



---

# GitLab Security Scanning & Management

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

# Agenda



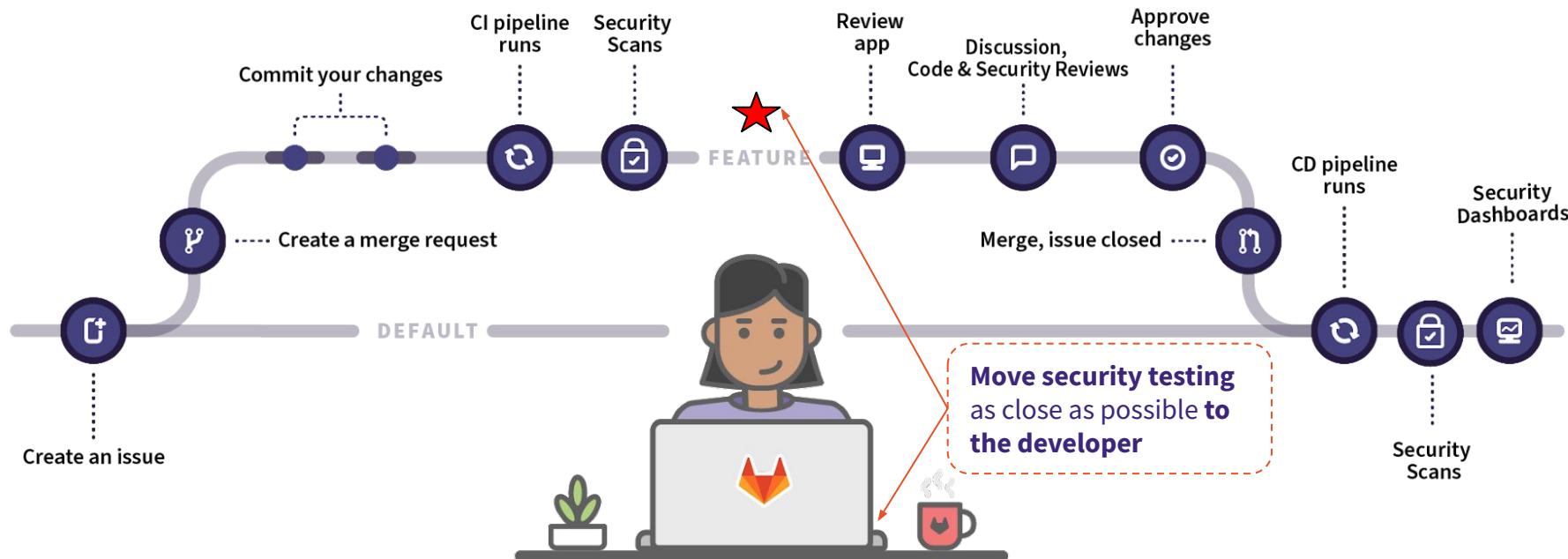
- GitLab as a DevSecOps tool
- What GitLab Offers
  - Available Scanners
  - Dashboard & Vulnerability Management
- Developer Workflow
- Security Workflow
- Q&A



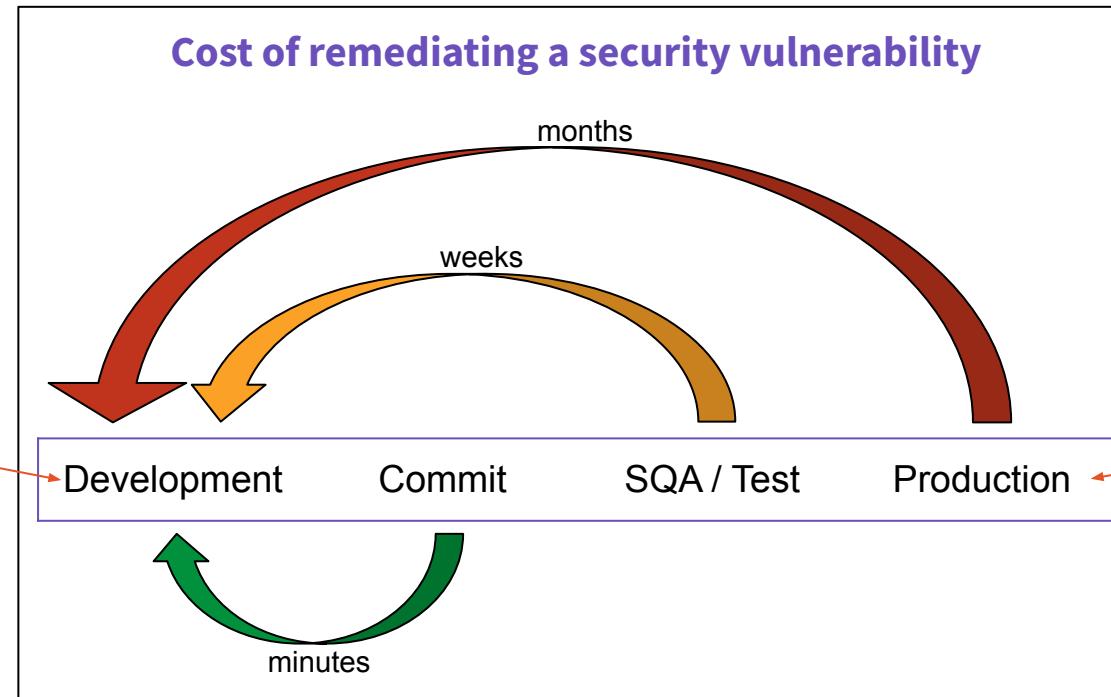
---

# 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/>

Security scanning detected **1 critical** and **4 high** severity vulnerabilities out of 22.  
Security report is out of date. Please update your branch with the latest changes from the target branch (master)

SAST detected no vulnerabilities.

Dependency scanning detected **1 critical** and **4 high** severity vulnerabilities out of 19.

New

- Critical Prototype pollution attack in extend
- High growl\_command\_injection in growl
- High A prototype pollution vulnerability in handlebars may lead to remote code execution if an attacker can control the template in handle...
- High A prototype pollution vulnerability in handlebars may lead to remote code execution if an attacker can control the template in handle...
- High Prototype pollution attack in mixin\_deep

Container scanning detected no vulnerabilities.

DAST detected 3 vulnerabilities.

