The Benefits of Vulnerability Discovery and Bug Bounty Programs:

Case Studies of Chromium and Firefox

Soodeh Atefi, Amutheezan Sivagnanam, Afiya Ayman, Jens Grossklags, Aron Laszka

UNIVERSITY OF HOUSTON

TECHNISCHE UNIVERSITÄT MÜNCHEN

PennState

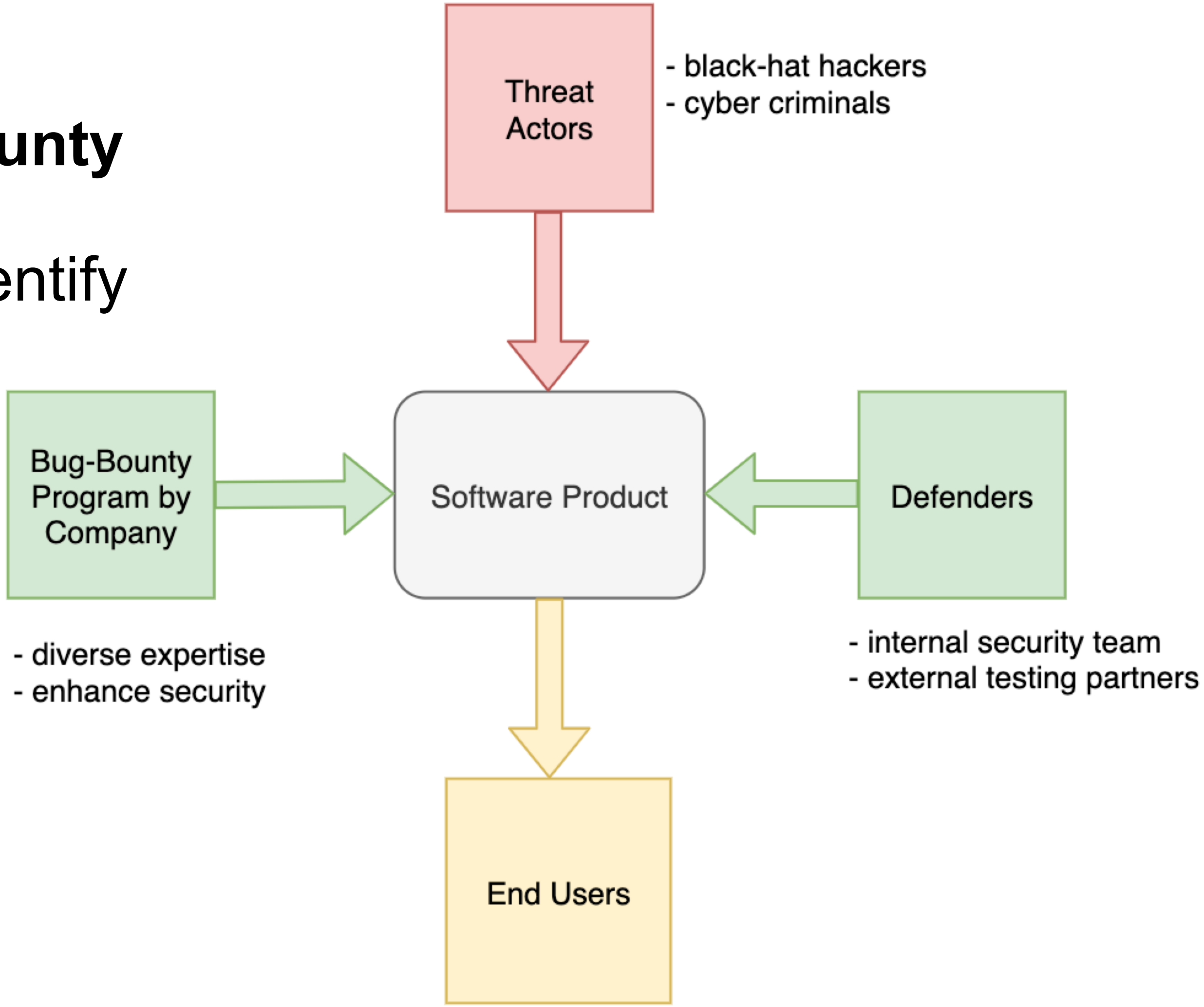
The Web Conference 2023

This material is based upon work sponsored by the National Science Foundation under Grant No. CNS-1850510.

