Zavisnosti sa poznatim ranjivostima + SonarQube

Informaciona bezbednost

FAKULTET TEHNIČKIH NAUKA

V8

Zavisnosti sa poznatim ranjivostima

Upotreba biblioteka, radnih okvira, softverskih modula i sl. koji imaju vec poznate i eksploatisane ranjivosti

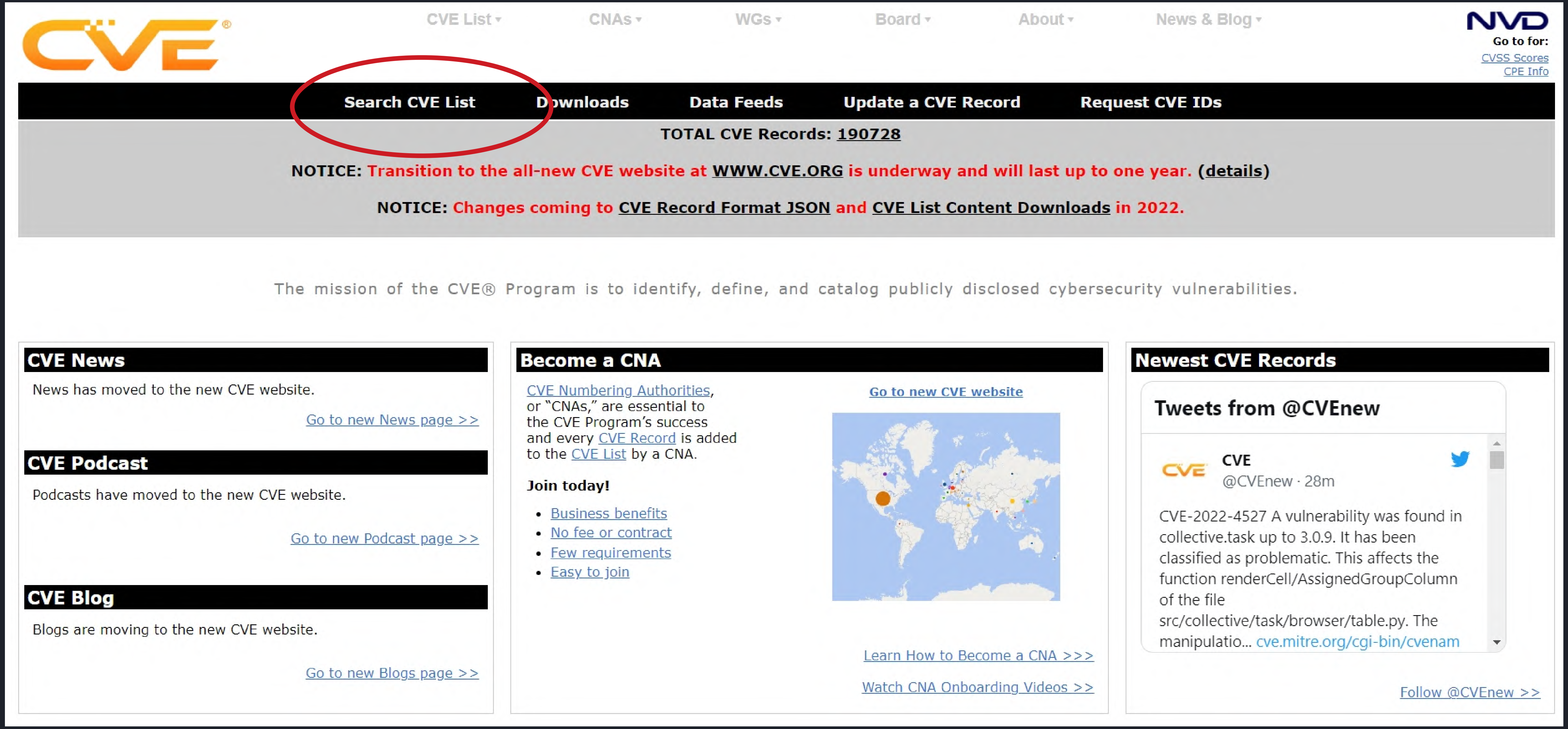
Mere zastite?

- Ukloniti sve sto nije u upotrebi
- Konstantna provera verzija klijentskih i serverskih komponenata

- CVE
- Java - OWASP dependency check

CVE

CVE



TOTAL CVE Records: 190728

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG is underway and will last up to one year. (details)

NOTICE: Changes coming to CVE Record Format JSON and CVE List Content Downloads in 2022.