New

- Low Web-Browser XSS Protection Not Enabled
- Low X-Content-Type-Options Header Missing
- Low X-Content-Type-Options Header Missing

License Compliance detected 3 licenses and policy violations for the source branch only

Denied  
Out-of-compliance with this project's policies and should be removed

- ✗ LGPL Used by sidekiq

Uncategorized  
No policy matches this license

- MIT Used by bundler, concurrent-ruby, connection\_pool, and 10 more

Allowed  
Acceptable for use in this project

- ✓ New BSD Used by pg, and puma

Merge You can merge after removing denied licenses



---

## Available Security Scanners

# GitLab Security and Compliance Scanners



SAST	Static Application Security Testing: Detects vulnerabilities in source code. (e.g. SQL Injection, XSS)	Infrastructure as Code (IaC) Scanning	Scans IaC configuration files (Terraform, Ansible, CloudFormation, Kubernetes) for known vulnerabilities
Dependency Scanning	Detects <b>known</b> vulnerabilities in libraries/components (e.g. CVE 2021-45046 in Apache log4j)	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++)
Secret Detection	Detects credentials/secrets/passwords in source code to prevent sensitive information leakage. (e.g. AWS Key)	DAST	Dynamic Application Security Testing: Analyzes your running web application for runtime vulnerabilities leveraging the Review App. (e.g. CSRF, XSS)
License Compliance	Searches for approved and disallowed licenses defined by custom policies. (e.g. AGPL License)	Web API Fuzz	Detects unexpected behaviors of running Web applications by generating random requests to the Web APIs. (e.g. 500 INTERNAL SERVER ERROR)
Container Scanning	Detects <b>known</b> vulnerabilities in container images (e.g. Heartbleed, ShellShock)		

Static Scan

Runtime Scan

Dynamic Scan

# Static Application Security Testing (SAST)



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

- 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

⚠ SAST detected **2 new critical** severity vulnerabilities out of 3. ?

## New

- Critical [ECB mode is insecure](#)
- Critical [Predictable pseudorandom number generator](#)
- ▼ Medium [Injection Vulnerability in puma](#)

[https://docs.gitlab.com/ee/user/application\\_security/sast/](https://docs.gitlab.com/ee/user/application_security/sast/)

# Dynamic Application Security Testing (DAST)



**OWASP ZAP**

- 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 ZAPProxy, 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/](https://docs.gitlab.com/ee/user/application_security/dast/)

# Secrets Detection



! Secret scanning detected **3 new critical** severity vulnerabilities. ?