Vulnerability Discovery and Bug-Bounty Programs

- Software companies launch **bug-bounty programs** and allow external **bug hunters** with diverse expertise to identify and **report vulnerabilities**.
  - e.g., Google, Mozilla, Facebook, and Microsoft

- Based on the validity/severity of the report, the software company will **reward the reporter**.



Do Vulnerability Discovery and Bug-Bounty Programs Improve Security?

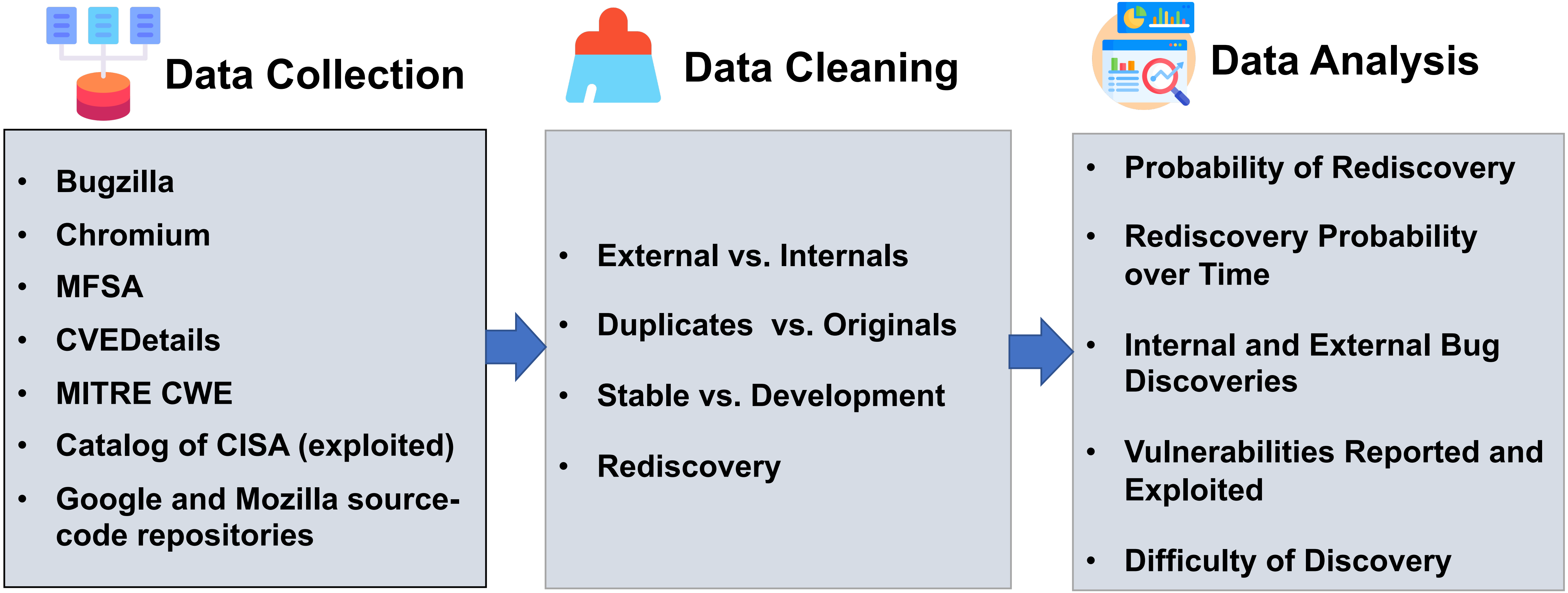
- Are vulnerabilities **rediscovered**? Or could **unpatched vulnerabilities** remain **hidden** forever?
- Are **certain types of vulnerabilities** more difficult to discover than others?
- Do **external bug hunters** complement the expertise of **internal security teams** by finding different types of vulnerabilities?
- Do **external bug hunters** report **the types of vulnerabilities** that would be **exploited by threat actors**?

