Vulnerability Research & Bug Bounty

INFR11158/11230 Usable Security and Privacy

Yangheran (Lawrence) Piao

18/03/2025



Overview

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

What is Hacking or Vulnerability Research?

Malwarebytes[®]

Malwarebytes

- https://www.youtube.com/watch?v=pxSp6HeM4RM
- https://www.youtube.com/watch?v=ID34wkOcCRE

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

- Attack
- Sell it
- Disclosure



Full Disclosure

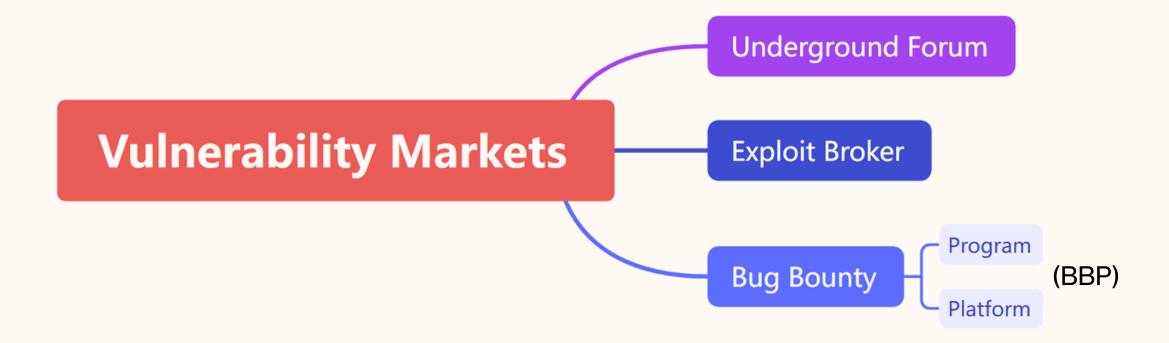
	Disagree		Agree
٠	Nobody except researchers need to know the details of flaws	٠	FD helps the good guys more than the bad guys
٠	FD results in information anarchy	•	Effective security cannot be based on obscurity
•	Good guys who publish virus code may also have malicious intention	•	Making vulnerabilities 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



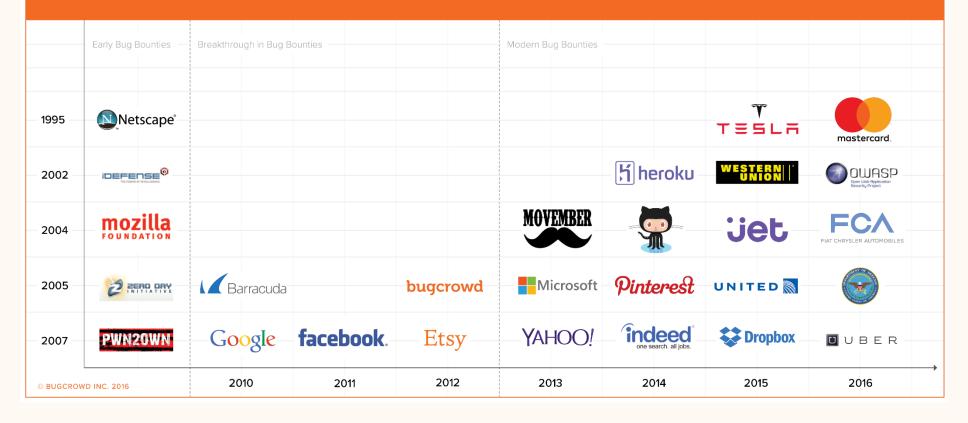
Bug Bounty

ia 이다 이다 이다 이다. ck Forward Home Relat	Ad Images Open Print Find Stop	
ation: about:		T
at's New! What's Cool! Hand	book Net Search Net Directory Software	
Ν	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.	
NETSCADE	Report any problems through the <u>feedback page</u> .	
NETSCAPE	Netscape Communications, Netscape, Netscape Navigator and the Netscape Communications logo are trademarks of Netscape Communications Corporation.	
Java: Commattane	Contains Java™ software developed by Sun Microsystems, Inc. Copyright © 1992-1995 Sun Microsystems, Inc. All Rights Reserved.	
_	Contains security software from RSA Data Security, Inc.	
	Copyright © 1994 RSA Data Security, Inc. All rights reserved.	
	This version supports International security with RSA Public Key Cryptography, MD2, MD5, RC4.	
e at FAR 52.227-19 when applicable, or i	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 Communication Contractor Restricted Rights nobsparagraph (c) (d) (iii) of the Rights in Technical Data and Computer Software clause at DFARS 252 227-7013, and in similar clauses in the NASA FAR Supplement. Contractorhandischurer is Netscope adiable Road, Mountain View, California, 94043.	
9		⊴?



