Vedette

Bug Deduplication Assistant

Eddy Peng, Sami Foell, Hitanshu Prajapati,
Harold Pham, Kyle Raychel

Information School UNIVERSITY of WASHINGTON

Google

android

The Convergence Crew

Eddy P.
Designer &
Project Manager

Sami F.
Designer &
Research Lead

Hitanshu P.
Full-Stack
Engineer

Harold P.
Tech Manager &
Back-end lead

Kyle R.
AI & Data
Engineer

Key Terms

01 BUGS/VULNERABILITIES/THREATS:

The terms represent system, service, or product flaws which could be exploited by bad actors.

02 BUG REPORT:

Formalized documentation of a flaw that is then reported for internal review.

Key Terms (Cont.)

03 BUG REPORTERS:

An external individual (not associated with Google) who finds and reports bugs.

04 ANDROID SECURITY ANALYSTS:

Google employees who respond to and evaluate reported bugs for legitimacy and severity.

Problem Overview

VULNERABILITY REWARDS PROGRAM (VRP)

Bug Reporter: finds a bug → files legit bug report → $$$ reward

01

90% of threat reports are not actionable

02

Duplicate bugs from different reporters

03

Waste time and energy on non threats

Problem Overview (Cont.)

PROBLEM STATEMENT

How might **Android Security Analysts** receive fewer duplicate submissions from **Bug Reporters** to arrive at a vetted 30% or more improvement in actionable reports?

* A benchmark of 30% less duplicate reports was set by our sponsors as a realistic goal

** Actionable: legit vulnerabilities Analysts can act on and reporters to be compensated

Solution Key Concepts

Reporter-Facing

To address the problem's source, internal information must be democratized for external reporter knowledge

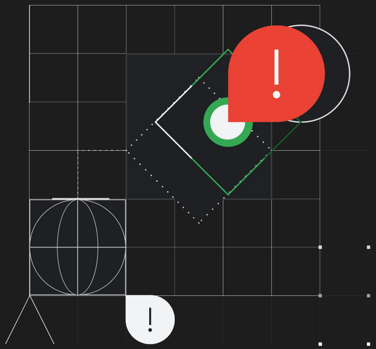
Duplicates Status

Incoming reports must be assessed for duplicate status to streamline review processes

System Automation

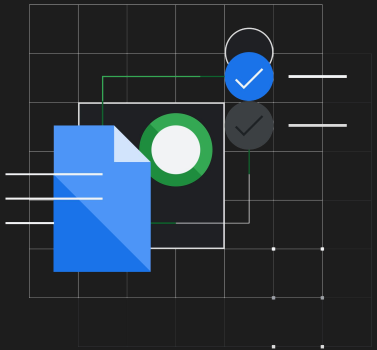
Manual and costly cybersecurity processes can be automated via AI for improved efficiency