Limitations of Previous Studies

Measuring the benefits of bug-bounties in terms of:

1. number of vulnerabilities reported;
2. inherent properties of the reported vulnerabilities, such as severity or exploitability;
3. **ignoring the likelihood of vulnerability discovery.**

Overview of Our Approach



Data Collection

- Bugzilla
- Chromium
- MFSA
- CVEDetails
- MITRE CWE
- Catalog of CISA (exploited)
- Google and Mozilla source-code repositories

Data Cleaning

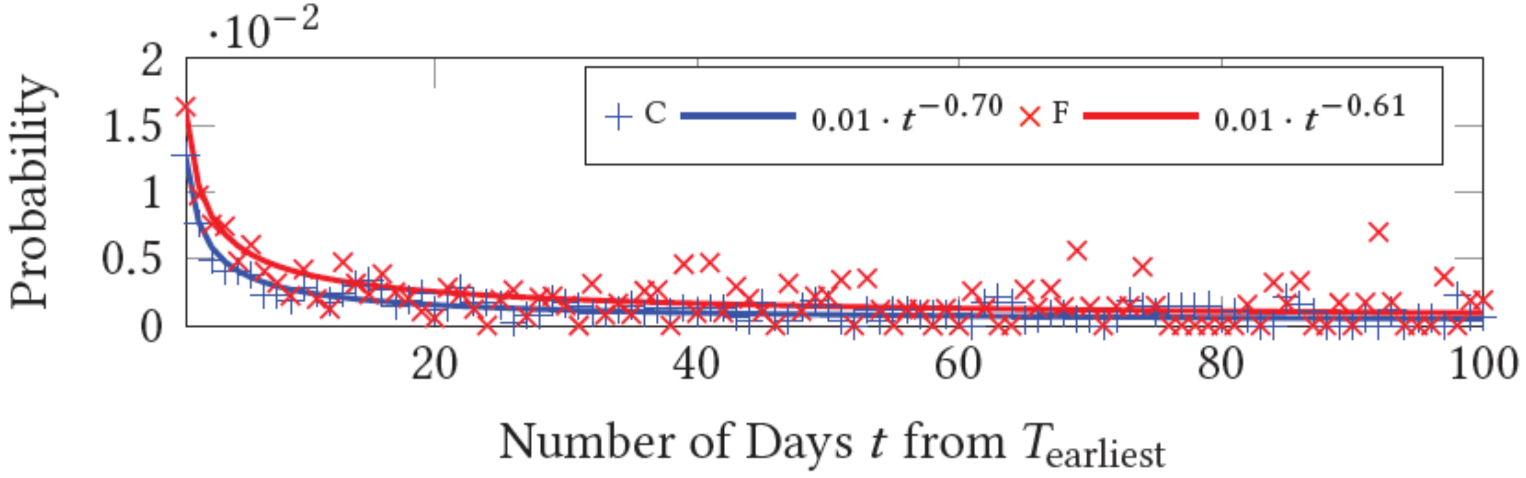
- External vs. Internals
- Duplicates vs. Originals
- Stable vs. Development
- Rediscovery

Data Analysis

- Probability of Rediscovery
- Rediscovery Probability over Time
- Internal and External Bug Discoveries
- Vulnerabilities Reported and Exploited
- Difficulty of Discovery

Our data and code are publicly available: https://doi.org/10.6084/m9.figshare.22056617

