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
•	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

etscape - [Version 2.07]	
Edit View Go Boolonerka Opt	iana <u>Directory</u> Window Help
(200 04) (20	
ation: about	• NI
hat's Newl What's Cool Hand	ack Nel Search Nel Directory Software
	Netscape Navigator (IIA)
NT	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. Flouse seed and agree to all terms before using this software.
	Report any problems through the <u>feerback page</u> .
NETSCAPE	Natarana Cremuningtions, Natarana, Nationale and the Natarana Cremuningtions lags on Includes of Natarana Cremuningtions Computing
Dece Coverance of	Containe J ara™ software developed by Sun Microsystems, Inc. Copysight © 1992-1995 Sun Microsystems, Inc. All Rights Reserved.
	Contains serveity software from NSA Data Serveity, Inc.
Pag RSÁ	Copyright © 1994 FSA Data Security, Inc. All rights reserved.
Contractor of the second second	This wession supports International security with RSA Public Key Cryptography, MD2, MD5, RC4.
orpanistics of Historys Solvers to U.S. U.S. ens. & FAR 13.337-19 vilon, applicable, or a semanticalities: Corporation, 303 Rot. Mod.	Commands in write "Surfmedingles" at Slidow: Two, dig Nation of Surfaces by the Government is object to metricline on both in edge-apply (2)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)
1-90	₩ ²

WANTED Bug Bounty Program

PATCHED or ALIVE

\$200,00

Development of Bug Bounty





• 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



Vulnerability Discovery Experience



Underlying System Knowledge



Access to Development Process



Motivation



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

- 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).

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).

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).

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

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).