The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

CVE News

News has moved to the new CVE website.

Go to new News page >>

CVE Podcast

Podcasts have moved to the new CVE website.

Go to new Podcast page >>

CVE Blog

Blogs are moving to the new CVE website.

Go to new Blogs page >>

Become a CNA

CVE Numbering Authorities, or "CNAs," are essential to the CVE Program's success and every CVE Record is added to the CVE List by a CNA.

Go to new CVE website

Join today!

- Business benefits
- No fee or contract
- Few requirements
- Easy to join

Learn How to Become a CNA >>>

Watch CNA Onboarding Videos >>

Newest CVE Records

Tweets from @CVEnew

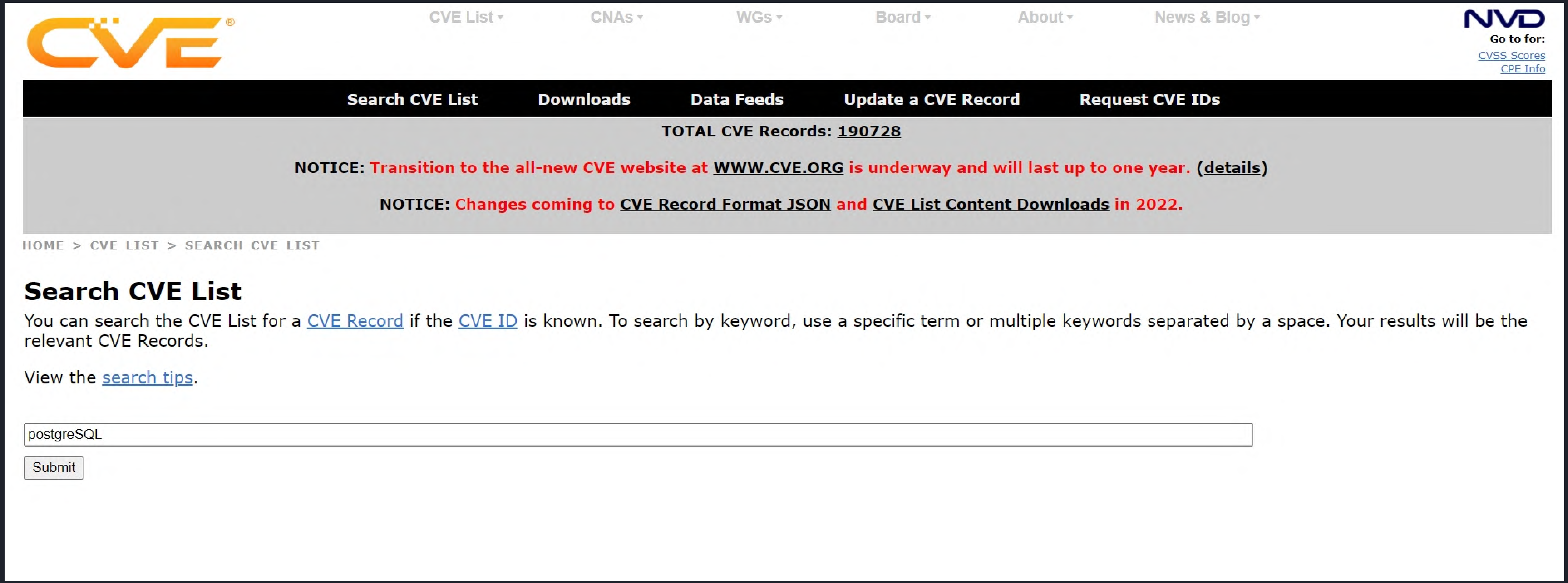
CVE
@CVEnew · 28m

CVE-2022-4527 A vulnerability was found in collective.task up to 3.0.9. It has been classified as problematic. This affects the function renderCell/AssignedGroupColumn of the file src/collective/task/browser/table.py. The manipulatio... cve.mitre.org/cgi-bin/cvenam

Follow @CVEnew >>

CVE

CVE



TOTAL CVE Records: 190728

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG is underway and will last up to one year. (details)

NOTICE: Changes coming to CVE Record Format JSON and CVE List Content Downloads in 2022.

