Vulnerability Research & Bug Bounty

INFR11158/11230 Usable Security and Privacy

Yangheran (Lawrence) Piao

18/03/2025

THE UNIVERSITY *of* EDINBURGH

Overview

- Vulnerability Research
- Why Companies Need Hackers
- Impact of Bug Bounties
- Hacker Collaboration
- Take-home

What is Hacking or Vulnerability Research?

- https://www.youtube.com/watch?v=pxSp6HeM4RM
- https://www.youtube.com/watch?v=lD34wkOcCRE

So, you found a bug. What's next?

- Attack
- Sell it
- Disclosure

Full Disclosure

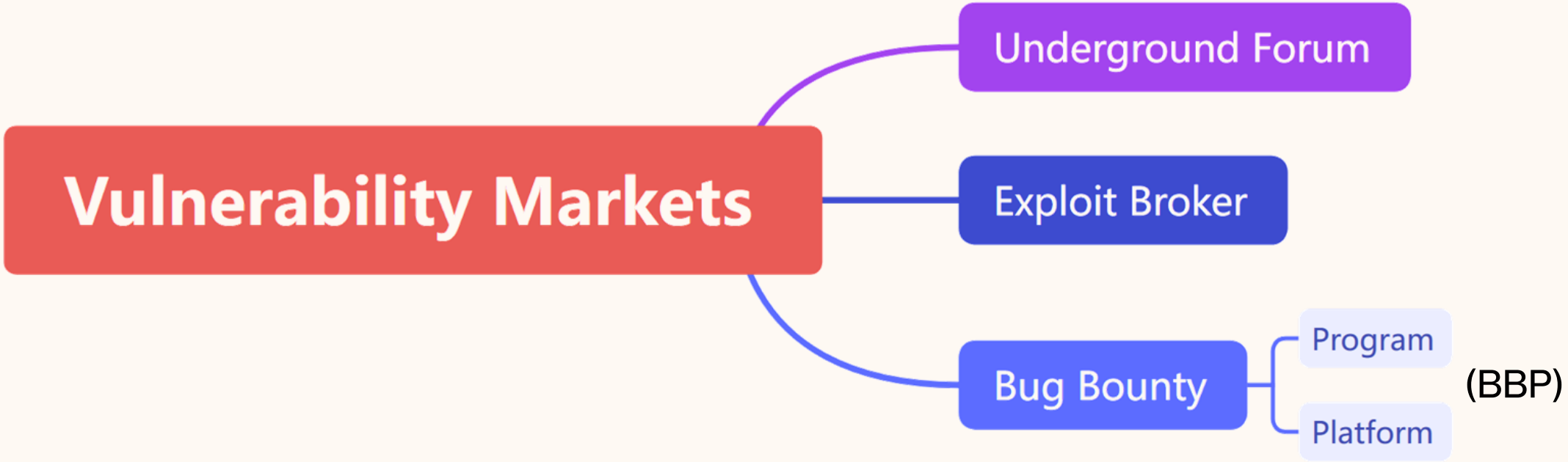
Disagree	Agree
• Nobody except researchers need to know the details of flaws	• FD helps the good guys more than the bad guys
• FD results in information anarchy	• Effective security cannot be based on obscurity
• Good guys who publish virus code may also have malicious intention	• Making vulnerabilities public is an important tool in forcing vendors to improve their products
• Safer if researchers keep details about vulnerabilities and stop arming hackers with offensive tools	• If an exploit is known and not shared, the vendor might be slower to fix the hole
• The risk associated with the publishing information outstrip its benefit	• Sharing information security with other professionals is an absolute necessity
• It serves to arm hackers with tools to break systems	

• Radianti, J. and Gonzalez, J.J. A preliminary model of the vulnerability black market. In 25th International System Dynamics Conference, 2007.

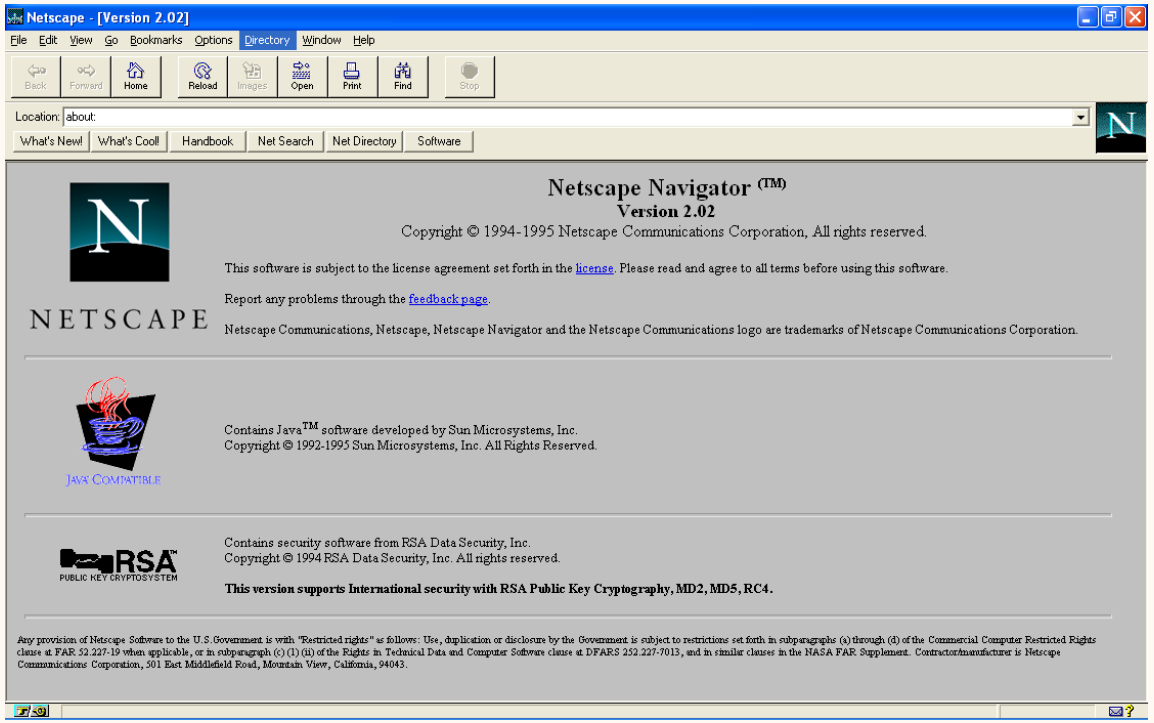
Responsible Disclosure

- Reporting directly to the affected company
- Follow the company’s disclosure process
- Allow time for the company to fix the bug
- Disclosure to the public after an embargo

Vulnerability Market

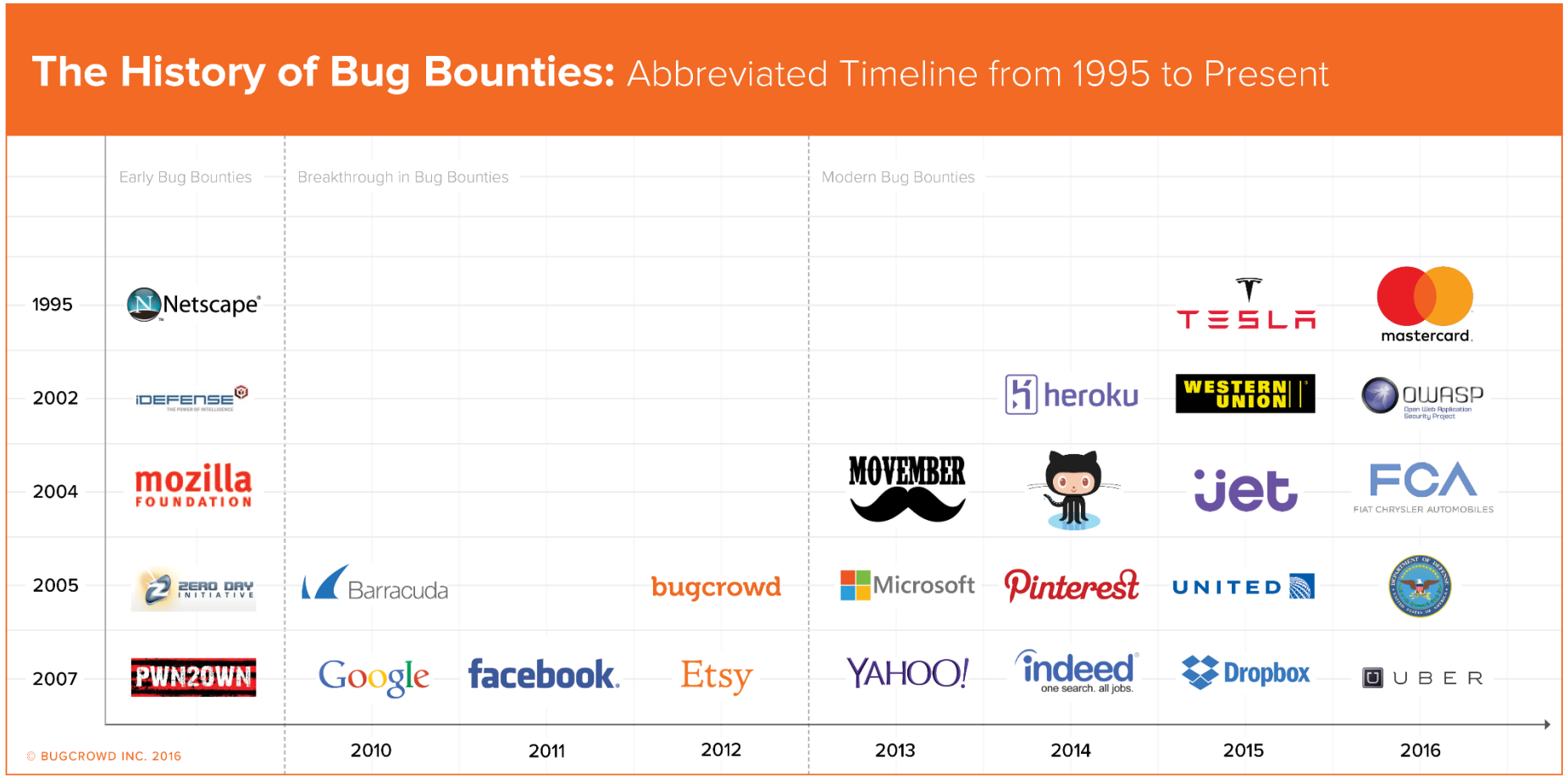


Bug Bounty


Netscape - [Version 2.02]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Reload Images Open Print Find Stop
Location: about:
What's New! What's Cool! Handbook Net Search Net Directory Software
Netscape Navigator (TM)
Version 2.02
Copyright © 1994-1995 Netscape Communications Corporation, All rights reserved.
This software is subject to the license agreement set forth in the license. Please read and agree to all terms before using this software.
Report any problems through the feedback page.
Netscape Communications, Netscape, Netscape Navigator and the Netscape Communications logo are trademarks of Netscape Communications Corporation.
NETSCAPE
Contains Java™ software developed by Sun Microsystems, Inc.
Copyright © 1992-1995 Sun Microsystems, Inc. All Rights Reserved.
JAVA COMPATIBLE
Contains security software from RSA Data Security, Inc.
Copyright © 1994 RSA Data Security, Inc. All rights reserved.
RSA PUBLIC KEY CRYPTOSYSTEM
This version supports International security with RSA Public Key Cryptography, MD2, MD5, RC4.
Any provision of Netscape Software to the U.S. Government is with "Restricted rights" as follows: Use, duplication or disclosure by the Government is subject to restrictions set forth in subparagraphs (a) through (d) of the Commercial Computer Restricted Rights clause at FAR 52.227-19 when applicable, or in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, and in similar clauses in the NASA FAR Supplement. Contractor/manufacturer is Netscape Communications Corporation, 501 East Middlefield Road, Mountain View, California, 94043.


