

**MICHIGAN STATE**  

---

**UNIVERSITY**

# Alpha Presentation

## Android Vulnerability Database

### The Capstone Experience

Team Google

Alessandro Bocchi

Brendan Wieferich

Omay Dogan

Frederick Fan

Trey Cosnowski

Seth Darling

Department of Computer Science and Engineering

Michigan State University

Spring 2024



*From Students...  
...to Professionals*

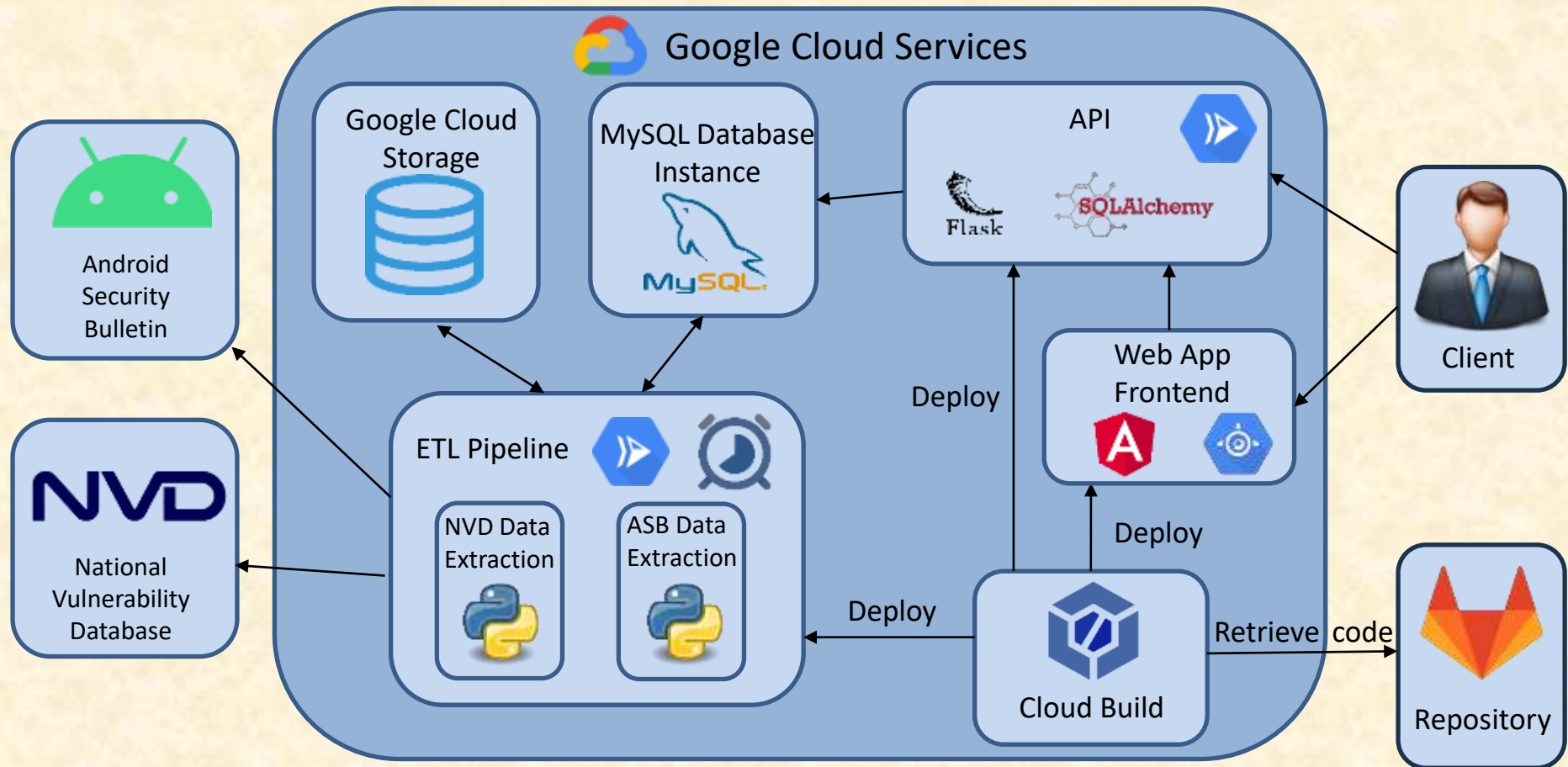


# Project Overview

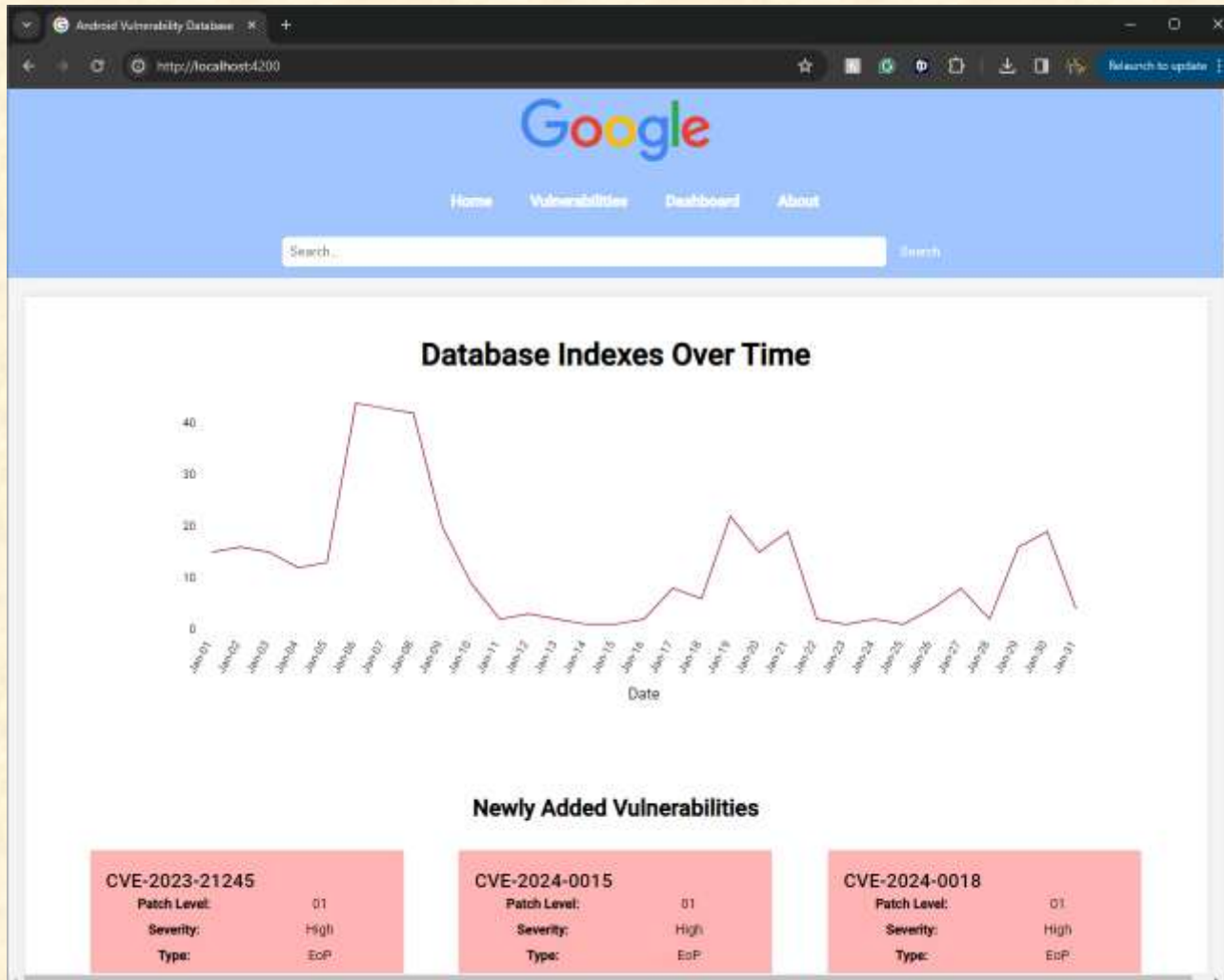
- Compile Android Security Bulletin and National Vulnerability Database vulnerabilities into one place.
- Enable OEMs to identify high priority security vulnerabilities.
- Easy to use web-application implementing our API to allow Users to query vulnerabilities.