## New

- Critical Password in URL in dir/sub-dir/file.gl
- Critical Password in URL in dir/sub-dir/file.gl
- Critical Password in URL in dir/sub-dir/file.gl

```
[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/](https://docs.gitlab.com/ee/user/application_security/secret_detection/)

# Dependency Scanning



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

- 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

! Dependency scanning detected **10 new critical** and **22 new high** severity vulnerabilities out of 72. ?

## New

- Critical [Bypass of a protection mechanism in libxslt in nokogiri](#)
- Critical [Command Injection in nokogiri](#)
- Critical [Improper Input Validation in rails](#)
- Critical [Path Traversal in rubyzip](#)
- Critical [Insufficient Entropy in cryptiles](#)

[https://docs.gitlab.com/ee/user/application\\_security/dependency\\_scanning/](https://docs.gitlab.com/ee/user/application_security/dependency_scanning/)

# Dependency List



Screenshot of the GitLab Dependency List interface for the project "Awesome project". The interface shows a table of dependencies with columns: Component, Packager, Location, License, and Severity (with a count of vulnerabilities detected). Key findings include:

Component	Packager	Location	License	Vulnerabilities
ffi 1.9.21	Ruby (Bundler)	Gemfile.lock	BSD 3-Clause "New" or "Revised" License	1 vulnerability detected
nokogiri 1.8.2	Ruby (Bundler)	Gemfile.lock	MIT License	9 vulnerabilities detected
puma 3.11.2	Ruby (Bundler)	Gemfile.lock	BSD 3-Clause "New" or "Revised" License	3 vulnerabilities detected
◆ High	Keepalive thread overload/DoS in puma			
● Unknown	HTTP Response Splitting vulnerability in puma			
● Unknown	Injection Vulnerability in puma			
rake 12.3.0	Ruby (Bundler)	Gemfile.lock	MIT License	1 vulnerability detected
actionview 5.0.0	Ruby (Bundler)	Gemfile.lock	MIT License	4 vulnerabilities detected
activejob 5.0.0	Ruby (Bundler)	Gemfile.lock	MIT License	1 vulnerability detected
loofah 2.2.0	Ruby (Bundler)	Gemfile.lock	MIT License	3 vulnerabilities detected
rack 2.0.4	Ruby (Bundler)	Gemfile.lock	MIT License	3 vulnerabilities detected
rails 5.0.0	Ruby (Bundler)	Gemfile.lock	MIT License	4 vulnerabilities detected
rails-html-sanitizer 1.0.3	Ruby (Bundler)	Gemfile.lock	MIT License	1 vulnerability detected
rubyzip 1.2.1	Ruby (Bundler)	Gemfile.lock		2 vulnerabilities detected
sprockets 3.7.1	Ruby (Bundler)	Gemfile.lock	MIT License	1 vulnerability detected
axios 0.17.1	JavaScript (Yarn)	yarn.lock		1 vulnerability detected
dot-prop 4.2.0	JavaScript (Yarn)	yarn.lock		1 vulnerability detected
eslint-utils 1.3.1	JavaScript (Yarn)	yarn.lock		1 vulnerability detected

- 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/](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/](https://docs.gitlab.com/ee/user/application_security/container_scanning/)

# License Compliance



Language	Package Managers	Scan Tool
JavaScript	<a href="#">Bower</a> , <a href="#">npm</a> , <a href="#">yarn (experimental support)</a>	<a href="#">License Finder</a>
Go	<a href="#">Godep</a> , <a href="#">go mod</a>	<a href="#">License Finder</a>
Java	<a href="#">Gradle</a> , <a href="#">Maven</a>	<a href="#">License Finder</a>
.NET	<a href="#">Nuget</a>	<a href="#">License Finder</a>
Python	<a href="#">pip</a>	<a href="#">License Finder</a>
Ruby	<a href="#">gem</a>	<a href="#">License Finder</a>

- 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/](https://docs.gitlab.com/ee/user/application_security/license_management/)

# Fuzz Testing



Language	Fuzzing Engine	Example
C/C++	<a href="#">libFuzzer</a>	<a href="#">c-cpp-example</a>
GoLang	<a href="#">go-fuzz (libFuzzer support)</a>	<a href="#">go-fuzzing-example</a>
Swift	<a href="#">libFuzzer</a>	<a href="#">swift-fuzzing-example</a>
Rust	<a href="#">cargo-fuzz (libFuzzer support)</a>	<a href="#">rust-fuzzing-example</a>
Java	<a href="#">JavaFuzz (recommended), JOF (not preferred)</a>	<a href="#">javafuzz-fuzzing-example</a> , <a href="#">jof-fuzzing-example</a>
JavaScript	<a href="#">jsfuzz</a>	<a href="#">jsfuzz-fuzzing-example</a>
Python	<a href="#">pythonfuzz</a>	<a href="#">pythonfuzz-fuzzing-example</a>
AFL (any language that works on top of AFL)	<a href="#">AFL</a>	<a href="#">afl-fuzzing-example</a>

- 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/coverage_fuzzing/)

[https://docs.gitlab.com/ee/user/application\\_security/api\\_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	High	Access Control	ECS Services must not have Admin roles, which means the attribute 'iam_role' must not be an admin role	<a href="#">Documental</a>
EFS With Vulnerable Policy	High	Access Control	EFS (Elastic File System) policy should avoid wildcard in 'Action' and 'Principal'.	<a href="#">Documental</a>
S3 Bucket Allows WriteACP Action From All Principals	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.	<a href="#">Documental</a>

- 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/](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

[Pipeline](#) [Needs](#) [Jobs 14](#) [Tests 0](#) [Security](#) [Licenses 6](#)

**Scan details** Hide details

Scanner	Vulnerabilities
DAST	12 vulnerabilities ( <a href="#">Download scanned resources</a> )
SAST	64 vulnerabilities
Container Scanning	167 vulnerabilities
Dependency Scanning	55 vulnerabilities

**Severity** Hide dismissed  **Scanner**

All severities	All scanners
<input type="checkbox"/> Severity	Vulnerability
<input type="checkbox"/> Critical	Improper Input Validation in rails dependency-scanning-files/Gemfile.lock
<input type="checkbox"/> Critical	eval with argument of type Identifier src/html/index.html
<input type="checkbox"/> Critical	Generic Object Injection Sink src/html/index.html

Identifier Scanner

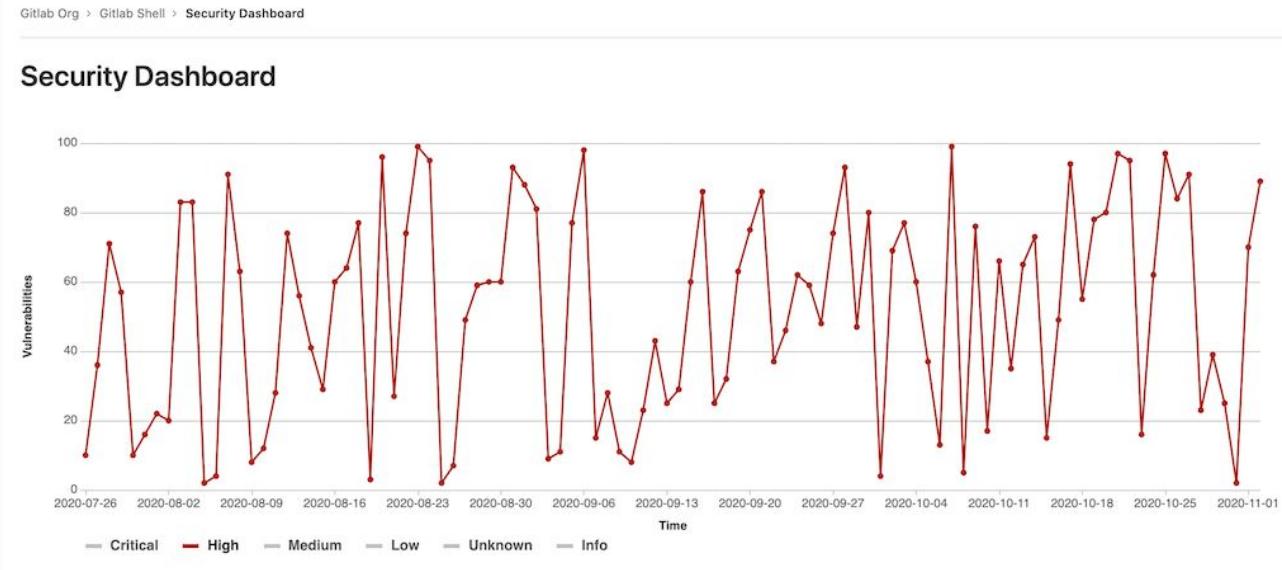
Identifier	Scanner	Actions
CVE-2019-5420 + 1 more	Dependency Scanning GitLab	<a href="#"></a> <a href="#"></a> <a href="#"></a>
ESLint rule ID security/detect-eval-with-expression + 1 more	SAST GitLab	<a href="#"></a> <a href="#"></a> <a href="#"></a>
ESLint rule ID security/detect-object-injection + 1 more	SAST GitLab	<a href="#"></a> <a href="#"></a> <a href="#"></a>

[https://docs.gitlab.com/ee/user/application\\_security/  
security\\_dashboard/](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

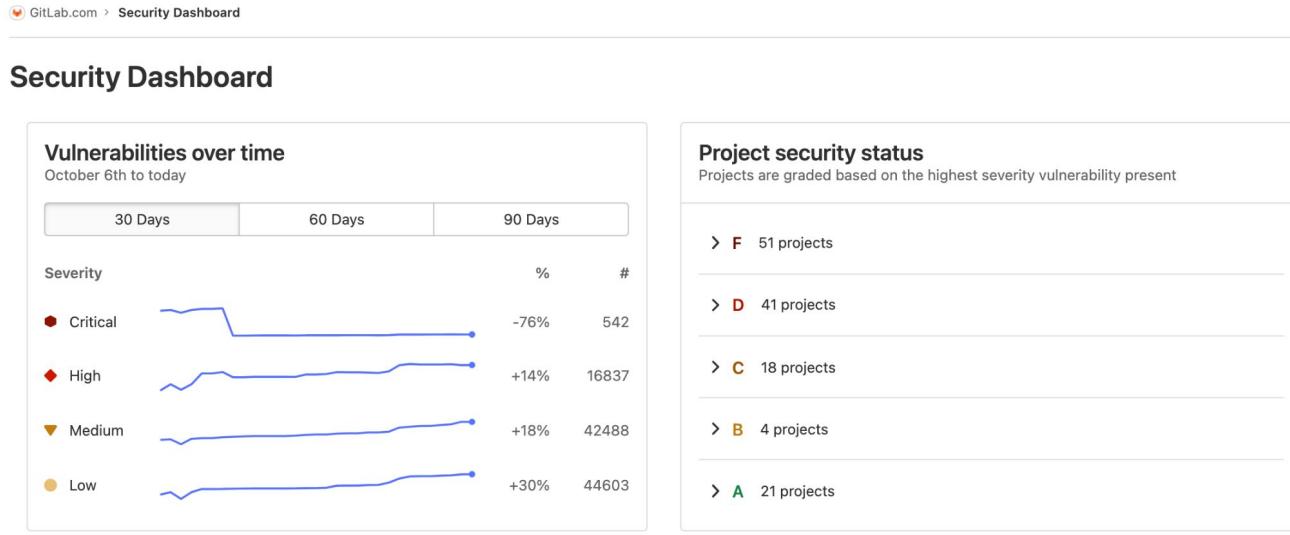


[https://docs.gitlab.com/ee/user/application\\_security/security\\_dashboard/](https://docs.gitlab.com/ee/user/application_security/security_dashboard/)

# 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/](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

Security > Security Dashboard

## Security Dashboard



### Project security status

Projects are graded based on the highest severity vulnerability present

> F 3 projects

> D 2 projects

> C 1 project

> B 0 projects

> A 0 projects

[https://docs.gitlab.com/ee/user/application\\_security/security\\_dashboard/](https://docs.gitlab.com/ee/user/application_security/security_dashboard/)

# Vulnerability Reports



GitLab-examples > security > simply-simple-notes > Vulnerability Report

## Vulnerability Report

The Vulnerability Report shows the results of the lastest successful pipeline on your project's default branch, as well as vulnerabilities from your latest container scan. [Learn more.](#)



Last pipeline run on the default branch

Project's current vulnerability state

Export

Export CSV of vulnerabilities



	Detected	Status	Severity	Description	Identifier	Tool	Activity
<input type="checkbox"/>	Detected	Confirmed	◆ High	Uncontrolled Memory Consumption in Django requirements.txt	CVE-2019-6975 + 1 more	Dependency Scanning	1

File and/or line where vulnerability resides

Scanner that identified the vulnerability

	Detected	Status	Severity	Description	Identifier	Tool	Activity
<input type="checkbox"/>	2020-04-13	Confirmed	◆ High	Uncontrolled Memory Consumption in Django requirements.txt	CVE-2019-6975 + 1 more	Dependency Scanning	1

	Detected	Status	Severity	Description	Identifier	Tool	Activity
<input type="checkbox"/>	2020-03-06	Detected	◆ High	Denial of service in Flask requirements.txt	CVE-2019-1010083 + 1 more	Dependency Scanning	1

	Detected	Status	Severity	Description	Identifier	Tool	Activity
<input type="checkbox"/>	2020-10-28	Detected	▼ Medium	X-Frame-Options Header Not Set	X-Frame-Options Header Not Set + 2 more	DAST	

	Detected	Status	Severity	Description	Identifier	Tool	Activity
<input type="checkbox"/>	2020-08-12	Detected	▼ Medium	HTTP Only Site /	HTTP Only Site + 2 more	DAST	

Issues related to vulnerability

Remediated vulnerability awaiting review

# Vulnerability Pages



**Detected** Detected 18 minutes ago in pipeline 4

Status **Detected** [Create issue](#)

**Dismiss**  
Will not fix or a false-positive

**Confirm**  
A true-positive and will fix

**Resolved**  
Verified as fixed or mitigated

Cancel Change status

## Improper Input Validation in com.fasterxml.jackson.core/jackson-core

### Description

A Polymorphic Typing issue was discovered in FasterXML jackson-databind (a specific property) for an externally exposed JSON endpoint and the service can provide a JNDI service to access, it is possible to make the application crash.

- Severity: critical
- Confidence: unknown
- Report Type: dependency\_scanning

### Location

- File: pom.xml

### Links

- <https://nvd.nist.gov/vuln/detail/CVE-2019-17531>

### Identifiers

- Gemnasium-fc79306c-cbe4-47bd-80a9-d2610a560930
- CVE-2019-17531

**Solution:** Upgrade to version 2.9.10.1 or above.

[Learn more about interacting with security reports ↗](#)

- 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/](https://docs.gitlab.com/ee/user/application_security/vulnerabilities/)



---

# Developer Workflow



GitLab Projects Groups More Search or jump to... To Do Add a to do >

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.

Approvers Approvals Commented by Approved by

Any eligible user Optional

License-Check 0 of 1

Vulnerability-Check 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

Oldest first Show all activity

Write Preview Write a comment or drag your files here...

To Do Add a to do >

0 Assignees None - assign yourself

0 Reviewers None

Milestone None

Time tracking No estimate or time spent

Labels None

Lock merge request 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... D 14 11 99% ? >

S Simply Simple Notes

Project overview Repository Issues Merge Requests 1 Requirements CI / CD Security Operations Packag Analytics Wiki Snippets Members Settings

Click on vulnerability for details

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: 'wja!rXUtnFEM!K7MDENG/bPxRfCYEXAMPLEKEY'

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 None - assign yourself Edit

0 Reviewers None Edit

Milestone None Edit

Time tracking No estimate or time spent

Labels None Edit

Lock merge request Unlocked Edit

1 participant

Notifications

Reference: fjdiaz/simply-simp... Source branch: add-additio...

« Collapse sidebar

All vulnerabilities are listed and sorted by scanner and severity

GitLab Projects Groups More

Search or jump to... 14 1 1 89 ?

S Simply Simple Notes

Project overview Repository Issues 1 Merge Requests 1 Requirements CI / CD Security & Compliance Operations Packages & Registries Analytics Wiki Snippets Members Settings

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

New

- High Chmod setting a permissive mask 0o777 on file (name)
- Medium Possibility of privilege escalation due to missing file permissions
- Medium Possibility of privilege escalation due to missing file permissions
- Low Possibility of privilege escalation due to missing file permissions

Fixed

- Dependents

New

- High Information disclosure via log file
- High Uncontrolled memory deallocation
- 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 required

Merge when pipeline succeeds  Delete source branch  Squash commits

4 commits and 1 merge commit will be added to master. Modify merge commit

To Do Add a to do

0 Assignees None - assign yourself

0 Reviewers None

Milestone None

Time tracking No estimate or time spent

Labels None

Lock merge request Unlocked

1 participant

Notifications

Reference: fjiaz/simply-simpl...

Source branch: add-addition...

« Collapse sidebar

Click to see where the vulnerability is located



## S Simply Simple Notes

Project overview

Repository

Files

Commits

Branches

Tags

Contributors

Graph

Compare

Locked Files

Issues 1

Merge Requests 1

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