WANTED
Bug Bounty Program
PATCHED or ALIVE
$200,000

Development of Bug Bounty

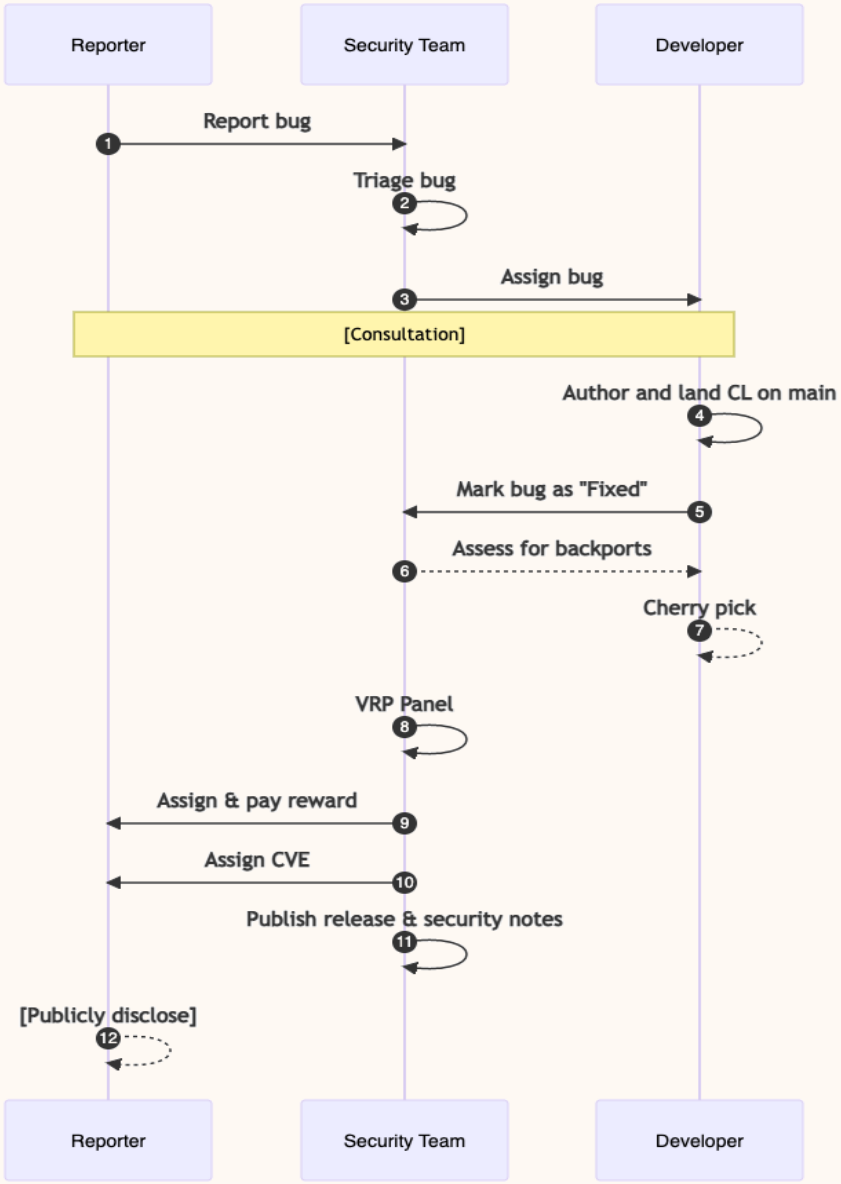


Synack
hackerone
bugcrowd

- Bugcrowd - History of Bug Bounties (https://bugcrowd.com/resources/history-of-bug-bounties)

Stakeholders

- Bug Hunter
- Platform
  - Operator
  - Triager
  - Mediator
- Vendor/Program
  - Reviewer/Security Team
  - Developer
- End User

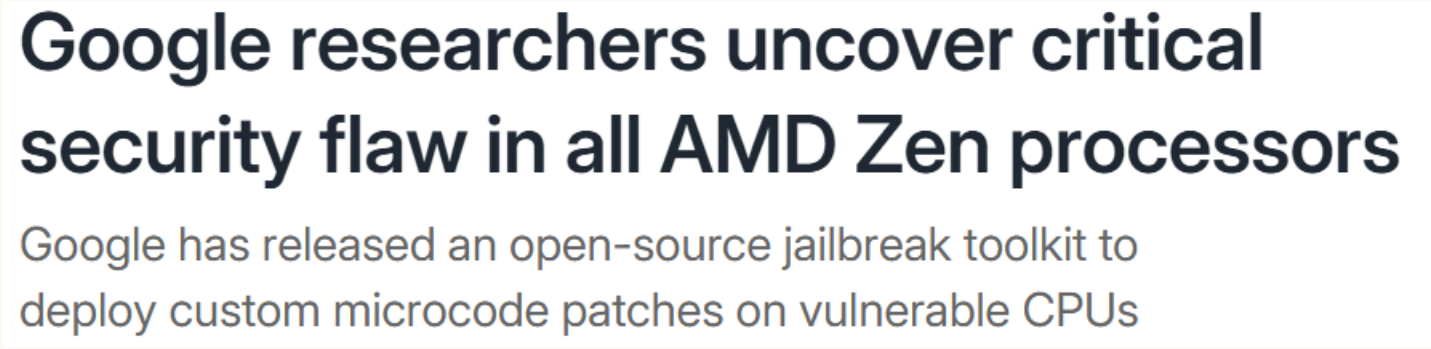


- Chromium - Life of a Security Issue (https://chromium.googlesource.com/chromium/src/+/main/docs/security/life-of-a-security-issue.md)

Why companies need hackers’ help?

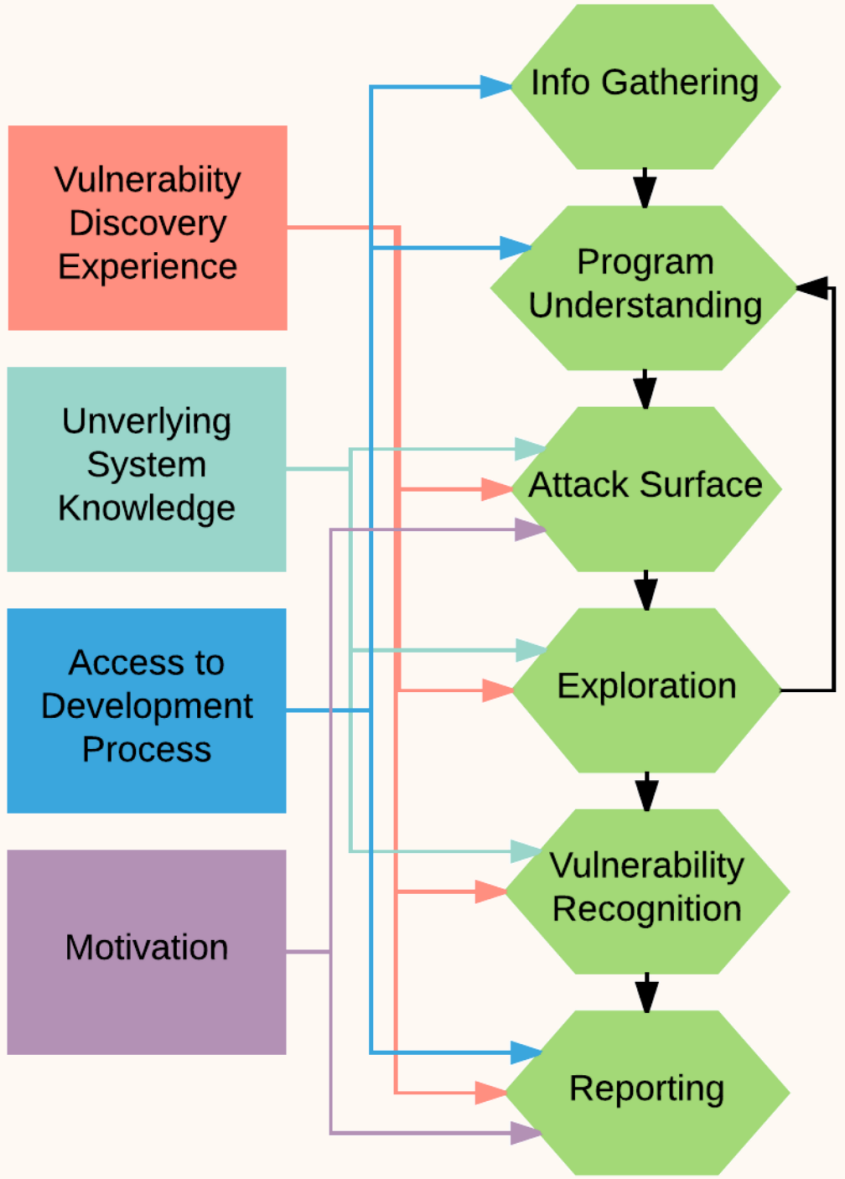
Why Companies Need Hackers

- Given that many tech companies have their own large security departments, why do they still need hackers' help?