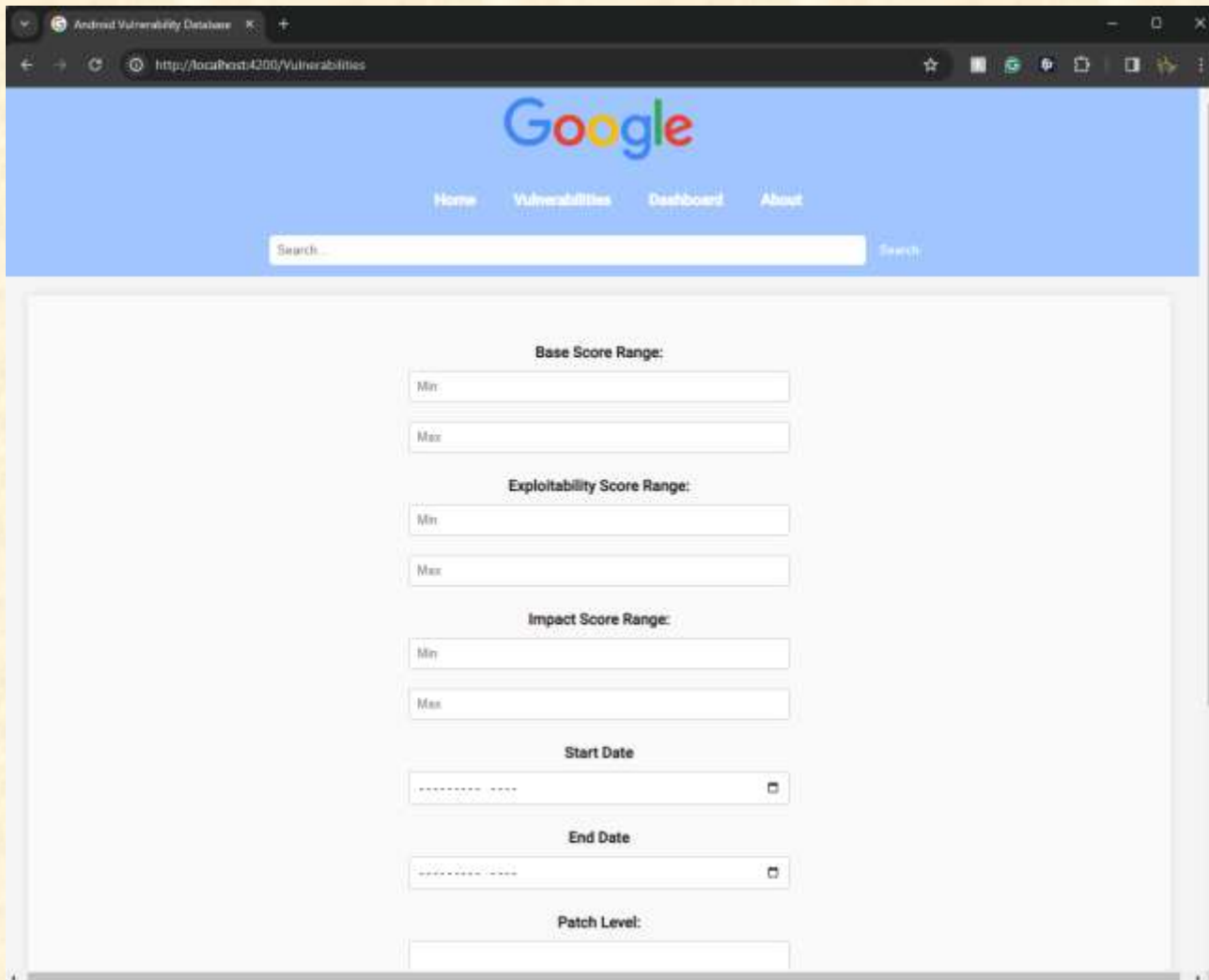
# System Architecture



# Home Screen



# Vulnerability Custom Query

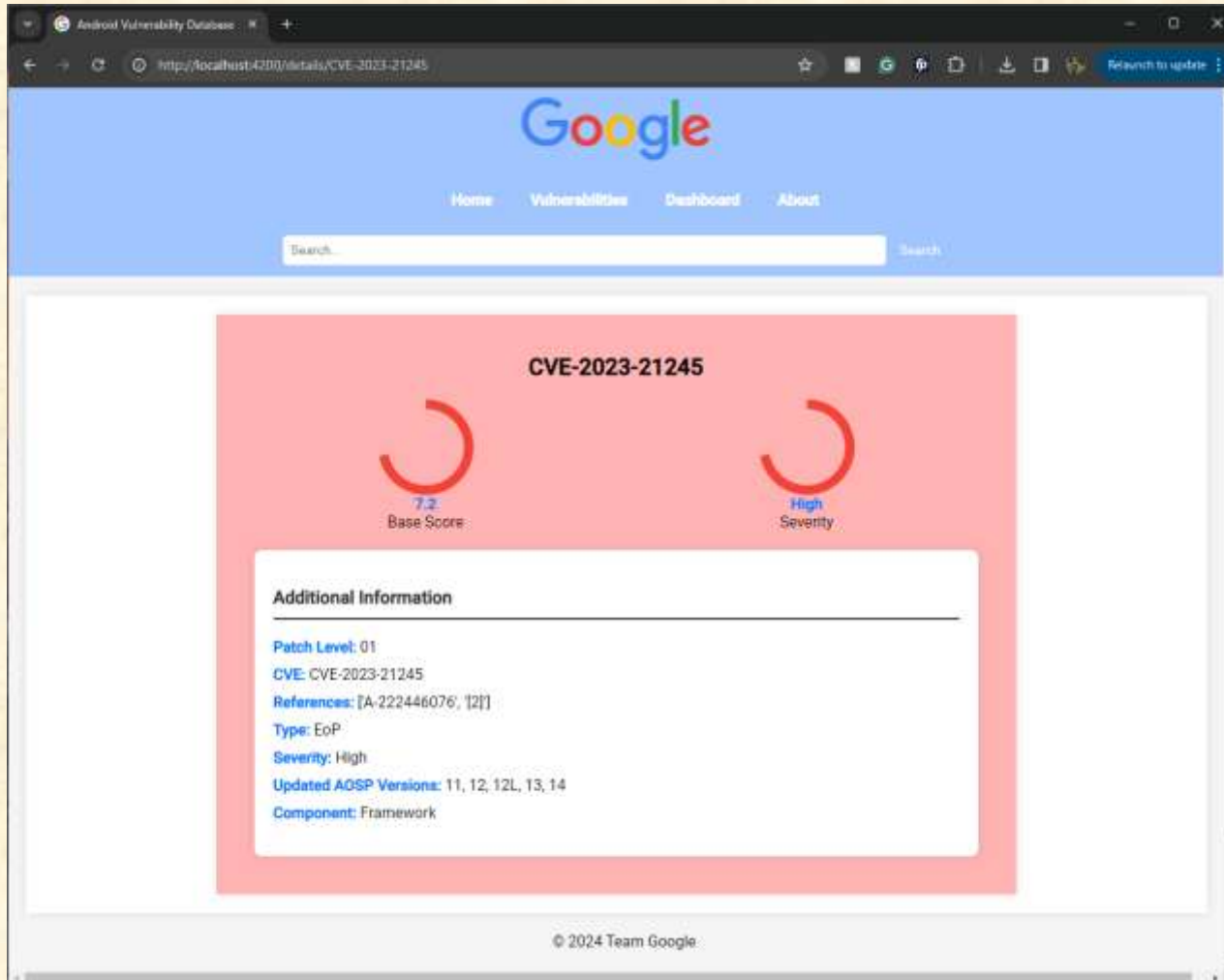


The screenshot shows a web browser window with the URL `http://localhost:4200/Vulnerabilities`. The page features a blue header with the Google logo and navigation links for Home, Vulnerabilities, Dashboard, and About. Below the header is a search bar. The main content area contains a form for creating a custom query with the following sections:

- Base Score Range:**
  - Min:
  - Max:
- Exploitability Score Range:**
  - Min:
  - Max:
- Impact Score Range:**
  - Min:
  - Max:
- Start Date:**
- End Date:**
- Patch Level:**