```
1 import os
2 import logging
3 import sqlite3
4 from sqlite3 import Error
5
6
7 def create_connection(name='notes.db'):
8     conn = None
9
10    try:
11        conn = sqlite3.connect(name)
12        os.chmod(name, 0o777)
13    except Error as e:
14        logging.error(e)
15
16    return conn
17
18
19 def create_table(conn, create_table_sql):
20    try:
21        c = conn.cursor()
22        c.execute(create_table_sql)
23    except Error as e:
24        print(e)
25
26
27 def create_note(conn, notes):
28     query = "INSERT INTO notes(data) VALUES(?)"
29
30     cur = conn.cursor()
31     cur.execute(query, notes)
32
33     return cur.lastrowid
34
35
36 def delete_note(conn, id):
37     query = 'DELETE FROM notes WHERE id=?'
38
39     cur = conn.cursor()
40     cur.execute(query, (id,))
41
42     conn.commit()
43
44 def select_note_by_id(conn, id=None):
45     query = "SELECT * FROM notes"
46
47     if id:
48         query = query + " WHERE id = '%s'" % id
49
50     cur = conn.cursor()
51     cur.execute(query)
```

The line of code containing the vulnerability can be seen here

GitLab Projects Groups More

Search or jump to... 14 1 1 89 ?

S Simply Simple Notes

Project overview Repository Issues 1 Merge Requests 1 Requirements CI / CD Security & Compliance Operations Packages & Registries Analytics Wiki Snippets Members Settings

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

New

- High Chmod setting a permissive mask 0o777 on file (name)
- Medium Possibility of privilege escalation due to missing file permissions
- Medium Possibility of privilege escalation due to missing file permissions
- Low Possibility of privilege escalation due to missing file permissions

Fixed

- Dependents

New

- High Information disclosure due to missing file permissions
- High Uncontrolled file creation
- 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 required

Merge when pipeline succeeds  Delete source branch  Squash commits

To Do Add a to do

0 Assignees None - assign yourself

0 Reviewers None

Milestone None

Time tracking No estimate or time spent

Labels None

Lock merge request Unlocked

1 participant

Notifications

Reference: fjiaz/simply-simpl...

Source branch: add-addition...

<< Collapse sidebar

>> 4 commits and 1 merge commit will be added to master. Modify merge commit

B103: Test for setting permissive file permissions

B104:  
hardcoded\_bind\_all\_interfaces

B105:  
hardcoded\_password\_string

B106:  
hardcoded\_password\_funcarg

B107:  
hardcoded\_password\_default

B108: hardcoded\_tmp\_directory

B109: Test for a password based config option not marked secret

B110: try\_except\_pass

B111: Test for the use of rootwrap running as root

B112: try\_except\_continue

B201: flask\_debug\_true

B501:  
request\_with\_no\_cert\_validation

B502: ssl\_with\_bad\_version

B503: ssl\_with\_bad\_defaults

B504: ssl\_with\_no\_version

B505: weak\_cryptographic\_key

B506: yaml\_load

B507:  
ssh\_no\_host\_key\_verification

B601: paramiko\_calls

B602:  
subprocess\_popen\_with\_shell\_equals\_true

B603:  
subprocess\_without\_shell\_equals\_true

B604:  
any\_other\_function\_with\_shell\_equals\_true

B605: start\_process\_with\_a\_shell

B606:

## 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
```