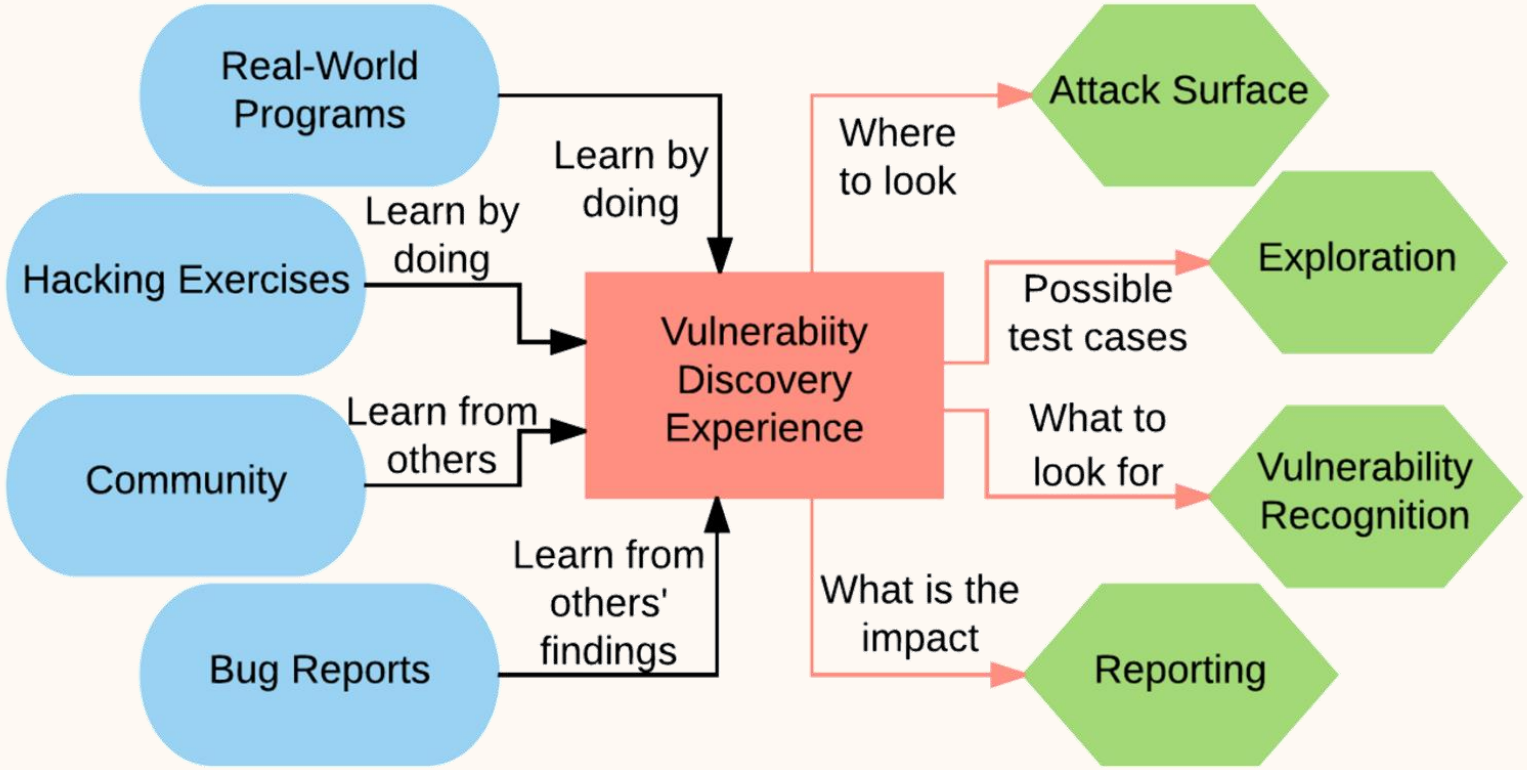
Hacker vs Tester

- What are the differences in the vulnerability discovery processes between external and internal?
- Four influencing factors



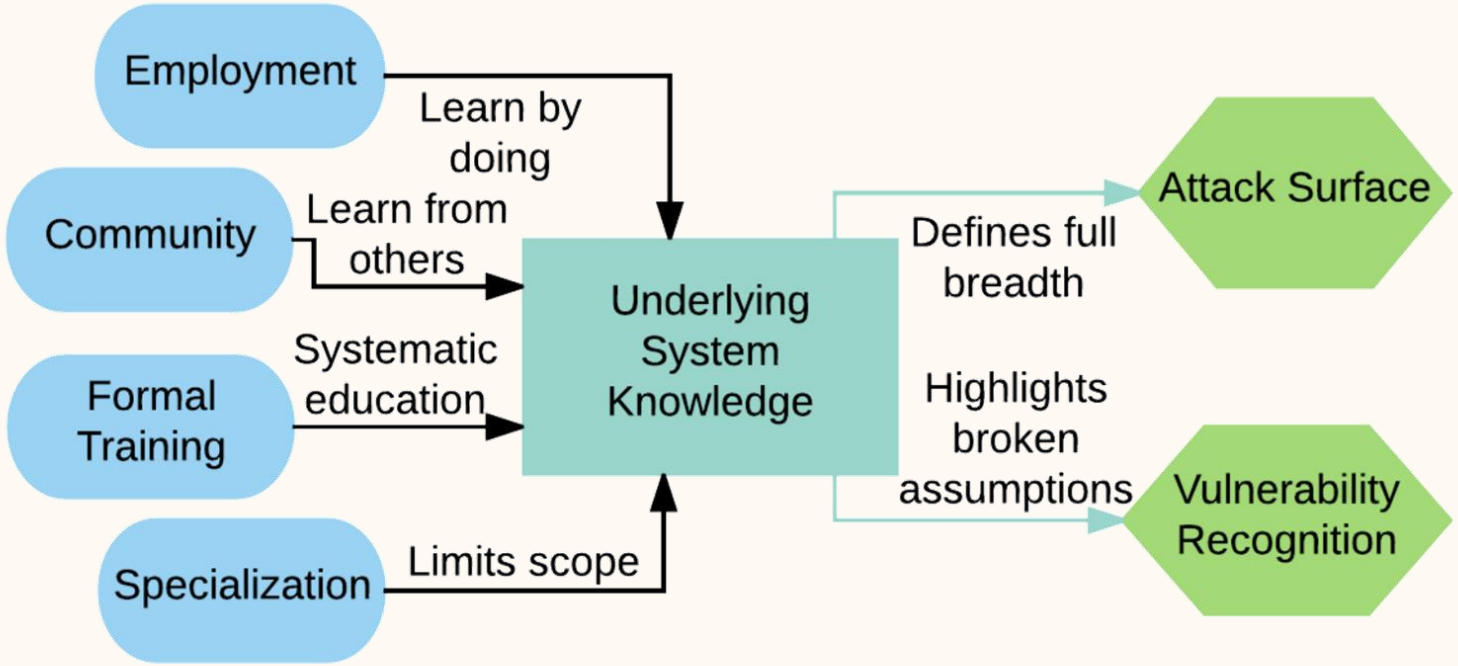
- Votipka, D., Stevens, R., Redmiles, E., Hu, J. and Mazurek, M. Hackers vs. testers: A comparison of software vulnerability discovery processes. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 374-391).

Vulnerability Discovery Experience



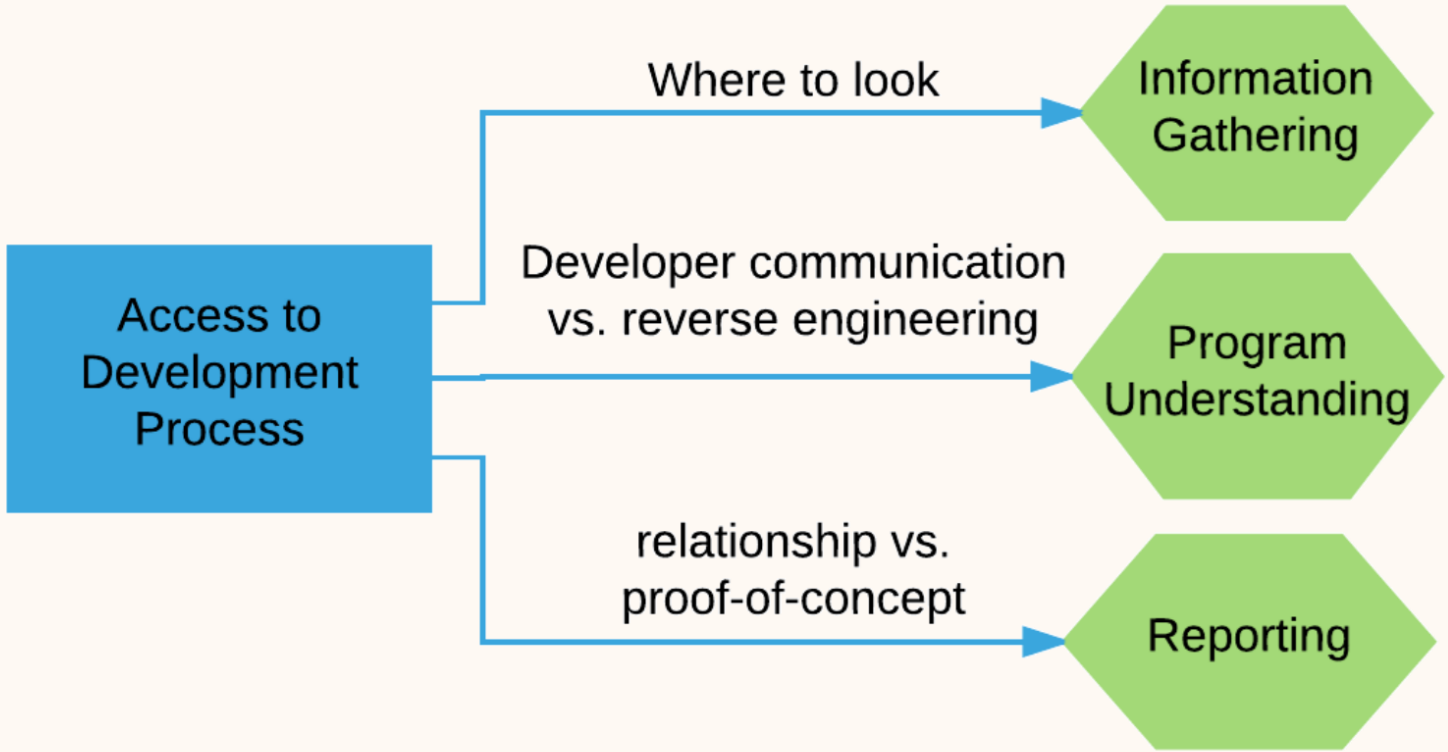
- Votipka, D., Stevens, R., Redmiles, E., Hu, J. and Mazurek, M. Hackers vs. testers: A comparison of software vulnerability discovery processes. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 374-391).

Underlying System Knowledge



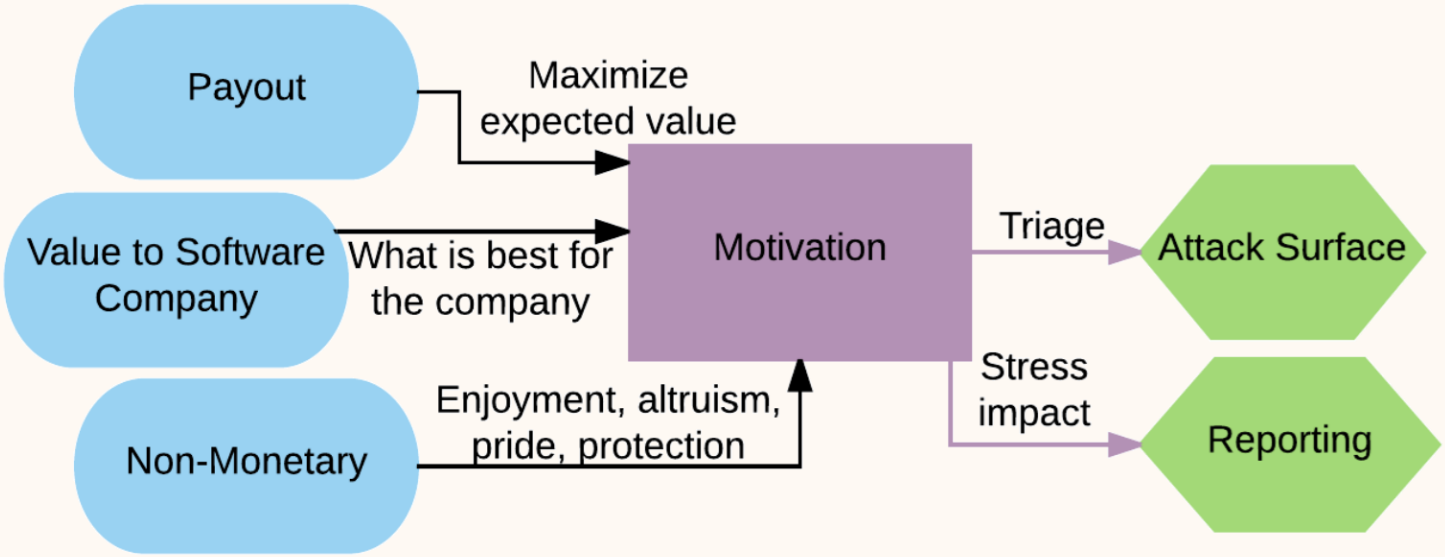
- Votipka, D., Stevens, R., Redmiles, E., Hu, J. and Mazurek, M. Hackers vs. testers: A comparison of software vulnerability discovery processes. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 374-391).