# Individual Vulnerability Page



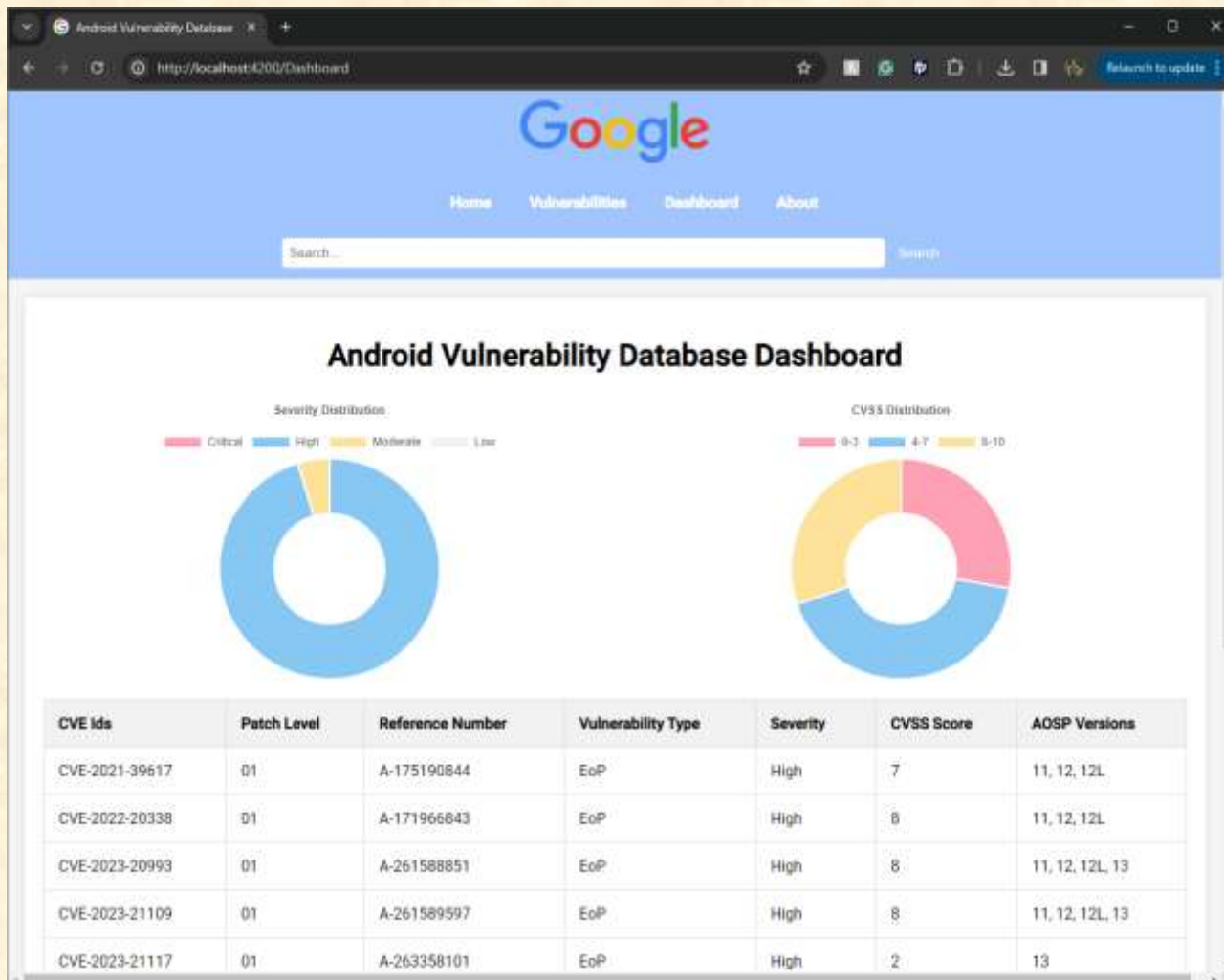
The screenshot shows a web browser window displaying the Android Vulnerability Database page for CVE-2023-21245. The page features a blue header with the Google logo and navigation links for Home, Vulnerabilities, Dashboard, and About. A search bar is located below the header. The main content area is highlighted with a red border and contains the following information:

- CVE-2023-21245**
- 7.2 Base Score** (represented by a red circular gauge)
- High Severity** (represented by a red circular gauge)
- Additional Information**
  - Patch Level: 01
  - CVE: CVE-2023-21245
  - References: [A-222446076, [2]]
  - Type: EoP
  - Severity: High
  - Updated AOSP Versions: 11, 12, 12L, 13, 14
  - Component: Framework

© 2024 Team Google



# Vulnerability Dashboard





# API ETL deploy

The screenshot shows the Google Cloud Cloud Build dashboard. The top navigation bar includes the Google Cloud logo, the user account 'cse498-teamgoogle-ss24', the current project 'cloud build', a search bar, and notification icons. The left sidebar contains navigation links for Dashboard, History, Repositories, Triggers, and Settings. The main content area is titled 'Dashboard' and shows the region 'us-central1'. A description states: 'This dashboard shows recently triggered builds. You can see all builds, including manually submitted builds, on the History page.' Below this is a filter input field. The main build list shows a successful build for the trigger '- API-ETL-deploy'. The table below details the build information:

Latest Build	Duration	Trigger description	Source	Commit
<a href="#">2/17/24, 12:45 PM</a>	00:08:56	-	-	-

Below the table, there are summary statistics: 'Build History' with a bar chart and a 'View all' link; 'Average Duration' of 00:08:17; and 'Pass - Fail %' of 100% - 0%.

At the bottom, there is a section for 'No Builds: - deploy' with the note 'This trigger has not run any builds. [Edit trigger](#)'.



# NVD Extract

The screenshot displays the Google Cloud Functions console interface. At the top, the Google Cloud logo and account information 'cse498-teamgoogle-ss24' are visible. A search bar is present with the text 'Search (/) for resources, docs, products, and more'. The main navigation bar shows 'Cloud Functions' and 'Function details' for the 'nvd-extract' function. The function is noted as '2nd gen' and 'Deployed at Feb 17, 2024, 12:52:37 PM'. The URL is 'https://us-central1-solid-gamma-411111.cloudfunctions.net/nvd-extract'. A 'Powered by Cloud Run' badge is also present.

The console tabs include METRICS, DETAILS, SOURCE (selected), VARIABLES, TRIGGER, PERMISSIONS, LOGS, and TESTING. The runtime is Python 3.11 and the entry point is 'main'. A 'DOWNLOAD ZIP' button is available.

The source code for 'main.py' is shown in a code editor:

```
1 import functions framework
2 from datetime import datetime, timedelta
3 from google.cloud import storage
4 import os
5 from nvd_extract_lib import nvd_data_extract
6
7 # execute the processes for extracting and storing the nvd data
8 @functions_framework.http
9 def main(request):
10     # connect to GCP bucket
11     client = storage.Client(project="solid-gamma-411111")
12     bucket = client.get_bucket('nvd-extract-data')
13
14     # generate start/end dates [to be changed later]
15     start = [2024, 1, 1]
16     stop = [2024, 2, 1]
17     end = [2024, 2, 1]
18     start_date = datetime(start[0], start[1], start[2])
19     stop_date = datetime(stop[0], stop[1], stop[2])
20     end_date = datetime(end[0], end[1], end[2])
21
```



# Cloud Scheduler

The screenshot displays the Google Cloud Cloud Scheduler interface. At the top, the Google Cloud logo and project name 'cse498-teamgoogle-ss24' are visible. A search bar contains the text 'cloud build'. Below this, the 'Cloud Scheduler' page title is shown, along with a 'Jobs' tab and several action buttons: '+ CREATE JOB', 'REFRESH', 'FORCE RUN', 'EDIT', 'COPY', 'PAUSE', 'RESUME', 'DELETE', and 'LEARN'. The interface is divided into two sections: 'SCHEDULER JOBS' (selected) and 'APP ENGINE CRON JOBS'. A 'Filter' button is present on the left. The main content is a table with the following columns: Name, Status of last execution, Region, State, Description, Frequency, Target, Last run, Next run, and Actions. Two jobs are listed: 'monthly-nvd-pull' (Success, Enabled, monthly frequency) and 'test-scheduler' (Has not run yet, Paused, daily frequency).

