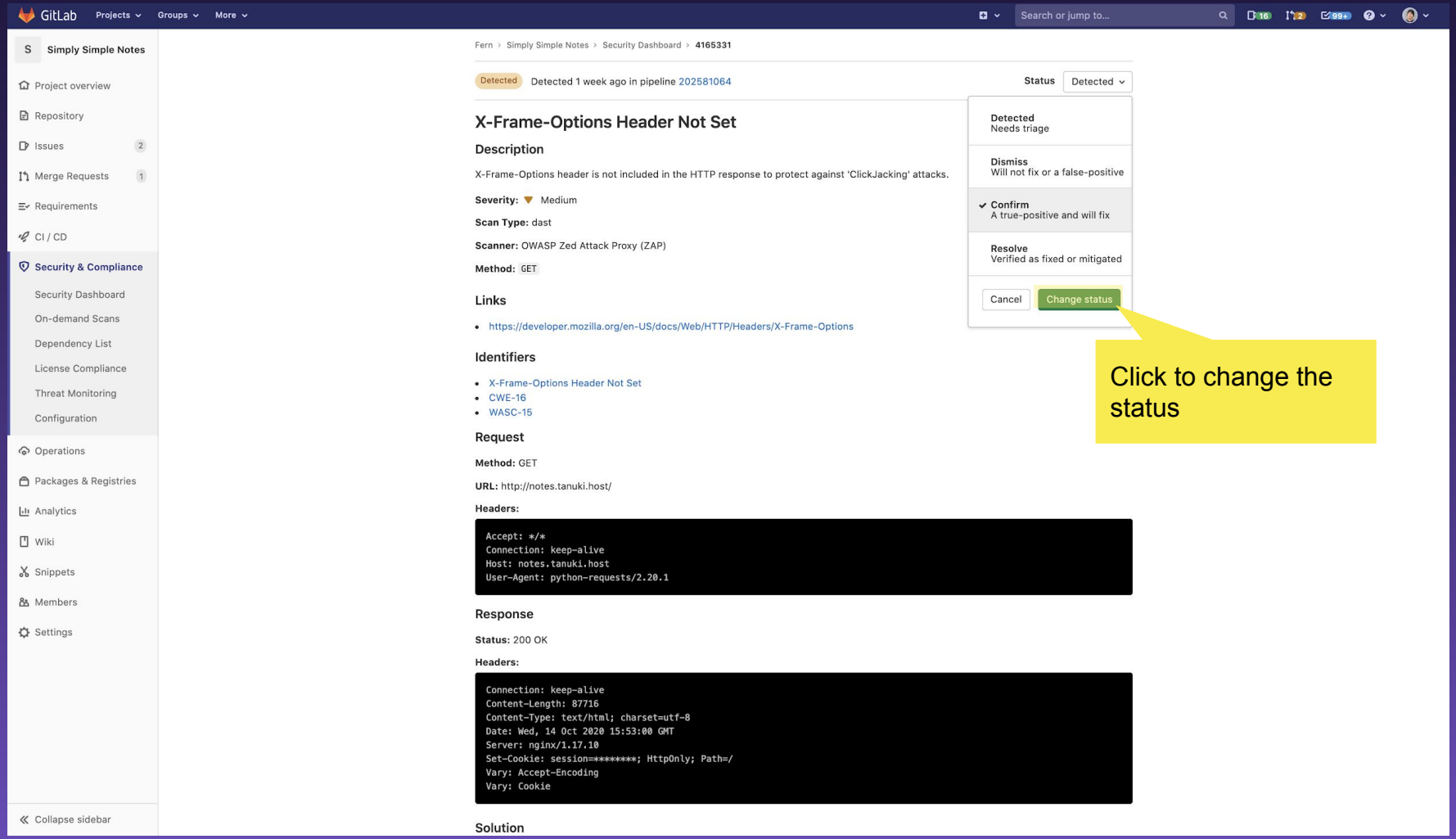

GitLab
Projects
Groups
More
Search or jump to...
Simply Simple Notes
Project overview
Repository
Issues
Merge Requests
Requirements
CI / CD
Security & Compliance
Security Dashboard
On-demand Scans
Dependency List
License Compliance
Threat Monitoring
Configuration
Operations
Packages & Registries
Analytics
Wiki
Snippets
Members
Settings
Collapse sidebar
Fern › Simply Simple Notes › Security Dashboard
Vulnerabilities
Export
The Security Dashboard shows the results of the last successful pipeline run on the default branch.
Last updated 5 days ago #202581064
Critical 1
High 3
Info 10
Unknown 0
Click to sort by severity
Status
Detected +1 more
Severity
All severities
Scanner
All scanners
Status
All
Detected
Confirmed
Dismissed
Resolved
Severity
Description
Identifier
Scanner
Activity
Critical
AWS API key
docs/creating_vulnerabilities.md (line: 35)
Gitleaks rule ID AWS
Secret Detection
High
CVE-2019-14697 in musl
registry.gitlab.com/fjdiaz/si… d1e9e915598c61f931fcaedb71ee04d
CVE-2019-14697
Container Scanning
2020-10-13 Detected High
CVE-2018-20843 in expat
registry.gitlab.com/fjdiaz/si… d1e9e915598c61f931fcaedb71ee04d
CVE-2018-20843
Container Scanning
2020-10-13 Detected High
Improper Input Validation in pip
requirements.txt
CVE-2018-20225
+ 1 more
Dependency Scanning
2020-10-14 Confirmed Medium
Insecure HTTP Method - DELETE
Insecure HTTP Method - DELETE
+ 2 more
DAST
2020-10-14 Confirmed Medium
X-Frame-Options Header Not Set
X-Frame-Options Header Not Set
+ 2 more
DAST
2020-10-14 Detected Medium
X-Frame-Options Header Not Set
X-Frame-Options Header Not Set
+ 2 more
DAST
X-Frame-Options Header