Access to Development Process



- Votipka, D., Stevens, R., Redmiles, E., Hu, J. and Mazurek, M. Hackers vs. testers: A comparison of software vulnerability discovery processes. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 374-391).

Motivation



- Votipka, D., Stevens, R., Redmiles, E., Hu, J. and Mazurek, M. Hackers vs. testers: A comparison of software vulnerability discovery processes. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 374-391).

What benefits can companies gain?

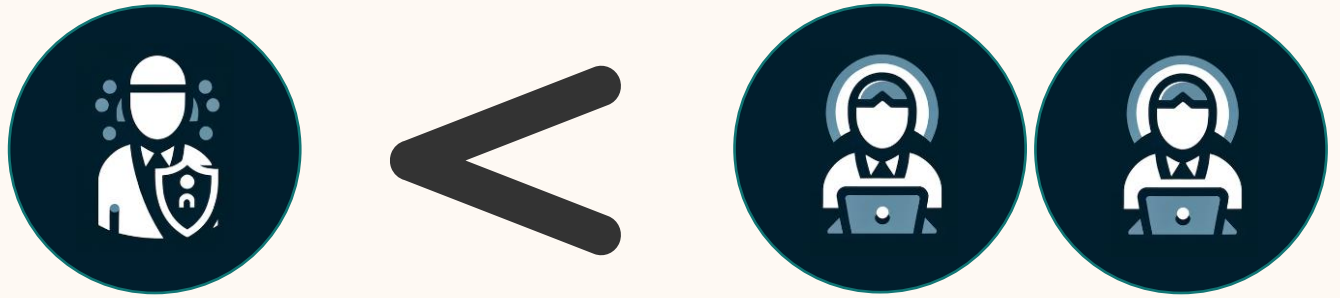
Benefits from Bug Bounties - Chromium

- Bugs are likely to be identified & patched during the development process
- BBP leverages the diverse expertise of external hackers
- Hackers discover bugs at a fairly constant rate

- Atefi, S., Sivagnanam, A., Ayman, A., Grossklags, J. and Laszka, . The benefits of vulnerability discovery and bug bounty programs: Case studies of Chromium and Firefox. In ACM Web Conference 2023 (pp. 2209-2219).
- Walshe, T. and Simpson, A. An empirical study of bug bounty programs. In 2020 IEEE 2nd international workshop on intelligent bug fixing (IBF) (pp. 35-44).

How about the cost?

- The average cost of operating a BBP for a year is less than the cost of hiring two additional software engineers.



- Walshe, T. and Simpson, A. An empirical study of bug bounty programs. In 2020 IEEE 2nd international workshop on intelligent bug fixing (IBF) (pp. 35-44).

Vendors’ Perspective

- Hackers use different methods than internal testers
- Hackers can find different kind of vulnerabilities
- Hackers are more economical than employees

What are hackers' perspectives on bug bounties?

Factors that Influence Hackers' Participation

Factors

- Benefits
- Challenges
- Platform Features
- Gig-work

Akgul, O., Eghtesad, T., Elazari, A, et al. Bug Hunters' Perspectives on the Challenges and Benefits of the Bug Bounty Ecosystem. In 32nd USENIX Security Symposium (USENIX Security 23) (pp. 2275-2291).

Factors that Influence Hackers' Participation

What are the benefits?

- Get monetary rewards
- Learning opportunities
- Legal safe harbor

Akgul, O., Eghtesad, T., Elazari, A, et al. Bug Hunters' Perspectives on the Challenges and Benefits of the Bug Bounty Ecosystem. In 32nd USENIX Security Symposium (USENIX Security 23) (pp. 2275-2291).

Factors that Influence Hackers' Participation

What are the keys to good programs?

- Ease of payment
- Ease of reporting
- Viewing disclosed vulnerabilities

Akgul, O., Eghtesad, T., Elazari, A, et al. Bug Hunters' Perspectives on the Challenges and Benefits of the Bug Bounty Ecosystem. In 32nd USENIX Security Symposium (USENIX Security 23) (pp. 2275-2291).

Factors that Influence Hackers' Participation

What are the challenges?

- Poor responsiveness
- Dissatisfaction with responses
- Unclear scope

Akgul, O., Eghtesad, T., Elazari, A, et al. Bug Hunters' Perspectives on the Challenges and Benefits of the Bug Bounty Ecosystem. In 32nd USENIX Security Symposium (USENIX Security 23) (pp. 2275-2291).

Factors that Influence Hackers' Participation

What related to Gig-works?

- Flexibility
- Stress and uncertainty

Akgul, O., Eghtesad, T., Elazari, A, et al. Bug Hunters' Perspectives on the Challenges and Benefits of the Bug Bounty Ecosystem. In 32nd USENIX Security Symposium (USENIX Security 23) (pp. 2275-2291).

Remaining Question

- Hunter main concerns:
  - Skills Development
  - Communication/Negotiating with Vendors
  - Income Uncertainty

- What is the potential solution?
  (Come from the government, industry, or hunters themselves)

Study Club, Labor Union or Start-Up?
Characterizing Teams and Collaboration in the Bug Bounty Ecosystem

Yangheran Piao
University of Edinburgh
Edinburgh, UK
lawrencepiao@ed.ac.uk

Temima Hrle
University of Edinburgh
Edinburgh, UK
temima.hrle@ed.ac.uk

Daniel W. Woods
University of Edinburgh
British University in Dubai
Edinburgh, UK
daniel.woods@ed.ac.uk

Ross Anderson[†]
University of Cambridge
University of Edinburgh
Cambridge, UK

***Abstract*—A unique bug bounty ecosystem has evolved in China. Platforms allow groups of hackers to register together to receive team-level awards. However, little is known about the prevalence and productivity of these teams, or how team members collaborate. To address this gap, we conducted a mixed-methods study.**

The first stage characterized teams from a top-down ecosystem perspective. We collected bug bounty rankings from 85 platforms, using fuzzy-matching to identify 2.1k unique teams and 5.9k hunters. We show that 46% of users are registered as part of a team, and hunters with teams are more

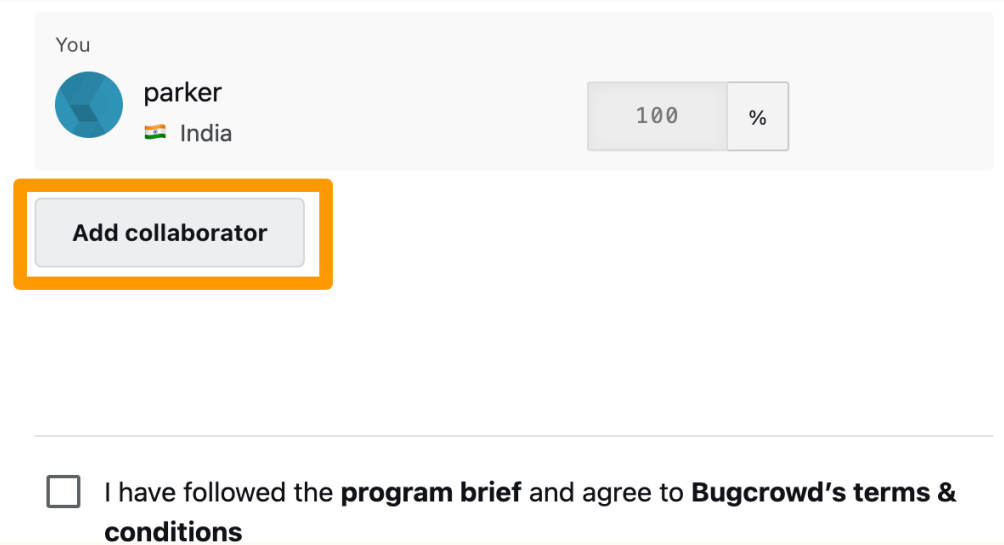
that BBPs are an efficient security investment [8], [32], [34], [50], [55], [60], which helps explain why Google paid out $10 million in bug bounties in 2023 [42].

Despite the success of BBPs, communications between vendors and hunters is challenging. Vendors complain about low quality bug submissions [25], meanwhile hunters complain about slow and non-transparent decisions [1]. Another problem is the lack of established development pathways, which is especially problematic for young hackers [12] and those from diverse backgrounds [10]. Put simply, solo hunters lack market power and development opportunities.

- Piao, Y., Hrle, T., Woods, D. and Anderson, R., 2024, November. Study Club, Labor Union or Start-Up? Characterizing Teams and Collaboration in the Bug Bounty Ecosystem. In 2025 IEEE Symposium on Security and Privacy (SP).

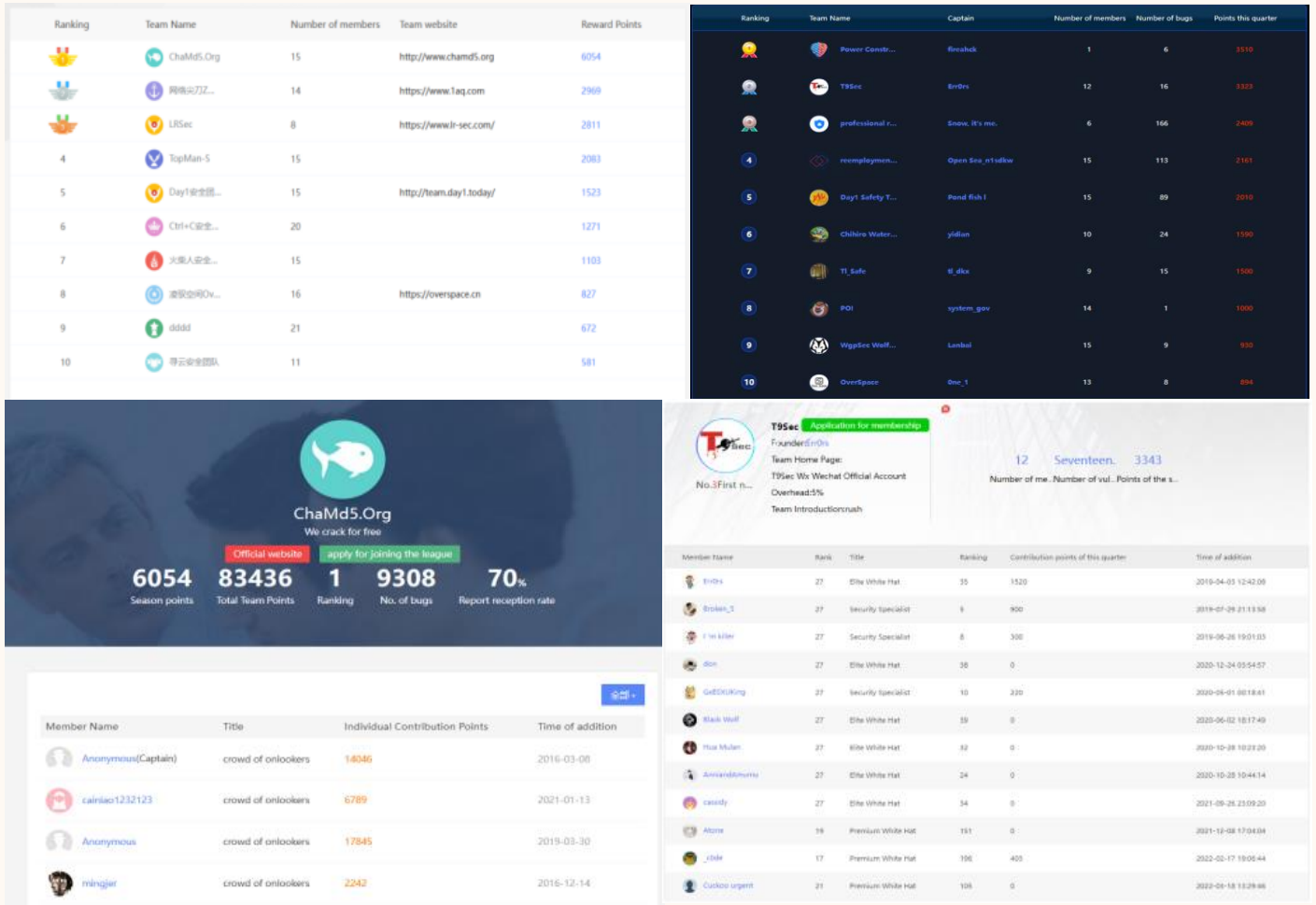
Hacker Collaboration

- Teamwork is common in cybersecurity
- Bugcrowd allows hunters to share bounties