Name	Status of last execution	Region	State	Description	Frequency	Target	Last run	Next run	Actions
<a href="#">monthly-nvd-pull</a>	Success	us-central1	Enabled	monthly job to pull the data from the NVD database	0 23 3 1-12 0-6 (America/Detroit)	URL : https://us-central1-solid-gamma-411111.cloudfunctions.net/nvd-extract	Feb 17, 2024, 1:06:24 PM	Feb 17, 2024, 11:00:00 PM	⋮
<a href="#">test-scheduler</a>	Has not run yet	us-central1	Paused	will run once a day	0 0 * * * (America/Detroit)	Topic : projects/solid-gamma-411111/topics/test-asb-topic	Feb 17, 2024, 12:00:00 AM		⋮



# Logging

The screenshot displays the Google Cloud Logging Explorer interface. The top navigation bar includes the Google Cloud logo, the project name 'cse498-teamgoogle-ss24', and a search bar containing 'cloud build'. The left sidebar shows navigation options: Logging, Overview, Dashboards, Explore (Metrics explorer, Logs explorer, Log analytics, Trace explorer), and Detect (Alerting, Metrics Scope, Release Notes). The main content area is titled 'Logs Explorer' and shows a 'Query' view for 'Cloud Scheduler Job +2' with a time range of '12:03:50 PM - 1:07:50 PM'. The interface includes a search bar for all fields, filters for 'Log fields' and 'Histogram', and a 'Query results' table with 2 log entries. The first entry is an 'AttemptStart' event at 13:06:24.022, and the second is an 'AttemptFinished' event at 13:07:19.317. The log entry details show a JSON object with fields like '@type', 'jobName', 'targetType', and 'url'.

Google Cloud | cse498-teamgoogle-ss24 | cloud build | Search | 4 | ? | [Profile]

Logging | Refine scope | Project | Share link | Learn

Query | Recent (12) | Saved (0) | Suggested (8) | Library | Clear query | Save | Stream logs | Run query

12:03:50 PM - 1:07:50 PM | Search all fields | Cloud Scheduler Job +2 | Log name | Severity | Show query

Log fields | Histogram | Create metric | Create alert | Jump to now | More actions

Log fields | Histogram

Search fields and values | Expand log fields

RESOURCE TYPE

- Cloud Scheduler Job

SEVERITY

- Info

LOG NAME

- cloudscheduler.googleapis.com/executions

PROJECT ID

- solid-gamma-411111

LOCATION

- us-central1

Query results | 2 log entries | Find in results | Correlate by | Download

SEVERITY	TIME	EST	SUMMARY
Info	2024-02-17 13:06:24.022		AttemptStart
Info	2024-02-17 13:07:19.317		AttemptFinished

```
{ "@type": "type.googleapis.com/google.cloud.scheduler.logging.AttemptStart", "jobName": "projects/solid-gamma-411111/locations/us-central1/jobs/monthly-nvd-pull", "targetType": "HTTP", "url": "https://us-central1-solid-gamma-411111.cloudfunctions.net/nvd-extract" }
```

Explain this log entry | NEW | Copy | Similar entries



# BigQuery

The screenshot displays the Google Cloud BigQuery Studio interface. At the top, there's a navigation bar with the Google Cloud logo, a project selector (cse498-teamgoogle-ss24), and a search bar. Below this, a notification banner states: "Your BigQuery projects will have new capabilities after February 14, 2024. Services and roles will be enabled automatically to help with these changes." The main workspace is titled "Untitled 2" and shows a SQL query: `1 SELECT * FROM EXTERNAL_QUERY("solid-gamma-411111.us-central1.nvd-data", "SELECT * FROM vulnerabilities.vulnerabilities_data;");`. The query has been executed successfully, as indicated by a "Query completed" status. Below the query editor, the "Query results" section is active, displaying a table with columns: Row, patch\_level, cve, references\_, reference\_links, and type. The table contains three rows of data. At the bottom right, there are pagination controls showing "Results per page: 50" and "1 - 50 of 2974".

Your BigQuery projects will have new capabilities after February 14, 2024. Services and roles will be enabled automatically to help with these changes.