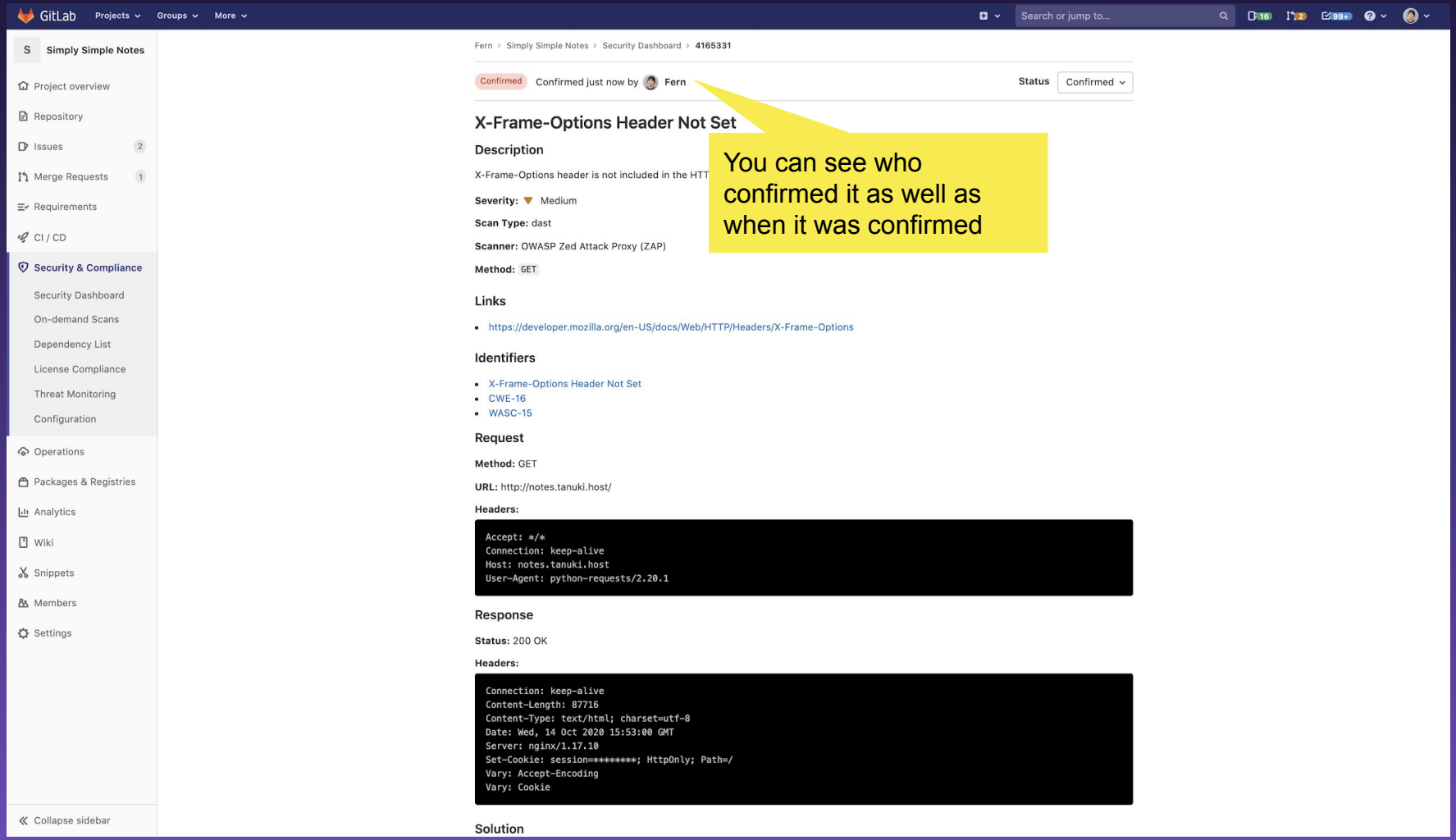

GitLab
Projects
Groups
More
Search or jump to...
Simply Simple Notes
Project overview
Repository
Issues
Merge Requests
Requirements
CI / CD
Security & Compliance
Security Dashboard
On-demand Scans
Dependency List
License Compliance
Threat Monitoring
Configuration
Operations
Packages & Registries
Analytics
Wiki
Snippets
Members
Settings
Collapse sidebar
Fern › Simply Simple Notes › Security Dashboard
Vulnerabilities
Export
The Security Dashboard shows the results of the last successful pipeline run on the default branch.
Last updated 5 days ago #202581064
Critical 1
High 3
Medium 6
Unknown 0
Click to sort by scanners
Status
Detected +1 more
Severity
All severities
Scanner
All scanners
Severity
All severities
Critical
High
Medium
Low
Unknown
Info
Detected
Status
Identifier
Scanner
Activity
2020-10-13 Detected
Gitleaks rule ID AWS
Secret Detection
2020-10-13 Detected
CVE-2019-14697
Container Scanning
2020-10-13 Detected
CVE-2018-20843
Container Scanning
2020-10-13 Detected High
CVE-2018-20225
+ 1 more
Dependency Scanning
requirements.txt
2020-10-14 Confirmed Medium
Insecure HTTP Method - DELETE
Insecure HTTP Method - DELETE
+ 2 more
DAST
2020-10-14 Confirmed Medium
X-Frame-Options Header Not Set
X-Frame-Options Header Not Set
+ 2 more
DAST
2020-10-14 Detected Medium
X-Frame-Options Header Not Set
X-Frame-Options Header Not Set
+ 2 more
DAST


GitLab
Projects
Groups
More
Search or jump to...
Simply Simple Notes
Project overview
Repository
Issues 2
Merge Requests 1
Requirements
CI / CD
Security & Compliance
Security Dashboard
On-demand Scans
Dependency List
License Compliance
Threat Monitoring
Configuration
Operations
Packages & Registries
Analytics
Wiki
Snippets
Members
Settings
Collapse sidebar
Fern › Simply Simple Notes › Security Dashboard
Vulnerabilities
Export
The Security Dashboard shows the results of the last successful pipeline run on the default branch.
Last updated 5 days ago #202581064
Critical 1
High 3
Medium 6
Low 39
Info 10
Unknown 0
Status
Detected +1 more
Severity