HOME > CVE LIST > SEARCH CVE LIST

Search CVE List

You can search the CVE List for a CVE Record if the CVE ID is known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be the relevant CVE Records.

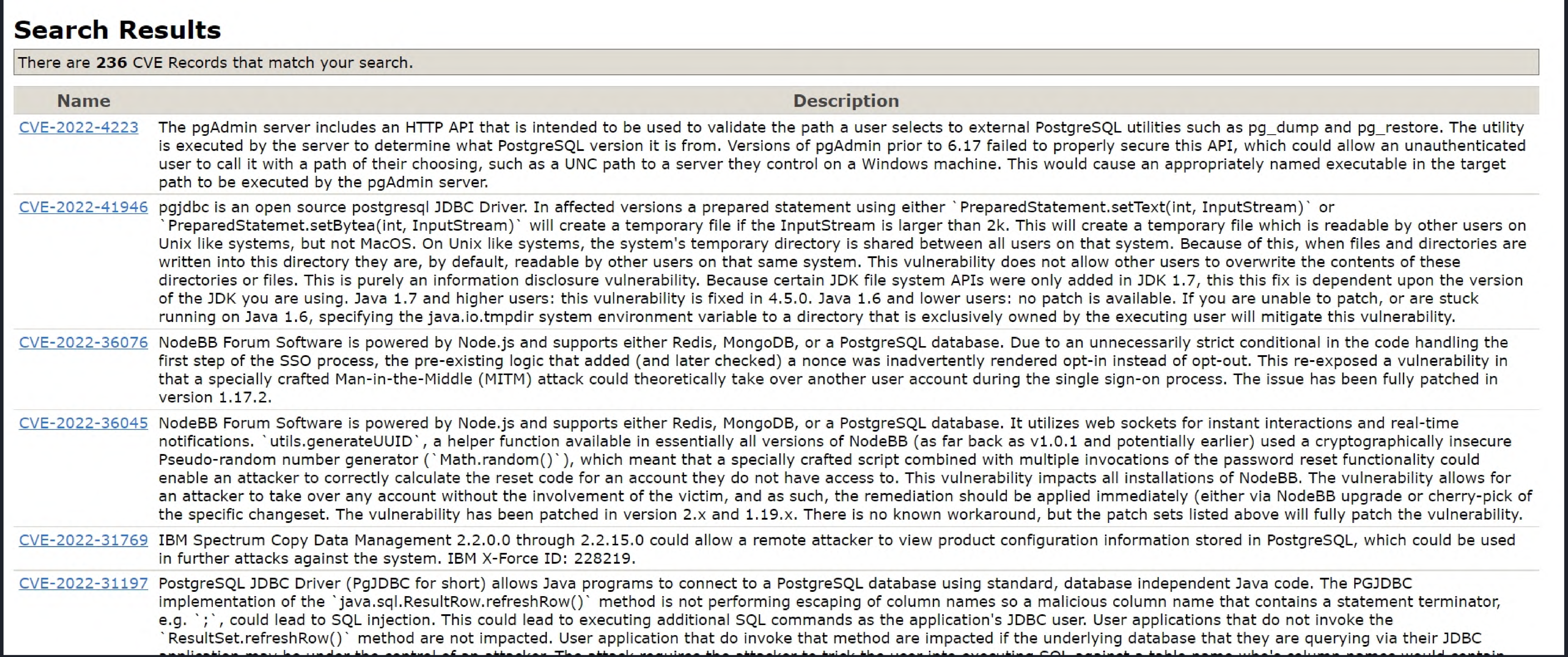
View the search tips.

postgreSQL

Submit

CVE

CVE



Search Results

There are **236** CVE Records that match your search.