Development of Bug Bounty

The History of Bug Bounties: Abbreviated Timeline from 1995 to Present

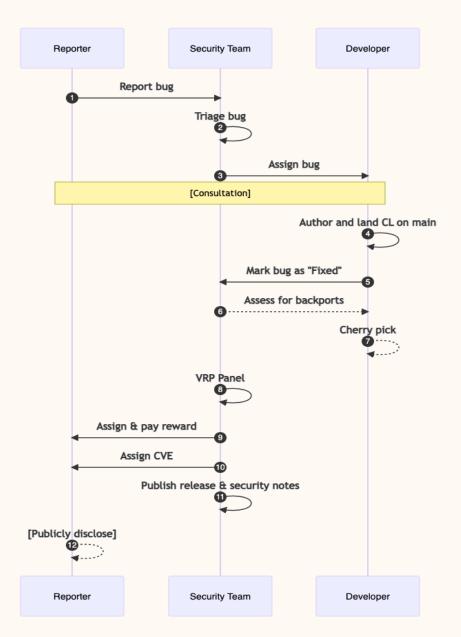




Bugcrowd - History of Bug Bounties (https://bugcrowd.com/resources/history-of-bug-bounties)

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?

Google researchers uncover critical security flaw in all AMD Zen processors

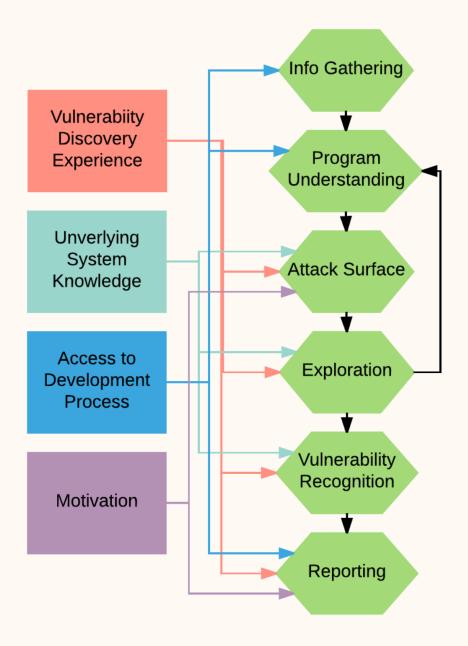
Google has released an open-source jailbreak toolkit to deploy custom microcode patches on vulnerable CPUs

Google Paid Out \$10 Million via Bug Bounty Programs in 2023

Google paid out \$10 million via its bug bounty programs in 2023, bringing the total to nearly \$60 million since 2010.

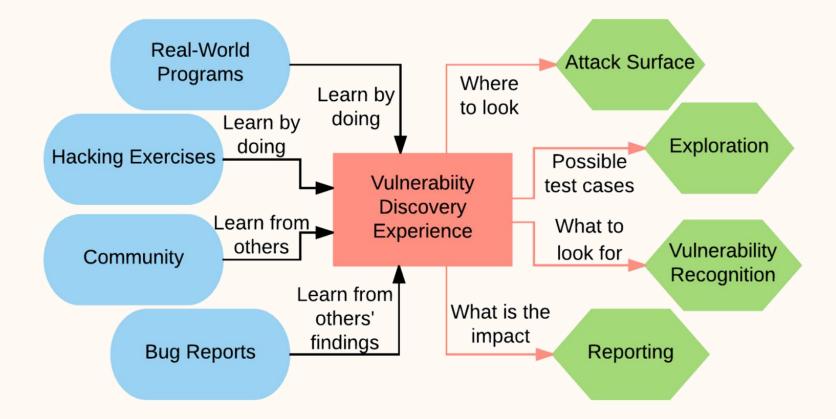
Hacker vs Tester

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



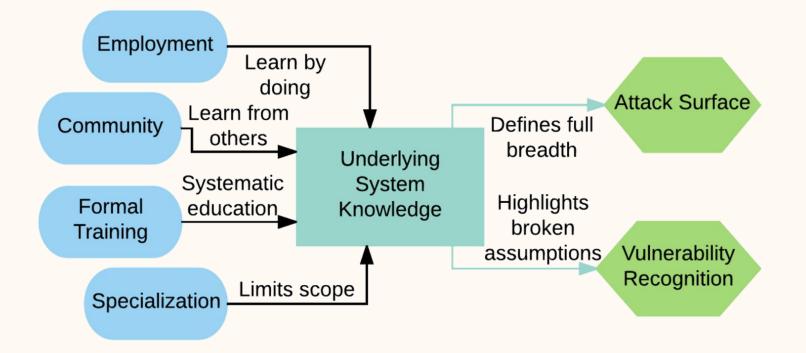
 Votipka, D., Stevens, R., Redmiles, E., Hu, J. and Mazurek, M. Hackers vs. testers: A comparison of software vulnerability discovery processes. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 374-391).