Each vulnerability has detailed information to enhance developer education

#### See also

- [https://security.openstack.org/guidelines/dg\\_apply-restrictive-file-permissions.html](https://security.openstack.org/guidelines/dg_apply-restrictive-file-permissions.html) # noqa
- [https://en.wikipedia.org/wiki/File\\_system\\_permissions](https://en.wikipedia.org/wiki/File_system_permissions)
- <https://security.openstack.org>

New in version 0.9.0.

GitLab Projects Groups More

Search or jump to... 14 1 1 89 ?

S Simply Simple Notes

Project overview Repository Issues 1 Merge Requests 1 Requirements CI / CD Security & Compliance Operations Packages & Registries Analytics Wiki Snippets Members Settings

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 B102 Severity: High Scanner: SAST Scanner Provider: Bandit

New

- High Chmod setting a permissive mask 0o777 on file (name)
- Medium Possibility of privilege escalation due to missing file permissions
- Medium Possibility of privilege escalation due to missing file permissions
- Low Possibility of privilege escalation due to missing file permissions

Fixed

- Dependents

New

- High Information disclosure via log files
- High Uncontrolled memory deallocation
- 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 required

Merge when pipeline succeeds  Delete source branch  Squash commits

4 commits and 1 merge commit will be added to master. Modify merge commit

To Do Add a to do

0 Assignees None - assign yourself

0 Reviewers None

Milestone None

Time tracking No estimate or time spent

Labels None

Lock merge request Unlocked

1 participant

Notifications

Reference: fjiaz/simply-simpl...

Source branch: add-addition...