Research Questions



01

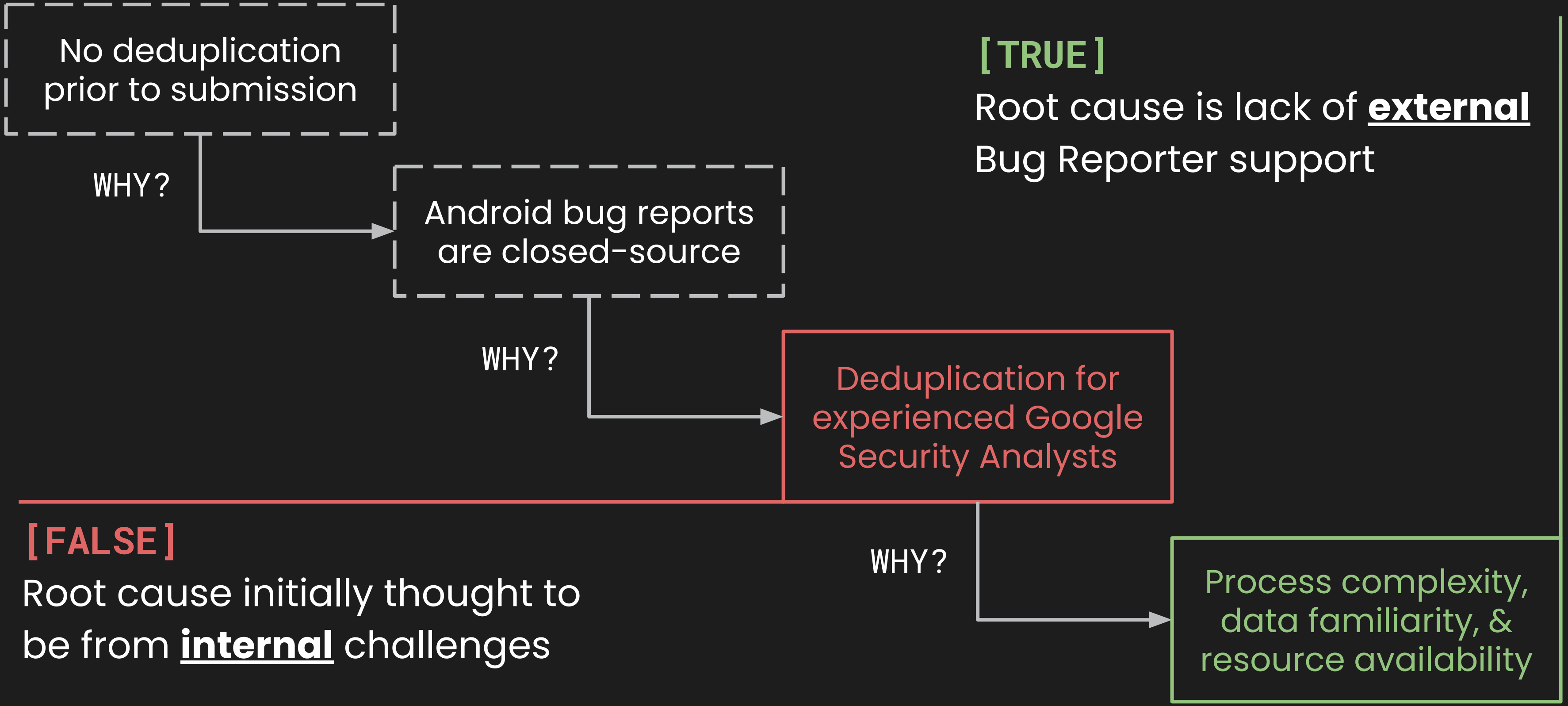
What are the primary challenges Google Security Analysts experience while triaging bug reports?



02

What kinds of human-AI interaction techniques are best suited to streamline the bug reporting process?

Root Cause Analysis



No deduplication prior to submission

WHY?

Android bug reports are closed-source

WHY?

Deduplication for experienced Google Security Analysts

WHY?

Process complexity, data familiarity, & resource availability

[TRUE]

Root cause is lack of **external** Bug Reporter support

[FALSE]

Root cause initially thought to be from **internal** challenges

Key Stakeholders

Two primary and one secondary personas were synthesized to ensure our next steps remained stakeholder-centric.

01 PRIMARY

Novice + Seasoned Bug Reporters

- Main source of duplicate bug reports
- Highly variable report quality
- Lack provided deduplication support

02 SECONDARY

Android Security Analysts

- Sole deduplication source
- Excessive investment on non-threats
- Unable to triage true threats

Novice Bug Reporter - Alex

Education: B.S. Computer Science

Job: Back-end Software Engineer

Pain-Points:

- Steep-learning curve = time-consuming
- Uncovering novel threats is a challenge

Goals:

- Enhance bug reporting best practices
- Develop a long-term growth mindset for hunting

Seasoned Bug Reporter - Jerry

Education: B.S. Information Security

Job: Senior Security Analyst

Pain-Points:

- Bug reporting = time-consuming & taxing
- Learning his bug report is a duplicate (no $$$)

Goals:

- Successfully uncover threats to earn $$$
- Pivot if he learns his report is a duplicate

Android Security Analyst - Kelly

Education: B.S. Cybersecurity & Assurance

Job: Android Security Analyst

Pain-Points:

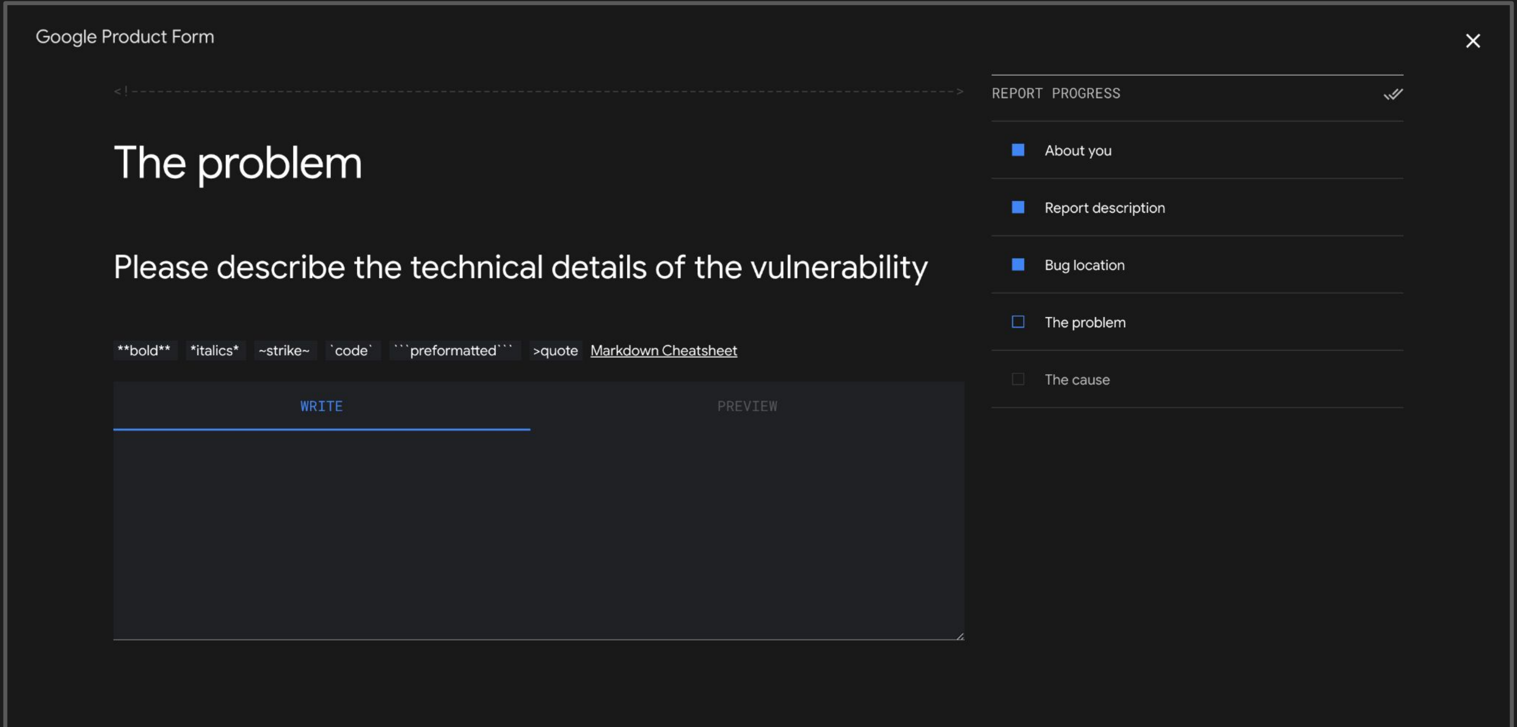
- Interactions with reporters who pedal false positives
- Discovering a duplicate report = wasted resources

Goals:

- A smooth triaging process with reporter collaboration
- Resolving real bugs efficiently

Google VRP Form

As a result of root cause analysis, we plan to add functionality to the existing bug reporting form while adhering to its design style.