Vulnerability Discovery Experience



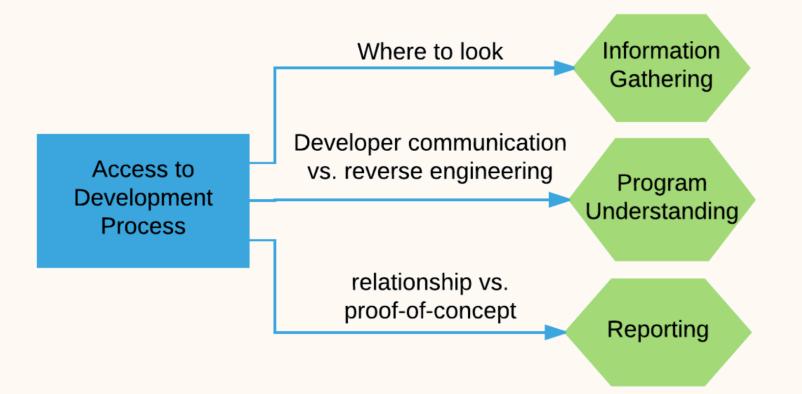
 Votipka, D., Stevens, R., Redmiles, E., Hu, J. and Mazurek, M. Hackers vs. testers: A comparison of software vulnerability discovery processes. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 374-391).

Underlying System Knowledge



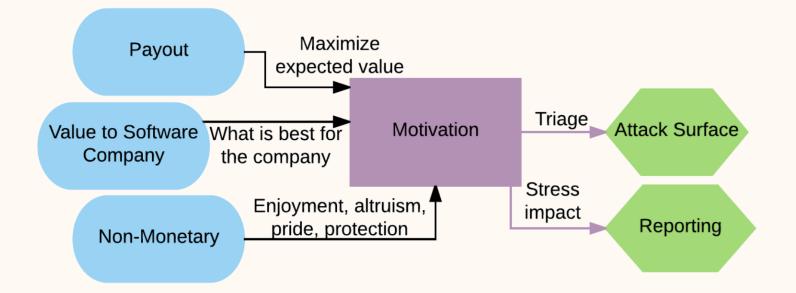
• Votipka, D., Stevens, R., Redmiles, E., Hu, J. and Mazurek, M. Hackers vs. testers: A comparison of software vulnerability discovery processes. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 374-391).

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.



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

- Benefits
- Challenges
- Platform Features
- Gig-work

What are the benefits?

- Get monetary rewards
- Learning opportunities
- Legal safe harbor

What are the keys to good programs?

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

What are the challenges?

- Poor responsiveness
- Dissatisfaction with responses
- Unclear scope

What related to Gig-works?

- Flexibility
- Stress and uncertainty

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

You parker ➡ India	100 %		
Add collaborator		BUGCROWD RESEARCHER COLLABORATION: REWARD SPLITTING & JOINT SUBMISSIONS	
I have followed the program k conditions	rief and agree to Bugcrowd's terms &	Now available in Crowdcontrol!	

Hacker Collaboration

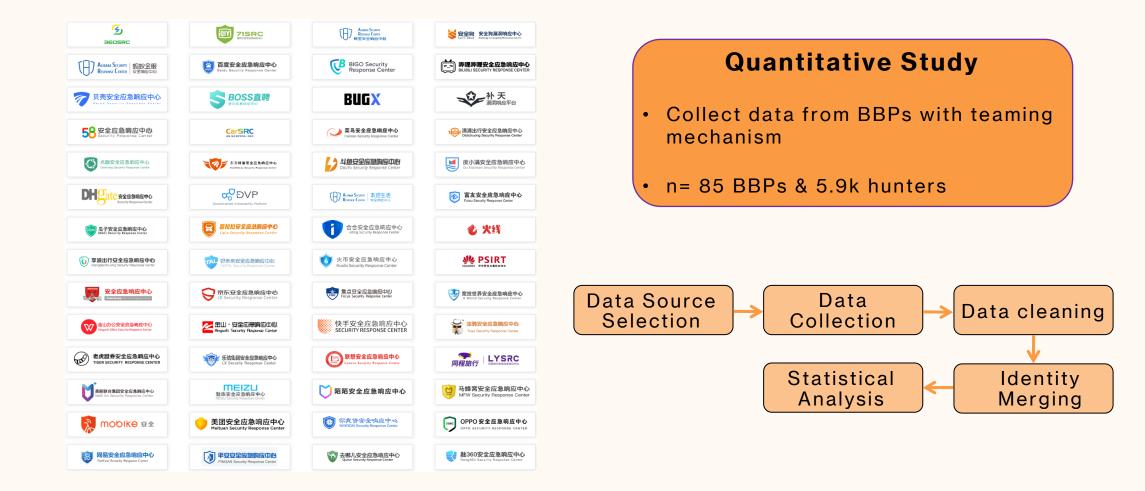
• A unique teaming ecosystem has evolved in China