Hacker Collaboration

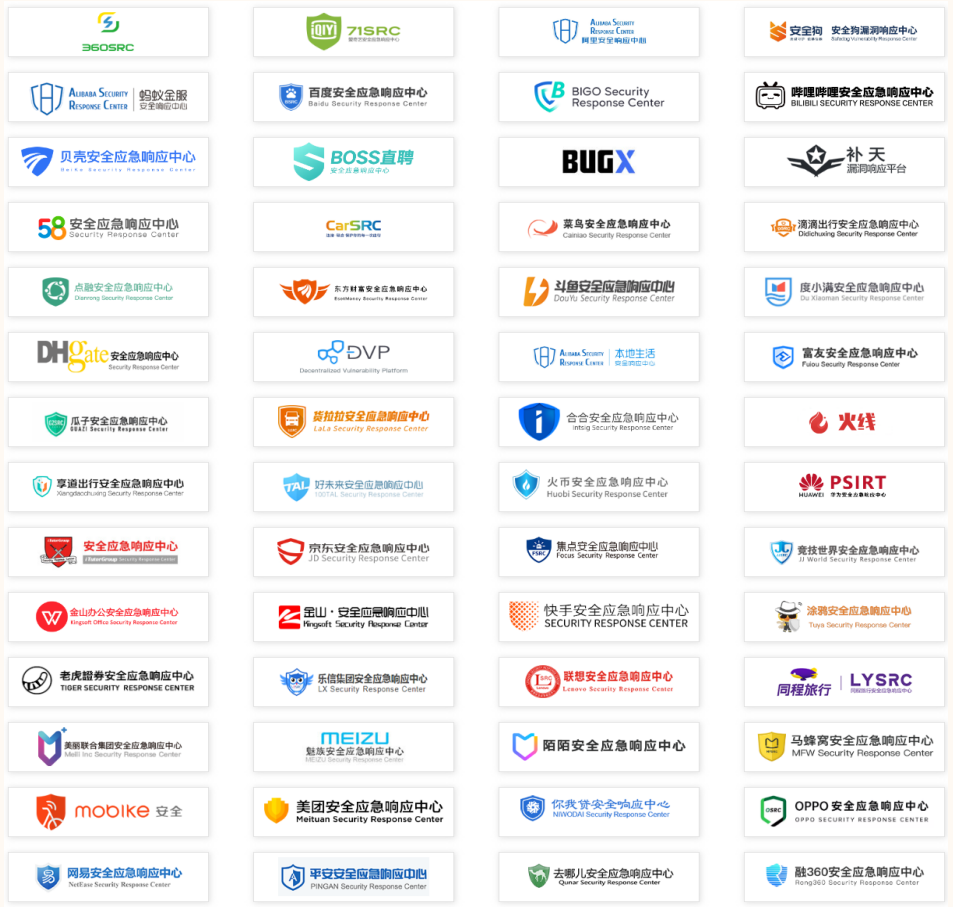
- A unique teaming ecosystem has evolved in China



Research Questions

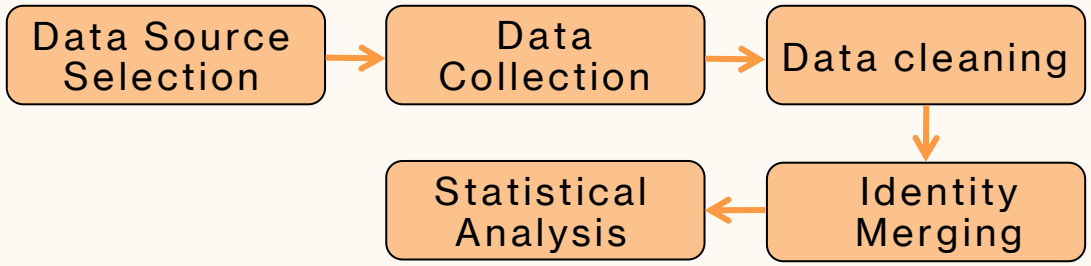
- How are teams, hunters and rewards distributed over BBPs?
- What are the functions of bug hunter teams?
- Why do bug hunters join and leave teams?