Analysis

- BigQuery Studio
- Data transfers
- Scheduled queries
- Analytics Hub
- Dataform
- Partner Center

Migration

- Assessment
- SQL translation

Administration

- Release Notes

Query results

Row	patch_level	cve	references_	reference_links	type
4	05	CVE-2012-6702	[A-29149404]	{A-29149404: 'https://android.googlesource.com/platform/external/expat/+/a11ff32280a863bff93df13ad643912ad9bf1302'}	None
5	05	CVE-2013-4397	[A-65944893]	None	N/A
6	05	CVE-2013-7446	[A-29119002]	None	None

Results per page: 50 1 - 50 of 2974



# What's left to do?

- Update ETL automation pipelines
- UI/UX improvements
- Minor web scraper adjustments
- Secure API from SQL injection attack
- Stretch Goals
  - Change Log
  - Scrape bulletins for other devices vulnerabilities



# Questions?

---

?

?

?

?

?

?

?

?

?





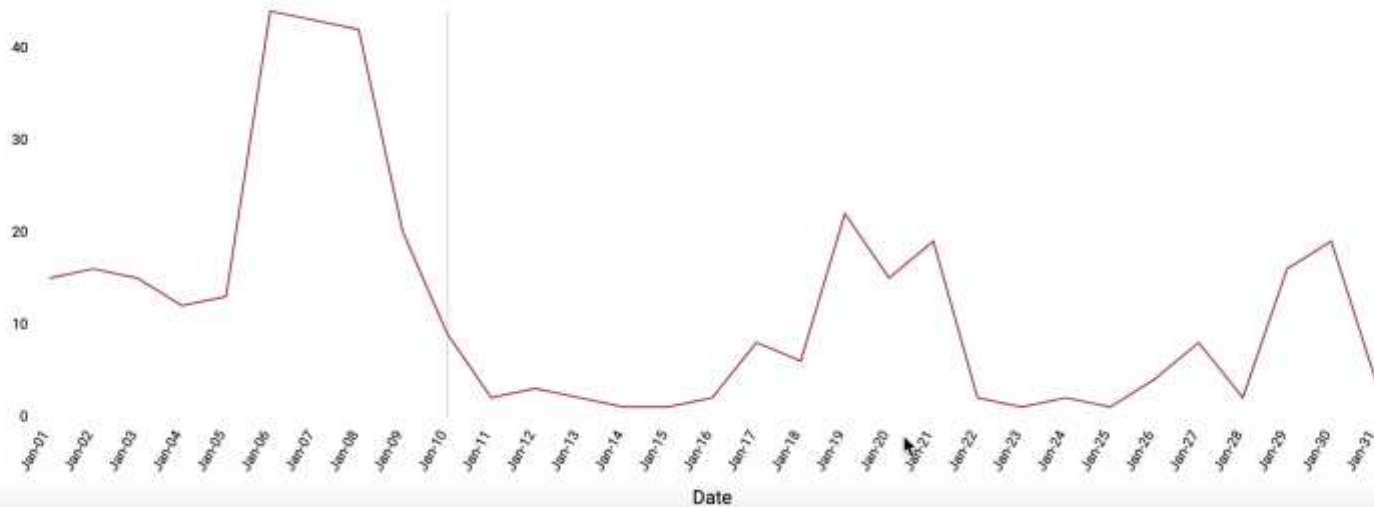


# Videos



[Home](#) [Vulnerabilities](#) [Dashboard](#) [About](#)

### Database Indexes Over Time



# Videos

The screenshot shows a web browser window with the URL `localhost:4200/vulnerabilities`. The page features a blue header with the Google logo and navigation links for Home, Vulnerabilities, Dashboard, and About. A search bar is located below the header. The main content area contains a search filter form with the following sections:

- Base Score Range:** Two input fields labeled "Min" and "Max".
- Exploitability Score Range:** Two input fields labeled "Min" and "Max".
- Impact Score Range:** Two input fields labeled "Min" and "Max".
- Start Date:** A date input field with a calendar icon.
- End Date:** A date input field with a calendar icon.
- Patch Level:** A single input field.
- Severity:** A dropdown menu.
- Search:** A button to execute the search.

At the bottom of the page, there is a copyright notice: © 2024 Team Google.