Ranking	Team Name	Number	of members Team website	Reward Points	Ranking	Team Na	11e	Captain	Number of members	Number of bugs	Points this
*	ChaMd5.Org	15	http://www.chamd5.org	6054		۰					
¥-	① 网络尖刀Z	14	https://www.laq.com	2969		•					
¥-	URSec	8	https://www.ir-sec.com/	2811	<u>ي</u>	0					
4	💽 TopMan-S	15		2083	۲						
5	🥑 Day1完全团	15	http://team.day1.today/	1523	(5)	۰					
6	🕑 Ctrl+Cgr.	20		1271	6						
7	💧 火栗人安全	15		1103	(7)	a	TI Safe				
8	 () 渡駅空间Ov 	16	https://overspace.cn	827							
9	dddd	21		672	(8)						
10	😨 寻云安全团队	11		581	9	۲					
	-				10						
					No.3First n Dw	ender din On m Home Page	Official Account	Nun	12 Seventeen. nber of ros. Number of vul Po		
A A		Wed	Md5.Org rack for free		No.3First n Tex Tex No.3First n Tex Tex	anderdin Ons m Home Page lec Wx Wechat enhead:5% m Introduction	: Officiai Account snuth	Nun	nber of me. Number of vulPo	ints of the s	
1 4	6054	We c	rack for free apply for joining the league		No.3First frame No.3First frame	inderdinion m Home Page lec Wx Wechat enhead:5% m Introduction nam	Official Account snah	Nun	nber of me. Number of vul. Po Cartribution points of this quarter	sints of the s	
No 2	Contraction and	We control of the con	rack for free	and the second	No.3First n No.3First n Norther taxee	enderdinion m Home Page iec Wx Wechat enhead:5% m Introduction nam 27	Official Account smath Title Dire White Hat	Nun Rassing 35	nber of me . Number of vul . Fo Cartrilation points of this quarter 1820	ents of the s	2010-04-05 12
(a a	Contraction and	We control of the con	rack for free apply for joining the imagine 1 9308 7(and the second	No.3First frame No.3First frame	inderdinion m Home Page lec Wx Wechat enhead:5% m Introduction nam	Official Account snah	Nun	nber of me. Number of vul. Po Cartribution points of this quarter	ints of the s.	2010-04-05 12 2018-07-29 21
a de y	Contraction and	We control of the con	rack for free apply for joining the imagine 1 9308 7(and the second	No.3First N=- No.4First N=- Newtien Name Newtien Name Protection Protection Newtien Name	anderdin On mi Home Page lec Wx Wechat echead:5% mi Introduction nami 27 27 27	Official Account snath Title Dire White Hat Security Specialist	Nun Rambing 35	nber of me. Number of vul. Fo Cartellarian points of this quarter 1520	ints of the s.	2019-04-03 12 2019-04-28 21 2019-06-26 19
a y	Contraction and	We control of the con	rack for free apply for joining the imagine 1 9308 7(and the second	No.3Fint h No.3Fint h Ref No.3Fint h Ref Ref Ref Ref Ref Ref Ref Ref	enderef in Oni m Home Page lec Wx Wechat enhead:5% m Introduction Rank 27 27 27 27	Official Account smath Title Ethe Vitrike Hat Security Specialist Security Specialist	Nun Besting 35 9 8	nber of me. Number of vul. Po Contribution priors of this quarter 1520 360	ints of the s.	2010-04-03 12- 2019-04-28 21 2019-06-26 19: 2020-12-24 03:
fember Name	Season pointa To	We control of the con	rack for free apply for joining the imagine 1 9308 7(option rate	Menter Tiane RosSFint In- Res Ros	andersfindon m Home Page lec Wx Wechat erhead:5% m Introduction 70 27 27 27 27 27	Official Account cruth Tate Site White Hat Security Specialist Security Specialist Ethe White Hat	Num Rainsing 25 9 8 20	Index of me. Number of vul. Po Contribution points of this sparter 1520 500 0	Aints of the s	2019-04-03 12 2019-07-29 21 2019-06-26 19 2020-12-24 05 2020-08-01 00
lember Name	Season points To	We c Official website 33436 Mail Tourn Points Ra	rack for free apply for joining the league 1 9308 7(mking No: of bags Report rece	grillon rate	No.5First n From No.5First n From No.5First n from Norther Have From From From From From From From From	anderfindos m Home Page ec Wx Wechat enhand:5% m Introduction 77 27 27 27 27 27 27 27	Official Account snah	Num 10 10 10	bee of me. Number of vol. Po Contribution points of this system 1920 900 0 200 200	Ants of the s	2019-04-03 12 2019-06-26 19 2019-06-26 19 2020-12-24 05 2020-06-01 00 2020-06-02 18
fember Name	Season points To	We concern the second s	rack for free apply for joining the league 1 9308 7(mking No: of bags Report rece Individual Contribution Points	ption rate	Mo-SFirst Anne No-SFirst Anne Moresser Zasse Strakes, 5 Strakes, 5	Inderfindin m Home Page iee Wx Wechat ehendd:5% m Introduction 27 27 27 27 27 27 27 27 27 27 27 27 27	Official Account of the Units Fat. Security Specialist Security Sp	Autory 23 9 8 8 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	bee of ms. Number of vol. Po Contribution points of this quarter 1320 300 0 300 0 0 0 0	ents of the s	2016-04-03 12 3018-01-34 21 2018-06-34 19 2020-12-34 05 2020-04-01 00 2020-04-02 10 2020-10-28 10
fember Name	Season points To	We c Official website 33436 stal Toarn Points Re	rack for free apply for joining the league 1 9308 7(mixing No. of bags Report rece Individual Contribution Points	ption rate	No.3First Par- No.3First Par- References Interest Interes	inderfindor m Horne Page iew Weichen iew Weichen iew Weichen zer zer zer zer zer zer zer zer zer zer	Cofficial Account crush Table Envirols Table Security Saecialist Security Saecialist Saecialist Security Saecialist S	Autority 23 8 8 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	ber of me. Number of vol. Po Contribution points of this quarter 1920 300 0 300 0 0 0 0 0	ents of the s	2016-04-03 12 2016-04-03 21 2016-04-03 19 2020-04-03 10 2020-04-03 10 2020-04-03 10 2020-10-28 10 2020-10-28 20
tember Name	Season points To nut(Captain) 4 32123 a	We concern the second s	rack for free apply for joining the league 1 9308 7(mking No: of bags Report rece Individual Contribution Points	ption rate	Mo-SFirst Anne No-SFirst Anne Weeksen Zasne Straken, 5 Straken, 5	Inderfindin m Home Page iee Wx Wechat ehendd:5% m Introduction 27 27 27 27 27 27 27 27 27 27 27 27 27	Official Account of the Units Fat. Second Se	Autory 23 9 8 8 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	bee of ms. Number of vol. Po Contribution points of this quarter 1320 300 0 300 0 0 0 0	ents of the s	Time of addition 2010-04-03 v2- 2010-04-03 v2- 2010-04-03 v1- 2020-04-01 00 2020-04-01 00 2020-04-03 v0- 2020-10-03 v0- 2021-04-04 v1- 2020-10-04 v1- 2020-10-04 v1- 2020-04-07 v0-