Phase I: BBP Measurement

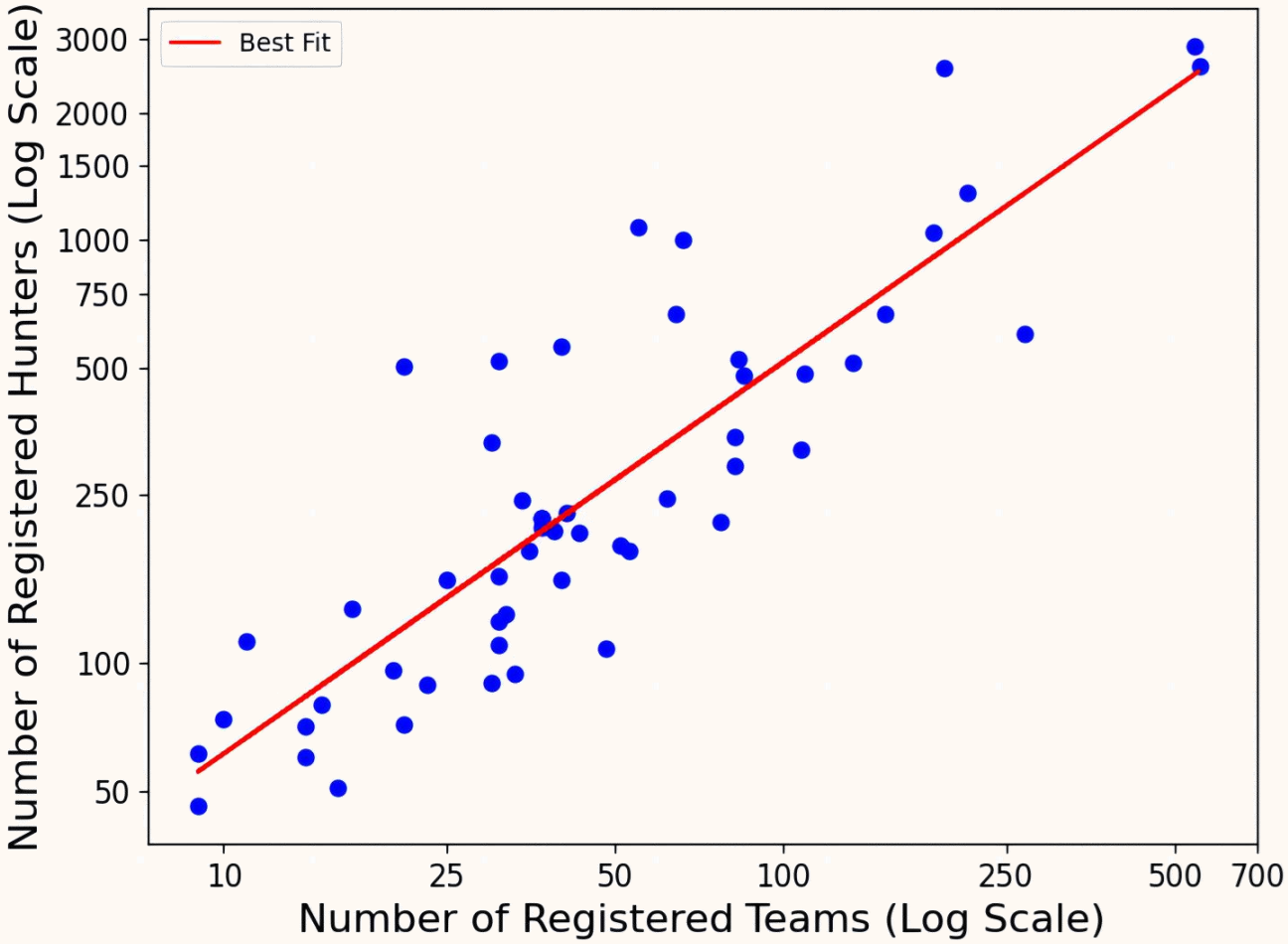


Quantitative Study

- Collect data from BBPs with teaming mechanism
- n= 85 BBPs & 5.9k hunters

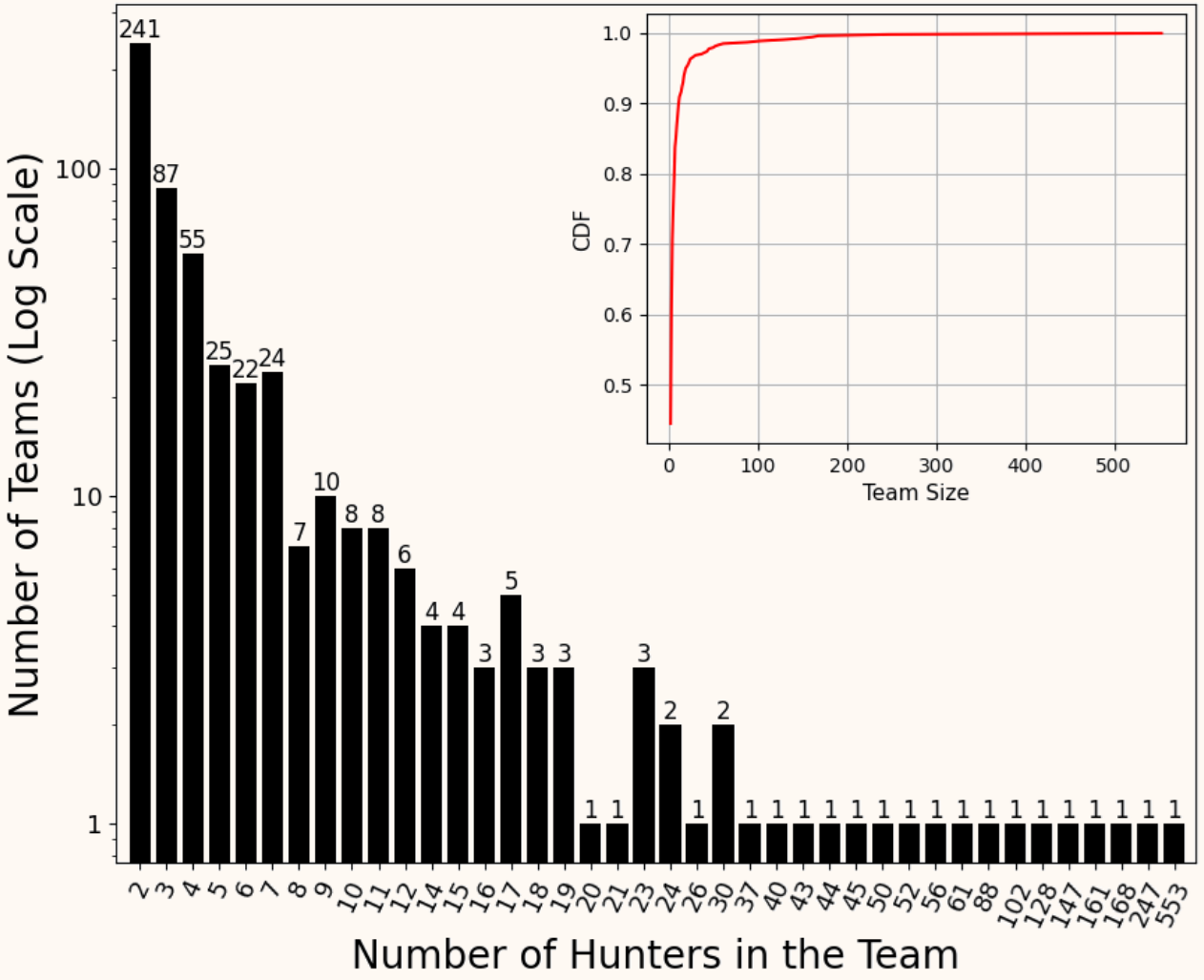


RQ1: Hunter Teaming Ecosystem

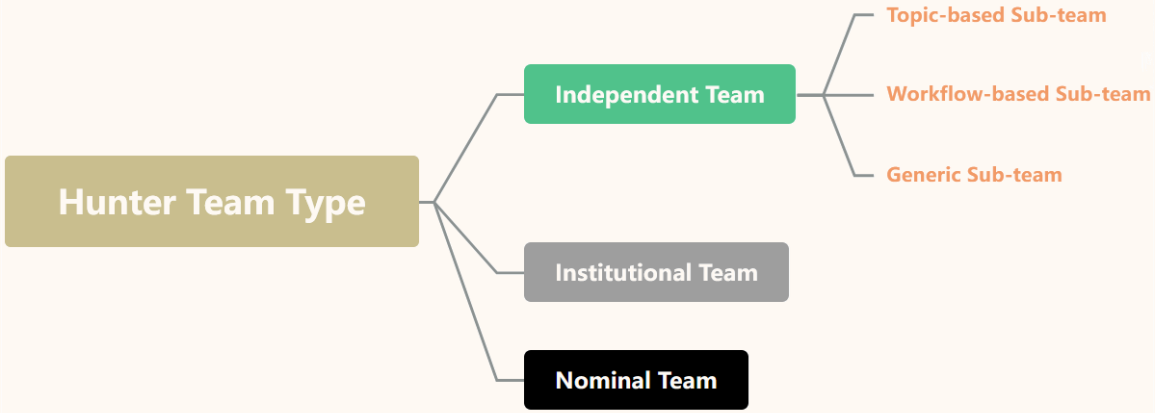


- 46% of users are part of a team
- The three largest BBPs have over 2.5k registered users

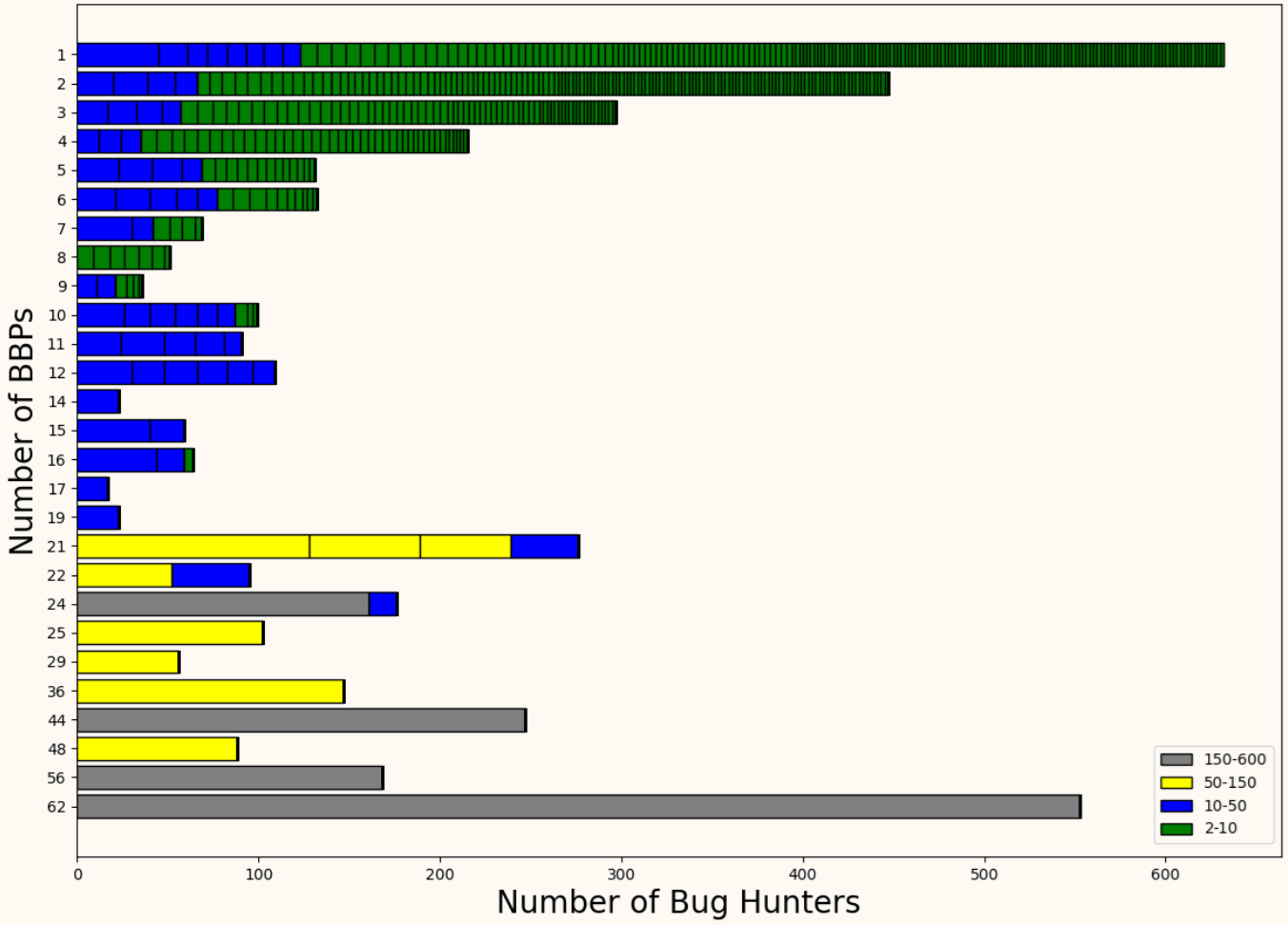
Prevalence of Users, Teams and BBPs (RQ1)



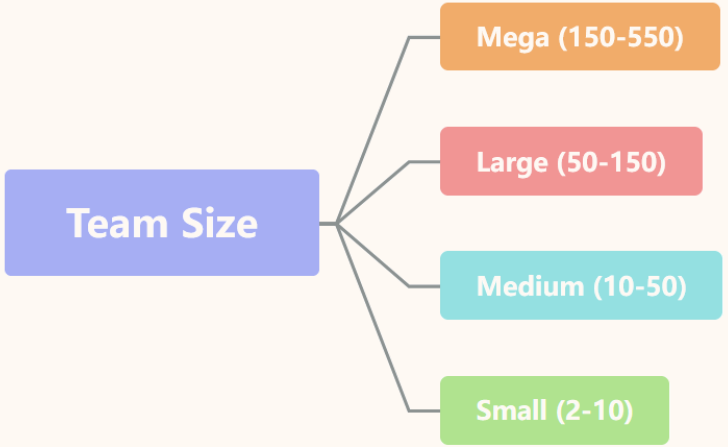
- 87% teams have less than 10 members



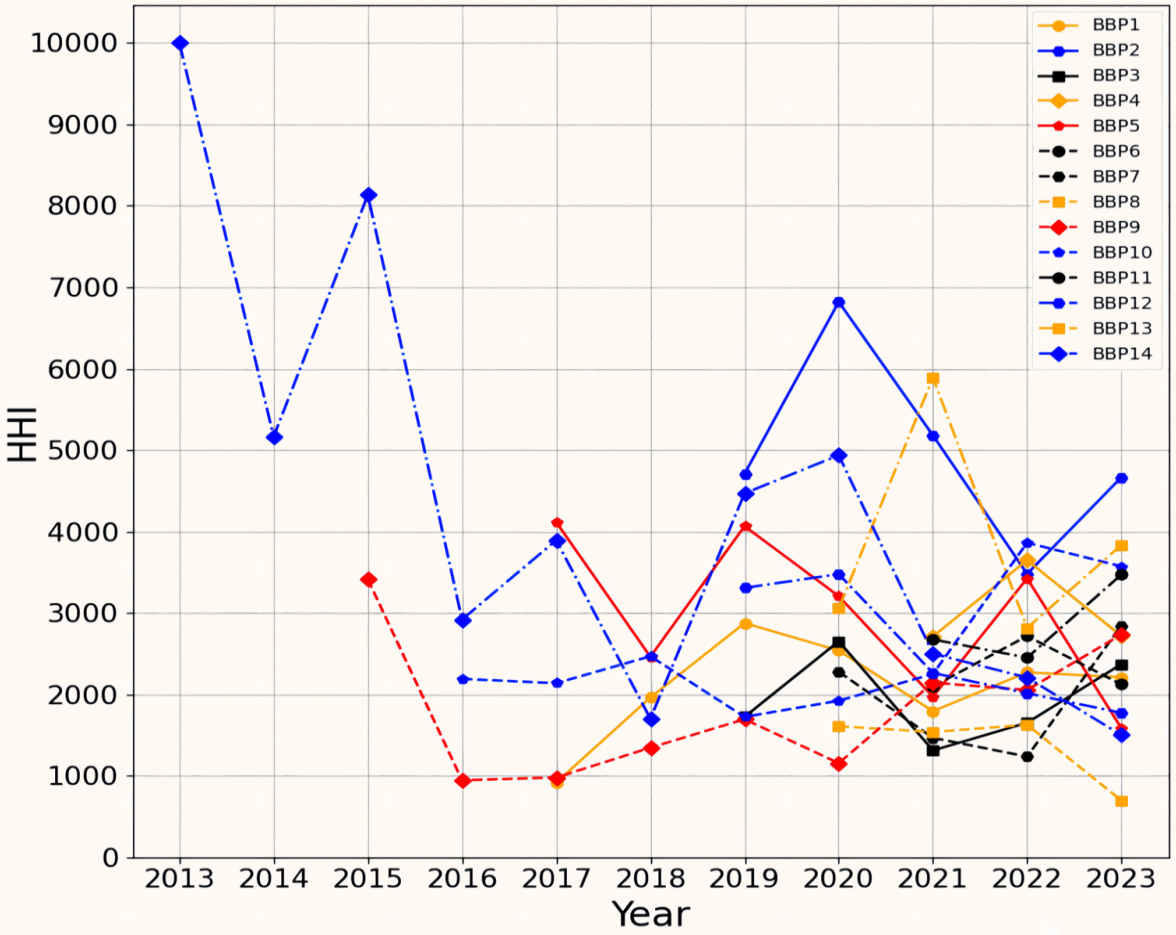
Prevalence of Users, Teams and BBPs (RQ1)