Google Product Form

The problem

Please describe the technical details of the vulnerability

REPORT PROGRESS

■ About you

■ Report description

■ Bug location

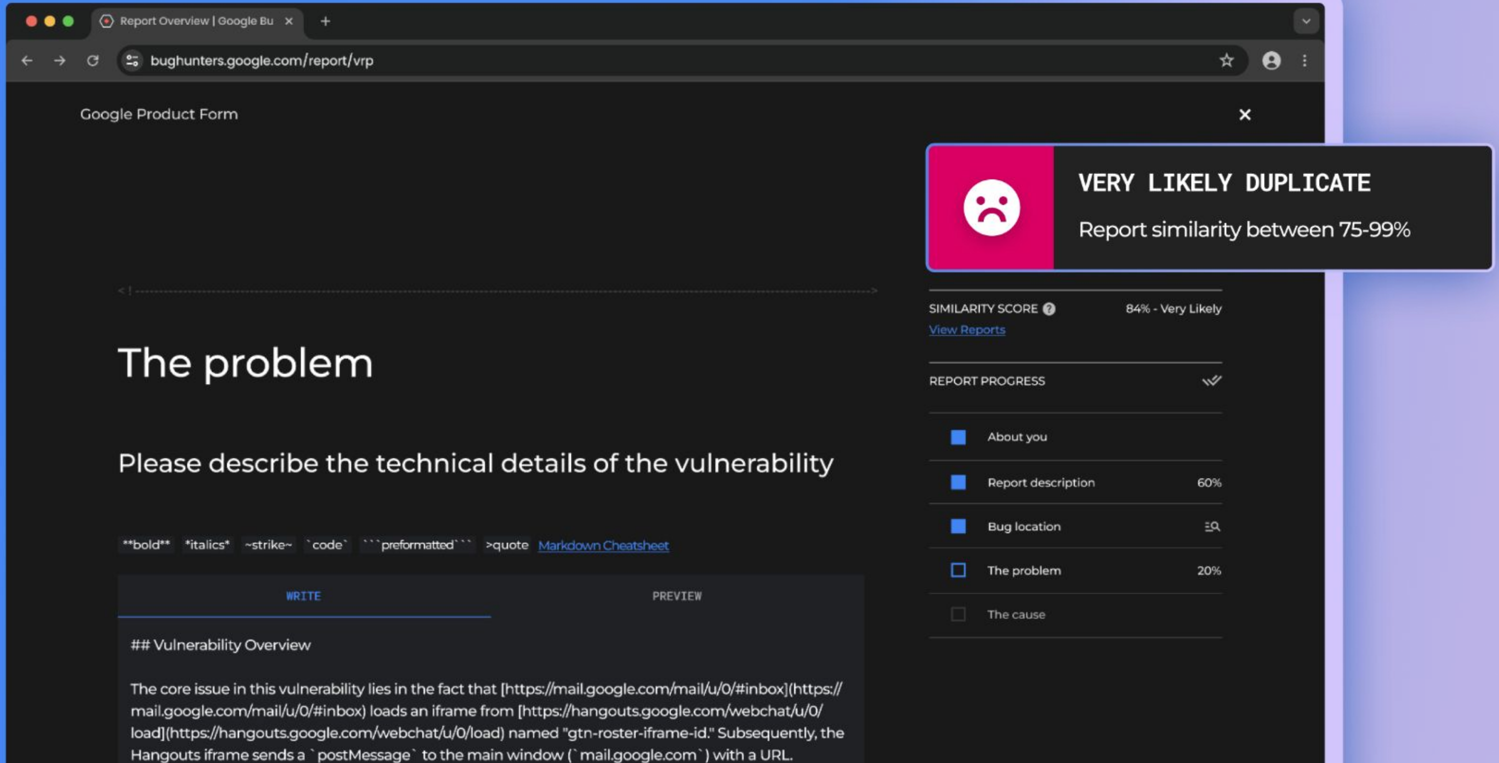
□ The problem

□ The cause

Introducing...

Vedette

Bug Deduplication Assistant



Report Overview | Google Bu
bughunters.google.com/report/vrp

Google Product Form

VERY LIKELY DUPLICATE

Report similarity between 75-99%

SIMILARITY SCORE ? 84% - Very Likely

View Reports

REPORT PROGRESS

■	About you	
■	Report description	60%
■	Bug location	
□	The problem	20%
□	The cause	

The problem

Please describe the technical details of the vulnerability

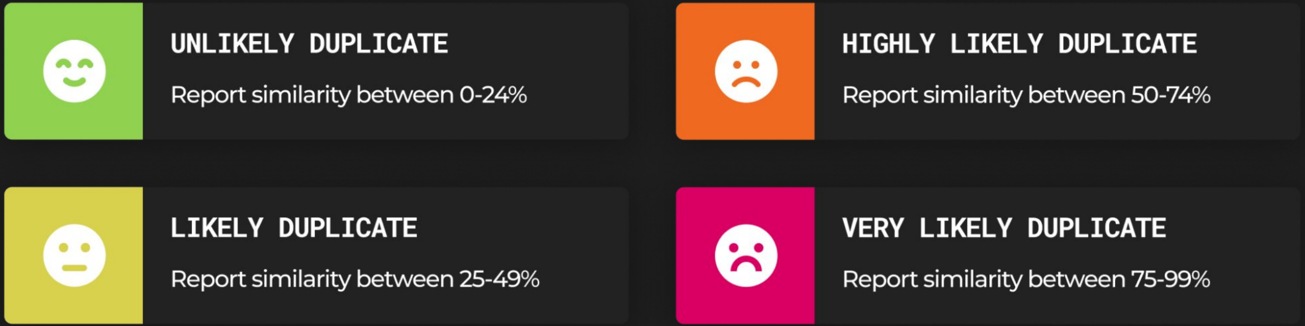
bold *italics* ~strike~ `code` ```preformatted``` >quote Markdown Cheatsheet
WRITE
PREVIEW

```
## Vulnerability Overview

The core issue in this vulnerability lies in the fact that [https://mail.google.com/mail/u/0/#inbox](https://mail.google.com/mail/u/0/#inbox) loads an iframe from [https://hangouts.google.com/webchat/u/0/load](https://hangouts.google.com/webchat/u/0/load) named "gtn-roster-iframe-id." Subsequently, the Hangouts iframe sends a `postMessage` to the main window (`mail.google.com`) with a URL.
```

Vedette - Similarity Score

The in-progress bug report is compared to other reports and assigned a status ranking based on 4 percentage thresholds.