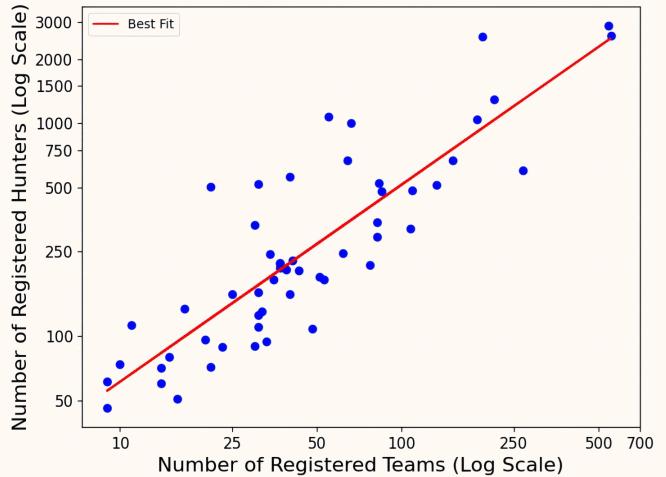
Research Questions

- 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

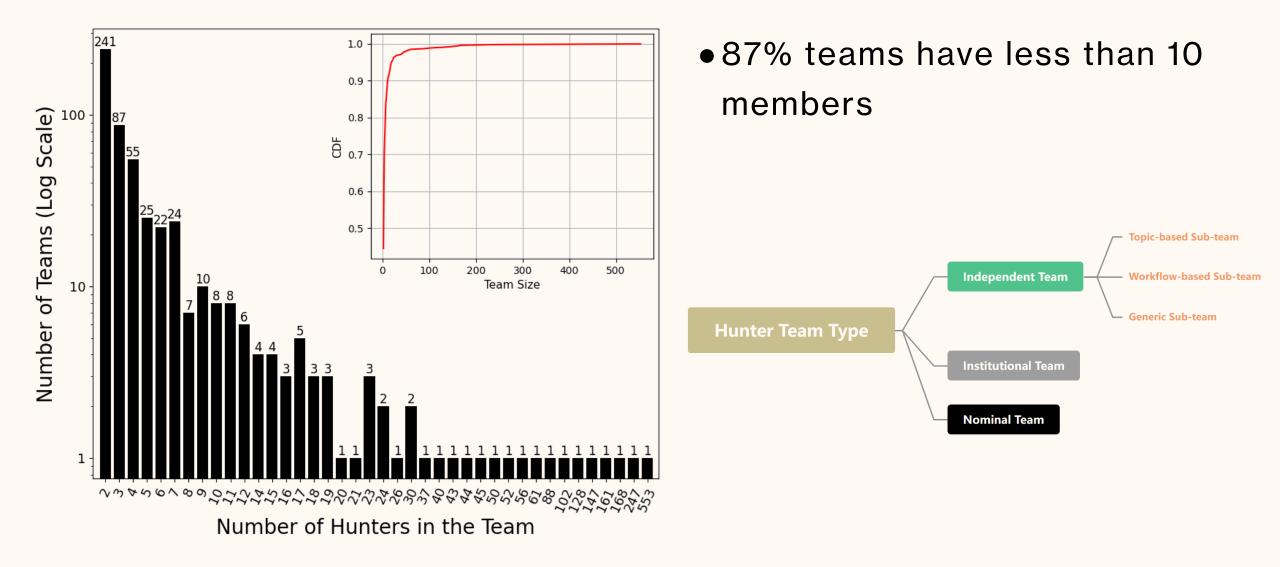


RQ1: Hunter Teaming Ecosystem

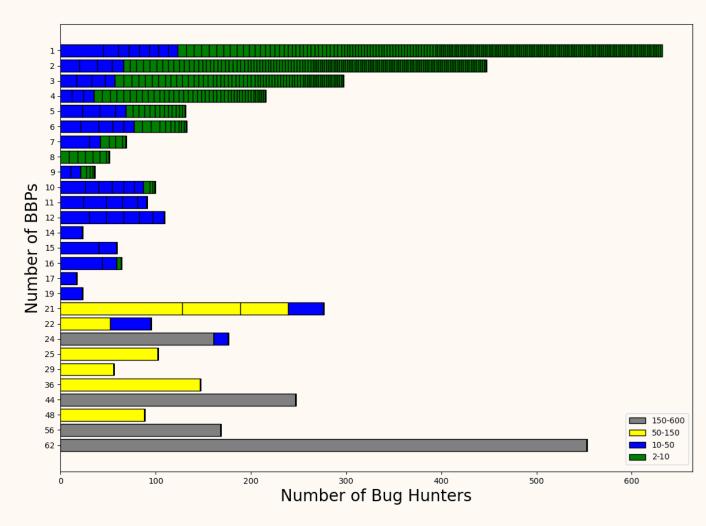


46% of users are part of a team
The three largest BBPs have over 2.5k registered users