All severities
Scanner
All scanners
Scanner
All scanners
Container Scanning
DAST
Dependency Scanning
SAST
Secret Detection
Coverage Fuzzing
Detected
Status
Severity
Identifier
Scanner
Activity
2020-10-13 Detected Critical Gitleaks rule ID AWS Secret Detection
2020-10-13 Detected High CVE-2019-14697 Container Scanning
2020-10-13 Detected High CVE-2018-20843 Container Scanning
2020-10-13 Detected High CVE-2018-20225 + 1 more Dependency Scanning
2020-10-14 Confirmed Medium Insecure HTTP Method -
2020-10-14 Confirmed Medium X-Frame-Options Header
+ 2 more
2020-10-14 Detected Medium X-Frame-Options Header Not Set
X-Frame-Options Header Not Set + 2 more DAST
X-Frame-Options Header
Click vulnerability to see more details


GitLab
Projects
Groups
More
Search or jump to...
Simply Simple Notes
Project overview
Repository
Issues
Merge Requests
Requirements
CI / CD
Security & Compliance
Security Dashboard
On-demand Scans
Dependency List
License Compliance
Threat Monitoring
Configuration
Operations
Packages & Registries
Analytics
Wiki
Snippets
Members
Settings
Collapse sidebar
Fern › Simply Simple Notes › Security Dashboard › 4165331
Detected
Detected 1 week ago in pipeline 202581064
Status
Detected
X-Frame-Options Header Not Set
Description
X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
Severity: Medium
Scan Type: dast
Scanner: OWASP Zed Attack Proxy (ZAP)
Method: GET
Links
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
Identifiers
X-Frame-Options Header Not Set
CWE-16
WASC-15
Request
Method: GET
URL: http://notes.tanuki.host/
Headers:
Accept: */*
Connection: keep-alive
Host: notes.tanuki.host
User-Agent: python-requests/2.20.1
Response
Status: 200 OK
Headers:
Connection: keep-alive
Content-Length: 87716
Content-Type: text/html; charset=utf-8
Date: Wed, 14 Oct 2020 15:53:00 GMT
Server: nginx/1.17.10
Set-Cookie: session=********; HttpOnly; Path=/
Vary: Accept-Encoding
Vary: Cookie
Solution
Click to change the vulnerability status
You can see a huge amount of information on the vulnerability and how to resolve it