Rediscovery Probability and Rediscovery Probability over Time



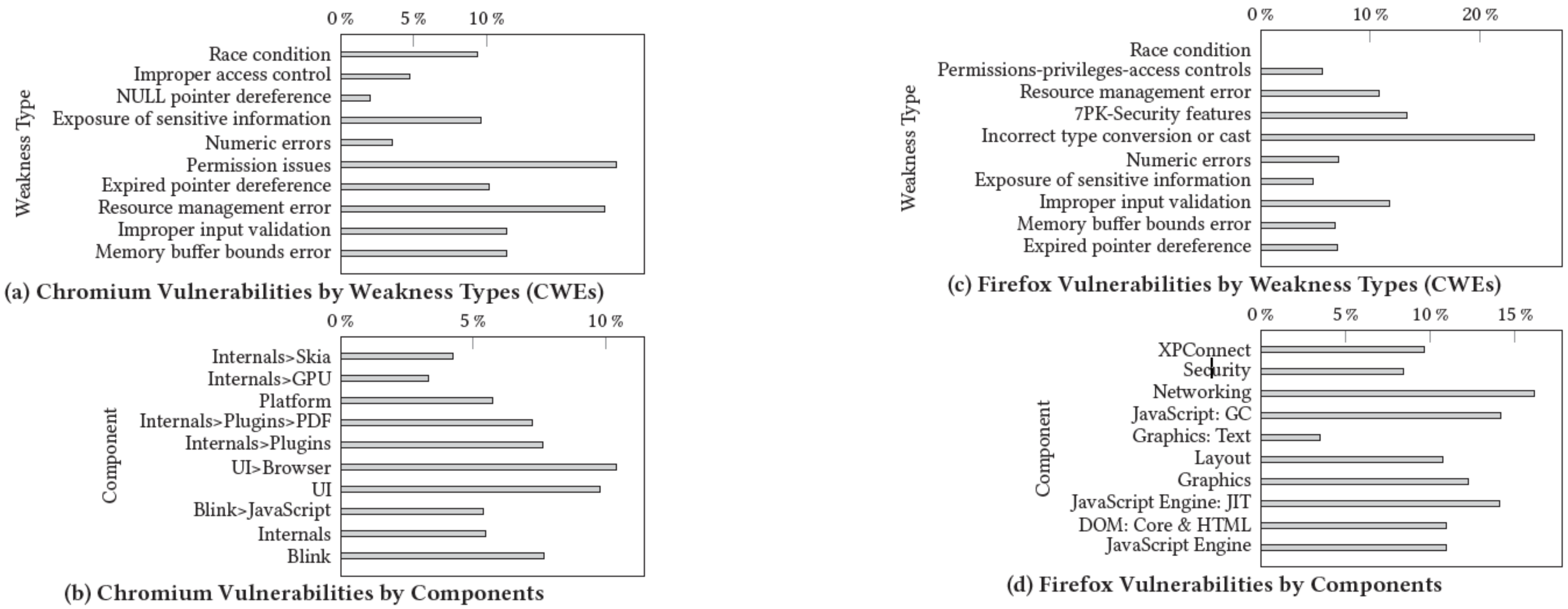
(a) Probability that a vulnerability is rediscovered on the t-th day after it is first reported ($\Pr[Re(t) | t < \Delta_{\text{fix}}]$).

- Some types of vulnerabilities seem to be much **easier to find** than others based on their rediscovery probabilities.
- Vulnerability discoveries are **clustered in time**, which suggests that there is a limited pool of easy-and-quick-to-discover vulnerabilities.
- Other vulnerabilities may **remain hidden for long**.

Difficulty of Discovery

Percentage of Vulnerabilities (**Chromium**)

Percentage of Vulnerabilities (**Firefox**)



(a) Chromium Vulnerabilities by Weakness Types (CWEs)

(b) Chromium Vulnerabilities by Components

(c) Firefox Vulnerabilities by Weakness Types (CWEs)