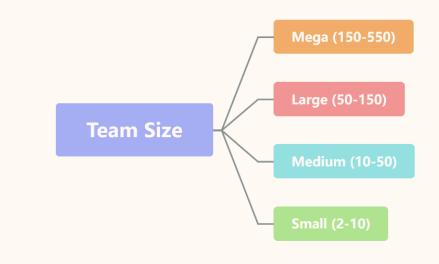
Prevalence of Users, Teams and BBPs (RQ1)



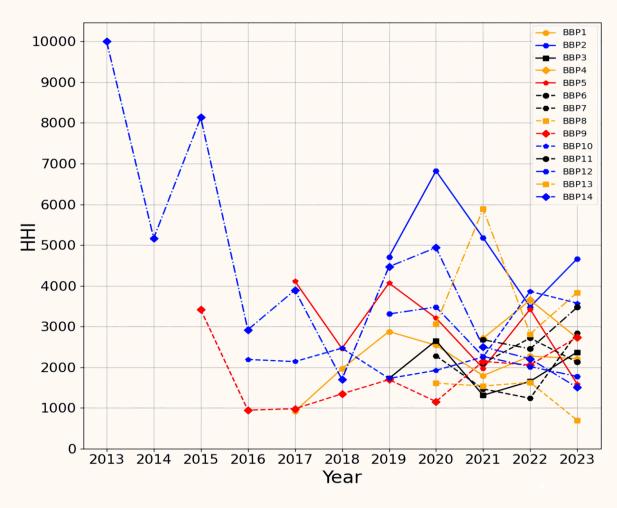
Prevalence of Users, Teams and BBPs (RQ1)



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



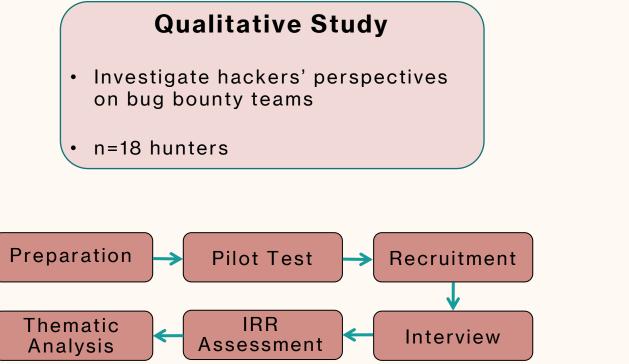
Team Productivity (RQ1)