« Collapse sidebar

Click to dismiss the vulnerability with comments

GitLab Projects Groups More Search or jump to... 14 1 1 89 ? < >

S Simply Simple Notes

Project overview Repository Issues Merge Requests Requirements CI / CD Security & Compliance Operations Packages & Registries Analytics Wiki Snippets Members Settings

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

Add comment about the dismissal.

Fern @fjiaz · Not a production file

Click to add the comment and dismiss

Cancel Add comment & dismiss

New

- High Informational
- High Uncommon
- High Denial of Service
- High Improvement

Medium

- Container

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 required ⓘ

Manage licenses View full report Expand

To Do Add a to do

0 Assignees None - assign yourself

0 Reviewers None

Milestone None

Time tracking No estimate or time spent

Labels None

Lock merge request Unlocked

1 participant

Notifications

Reference: fjiaz/simply-simpl... Source branch: add-addition...

<< Collapse sidebar

Dismissed 'Chmod setting a permissive mask 0o777 on file (name).'

**Simply Simple Notes**

Project overview Repository Issues Merge Requests Requirements CI / CD Security & Compliance Operations Packages & Registries Analytics Wiki Snippets Members Settings

Overview 0 Commits 4 Pipelines 5 Changes 7

**Security scanning detected 1 critical and 5 high severity vulnerabilities**

**SAST detected 1 high severity vulnerability out of 10**

**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 required**

To Do Add a to do

0 Assignees None - assign yourself

0 Reviewers None

Milestone None

Time tracking No estimate or time spent

Labels None

Lock merge request Unlocked

1 participant

Notifications

Reference: fjdiaz/simply-simpl...

Source branch: add-addition...

Dismissed 'Chmod setting a permissive mask 0o777 on file (name).'

Search or jump to...

Collapse sidebar

GitLab Projects Groups More Search or jump to... To Do Add a to do

Simply Simple Notes Project overview Repository Issues Merge Requests Requirements CI / CD Security & Compliance Operations Packages & Registries Analytics Wiki Snippets Members Settings

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

New

- High Chmod
- Medium Possibility
- Medium Possibility
- Low Possibility

Fixed

- Dependents

New

- High Information
- High Uncommon
- High Denial
- High Improvement
- Medium Incidence

Container

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 required

Manage licenses View full report Expand

0 Assignees None - assign yourself Edit

0 Reviewers None Edit

Milestone None Edit

Time tracking No estimate or time spent Edit

1 participant Notifications

Reference: fjdiaz/simply-simpl... Source branch: add-addition...

Click to create an issue to keep track of the vulnerability

Cancel Undo dismiss Create issue

GitLab Projects Groups More

Search or jump to...

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 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... D 14 I 11 E 99 ? < >

S Simply Simple Notes Fern > Simply Simple Notes > Merge Requests > !2

Project overview Repository Issues Merge Requests Requirements CI / CD Security & Compliance Operations Packages & Registries Analytics Wiki Snippets Members Settings

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.

Approvers Approvals Commented by Approved by

Any eligible user Optional

License-Check 0 of 1

Vulnerability-Check 0 of 1

2 more

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

Oldest first Show a

Write Preview Write a comment or drag your files here...

To Do Add a to do

0 Assignees None - assign yourself

0 Reviewers None

Milestone None

Time tracking No estimate or time spent

Labels None

Lock merge request 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... + 14 1 1 99+ ? < > 0

S Simply Simple Notes

Project overview Repository Issues Merge Requests Requirements CI / CD Security & Compliance Operations Packages & Registries Analytics Wiki Snippets Members Settings

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 detected License Compliance detected required

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

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 None - assign yourself

0 Reviewers None

Milestone None

Time tracking No estimate or time spent

Labels None

Lock merge request Unlocked

1 participant

Notifications

Reference: fjdiaz/simply-simpl... Source branch: add-addition...

« Collapse sidebar

Approval is required, because a denied license was detected



---

# Security Team Workflow

**S** security**H** Subgroup overview

Details

Activity

**E** Epics

0

**I** Issues

54

**M** Merge Requests

6

**🛡** Security & Compliance

Security Dashboard

**⚡** Push Rules

Vulnerability Report

**☸️** Kubernetes**📦** Packages & Registries**⚠** Alerts**💡** Workflows**🔗** Merges

Click to access the group level security dashboard

**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	<a href="#">go-fuzz-it</a> ⓘ Maintainer	A getting started template for go-micro ( <a href="https://micro.mu/docs/go-micro.html">https://micro.mu/docs/go-micro.html</a> )	★ 0	1 month ago
 S	<a href="#">simply-simple-notes-whitesource</a> ⓘ Maintainer	Simply Simple Notes is a simple Flask application that stores notes in a SQLite file. ...	★ 1	1 month ago
 S	<a href="#">simply-simple-notes</a> ⓘ Maintainer	Simply Simple Notes is a simple Flask application that stores notes in a SQLite file. ...	★ 10	3 weeks ago
 Y	<a href="#">Yarn Vulnerabilities</a> ⓘ Maintainer	This project includes some known yarn vulnerabilities for testing purposes	★ 0	8 months ago
 S	<a href="#">security-reports</a> ⓘ		★ 18	4 days ago
 N	<a href="#">npm-package-lock</a> ⓘ	A test repository for testing apps using NPM with a package-lock.json file.	★ 0	1 year ago
 R	<a href="#">rails-and-yarn</a> ⓘ	A test repository for testing apps using Rails and Yarn.	★ 0	1 year ago

## S security

[Subgroup overview](#)[Epics 0](#)[Issues 54](#)[Merge Requests 6](#)

## Security &amp; Compliance

## Security Dashboard

## Vulnerability Report

[Push Rules](#)[Kubernetes](#)[Packages & Rego](#)[Analytics](#)[Wiki](#)[Members](#)

Click to access the vulnerability report

GitLab-examples &gt; security &gt; Security Dashboard

## Security Dashboard

## Vulnerabilities over time

September 20th to today

[30 Days](#) [60 Days](#) [90 Days](#)

Severity % #

● Critical +0% 0◆ High - 2▼ Medium - 13● Low - 30

Vulnerabilities over time  
can be seen here

## 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

Projects are rated A-F  
depending on severity of  
vulnerabilities

GitLab Projects Groups More Search or jump to... 16 1 2 99+ ?