UNLIKELY DUPLICATE

Report similarity between 0-24%

LIKELY DUPLICATE

Report similarity between 25-49%

HIGHLY LIKELY DUPLICATE

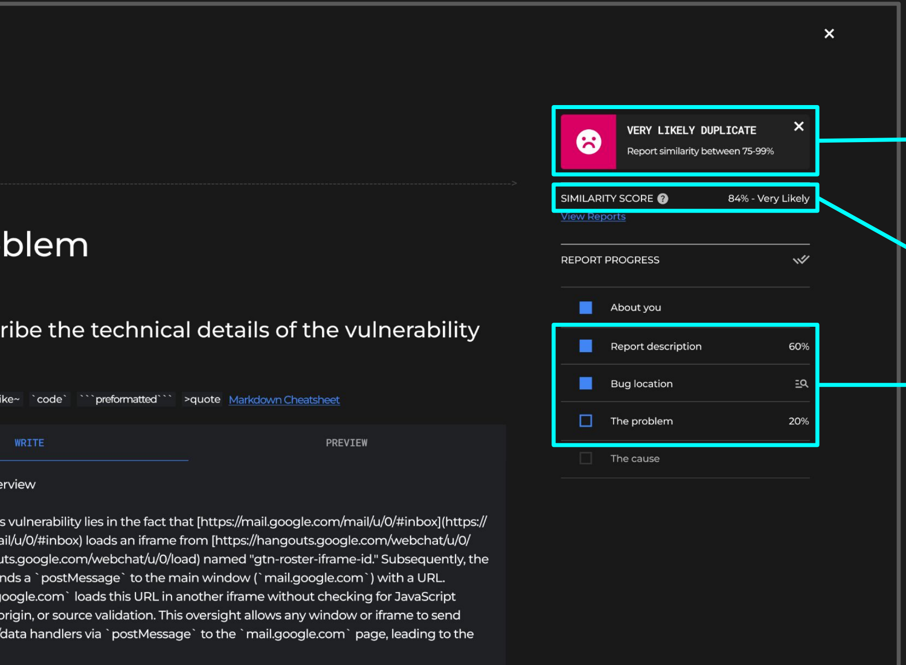
Report similarity between 50-74%

VERY LIKELY DUPLICATE

Report similarity between 75-99%

Vedette - Modified Sidebar

Bug reporters will be notified when their total similarity score crosses a threshold while field similarity offer granular insights.



VERY LIKELY DUPLICATE ✕

Report similarity between 75-99%

SIMILARITY SCORE ? 84% - Very Likely

View Reports

REPORT PROGRESS

■ About you

■ Report description 60%

■ Bug location

□ The problem 20%

□ The cause

blem

ribe the technical details of the vulnerability

ike~ `code` ```preformatted``` >quote Markdown Cheatsheet

WRITE PREVIEW

erview

s vulnerability lies in the fact that [https://mail.google.com/mail/u/0/#inbox](https://
ail/u/0/#inbox) loads an iframe from [https://hangouts.google.com/webchat/u/0/
uts.google.com/webchat/u/0/load) named "gtn-roster-iframe-id." Subsequently, the
nds a `postMessage` to the main window (`mail.google.com`) with a URL.
oogle.com` loads this URL in another iframe without checking for JavaScript
origin, or source validation. This oversight allows any window or iframe to send
data handlers via `postMessage` to the `mail.google.com` page, leading to the