- The largest team has 553 members and on 62 BBPs
- 39% of small teams participate in just one BBP



Team Productivity (RQ1)



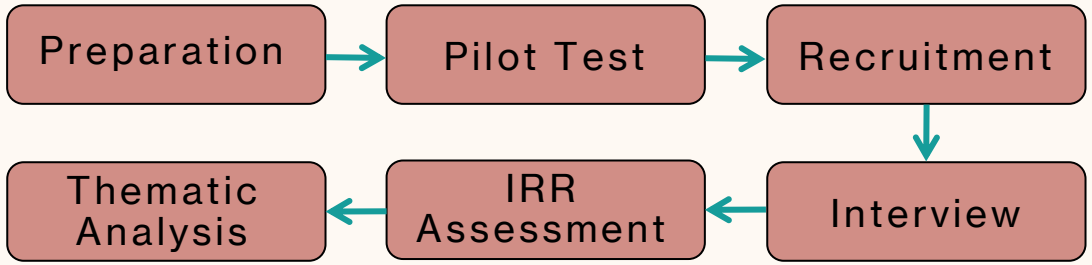
- Team members are more than twice (2.47) as productive as solo hunters
- There is a high level of market concentration

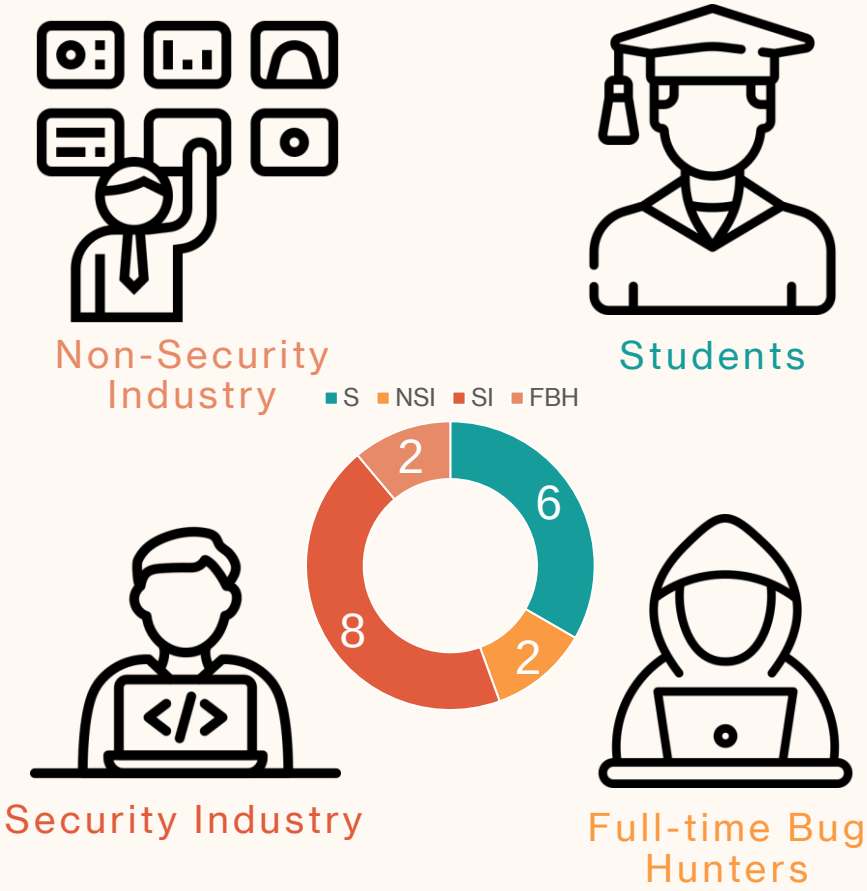
$$HHI_n = \sum_{i=1}^{N} x_i^2$$

Phase II: Interview

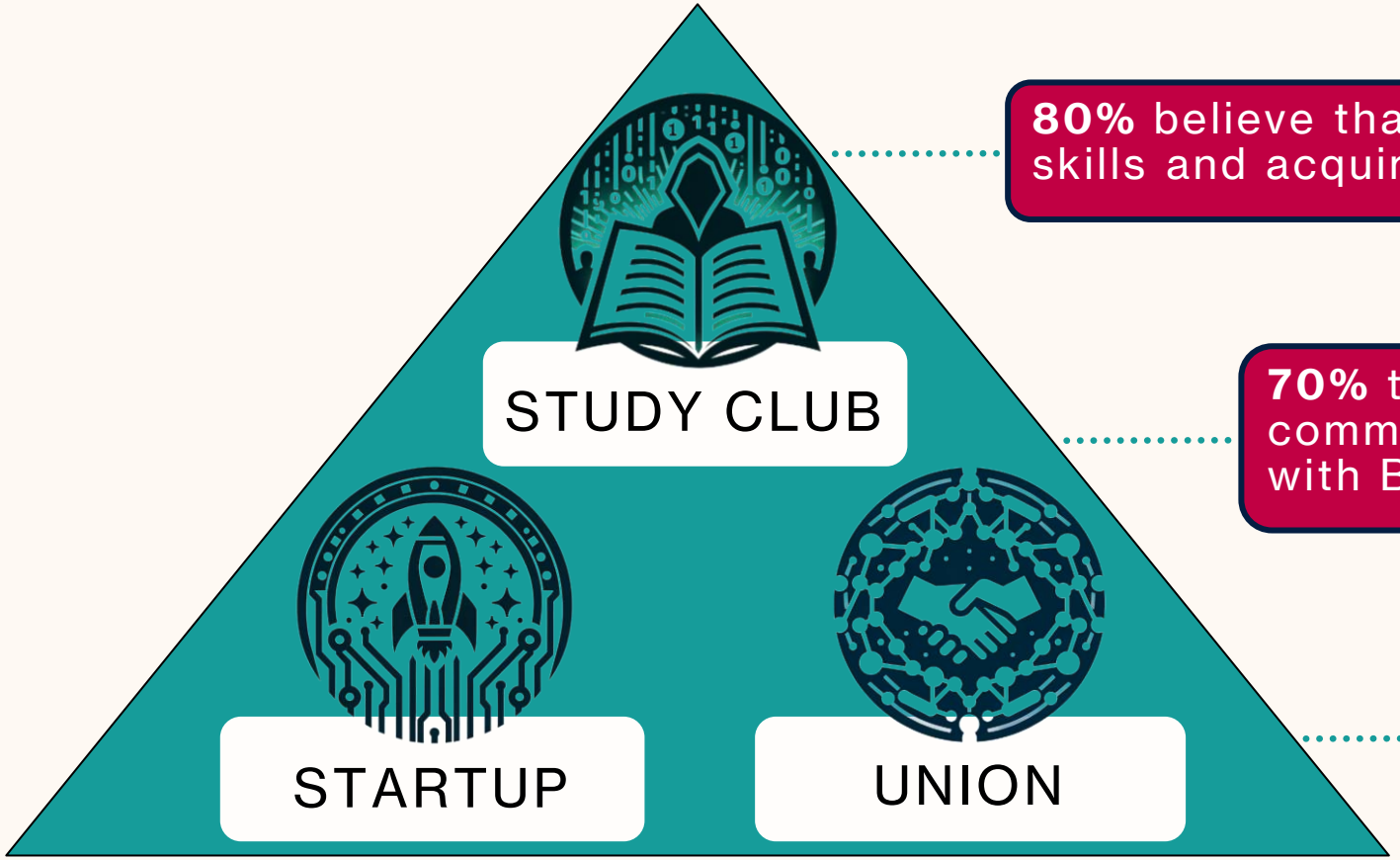
Qualitative Study

- Investigate hackers' perspectives on bug bounty teams
- n=18 hunters





RQ2: Multifaceted Functions of Team



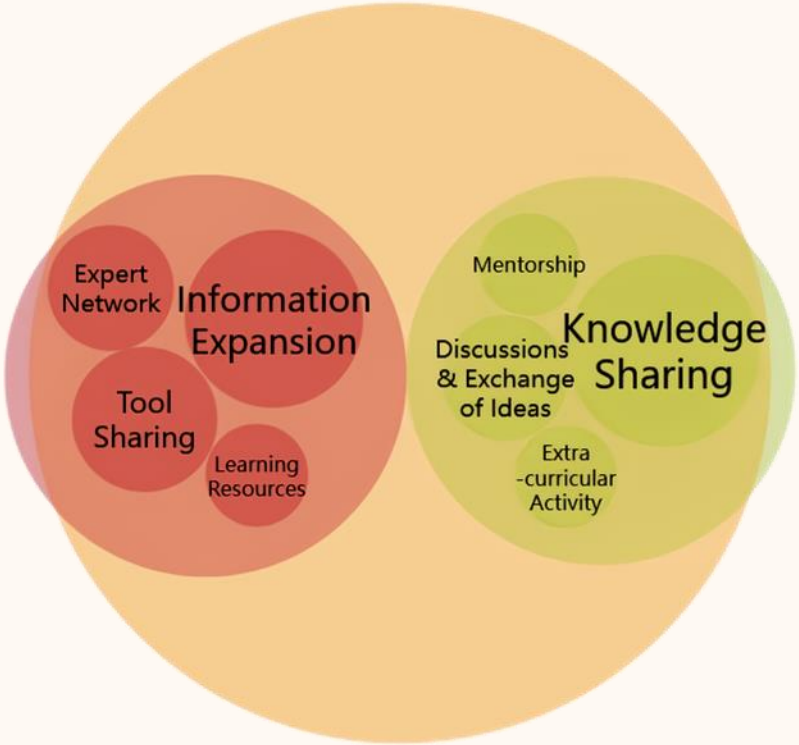
80% believe that teams help enhance skills and acquiring knowledge.

70% thought teams contribute to equal communication and handle disputes with BBPs.

40% said team leaders operate the team under a company-like model, with additional revenue streams.

Study Club (RQ2)

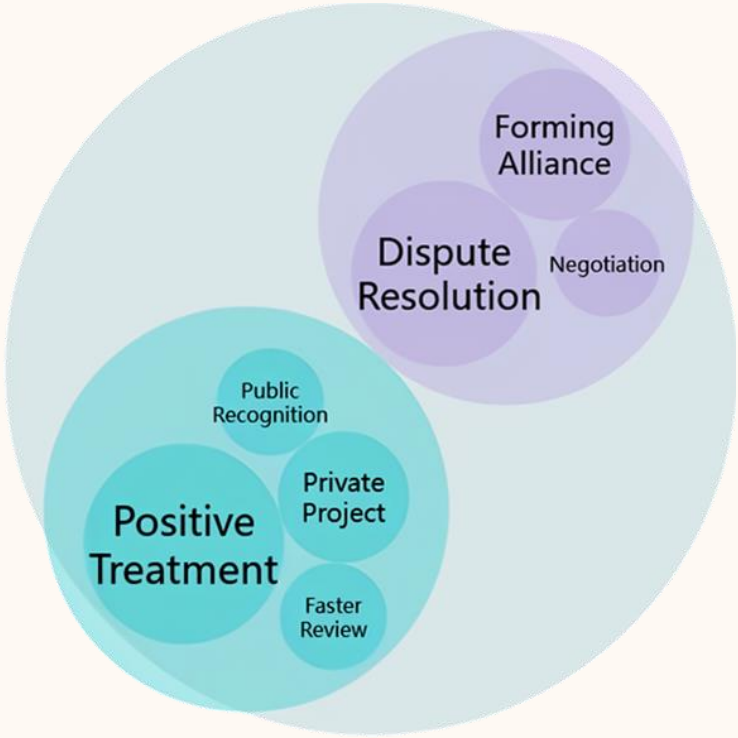
- **Educational Relationships**
  - Discussions and exchange of ideas
  - Private chats with experts
  - Extra-curricular activities
- **Resources and Shared Tools**
  - Expand the availability of information
  - Share auto-scripts, knowledge bases and cyber ranges



"Once inside, I felt the study atmosphere was good, and everyone was around my age, without any exceptionally skilled individuals. It was more about progressing together and having a competitive spirit."

