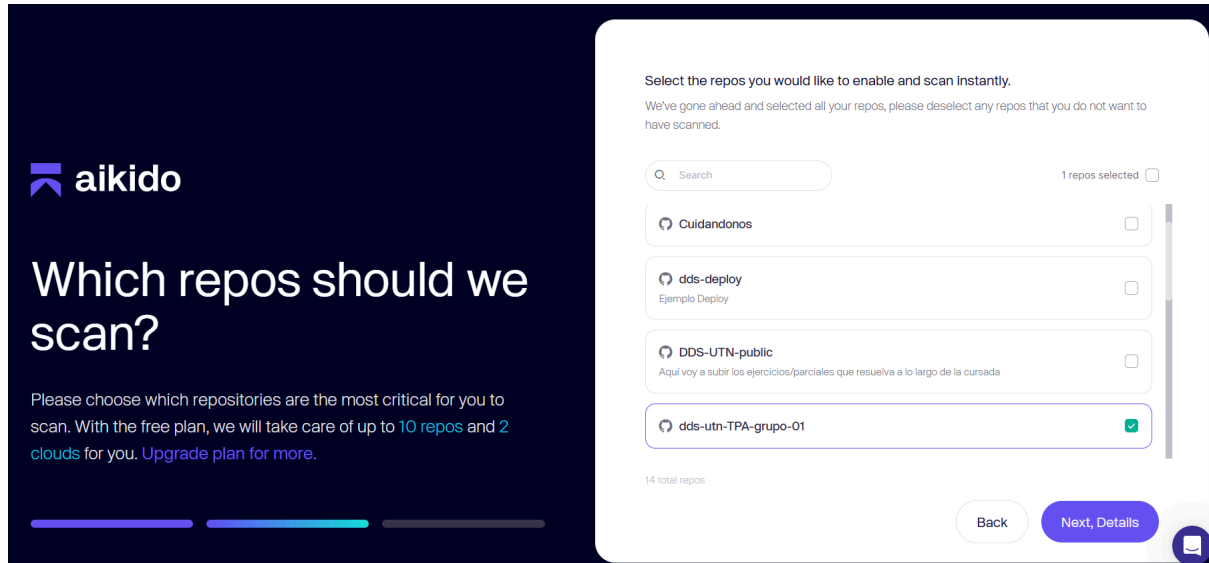
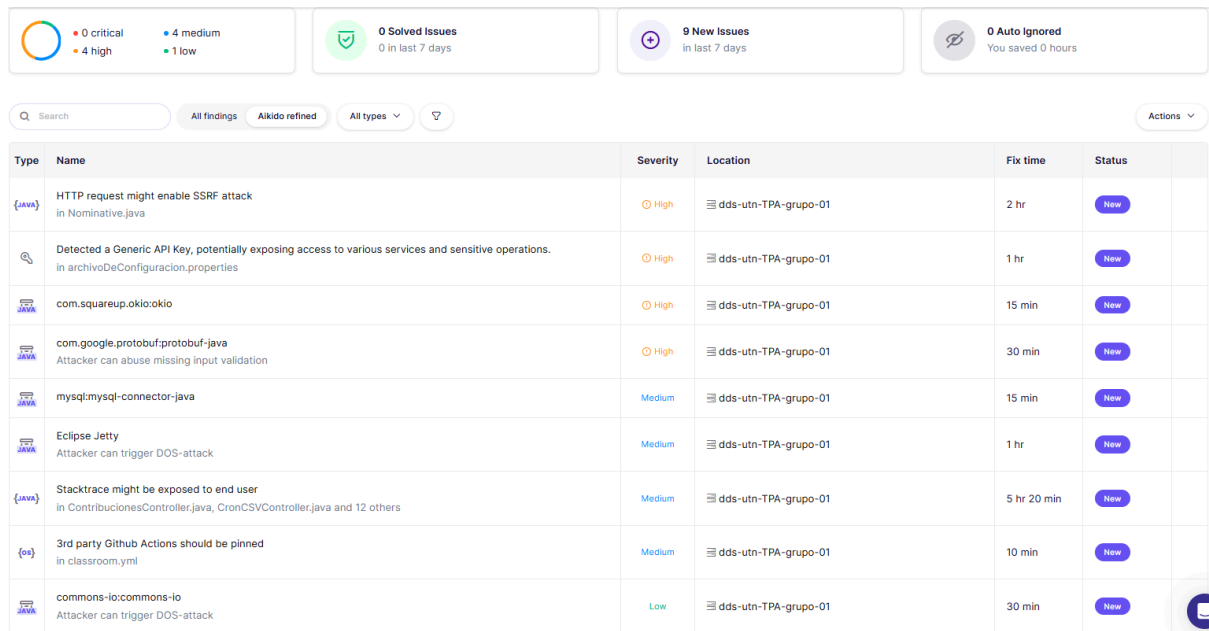


## Análisis de código estático con *Aikido Security*

Seleccionamos el repositorio de github que queremos analizar.



Realiza el análisis y redirige al dashboard principal con las vulnerabilidades encontradas.



Por cada vulnerabilidad, nos brinda ayuda de cómo solucionarla.

89

High Risk

HTTP request might enable SSRF attack

We found 2 issues: last detected 5 minutes ago

New

SAST

Overview

Notes

Tasks

Education

TL;DR

If an attacker can control the URL input leading into this http request, the attack might be able to performn a SSRF attack. This kind of attack is even more dangerous is the application returns the result of the URL fetch to the user. It can serve as an initial access point for an attacker for stealing credentials in the cloud.

How do I fix it?

If possible, only allow requests to whitelisted domains. If not, consult the article linked above to learn about other mitigating techniques such as disabling redirects, blocking private IPs and making sure private services have internal authentication. If you return data coming from the request to the user, validate the data before returning it to make sure you don't return random data.

[More information](#)

Show more

Subissues

Subissue

backend dds-utn-TPA-grupo-01

src/main/java/ar/utn/frba/dds/modelos/entidades/geografia/Nominative.java

High

Line 28 in Nominative.java

HttpURLConnection connection = (HttpURLConnection) new URL(url).openConnection();

View file →

src/main/java/ar/utn/frba/dds/modelos/entidades/geografia/Nominative.java

High

Line 69 in Nominative.java

URL url = new URL(urlString);

View file →

También, nos provee un Autofix para la solución de las vulnerabilidades que detecta que puede solucionar automáticamente.

Autofix

Automate your security with mass upgrades for your repositories

5 Dependency issues1 SAST issue0 IaC issues

Enable Autofix

Dependencies

SAST

IaC

Search

dds-utn-TPA-grupo-01 | pom.xml

Create PR

	Name	Severity	CVE	Version Upgrade	Status
<input type="checkbox"/>	com.google.protobuf:protobuf-java This package has 6 vulnerabilities	High	CVE-2022-35095 more	3.6.1 → 3.25.5minor	New
<input type="checkbox"/>	com.squareup.okio:okio This package has 1 vulnerability	High	CVE-2023-3635	1.17.2 → 1.17.6patch	New
<input type="checkbox"/>	mysql:mysql-connector-java This package has 2 vulnerabilities	Medium	CVE-2022-213631 more	8.0.17 → 8.0.28patch	New
<input type="checkbox"/>	Eclipse Jetty This package has 2 vulnerabilities	Medium	CVE-2024-81841 more	11.0.23 → 12.0.12major	New
<input type="checkbox"/>	commons-io:commons-io Attacker can trigger DOS-attack	Low	CVE-2024-47554	2.7 → 2.14.0minor	New