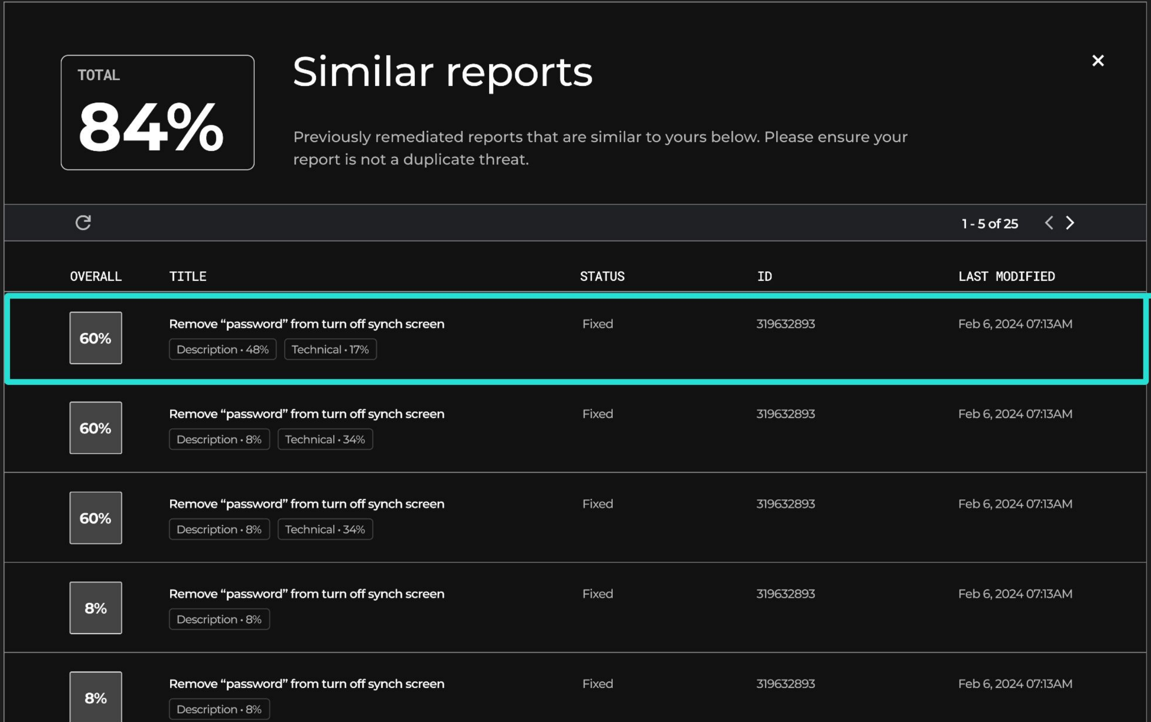
Similarity Status Update

Total Similarity Score

Form Field Similarity

Vedette - Similar Reports

Bug Reporters can view the reports that are contributing to their report's overall similarly score. The table also displays metadata.



TOTAL

84%

Similar reports

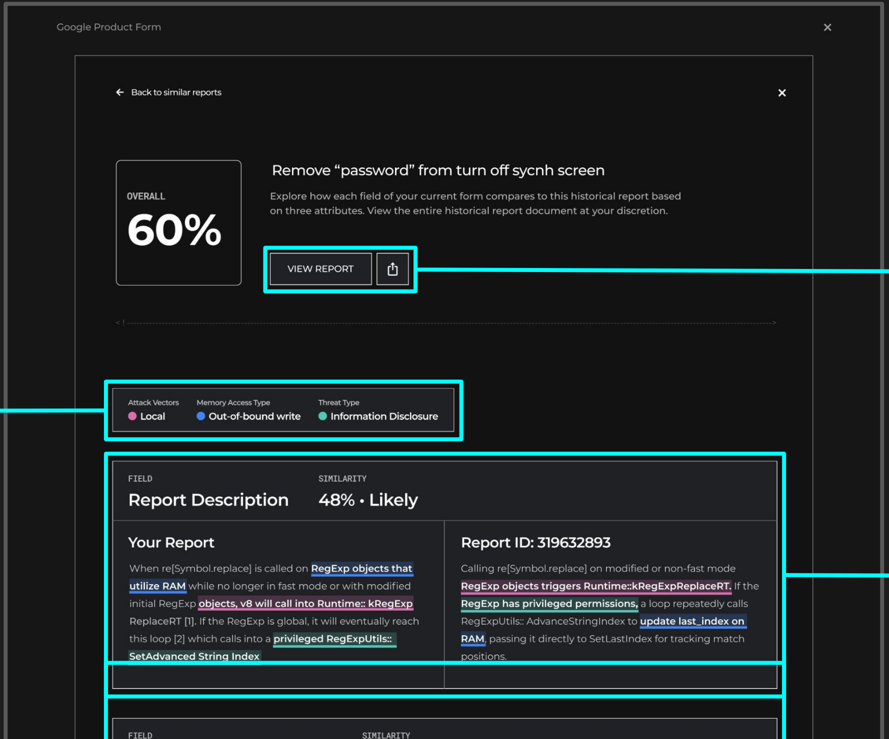
Previously remediated reports that are similar to yours below. Please ensure your report is not a duplicate threat.