S security

Subgroup overview

Epic 0

Issues 54

Merge Requests 6

Security & Compliance

Security Dashboard

Vulnerability Report

Push Rules

Kubernetes

Packages & Registries

Analytics

Wiki

Members

Collapsible sidebar

GitLab-examples > security > Vulnerability Report

## Vulnerability Report

Export

Status Severity Scanner Project

Detected +1 more All severities All scanners All projects

Click to sort by project

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... D 15 10 99+ ? 1

S security

Subgroup overview

Epic 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	Severity	Scanner	Project
D Detected +1 more	All severities	All scanners	All projects
Detected	Status	Severity	Description
<input type="checkbox"/>	2020-08-13	D Detected	Critical RSA private key GitLab-examples / security / security-reports testdata/id_rsa (line: 1)
<input type="checkbox"/>	2020-08-10	D Detected	Critical Password in URL GitLab-examples / security / security-reports testdata/urls (line: 3)
<input type="checkbox"/>	2020-08-04	D Detected	Critical Slack Token GitLab-examples / security / security-reports testdata/main.go (line: 65)
<input type="checkbox"/>	2020-07-27	D Detected	Critical Heroku API key GitLab-examples / security / security-reports testdata/main.go (line: 10)
<input type="checkbox"/>	2020-07-27	D Detected	Critical Password in URL GitLab-examples / security / security-reports testdata/Dockerfile (line: 9)
<input type="checkbox"/>	2020-07-26	D Detected	Critical Path Traversal in rubyzip GitLab-examples / security / security-reports dependency-scanning-files/Gemfile.lock
<input type="checkbox"/>	2020-07-26	D Detected	Critical Command Injection in nokogiri GitLab-examples / security / security-reports dependency-scanning-files/Gemfile.lock
<input type="checkbox"/>	2020-07-26	D Detected	Critical Bypass of a protection mechanism in libxml in nokogiri GitLab-examples / security / security-reports dependency-scanning-files/Gemfile.lock

Project X

All projects

simply-simple-notes

security-reports

Gitleaks rule ID RSA SAST 1

Gitleaks rule ID Password in URL SAST 1

Gitleaks rule ID Slack Token SAST

Gitleaks rule ID Heroku API Key SAST

Gitleaks rule ID Password in URL SAST

CVE-2018-1000544 + 1 more Dependency Scanning

CVE-2019-5477 + 1 more Dependency Scanning

CVE-2019-11068 + 1 more Dependency Scanning



## S security

### Subgroup overview

[Details](#)[Activity](#)

### Epics

0

### Issues

54

### Merge Requests

6

### Security & Compliance

### Push Rules

### Kubernetes

### Packages & Registries

### Analytics

### Wiki

### Members

### Security Dashboard

### Vulnerability Report



## 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 <small>Maintainer</small> A getting started template for go-micro ( <a href="https://micro.mu/docs/go-micro.html">https://micro.mu/docs/go-micro.html</a> )	0	1 month ago
	simply-simple-notes-whitesource <small>Maintainer</small> Simply Simple Notes is a simple Flask application that stores notes in a SQLite file. ...	1	1 month ago
	simply-simple-notes <small>Maintainer</small> Simply Simple Notes is a simple Flask application that stores notes in a SQLite file. ...	10	3 weeks ago
	Yarn Vulnerabilities <small>Maintainer</small> This project includes some known yarn vulnerabilities for testing purposes	0	8 months ago
	security-reports <small></small>	18	4 days ago
	npm-package-lock <small></small> A test repository for testing apps using NPM with a package-lock.json file.	0	1 year ago
	rails-and-yarn <small></small> A test repository for testing apps using Rails and Yarn.	0	1 year ago

Click to access and independent project

## S Simply Simple Notes

### Project overview

[Details](#)[Activity](#)[Releases](#)

### Repository

### Issues 2

### Merge Requests 1

### Requirements

### CI / CD

### Security & Compliance

### Operations

### Packages & Registries

### Analytics

### Wiki

### Snippets

### Members

### Settings

### Security Dashboard

[On-demand Scans](#)[Dependency List](#)[License Compliance](#)[Threat Monitoring](#)[Configuration](#)

Fern &gt; Simply Simple Notes &gt; Details

## Simply Simple Notes

Project ID: 21763006



Star

0



Fork

0

66 Commits 15 Branches 0 Tags 471 KB Files 7.1 MB Storage



History

Find file

Web IDE



Clone



09330714

[CI/CD configuration](#)[Add CHANGELOG](#)[Add CONTRIBUTING](#)

Name	Last commit	Last update
.gitlab/managed-apps	Update values.yaml	2 months ago
docs	Update usage_guide.md	1 month ago
helm	Update notes.yaml	5 days ago
notes	Add DNS name to Simply Simple Notes	2 months ago
tests	Enhance the documentation and add some test	2 months ago
.gitignore	Add a working Flask Application	6 months ago
.gitlab-ci.yml	Update .gitlab-ci.yml	5 days ago
Dockerfile	Update Dockerfile	6 months ago
LICENSE	Add a working Flask Application	6 months ago
README.md	Add instructions on creating vulnerabilities and more	2 months ago
config.py	Make this application Graphical	2 months ago
requirements.txt	Add some style	2 months ago
run.py	Make this application Graphical	2 months ago

[README.md](#)

Collapse sidebar

<https://gitlab.com/fjdz/simply-simple-notes/-/security/dashboard>

Click to access the security dashboard for a project

**S** Simply Simple Notes

Project overview

Repository

Issues

Merge Requests

Requirements

Overview of all vulnerabilities on default branch based on sorting

Fern &gt; Simply Simple Notes &gt; Security Dashboard

**Vulnerabilities**

The Security Dashboard shows the results of the last successful pipeline run on the default branch.