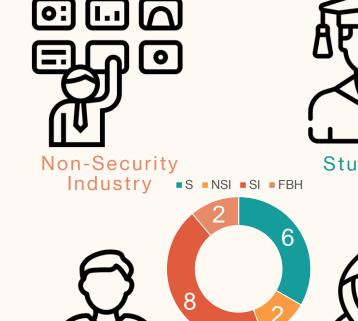


- Team members are more than twice (2.47) as productive as solo hunters
- There is a high level of market concentration

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

Phase II: Interview







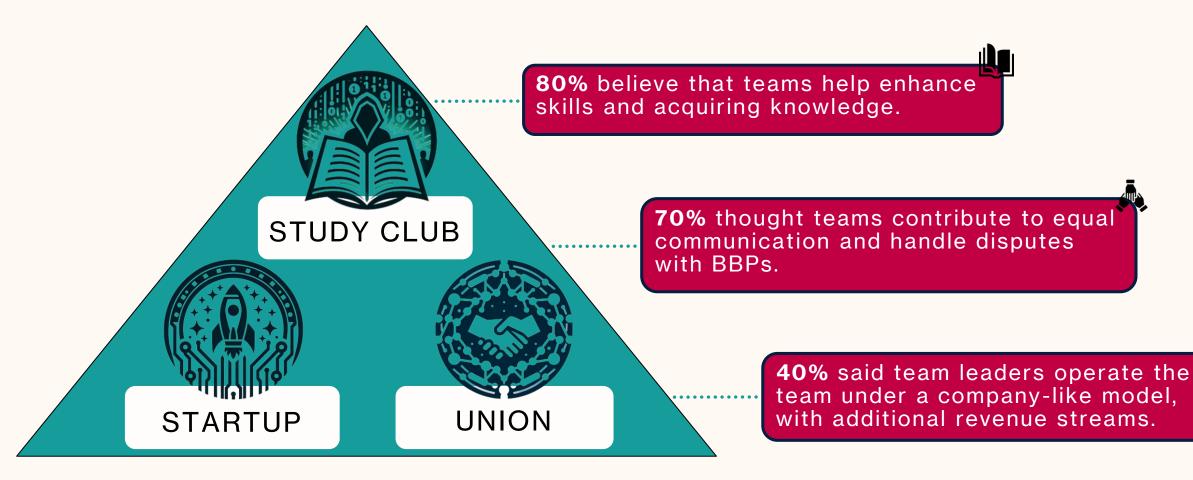
Students



Security Industry

Full-time Bug Hunters

RQ2: Multifaceted Functions of Team



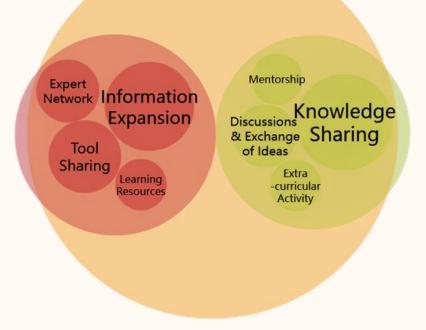
Study Club (RQ2)

Educational Relationships

- Discussions and exchange of ideas
- Private chats with experts
- Extra-curricular activities

Resources and Shared Tools

- Expand the availability of information

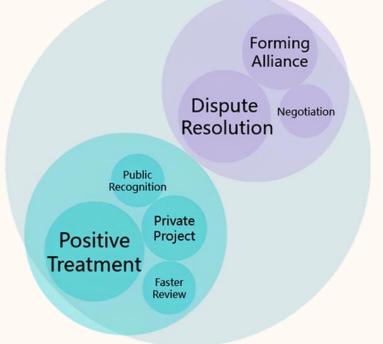


- Share auto-scripts, knowledge bases and cyber ranges

"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.

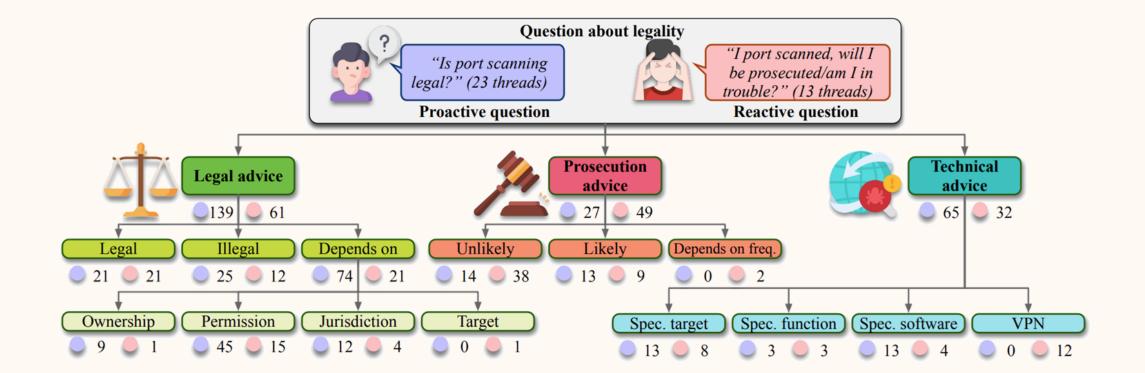
Legal Concerns of Would-be Vulnerability Researcher