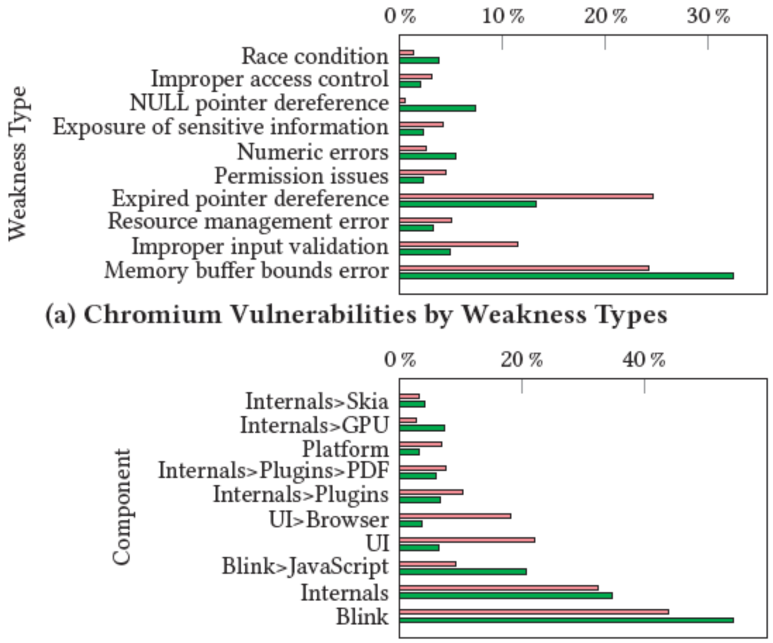
(d) Firefox Vulnerabilities by Components

Fraction of vulnerabilities that are rediscovered at least once in Chromium and Firefox.

- **Significant differences** between the rediscovery probabilities of **different types of vulnerabilities**.
- More **severe vulnerabilities receive higher rewards** and are also **rediscovered more** often than other vulnerabilities.
- **Therefore, vendors could include other properties of vulnerabilities in their reward policy to incentivize external bug hunters.**

Comparison of Internal and External Reports

Percentage of Vulnerabilities (Chromium)

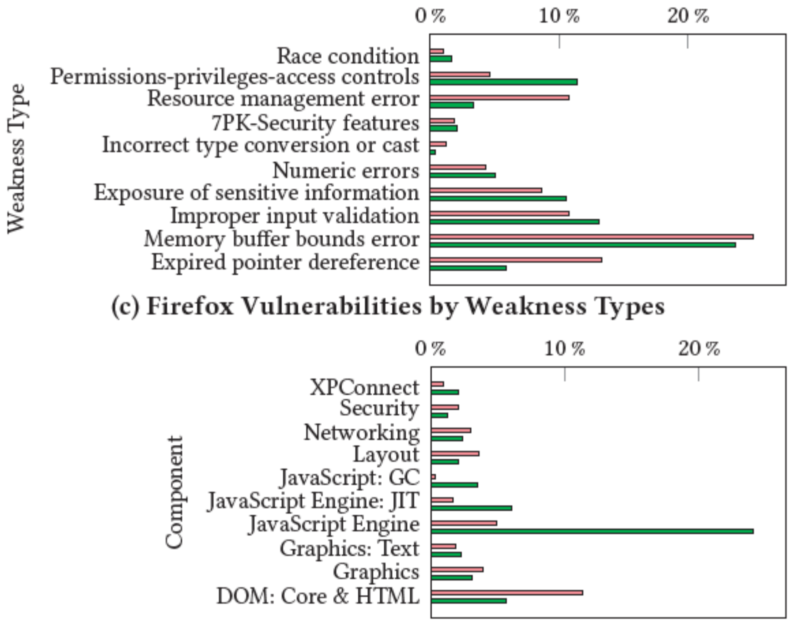


(a) Chromium Vulnerabilities by Weakness Types

(b) Chromium Vulnerabilities by Components

internal (🟩) and external (🟥)

Percentage of Vulnerabilities (Firefox)