Last updated 1 week ago #202581064

A csv of all the vulnerabilities can be exported



Click to sort by status

Vulnerability count based on severity



Status Severity Scanner

Detected +1 more

All severities

All scanners

<input type="checkbox"/> Detected	Status	Severity	Description	Identifier	Scanner	Activity
<input type="checkbox"/> 2020-10-13	Detected	● Critical	AWS API key docs/creating_vulnerabilities.md (line: 35)	Gitleaks rule ID AWS	Secret Detection	
<input type="checkbox"/> 2020-10-13	Detected	◆ High	CVE-2019-14697 in musl registry.gitlab.com/fjdiaz/simple91e915598c61f931fcadb71ee04d	CVE-2019-14697	Container Scanning	
<input type="checkbox"/> 2020-10-13	Detected	◆ High	CVE-2018-20843 in expat registry.gitlab.com/fjdiaz/simple91e915598c61f931fcadb71ee04d	CVE-2018-20843	Container Scanning	
<input type="checkbox"/> 2020-10-13	Detected	◆ High	Improper Input Validation in pip requirements.txt	CVE-2018-20225 + 1 more	Dependency Scanning	
<input type="checkbox"/> 2020-10-14	Confirmed	▼ Medium	Insecure HTTP Method - DELETE	Insecure HTTP Method - DELETE + 2 more	DAST	
<input type="checkbox"/> 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... D 14 1 1 89+ ? ⓘ

S 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

Fern > Simply Simple Notes > Security Dashboard

## Vulnerabilities

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	Severity	Scanner			
Detected +1 more	All severities	All scanners			
Status X					
All	Severity	Description	Identifier	Scanner	Activity
✓ Detected	Critical	AWS API key docs/creating_vulnerabilities.md (line: 35)	Gitleaks rule ID AWS	Secret Detection	
✓ Confirmed	High	CVE-2019-14697 in musl registry.gitlab.com/fjdiaz/si... d1e9e915598c61f931fcaedb71ee04d	CVE-2019-14697	Container Scanning	
Dismissed					
Resolved					
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 + 2 more	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	X-Frame-Options Header	

« Collapse sidebar

**S** 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](#)

## 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	Severity	Scanner	Identifier	Scanner	Activity
<a href="#">Detected +1 more</a>	All severities	All scanners			
<input type="checkbox"/> <a href="#">Detected</a>	Status	<b>Severity</b> X			
<input type="checkbox"/> <a href="#">2020-10-13</a>	<a href="#">Detected</a>	<input checked="" type="checkbox"/> All severities			
<input type="checkbox"/> <a href="#">2020-10-13</a>	<a href="#">Detected</a>	Critical	1697 in musl_vulnerabilities.md (line: 35)	Gitleaks rule ID AWS	Secret Detection
<input type="checkbox"/> <a href="#">2020-10-13</a>	<a href="#">Detected</a>	High	1697 in musl_vulnerabilities.md (line: 35)	Gitleaks rule ID AWS	Secret Detection
<input type="checkbox"/> <a href="#">2020-10-13</a>	<a href="#">Detected</a>	Medium	1697 in musl_vulnerabilities.md (line: 35)	CVE-2019-14697	Container Scanning
<input type="checkbox"/> <a href="#">2020-10-13</a>	<a href="#">Detected</a>	Low	1697 in musl_vulnerabilities.md (line: 35)	CVE-2019-14697	Container Scanning
<input type="checkbox"/> <a href="#">2020-10-13</a>	<a href="#">Detected</a>	Unknown	8043 in expat	CVE-2018-20843	Container Scanning
<input type="checkbox"/> <a href="#">2020-10-13</a>	<a href="#">Detected</a>	Info	8043 in expat	CVE-2018-20843	Container Scanning
<input type="checkbox"/> <a href="#">2020-10-14</a>	<a href="#">Confirmed</a>	<input checked="" type="checkbox"/> High	improper input Validation in pip requirements.txt	CVE-2018-20225 + 1 more	Dependency Scanning
<input type="checkbox"/> <a href="#">2020-10-14</a>	<a href="#">Confirmed</a>	<input checked="" type="checkbox"/> Medium	Insecure HTTP Method - DELETE	Insecure HTTP Method - DELETE + 2 more	DAST
<input type="checkbox"/> <a href="#">2020-10-14</a>	<a href="#">Confirmed</a>	<input checked="" type="checkbox"/> Medium	X-Frame-Options Header Not Set	X-Frame-Options Header Not Set + 2 more	DAST
<input type="checkbox"/> <a href="#">2020-10-14</a>	<a href="#">Detected</a>	<input checked="" type="checkbox"/> Medium	X-Frame-Options Header Not Set	X-Frame-Options Header Not Set + 2 more	DAST
<input type="checkbox"/> <a href="#">2020-10-14</a>	<a href="#">Detected</a>	<input checked="" type="checkbox"/> Medium	X-Frame-Options Header Not Set	X-Frame-Options Header Not Set + 2 more	DAST

GitLab Projects Groups More Search or jump to... D 14 1 1 99+ ? ⓘ

S 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

Fern > Simply Simple Notes > Security Dashboard

## Vulnerabilities

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	Severity	Scanner
Detected +1 more	All severities	All scanners
<input type="checkbox"/> Detected	Status	Scanner
<input type="checkbox"/> 2020-10-13	Detected	<b>Critical</b>
<input type="checkbox"/> 2020-10-13	Detected	<b>High</b>
<input type="checkbox"/> 2020-10-13	Detected	<b>High</b>
<input type="checkbox"/> 2020-10-13	Detected	<b>High</b>
<input type="checkbox"/> 2020-10-14	Confirmed	<b>Medium</b>
<input type="checkbox"/> 2020-10-14	Confirmed	<b>Medium</b>
<input type="checkbox"/> 2020-10-14	Detected	<b>Medium</b>

Scanner X

- ✓ All scanners
- Container Scanning
- DAST
- Dependency Scanning
- SAST
- Secret Detection
- Coverage Fuzzing

Identifier Scanner Activity

35) Gitleaks rule ID AWS Secret Detection

98c61f931fcaedb71ee04d CVE-2019-14697 Container Scanning

98c61f931fcaedb71ee04d CVE-2018-20843 Container Scanning

CVE-2018-20225 + 1 more Dependency Scanning

+ 2 more

X-Frame-Options Header Not Set DAST

X-Frame-Options Header Not Set + 2 more

X-Frame-Options Header

Click vulnerability to see more details

« Collapse sidebar

GitLab Projects Groups More

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
```

S 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... D 16 I 2 99+ ? ⓘ

S 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

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

✓ 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

Click to confirm the new status

GitLab Projects Groups More ▾

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
```

S Solution

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

Click to change the status

GitLab Projects Groups More Search or jump to... D:16 I:2 E:99% ? ⓘ

S 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 HTTP response.

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
```

You can see who confirmed it as well as when it was confirmed



---

# Q&A