Name	Description
CVE-2022-4223	The pgAdmin server includes an HTTP API that is intended to be used to validate the path a user selects to external PostgreSQL utilities such as pg_dump and pg_restore. The utility is executed by the server to determine what PostgreSQL version it is from. Versions of pgAdmin prior to 6.17 failed to properly secure this API, which could allow an unauthenticated user to call it with a path of their choosing, such as a UNC path to a server they control on a Windows machine. This would cause an appropriately named executable in the target path to be executed by the pgAdmin server.
CVE-2022-41946	pgjdbc is an open source postgresql JDBC Driver. In affected versions a prepared statement using either `PreparedStatement.setText(int, InputStream)` or `PreparedStatemet.setBytea(int, InputStream)` will create a temporary file if the InputStream is larger than 2k. This will create a temporary file which is readable by other users on Unix like systems, but not MacOS. On Unix like systems, the system's temporary directory is shared between all users on that system. Because of this, when files and directories are written into this directory they are, by default, readable by other users on that same system. This vulnerability does not allow other users to overwrite the contents of these directories or files. This is purely an information disclosure vulnerability. Because certain JDK file system APIs were only added in JDK 1.7, this this fix is dependent upon the version of the JDK you are using. Java 1.7 and higher users: this vulnerability is fixed in 4.5.0. Java 1.6 and lower users: no patch is available. If you are unable to patch, or are stuck running on Java 1.6, specifying the java.io.tmpdir system environment variable to a directory that is exclusively owned by the executing user will mitigate this vulnerability.
CVE-2022-36076	NodeBB Forum Software is powered by Node.js and supports either Redis, MongoDB, or a PostgreSQL database. Due to an unnecessarily strict conditional in the code handling the first step of the SSO process, the pre-existing logic that added (and later checked) a nonce was inadvertently rendered opt-in instead of opt-out. This re-exposed a vulnerability in that a specially crafted Man-in-the-Middle (MITM) attack could theoretically take over another user account during the single sign-on process. The issue has been fully patched in version 1.17.2.
CVE-2022-36045	NodeBB Forum Software is powered by Node.js and supports either Redis, MongoDB, or a PostgreSQL database. It utilizes web sockets for instant interactions and real-time notifications. `utils.generateUUID`, a helper function available in essentially all versions of NodeBB (as far back as v1.0.1 and potentially earlier) used a cryptographically insecure Pseudo-random number generator (`Math.random()`), which meant that a specially crafted script combined with multiple invocations of the password reset functionality could enable an attacker to correctly calculate the reset code for an account they do not have access to. This vulnerability impacts all installations of NodeBB. The vulnerability allows for an attacker to take over any account without the involvement of the victim, and as such, the remediation should be applied immediately (either via NodeBB upgrade or cherry-pick of the specific changeset. The vulnerability has been patched in version 2.x and 1.19.x. There is no known workaround, but the patch sets listed above will fully patch the vulnerability.
CVE-2022-31769	IBM Spectrum Copy Data Management 2.2.0.0 through 2.2.15.0 could allow a remote attacker to view product configuration information stored in PostgreSQL, which could be used in further attacks against the system. IBM X-Force ID: 228219.
CVE-2022-31197	PostgreSQL JDBC Driver (PgJDBC for short) allows Java programs to connect to a PostgreSQL database using standard, database independent Java code. The PGJDBC implementation of the `java.sql.ResultRow.refreshRow()` method is not performing escaping of column names so a malicious column name that contains a statement terminator, e.g. `;`, could lead to SQL injection. This could lead to executing additional SQL commands as the application's JDBC user. User applications that do not invoke the `ResultSet.refreshRow()` method are not impacted. User application that do invoke that method are impacted if the underlying database that they are querying via their JDBC application may be under the control of an attacker. The attack requires the attacker to trick the user into executing SQL against a table name who's column names would contain