(c) Firefox Vulnerabilities by Weakness Types

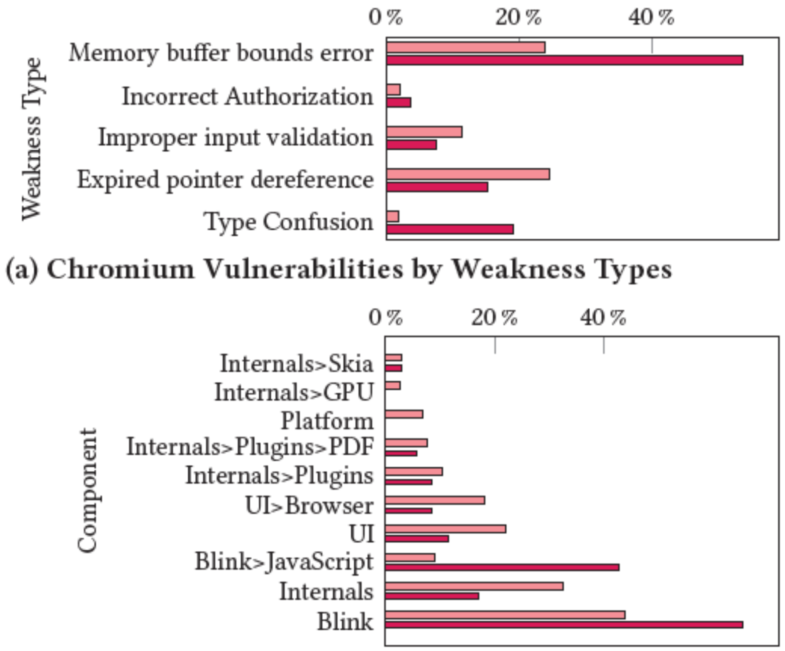
(d) Firefox Vulnerabilities by Components

internal (🟩) and external (🟥)

- **External** bug hunters and **internal** security teams report **different types of vulnerabilities.**
- This indicates that **bug-bounty programs do complement the expertise of internal teams**.

Comparison of Exploited Vulnerabilities and External Reports

Percentage of Vulnerabilities (**Chromium**)

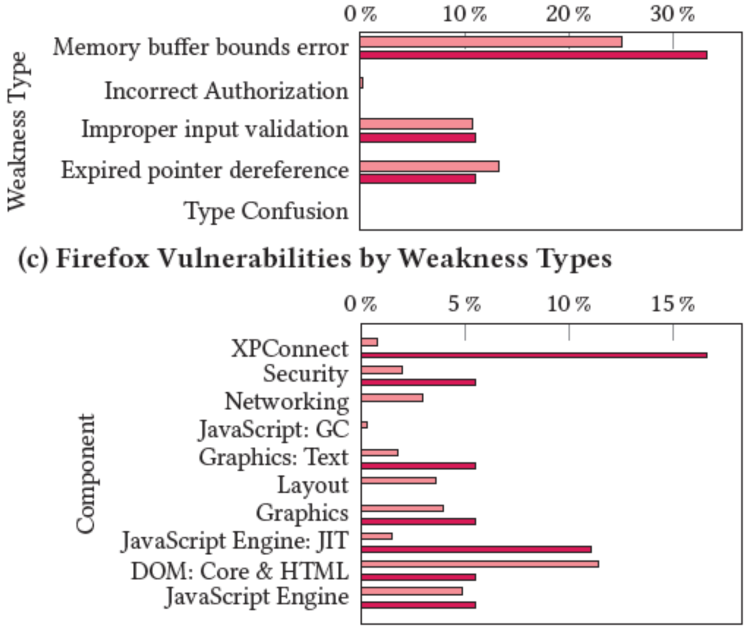


(a) Chromium Vulnerabilities by Weakness Types

(b) Chromium Vulnerabilities by Components

exploited vulnerabilities (🟥) external security reports (🟧)

Percentage of Vulnerabilities (**Firefox**)



(c) Firefox Vulnerabilities by Weakness Types

(d) Firefox Vulnerabilities by Components

exploited vulnerabilities (🟥) external security reports (🟧)

- There are **significant differences** between the **types of vulnerabilities** that are reported by **bug hunters** and those that are **exploited by threat actors**,
- This suggests that bug bounties could be more effective if they **incentivized bug hunters to shift their focus**.

Key Findings

- Some types of vulnerabilities seem to be much **easier to find** than others based on their rediscovery probabilities.
- There is a **limited pool of easy-and-quick-to-discover** vulnerabilities.
- There are significant **differences** between **the rediscovery probabilities** of **different types** of vulnerabilities.
- **External bug hunters complement internal security** by reporting different types of vulnerabilities.
- **Threat actors exploit different types of vulnerabilities** than external bug hunters.
  - Security might be improved by incentivizing bug hunters to search for different types of vulnerabilities.