MICHIGAN STATE UNIVERSITY Project Plan 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 Sponsor Overview

- Founded in 1998 by Larry Page and Sergey Brin, later reorganized under alphabet
- Best known for its search engine ("Just Google it"), acquired Android (aka Android Open-Source Project) in 2005
- Android is the most widely utilized mobile OS (Over 3 Billion active monthly users)
- Our sponsor Shailesh Saini, head on Android Platform Security and Assurance is responsible for ensuring that security issues for Android OS are handled efficiently
 android

Project Functional Specifications

- Situation: Android vulnerability data can be found in ASB and NVD.
- Problem: It is not intuitive to get the information needed from these sources.
- Solution: An API that provides this data and more.

Project Design Specifications

- Google Cloud
- Restful API to connect the web interface to the database
- User friendly Flask web interface to show API results
- Predetermined API calls for users
- Ability to create user specific API calls

Screen Mockup: Home Screen

Anthoid Vulnetabliky Datable O 22 https://wei	5-арр-1 <u>9</u> 6и/4q5иа-иса.	nunapp/home			x) 🖬 🔍 🖗 1	5 I 🖬
		Horo Searth	Goo vulnerabilities	gle Dashboard Con	end 0	
		Ar	ndroid Vulnerab	ility Database		
			A A - VISI		7 8 9	
CVE		Refrences	Type	Severity	Updated AOSP versions	
CVE-	2023-21245	A-222446076 2	EoP	High	11, 12, 12L, 13, 14	
CVE-	2024-0015	A-300090204	EoP	High	11, 12, 12L, 13	
CVE	2024-0018	A-300476626	EoP	High	11, 12, 12L, 13, 14	

The Capstone Experience

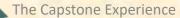
Team Google Project Plan Presentation

Screen Mockup: Database Dashboard

	080/dashboant		è 🔲 单 🗗
		Google	
		Home Vuinerabilities Dashboard Contact	
	Search		
		MySQL Dashboard	
An	troid Security Bulletin Data		NVD Data
	Litw	burn	0 0 5 5 9 5 1 - 7 0 7 1 - 10
Column1	Column2		
Column1 01		0	RCE
		0 [A-174737879', 'Upstream kernef', [2]', [3]', [4]', [5]', [6]']	
.01	Column2		RCE

Screen Mockup: Vulnerability Index

 Android Vulnerability Detabase -X + 		- 0
⊢ → C Q http://localhost.8080/vulnessbrility		* • • • •
	Google	
	Home Vulnerabilities Dashboard Contact	
Sam	ch	
	Vulnerability 1	
	CVE Code: CVE-2022-1234	
	References: Reference 1, Reference 2	
	Type: Type XYZ	
	Severity: High	
	Updated AOSP Versions: AOSP 10.0, AOSP 11.0	
	Base Score: 7.8 HIGH	
	Vulnerability 2	
	CVE Code: CVE-2022-5678	Date Range
	References: Reference 3, Reference 4	mi/dd/yyyy
	Type: Type ABC	ww/dd/yyyy
	Severity: Medium	
	Updated AOSP Versions: AOSP 9.0, AOSP 12.0	Filter by Field:
	Base Score: 8.8 HIGH	Severity
		Apply Fiters
	# 1014 Toom Cooks	



Team Google Project Plan Presentation

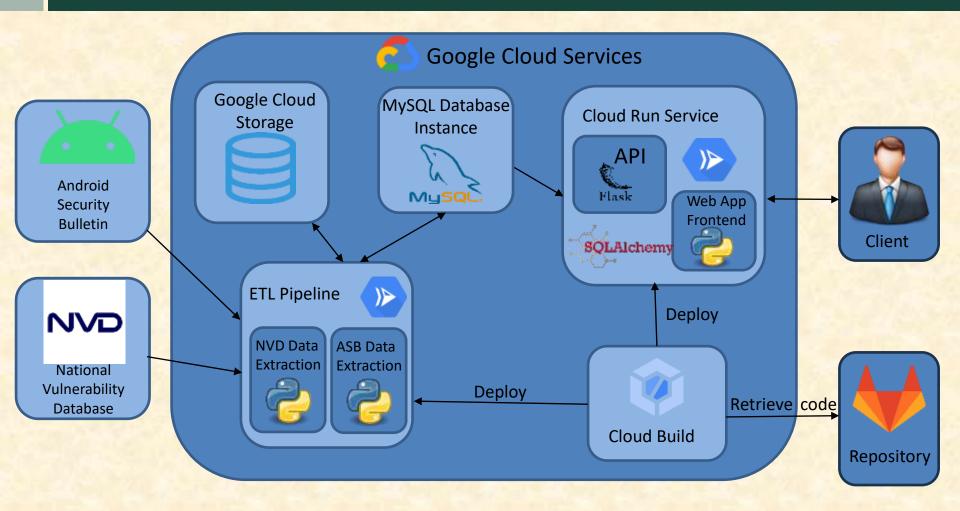
Screen Mockup: Vulnerability Page

← → ♂ Φ http://localhost.0060	ValmerabilityPage	🖈 🗉 💿 🗣 🖸 i 🛛 🞋
	Google	
	Home Volterabilities Dashkeard Contact	
	Search.	
		-
	CVE Code: CVE-2022-XXXX	
	References: Reference 1, Reference 2	
	Type: Type XYZ	
	Severity: High	
	Updated AOSP Versions: AOSP 10.0, AOSP 11.0	
	Base Score: 7.8 HIGH	
	For more details and mitigation steps, please refer to the official Android Security Bulletin, Android Security Bulletin	
	Back to Vulnerability List	
	© 2924 Team Google	

Project Technical Specifications

- Python Scripts for Web Scraping Data
- Store data and scripts in Google Cloud Storage
- MySQL database hosted on Google Cloud
- Virtual Machine hosted on Google Cloud
- Flask Web Application
- Flask REST API and SQL Alchemy for communication between website and MySQL database

Project System Architecture



Project System Components

- Hardware Platforms
 - Local Environments
 - Google Cloud Computing
- Software Platforms / Technologies
 - Google Cloud Platform
 - Cloud Run
 - Cloud Build
 - Cloud Storage
 - O MySQL Instance
 - Python
 - Flask
 - SQLAlchemy

Project Risks

Visualizing Data Patterns

- We are unsure what patterns to look for in our data and if there are patterns that are identifiable
- Communicate in detail with our customer for what patterns to look for and look at other vulnerability databases

Google Cloud APIs and services

- Don't know which of Google Cloud's many API's will best suit our needs
- Google has first party documentation on their APIs we can read
- Data Verification
 - Need to verify that the data we collect and store is correct
 - We have identified that Google Cloud has a Data Validation Tool (DVT) that we are testing

Questions?