IZVEŠTAJ

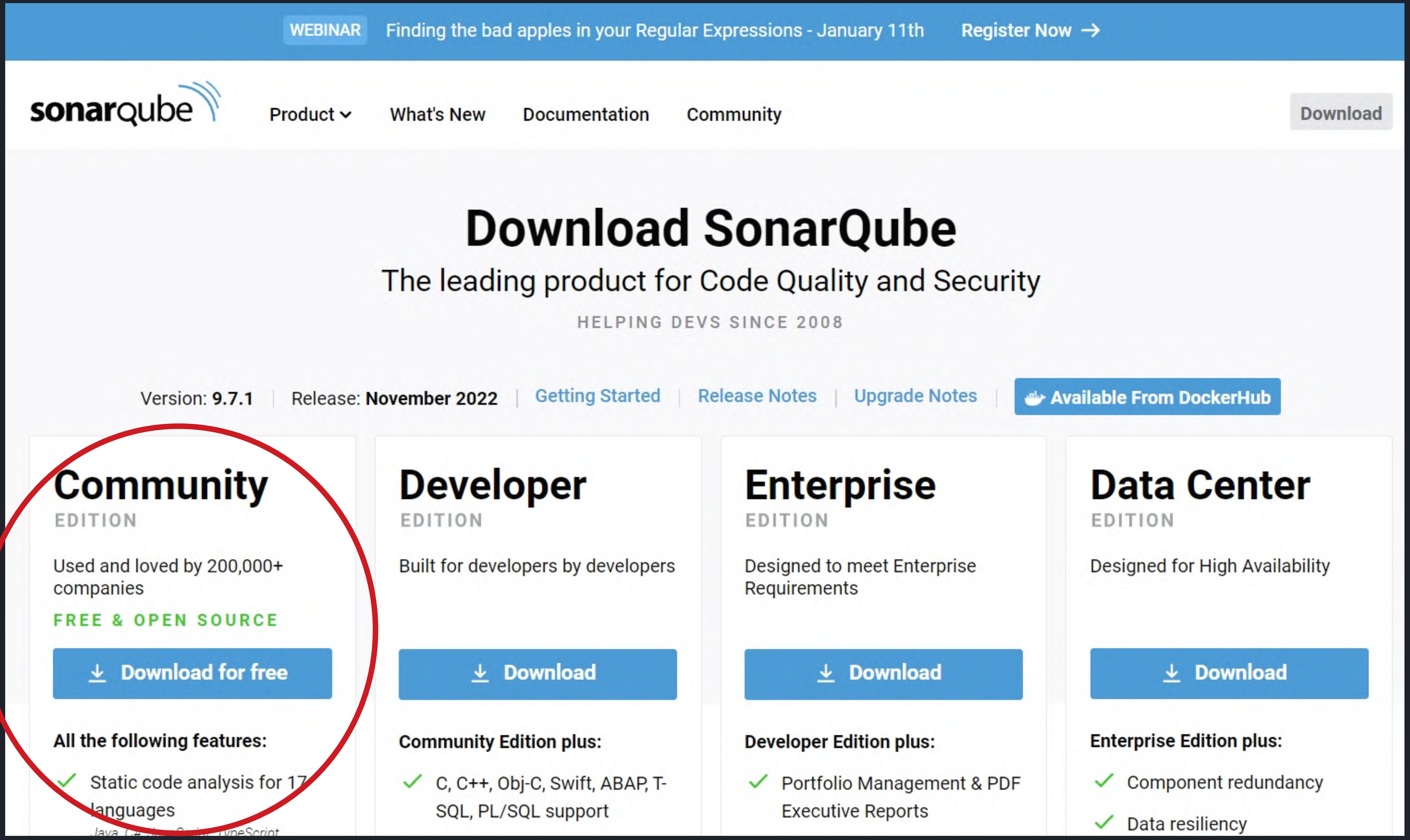
- Pretražiti sve dependency-e koje koristite u aplikaciji
- Napraviti spisak propusta za sve verzije biblioteka koje se koriste u projektu

- Koji bi bili mehanizmi zastite?
- Izvestaj dostaviti u proizvoljnom formatu (Word/PDF)

Ideja-upoznati se sa trenutnim i aktuelnim ranjivostima biblioteka koje ste koristili u projektu

SonarQube

Alat za statičku analizu koda



Finding the bad apples in your Regular Expressions - January 11th

Download SonarQube

The leading product for Code Quality and Security

HELPING DEVS SINCE 2008

Version: **9.7.1** | Release: **November 2022** | Getting Started | Release Notes | Upgrade Notes | Available From DockerHub

Community

EDITION

Used and loved by 200,000+ companies

FREE & OPEN SOURCE

Download for free

All the following features:

✓ Static code analysis for 17 languages

Java, C#, JavaScript, TypeScript

Developer

EDITION

Built for developers by developers

Download

Community Edition plus:

✓ C, C++, Obj-C, Swift, ABAP, T-SQL, PL/SQL support

Enterprise

EDITION

Designed to meet Enterprise Requirements

Download

Developer Edition plus:

✓ Portfolio Management & PDF Executive Reports

Data Center

EDITION

Designed for High Availability

Download

Enterprise Edition plus:

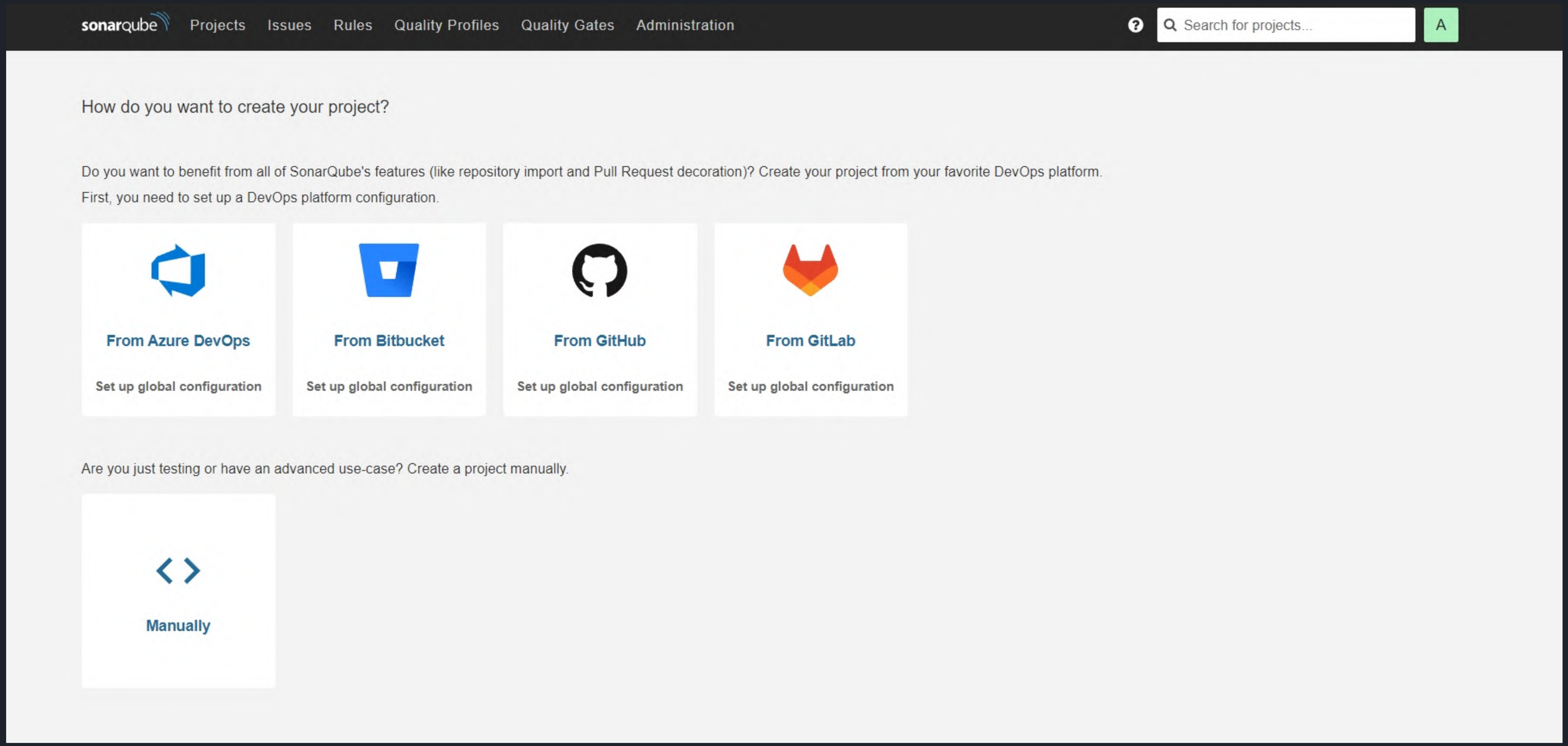
✓ Component redundancy

✓ Data resiliency

SonarQube

http://localhost:9000/projects

Create project →



How do you want to create your project?