GitLab
Projects
Groups
More
Search or jump to...
Simply Simple Notes
Project overview
Repository
Issues
Merge Requests
Requirements
CI / CD
Security & Compliance
Security Dashboard
On-demand Scans
Dependency List
License Compliance
Threat Monitoring
Configuration
Operations
Packages & Registries
Analytics
Wiki
Snippets
Members
Settings
Collapse sidebar
Fern › Simply Simple Notes › Security Dashboard › 4165331
Detected
Detected 1 week ago in pipeline 202581064
Status
Detected
Detected
Needs triage
Dismiss
Will not fix or a false-positive
Confirm
A true-positive and will fix
Resolve
Verified as fixed or mitig
Cancel
Change stat
Click to confirm the new status
X-Frame-Options Header Not Set
Description
X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
Severity: Medium
Scan Type: dast
Scanner: OWASP Zed Attack Proxy (ZAP)
Method: GET
Links
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
Identifiers
X-Frame-Options Header Not Set
CWE-16
WASC-15
Request
Method: GET
URL: http://notes.tanuki.host/
Headers:
Accept: */*
Connection: keep-alive
Host: notes.tanuki.host
User-Agent: python-requests/2.20.1
Response
Status: 200 OK
Headers:
Connection: keep-alive
Content-Length: 87716
Content-Type: text/html; charset=utf-8
Date: Wed, 14 Oct 2020 15:53:00 GMT
Server: nginx/1.17.10
Set-Cookie: session=********; HttpOnly; Path=/
Vary: Accept-Encoding
Vary: Cookie
Solution


GitLab
Projects
Groups
More
Search or jump to...
Simply Simple Notes
Project overview
Repository
Issues
Merge Requests
Requirements
CI / CD
Security & Compliance
Security Dashboard
On-demand Scans
Dependency List
License Compliance
Threat Monitoring
Configuration
Operations
Packages & Registries
Analytics
Wiki
Snippets
Members
Settings
Collapse sidebar
Fern › Simply Simple Notes › Security Dashboard › 4165331
Detected
Detected 1 week ago in pipeline 202581064
Status
Detected
Detected
Needs triage
Dismiss
Will not fix or a false-positive
Confirm
A true-positive and will fix
Resolve
Verified as fixed or mitigated
Cancel
Change status
X-Frame-Options Header Not Set
Description
X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
Severity: Medium
Scan Type: dast
Scanner: OWASP Zed Attack Proxy (ZAP)
Method: GET
Links
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
Identifiers
X-Frame-Options Header Not Set
CWE-16
WASC-15
Request
Method: GET
URL: http://notes.tanuki.host/
Headers:
Accept: */*
Connection: keep-alive
Host: notes.tanuki.host
User-Agent: python-requests/2.20.1
Response
Status: 200 OK
Headers:
Connection: keep-alive
Content-Length: 87716
Content-Type: text/html; charset=utf-8
Date: Wed, 14 Oct 2020 15:53:00 GMT
Server: nginx/1.17.10
Set-Cookie: session=********; HttpOnly; Path=/
Vary: Accept-Encoding
Vary: Cookie
Solution
Click to change the status


GitLab
Projects
Groups
More
Search or jump to...
Simply Simple Notes
Project overview
Repository
Issues
Merge Requests
Requirements
CI / CD
Security & Compliance
Security Dashboard
On-demand Scans
Dependency List
License Compliance
Threat Monitoring
Configuration
Operations
Packages & Registries
Analytics
Wiki
Snippets
Members
Settings
Collapse sidebar
Fern › Simply Simple Notes › Security Dashboard › 4165331
Confirmed
Confirmed just now by Fern
Status
Confirmed
X-Frame-Options Header Not Set
Description
X-Frame-Options header is not included in the HTT
Severity: Medium
Scan Type: dast
Scanner: OWASP Zed Attack Proxy (ZAP)
Method: GET
Links
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
Identifiers
X-Frame-Options Header Not Set
CWE-16
WASC-15
Request
Method: GET
URL: http://notes.tanuki.host/
Headers:
Accept: */*
Connection: keep-alive
Host: notes.tanuki.host
User-Agent: python-requests/2.20.1
Response
Status: 200 OK
Headers:
Connection: keep-alive
Content-Length: 87716
Content-Type: text/html; charset=utf-8
Date: Wed, 14 Oct 2020 15:53:00 GMT
Server: nginx/1.17.10
Set-Cookie: session=********; HttpOnly; Path=/
Vary: Accept-Encoding
Vary: Cookie
Solution
You can see who confirmed it as well as when it was confirmed

Q&A