OVERALL	TITLE	STATUS	ID	LAST MODIFIED
60%	Remove "password" from turn off synch screen Description · 48% Technical · 17%	Fixed	319632893	Feb 6, 2024 07:13AM
60%	Remove "password" from turn off synch screen Description · 8% Technical · 34%	Fixed	319632893	Feb 6, 2024 07:13AM
60%	Remove "password" from turn off synch screen Description · 8% Technical · 34%	Fixed	319632893	Feb 6, 2024 07:13AM
8%	Remove "password" from turn off synch screen Description · 8%	Fixed	319632893	Feb 6, 2024 07:13AM
8%	Remove "password" from turn off synch screen Description · 8%	Fixed	319632893	Feb 6, 2024 07:13AM

All Similar Reports
Overall, field, metadata

Vedette - Report Comparison

Bug Reporters can view the 3 attributes that cause the similarity and have the option to conduct analysis by exporting the report.



Google Product Form ×

← Back to similar reports ×

OVERALL

60%

Remove “password” from turn off sycnh screen

Explore how each field of your current form compares to this historical report based on three attributes. View the entire historical report document at your discretion.

Attack Vectors	Memory Access Type	Threat Type
● Local	● Out-of-bound write	● Information Disclosure

FIELD

Report Description

SIMILARITY

48% • Likely

Your Report

When re[Symbol.replace] is called on RegExp objects that utilize RAM while no longer in fast mode or with modified initial RegExp objects, v8 will call into Runtime:: kRegExp ReplaceRT [1]. If the RegExp is global, it will eventually reach this loop [2] which calls into a privileged RegExpUtils:: SetAdvanced String Index

Report ID: 319632893

Calling re[Symbol.replace] on modified or non-fast mode RegExp objects triggers Runtime::kRegExpReplaceRT. If the RegExp has privileged permissions, a loop repeatedly calls RegExpUtils:: AdvanceStringIndex to update last_index on RAM, passing it directly to SetLastIndex for tracking match positions.

FIELD SIMILARITY

View/Export Full Report

Threat Attributes

Report Content Comparison

Solution Validation Insights

7 EXPERT INTERVIEWS

Android Security + AWS Engineering + UW Academia

01

Utilize clear & simple language in solution

02

Export full report options for Bug Reporters

03

GPT prompting & similarity calculation guidance

Testing Methods

Inter-rater Reliability

- Rater agreement → κ=[-1, 1]
- **Goal:** Fair Agreement (≥ 0.2) between Vedette & Google Analysts

Percentage Difference

- (Avg. AI Deduplication Speed / Avg. Human Deduplication Speed) * 100%
- **Goal:** Extremely Fast (≥50%) compared to Google Analysts

Accuracy Ratio

- “X” AI identified duplicate reports / 10 true duplicate reports
- **Goal:** Fair Accuracy (≥ 30%) between Vedette and Google Analysts

Key Results

Vedette exceeded test benchmarks across 2/3 methodologies, proving to be an AI assistant of high efficacy.

.34
AGREEMENT

Inter-Rater Reliability

99%
FASTER

Percentage Difference

IP
ACCURATE

Deduplication Accuracy
(In progress)

Next Steps

After Capstone

Use Android Bug Reports

As NDAs were not signed, the current solution uses open-source Chromium bug reports rather than official Android VRP reports.

Usage Benefits:

- Fits solution’s UI
- Scaling Vedette to the entire platform is easier
- Less variability in report form structure

*Converting to Android reports is technically feasible
with solution architecture designed to fit bug reports across industry

Bug Reporters’ Perspective

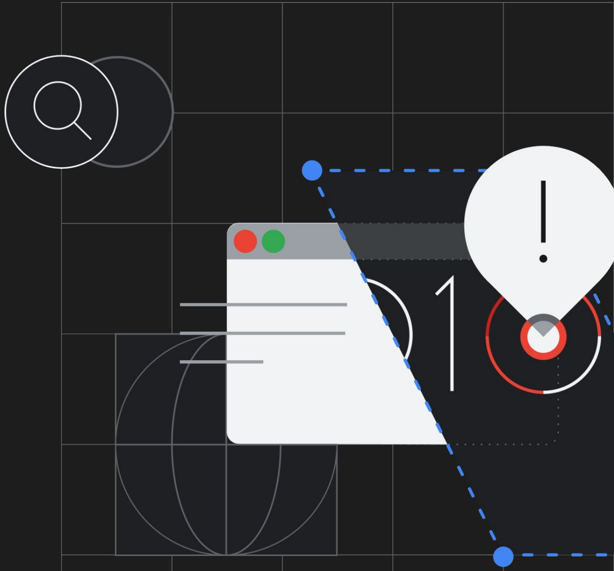
Though validated internally due to project scope, Vedette’s primary users are Bug Reporters. Thus, further research must be pursued.