(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

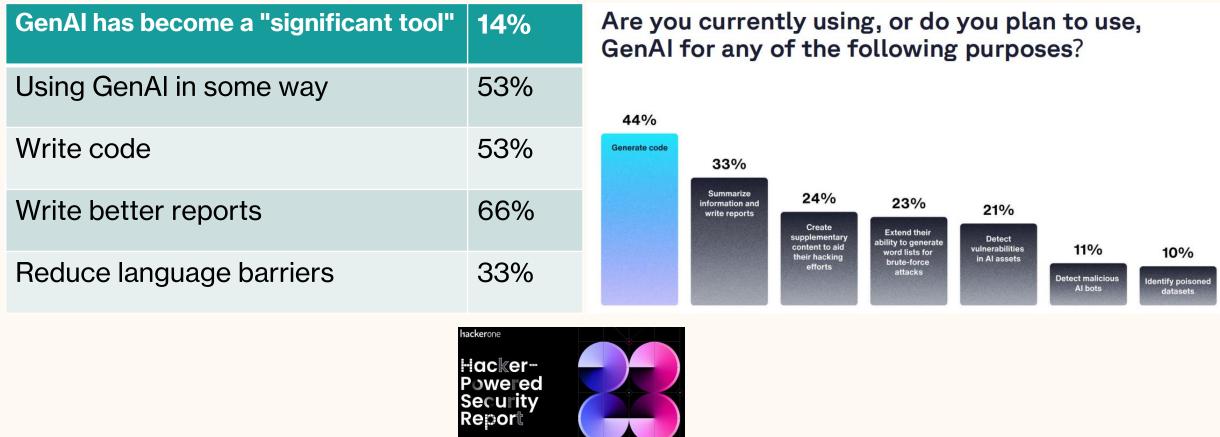


 Hrle, T., Milad, M., Li, J., & Woods, D. "Just a tool, until you stab someone with it": Exploring Reddit Users' Questions and Advice on the Legality of Port Scans. In 2024 European Symposium on Usable Security (EuroUSEC 24) (pp. 322-336).

AI+ Bug Hunting

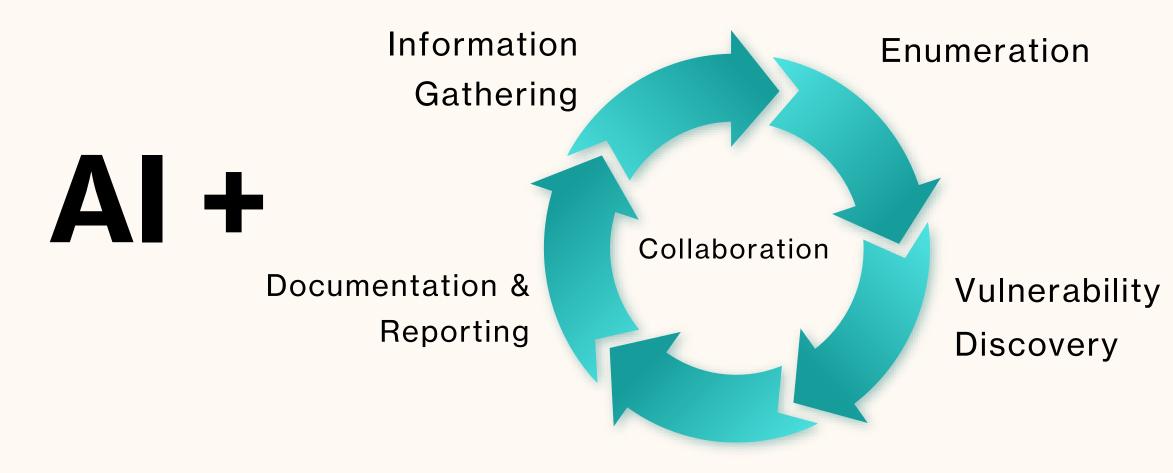
2023/2024

2024/2025



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

(The near) Future?



Exploitation

Take-home

- Akgul, O., Eghtesad, T., Elazari, A, et al. <u>Bug Hunters' Perspectives</u> 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. <u>Vulnerability discovery for</u> <u>all: Experiences of marginalization in vulnerability discovery</u>. In 2023 IEEE Symposium on Security and Privacy (SP) (pp. 1997-2014).
- The Record Media <u>'UK Home Office's new vulnerability reporting</u> mechanism leaves researchers open to prosecution'