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

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

Hacker Collaboration

• A unique teaming ecosystem has evolved in China

	reaction services								West Street	Contraction of	CILLARS SERVICE IN COMME
	ChuMats.Org	15	http://www.chamd5.org	0254	2						
	() NA277	14	https://www.taq.com	2959		6					
*	🧿 LRSer	6	https://www.la-sec.com/	2011	2	0					
4	😵 Tiphtan-S	15		2003	۲						
5	Oay1mmin.	15	http://heam.day1.today/	1523	(6)						
6	O 06+082-	20		1271	(4)	-					
i i	() XRABE.	15		(9900							
3	() #82960v	16	https://ovenpace.cn	827							
12	0 0000	23		672	(8)	•					
iΩ	 • • • • • • • • • • • • • • • • • • •	13		ser	(2)	٠					
					(B)		17771997	752	1959 -	2222	: 辨
					No.3First n	ISec 1995 under Entre em Home Pa Sec Wx Wech sechead:5%	pe: pe: lat Official Account	Nu	12 Seventeen. mber of me. Number of vul. Pob	1343 rts of the s	
		ChaN	Id5.Org ax for free		No.3First n	ISec 1775 under 2110/4 am Horse Pa Sec Wx West serhead:5% am Introduct	uation for manufantatip ge: aat Official Account oncrush	Nu	12 Seventeen. mber of me. Number of vul. Poin	3343 rts of the s	
		ChaN We ca	Id 5. Org eck for free page tar joining the league		No.3First n The second seco	ISec Water under Entite am Horse Pa Sec Wx Wech schead:5% am Introduct	sation for mendenologo pe: ant Official Account persuan.	Nu	1.2 Seventeen. mber of me. Number of vul. Pob ceretification parents of this quarter	1343 rits of the s	eren ul aubbiore
	6054 a	Chai Vé ca Constitut versione Bad Ada 6 Bad Fasn Points – Ran	Id5.Org extorne uptrojoning the league I 900 fb 2008 700 Max No of bas Record new) _N	No.3First n The second seco	ISec Water underdintite am Home Pa Sec Wx West serhead:5% am Introduct tern 27	pe: art Official Account oncrush. Table Dis White Hall	Nu Residence 25	12 Seventeen mber of me. Number of vol. Poi Ceretification points of this quote 1920	3343 vito of the s. s	Gene al addition 018-04-03 12-02.09
	6054 a	ChaN We ca CONCLEA version 33436 1 Stat Team Points Ram	Id5.Org ck for five and for joining the league I 9308 700 No. of bags Report new	Dec.	No.3First In	Sec 500 am Horse Pa Sec Wx Web erhead:25 am Introduct filerit 27 ar	pe: art Official Account onerush Dise Units Hat Dise Units Hat beside from that	Ner Renking 55 9	12 Seventeen. mber of mr. Namber of vol. Poi centilution points of this system 1100 1001	3343 rds of the s.	5mm of addition 018-04-03 12-42.00 019-04-03 12-1112.00
A B B	6054 Season points	ChaN We ra Concise weekee 33436 cal Town Florids Ram	Id5.Org ek for frør andr for jonning i the instatue I 9308 70 Mar No: of bugs Report recen) s storn take	No.3First nu No.3First nu Monitor name Monitor name Monit	ISec Construction onder Entropy and Home Pa Sec Wx Weck serhead 3% and Introduct files 27 27 27 27	pe: art Official Account comman. 556 Dife When Hal Security Security Security Security Dec When Hal	Nut National SS 8 8 8 8	12 Seventeen. mber of me. Namber of vol. Peri constitution protein of this space. Visio 400 5	1343 encoffice s. 	See of Jubility 1989-44-03 (2020) 1989-05-20 (2020) 1989-05-20 (2020) 1989-05-20 (2020) 1999-05-20 (2020) 1999-05-20 (2020)
No and	6054 Season points	Chak We ca Official wereken 8334366 4de Team Points Ram	Id5.Org ek tief me add for growing the levelue I 9308 700 king No. of bugs Report nevel)s stor rate	No.3First n	ISec Construction or and the second second second sectors and the second second second second second second second second second second second second second second second second second second	Jatua Romendeel Naz pe at Official Account connuch Star Des Vision Hal Security Security Security Security Security Security Security Security Security Jaccalet	New NewNamp 55 8 30 30 30	12 Seventeen. mber of mer. Number of val. Peol Contribution provid of this quarter 1920 2020	3343 Hoto of the s.	See of Jubblich 1914-6-03 (2-04) 1914-6-03 (2-14) 1914-6-34 (1903) 1914-6-34 (1903) 1914-6-34 (1903) 1914-6-34 (1903) 1914-6-34 (1903) 1914-6-34 (1903)
Member Name	6054 a	Chak We ca Official works and 834366 and 834366 and 844366 and 844566 and 8445666 and 8445666 and 844566666666666666666666666666666666666	Id5.Org by for large the loader of the large the loader 1 9308 700 May No. of bugs Report incest	9% ption rate €ar • Tang of addition	No. Sfirst n	ISec Constraints ander diritin en Horve Pa ser Wx Weck enhead 3% am Introduct film 27 27 27 27 27 27 27 27	vatura four mendeal valaz pr and Official Account consults. 1968 Dires Voltes real Security Samular Security Samular Security Samular Security Samular Security Samular Security Samular	Net 93 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	12 Seventeen. mber of mat. Number of val. Pool Centritudion parotis of this quarter 1930 200 201 201 201 201 201 201 20	1343 em of the s. 3 4 5 5 6 6 6 6 7 7 8 7 8 8 8 8 8 8 8 8 8 8 8 8	New of Jubility 1915-54-03 12-02 (J) 1916-65-28 (J) 1115 1916-65-28 (J) 1115 1916-65-28 (J) 1115 1910-66-28 (J) 1115 1910-66-02 (J01) 1140
Member Name	6054 a	ChaN We ca Official workshowshowshowshowshowshowshowshowshowshow	Id5.Org bit for any the leader of the leader the leader Argent Nec of brass Report income Many Nec of brass Report income Indfudduat Contribution Points	Stion rate	No.3First n No.3First n S trob S trob S trob S traban S traban	Sec Control under die film am am Horse Har Bie sern lotten Har Bie film Bie die Bie	value for www.delay.delay pri- and Official Account consult. 2016 Vintue real Security Security Security Security	Nee 90 90 90 90 90 90 90 90 90 90 90 90 90	12 Seventeen. maar of mar. Naindair of val. Pool Cestellustions parote of this quartee 1120 200 0 201 201	1345 period the s	See of publicar D10-54-03 12-80 (0 919-67-29 (1115) 010-68-20 (1014) 010-68-20 (1014) 010-68-20 (1014) 010-68-03 (1014) 010-68-03 (1014)
Momber Name	6054 T	ChaN We ca Confide weeken B334366 Stat Town Florets Rear Title crowed of onlockers	Id5.Org Id5.Org Id5 for lange the league Id6 for lange the league Id6 for lange the league May No. of Dags Report more Indfuddual Contribution Points Id60	se otion rate Time of addition 2016-03-08	No.3First n No.3First n S trob S trob S trob S trab S trab	Sec Condension Condensio Condension Condension Condension Condension Condension Condensi	Addres Normendeet Adapt prime and Official Account and Official Account consumers Descriptions Head Security Security Security Security	Nution 75 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	12 Seventeen. mater of mar. Naindair of vail. Pool Constitutions parotic of loss quartee Yisto Sela Sel	3343 en of the s. 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	Some of Jubbility (11-5-4-0) 12-04 (JB (11-6-4-0) 12-14 (JB)(12-14-0) 12-14-0) 12-14 (JB)(12-14-0) 12-14-0) 12-14-0) 12-14-00-00-00-00-00-00-00-00-00-00-00-00-00
Member Name	6054 T Season points T	Chan We can Conside weeken B334366 B34456 B34456 B34456 B3	Id5.Org Id5.Org kt for five p 9308 700 Krig No: of bags Report more Indfuddual Contribution Points 1886 1886	Se, ption rate store of addition 2016 03-00 2021-01-13	No.3First n= No.3First n= Constant range Strates Strat	Sec Constant Constant Constant Constant Sec We Weck enclosed State and Introduct Sec We Weck enclosed State and Introduct Sec	Addition Room Network of Addition pre- dent Official Account and Official Account Sense Writers Hall Sensering Sales and a Sensering Sales and a Senserin	Nue 25 30 30 30 30 30 30 30 30 30 30 30 30 30	12 Seventeen. mater of mar. Naindair of val. Pois Constitution points of los quarter 1520 15	3343 vin of the s.	Some of Jubbility (11-3-4-0) 12-14-0.09 (11-4-4-0) 12-14-0.09 (11-4-4-0) 12-14-0.09 (11-4-4-0) 12-14-0 (11-4-0) 12-14-0 (11-1
Member Name Member Name Image: Construction of the second seco	6054 T	Chan We as Confide weeks B34366 B3456 B36	Id5.Org id5.Org bit 2016 9308 70 May No. of bags Report near Ind2Addual Contribution Points 1000 1000 11205	% sign + picen state sign + Time of addition 2016-03-00 2021-01-13 2019-03-20	No.3First h No.3First h S tribs S tribs	Sec Constant Constant under Ein March Farr March March Sec Warkbadd 25 am Introduct 27 27 27 27 27 27 27 27 27 27 27 27 27	Addition Ruo Insured and Addition pre- and Cefficial Account and Cefficial Account Cefficial Account Delications Field Delications Field De	Net 25 9 4 36 36 36 36 36 36 36 36 36 36 36 36	12 Seventeen. mater of mar. Number of val. Pois Ceretrisation points of loss quarter 1120 100 100 100 100 100 100 10	3343 oth of the s.	Tere of addition 018-44-03 12-42 09 018-44-03 12-42 09 019-44-03 12-42 09 019-44-03 12-42 09 019-44-03 12-42 09 019-45-24 03-44 019-45-24 03-12 019-45-24 03-12 019-45-24 03-12 019-45-25 03-00 019-45-25 03-00 019-55-25 03-00 019-55-25 019-55