Research Conducted:

- Bug Reporter online channels (Reddit/Internet Articles)
- Experts’ knowledge on general Bug Reporter behaviors

Research Requirements:

- Learn how Bug Reporters interact with the VRP
- Usability testing on solution with Bug Reporters



Form Suggestions & Templates

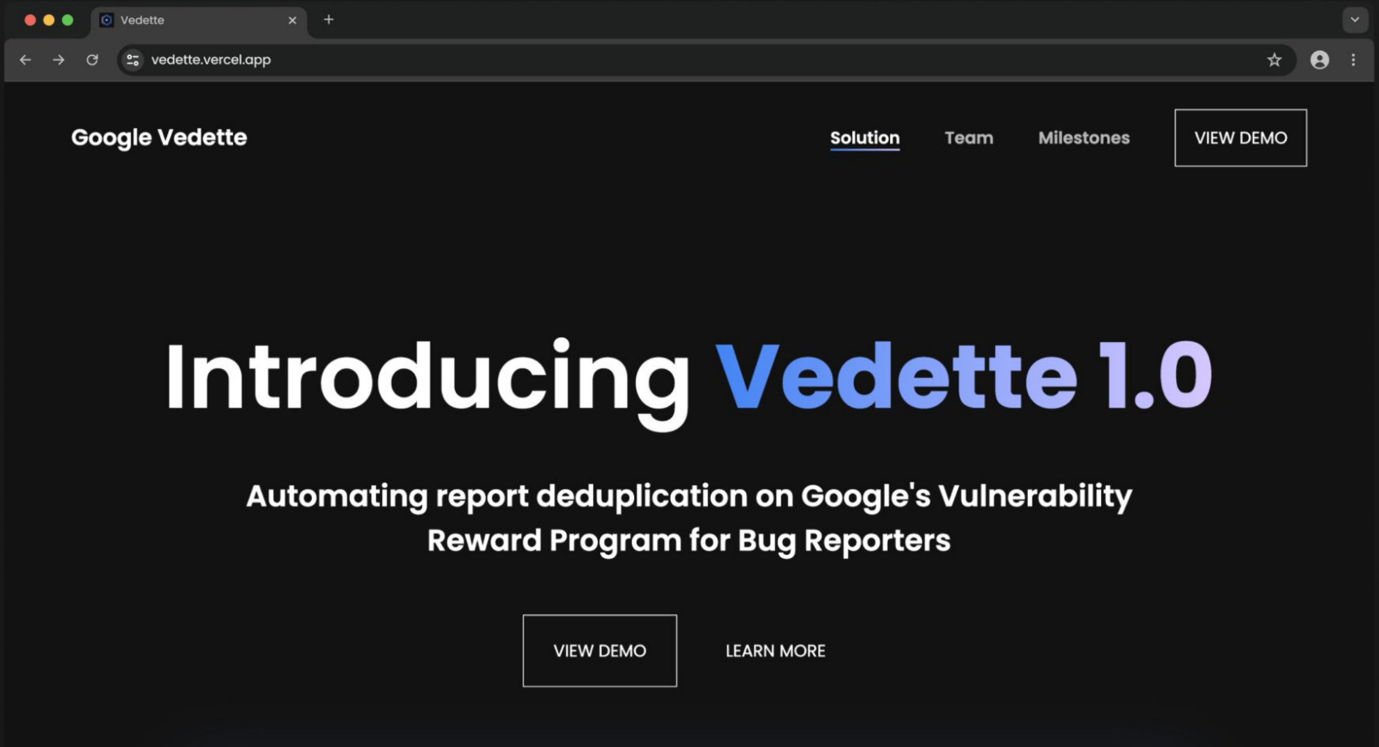
Due to time constraints and template knowledge-gaps, the 2nd epic was left as mid-fidelity wireframes. Yet, the feature is still viable.

Suggested Tasks:

- Confirm feasibility with Google Android Team
- Research common VRP bug report templates
- Flush out high-fidelity prototype
- Usability testing
- Implementation

vedette.vercel.app

To protect our sponsor’s GPT API key, the solution will stay internal.
This landing page showcases the solution to the public.



Introducing Vedette 1.0

Automating report deduplication on Google's Vulnerability Reward Program for Bug Reporters

Thank You!

Let's Connect!

Team's Linktree