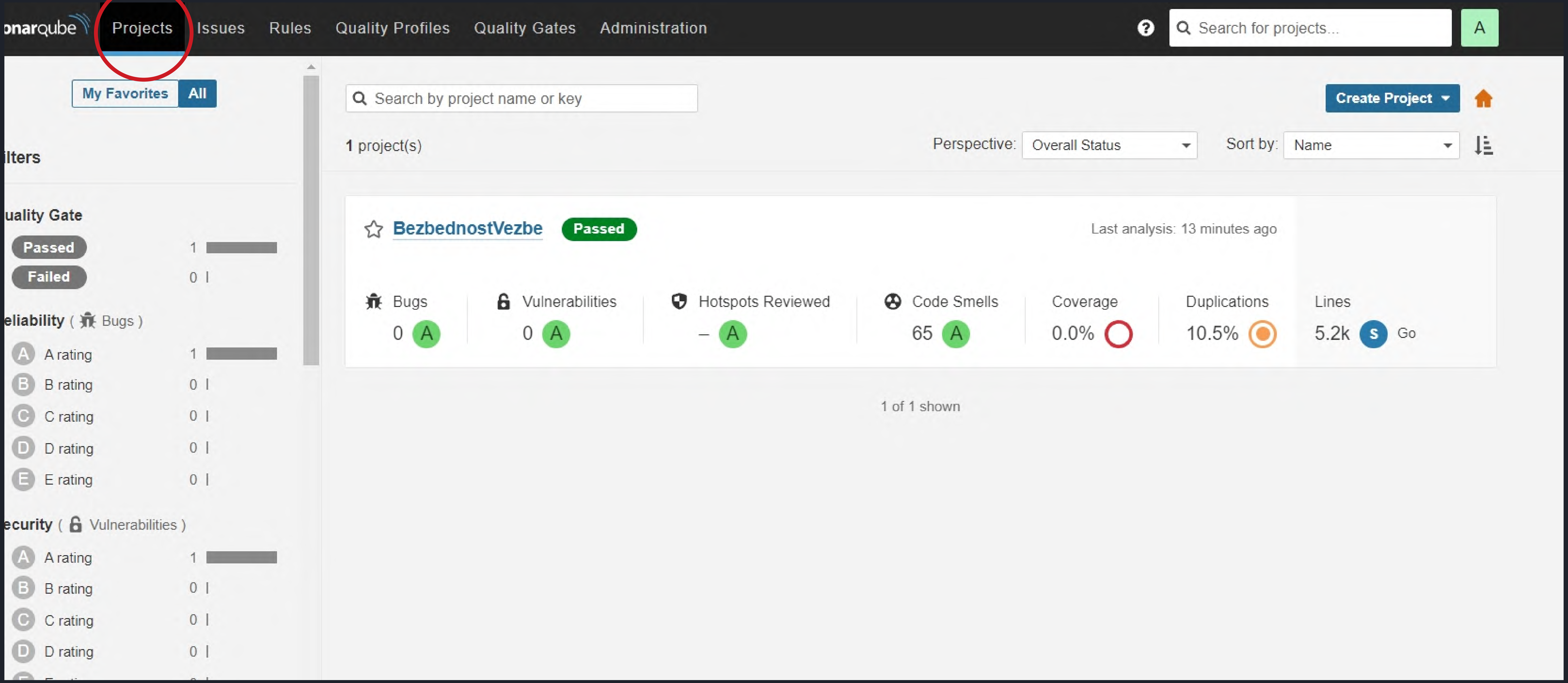
Do you want to benefit from all of SonarQube's features (like repository import and Pull Request decoration)? Create your project from your favorite DevOps platform.
First, you need to set up a DevOps platform configuration.

From Azure DevOps
Set up global configuration
From Bitbucket
Set up global configuration
From GitHub
Set up global configuration
From GitLab
Set up global configuration

Are you just testing or have an advanced use-case? Create a project manually.

SonarScanner

SonarQube



1 project(s)

Perspective: Overall Status

Sort by: Name

ilters

uality Gate

Passed	1	
Failed	0	

eliability (Bugs)

A rating	1
B rating	0
C rating	0
D rating	0
E rating	0

ecurity (Vulnerabilities)