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)



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







Non-Security Industry S NSI SI FBH Students



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 Unior

Positive Treatr

Dispute Resolution

- Intervene
- Forming

According to several members of the ChaMd5 security team, there have been many disputes with SRC over the past few years after vulnerability reports. They could not reach a consensus on the value of the vulnerability, the impact of the hazard, and the security rating. In addition, the vulnerability auditors were overly paranoid and showed a lot of disrespect for the work of white hats.

After considering many aspects with several co-founders, it was finally decided that the ChaMd5 security team would "terminate cooperation with "SRC vulnerability" from November 13, 2020. This decision was not a momentary idea. We have communicated. 2021 is coming, and we will cooperate with better SRCs, so some SRCs will also terminate cooperation.

The specific adjustments are as follows:

To all ChaMd5 members:

- All team members will stop submitting any relevant vulnerabilities and intelligence information to SRC from now on;
- 2. The team voluntarily waives any related thanks and rewards to ChaMd5 from
 - SRC, including but not limited to ;
- 3. Members have redeemed the rewards they received for submitting vulnerabilities as scheduled to protect their work results and legal rights;
- 4. If there are still serious vulnerabilities that have not been submitted, report them to the National Information Security Vulnerability Sharing Platform;

"Some teams un the severity of u

In order to better coordinate the communication between team members and major vulnerability platforms and manufacturer SRCs and establish a more fair cooperative relationship, the ChaMd5 security team officially joined the " White Hat Self-Discipline Committee " today to establish a unified external communication channel for controversial vulnerability ratings, value identification, communication and other issues.



Faster

Review

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)

Æ 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 GenAl has become a "significant tool" Are you currently using, or do you plan to use, 14% GenAl for any of the following purposes? Using GenAl in some way 53% 44% Write code 53% Generate code 33% Summarize 24% nformation and 23% Write better reports 66% 21% write reports Create Extend their supplementary content to aid Detect word lists for 11% 10% their hacking in Al assets brute-force attacks **Reduce language barriers** 33% Detect maliciou Al bots lentify pois hackerone Hacker-Powered Security Report

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





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'

Join Our Research Project

- Unfairness of Bug Bounties
- Legal Concern of Vulnerability Researchers
- Cooperative Work in Bug Reviewing
- Hacker Teaming Mechanism (Chinese)



(Generated by ChatGPT)

Contact us if you are interested! https://blogs.ed.ac.uk/yangheran_piao/ lawrence.piao@ed.ac.uk

. . .