Labor Union (RQ2)

- **Positive Treatment by BBPs**
- **Dispute Resolution**
  - Intervene in the conflict with BBP
  - Forming alliances



"Some teams unite to prevent bug bounty programs intentionally downgrading the severity of vulnerabilities [to reduce the payout]."

Start-Up (RQ2)

- **Earning & Sharing Revenue**
  - Sharing Individual & Team Rewards
  - Additional Revenue Streams
- **Collaboration Strategies**
  - Collaborative Hunting
  - BBP Selection
- **Management**
  - Code of Conduct
  - Confidentiality
  - Engagement

RQ3: Reasons for Joining & Leaving

- **Motivations**
  - Learning and Growth
  - Revenue Sharing
  - Team Prestige

- **Issues and Challenges**
  - Lack of activity
  - Interpersonal conflicts
  - Lack of time

Key Insights

- **Teams are central to the Chinese bug bounty ecosystem**
  - Almost half of hunters are team members
  - Team members have over twice the productivity of solo ones
  - The largest team participates in 73% of BBPs

Key Insights

- **Functions of hunter teams could solve concerns**

 Maintaining educational resources (*Skills development*)

 Earning more revenue like additaional bounties (*Income Uncertainty*)

 Establish equal communication channels with BBPs (*Negotiation*)

What left?

- Legal Concerns
- AI + Hunting

...

UK Home Office's new vulnerability reporting mechanism leaves researchers open to prosecution February 25th, 2025

Individuals in the United Kingdom who report cybersecurity vulnerabilities to the Home Office are at risk of facing prosecution for the simple act of discovering those vulnerabilities — even if they comply with new guidance the government department published on Monday.

4 Nov 2024

Google researchers discover first vulnerability using AI

Google researchers have announced the discovery of the first vulnerability using a large language model.

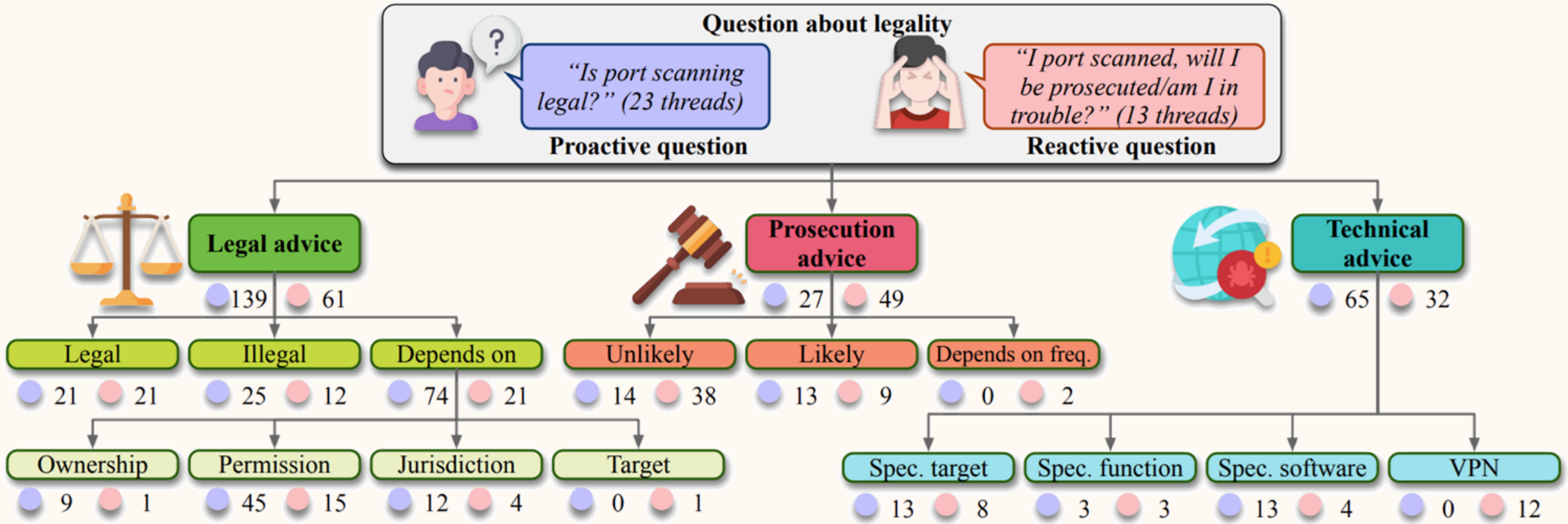
Legal Concerns of Would-be Vulnerability Researcher

(Ongoing work)

- OPs on Reddit expressed confusion and fear regarding the legality of hacking and disclosure
  - Deterring experimentation leads to beginners being discouraged at the first step

- Repliers offered useful mitigation strategies
  - The community's effort to guide newcomers to safer, low-risk environments

Legal Concerns on Port Scanning



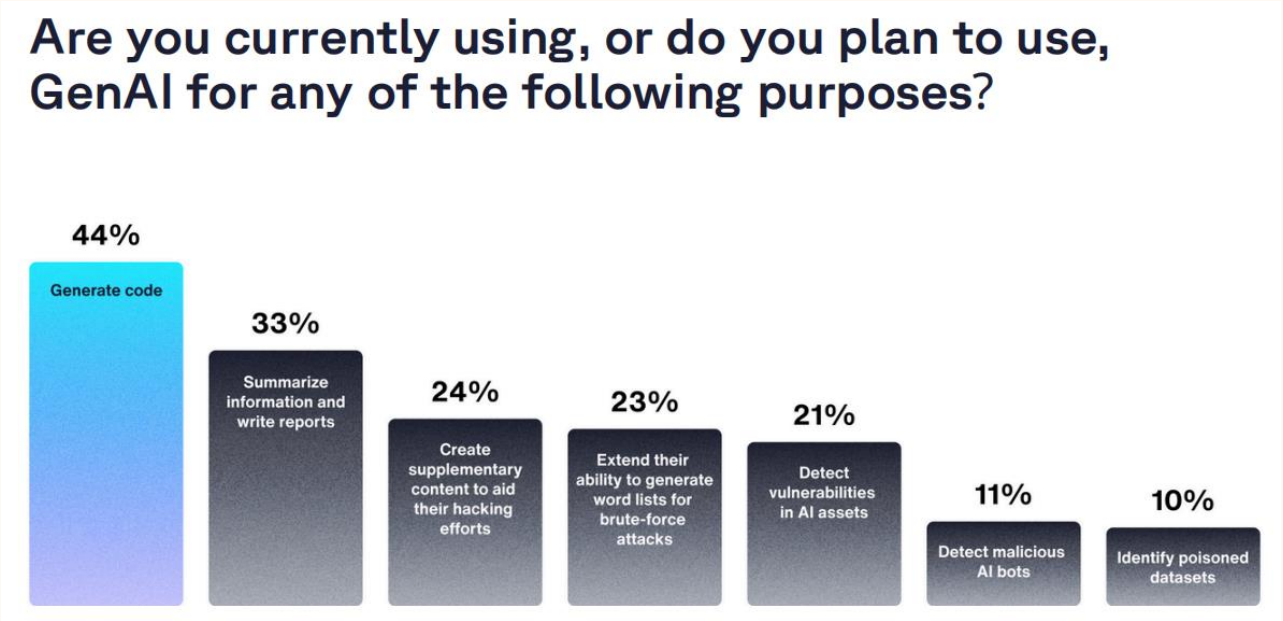
- Hrle, T., Milad, M., Li, J., & Woods, D. "Just a tool, until you stab someone with it": Exploring Reddit Users' Questions and Advice on the Legality of Port Scans. In 2024 European Symposium on Usable Security (EuroUSEC 24) (pp. 322-336).

AI+ Bug Hunting

2023/2024

GenAI has become a "significant tool"	14%
Using GenAI in some way	53%
Write code	53%
Write better reports	66%
Reduce language barriers	33%

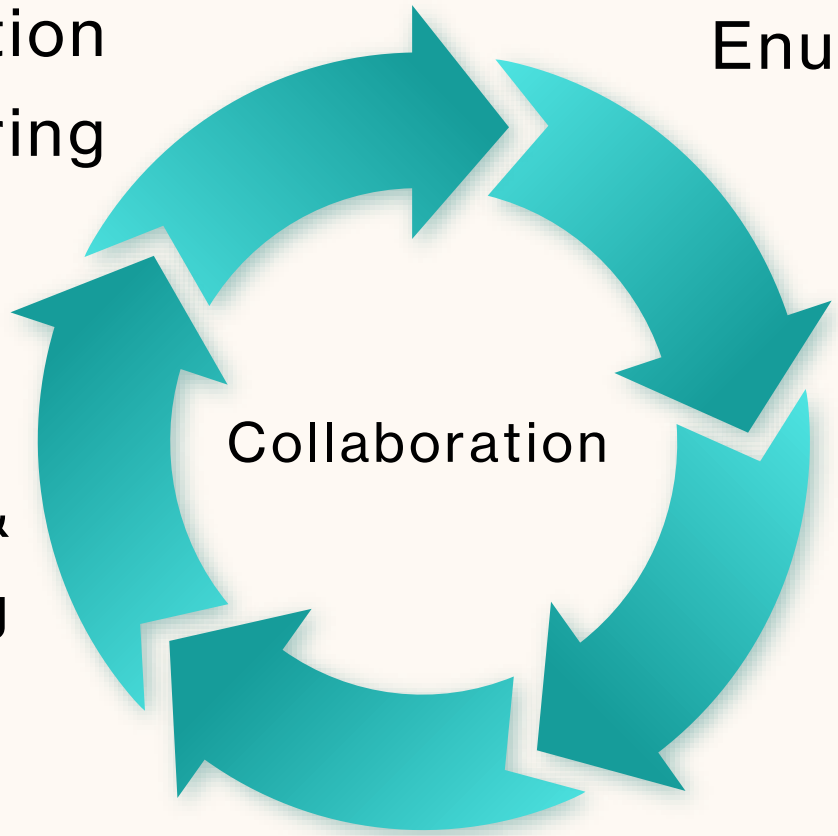
2024/2025



- HackerOne – Hacker-Powered Security Report 2024/25 (https://hackerpoweredsecurityreport.com/)

(The near) Future?

AI +



Take-home

- Akgul, O., Eghtesad, T., Elazari, A, et al. Bug Hunters' Perspectives on the Challenges and Benefits of the Bug Bounty Ecosystem. In *32nd USENIX Security Symposium (USENIX Security 23)* (pp. 2275-2291).
- Fulton, K.R., Katcher, S., Song, K., et al. Vulnerability discovery for all: Experiences of marginalization in vulnerability discovery. In 2023 IEEE Symposium on Security and Privacy (SP) (pp. 1997-2014).
- The Record Media – 'UK Home Office's new vulnerability reporting mechanism leaves researchers open to prosecution'