A rating	1
B rating	0
C rating	0
D rating	0

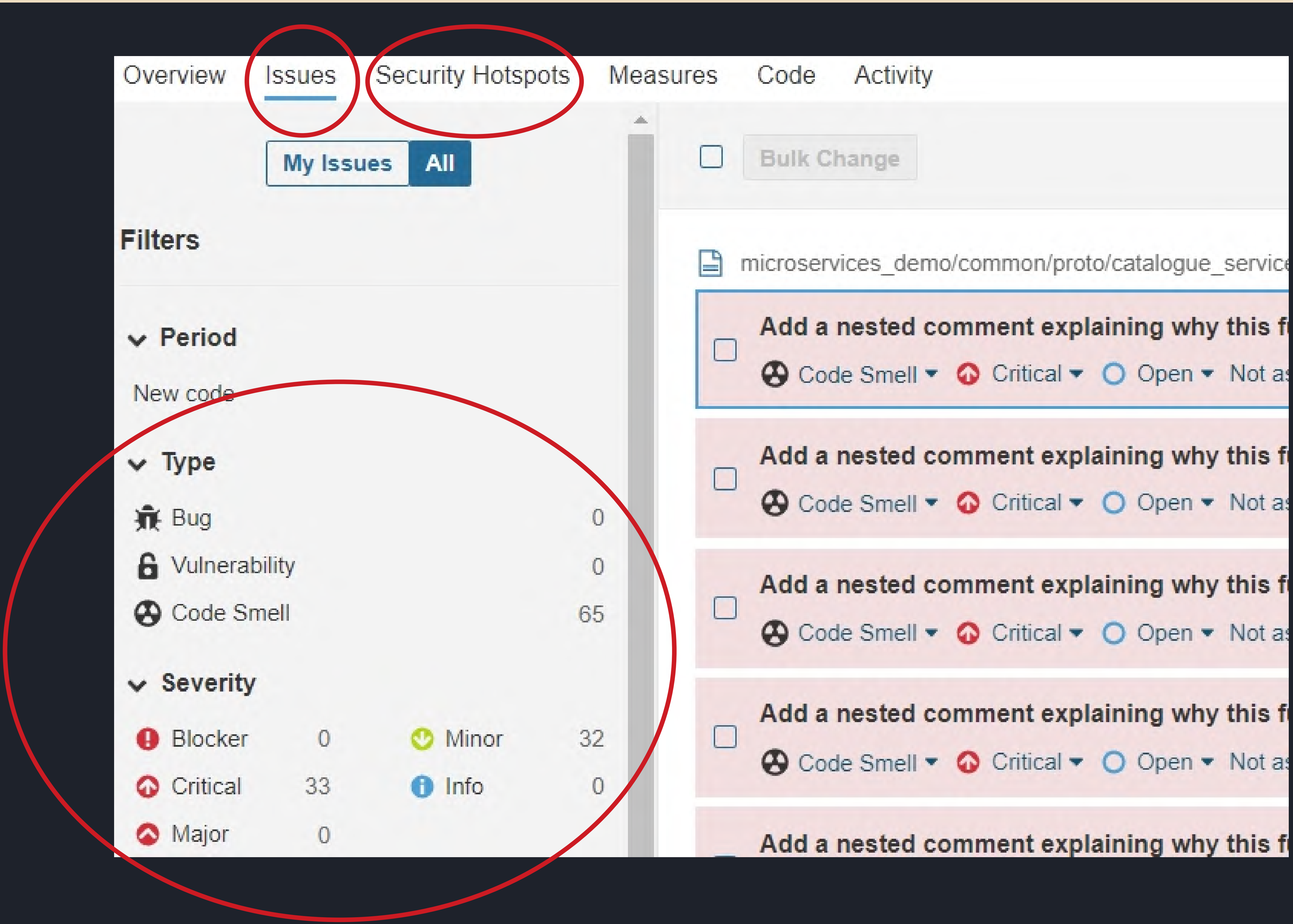
BezbednostVezbe Passed

Last analysis: 13 minutes ago

Bugs	Vulnerabilities	Hotspots Reviewed	Code Smells	Coverage	Duplications	Lines
0 A	0 A	– A	65 A	0.0%	10.5%	5.2k S Go

1 of 1 shown

SonarQube



Overview Issues Security Hotspots Measures Code Activity

My Issues All

□ Bulk Change

Filters

Period

New code

Type

Bug	0
Vulnerability	0
Code Smell	65

Severity

Blocker	0	Minor	32
Critical	33	Info	0
Major	0		

microservices_demo/common/proto/catalogue_service

□ Add a nested comment explaining why this f
Code Smell ▾ Critical ▾ Open ▾ Not as

□ Add a nested comment explaining why this f
Code Smell ▾ Critical ▾ Open ▾ Not as

□ Add a nested comment explaining why this f
Code Smell ▾ Critical ▾ Open ▾ Not as

□ Add a nested comment explaining why this f
Code Smell ▾ Critical ▾ Open ▾ Not as

Add a nested comment explaining why this f

SonarQube - izveštaj

U pisanoj formi dostaviti izveštaj o analizi koda od strane SonarQube (tekst+skrinšotovi)

- Analizirati ranjivosti
- Rešiti ranjivosti