UNIVERSITY OF LONDON | INTERNATIONAL PROGRAMMES

UNIVERSITY OF LONDON

Using crowdsourcing to find security bugs: The emerging role of bug-bounty programs

UOL159 Research Project in Digital Innovation, BSc Information Systems and Management

Student Name: Huang, Pei Yu

Student ID: 180329021

Date Submitted: May 1st 2021

Abstract

Bug-bounty programs (BBPs) are a method utilising crowdsourcing by ethical hackers to improve organisations' information security. This study aims at showing perspectives from BBPs' end users through online questionnaire and interviews on ethical hackers, companies, government department and third-party platforms. Before introducing BBPs, some ethical hackers would report bugs to company, but some were not willing to report because of legal jeopardies and unresponsive attitudes from companies. Hence, some may conceal the information or selling it to black market. For organisations, they consider unauthorised testing on websites and systems from unknown testers as illegal or extort actions. Not to mention most companies did not have a proper channel to deliver and response to these reports.

BBPs are a solution to the problems. BBPs provide a cost-effective method for organisations. In the questionnaire, ethical hackers showed positive attitude to keep joining BBPs but have concerns with bugs undervalued. In the interviews, companies shared the insights on running BBPs is a way to build reputation. Government department talked about not using BBPs because of hackers' unknown identities and law restrictions. They also considered clarity in policies and costs reduction is the benefits of joining BBPs through a third-party platform. To conclude, BBPs is an innovative method for companies to improve information security compare to the traditional way of relying on limited source of IT security expertise such as an IT security company or invited penetration testers. BBPs is a means of utilising crowdsourcing by incentivising skilful ethical hackers with bounties and accumulated reputations. With the access to relatively large pools of expertise and a competitive bounty-earning environment, companies are able to find bugs efficiently and fix it effectively. At the same time, it also mitigates the risks of participants hiding bugs for malicious use. Therefore, BBPs creates a win-win situation for companies and ethical hackers in improving information security.

Keywords: Bug-bounty programs, BBPs, Ethical hackers, Crowdsourcing, Information security

Contents

List of Figures

List of Tables

Chapter 1. Introduction

Despite the skills in software-engineering practices have evolved and matured in recent decades, organisations' product and software remain insecure. Cyber-attacks have rapidly increased among personal devices and companies with article showing that there were 80,000 cyberattacks per day or over 30 million attacks per year in the record in 2018 [22].

Organisations and companies are searching for effective approaches to cope with cyber threat. Protection against cyber-crime has constantly been a demanding task for worldwide organisations and companies. A report sponsored by McAfee in 2014, estimated that the annual damage to the global economy was US$445 billion [20]. One of the most famous ongoing cyber-attack is the event of SolarWinds Orion exploit. FireEye has uncovered a widespread campaign that spread its attack through SolarWinds Orion IT management software to their clients, which includes numerous public and private organizations around the world [8]. Thus, improving information security and system protection is a universal focus for every organisation and company and should not be neglected.

To overcome the challenges, companies have started to consider leveraging expertise crowd to find bugs, mostly security vulnerabilities. These ethical hackers that submit valid reports are rewarded with monetary bounties or reputation for their contributions to enhancing companies' system security. This approach that takes advantage of crowdsourcing efforts is called a bug bounty program (BBP).

BBPs have been implemented by many organizations, including Mozilla, Google, Reddit, Microsoft, and Facebook. For instance, Google has announced to pay US$1 million as the top award to the ethical hackers who can find vulnerabilities in its Pixel series smartphone. An additional bonus of US$1.5 million if an exploit on "specific developer preview versions of Android" is found. The Chrome Vulnerability Reward Program (VRP) has cost approximately US$580,000 over 3 years and has resulted in 501 bounties paid for the identification of security vulnerabilities. In addition, Firefox VRP has cost approximately US$570,000 over the last 3 years and has yielded 190 bounties [9]. There are several commercial BBP platforms such as HackerOne, BugCrowd, Cobalt, Yes We Hack, etc. These third-party platforms aim to facilitate the process of building and maintaining the trust and stability of transaction in bounty and bug information between ethical hackers and organisations.

On HackerOne, over 181,000 vulnerabilities were found and awarded more than $107 million in bug bounties to a growing community of over 830,000 hackers [15]. HackerOne has more than 1,700 customer programs, including well-known organisations and enterprises. such as the U.S. Department of Defense, Google, Adobe, PayPal, Twitter, GitHub, Uber, Microsoft, IBM, Starbucks, Dropbox, and Intel.

Stated in HackerOne's 2020 report, nearly two-thirds of hackers said they have found bugs but chose not to report to the organisation, and with 38% of them indicating that it was because of the threatening legal language posed by the organisation regarding the discovery of vulnerabilities. On the other hand, 21% of hackers stated that most companies do not have a clear channel for them to report the bugs and with 15% said the companies were mostly unresponsive to the reports [14]. Thousands of bugs may have gone concealed or even worse got traded in the black market for malicious purposes. Therefore, BBPs are an ongoing means of organisations using crowdsourcing effort to secure product and system security.

1.1 Aims and scope

This study investigates the reasons why BBPs become an emerging business in information security, and how end-users interpret it. This study also lists the overall advantages and disadvantages of BBPs provided from interviews and questionnaire, and the advantages and disadvantages for the choice of cooperating with a third-party platform. The findings also highlight the concerns and factors that affect their attitude in continuing engagement.

1.2 Reasons for choice of topic and scope

This research aims at investigating how and why hackers from different countries, companies, government department, and third-party platform interpret BBPs.

Apart from hiring security companies to do penetration testing, several organisations have started to put crowd effort in their security methods to find vulnerabilities in software and websites. The average bounty paid for critical vulnerabilities increased to

US$3,650 in the past year, up 8% year-over-year. Organisations that are rather conservative have also started to accept this novel way of testing their systems. In 2020, individual countries such as China have increased year-over-year bounty awards by 582%, Spain by 307%, France by 297%, and more countries paid bounties for the first time [15].

These numbers show that governments are also attempting to use crowdsourcing power and investing in bounty. This study focuses on collecting the feedback from BBPs end-users and elaborating the reasons why they choose this method.

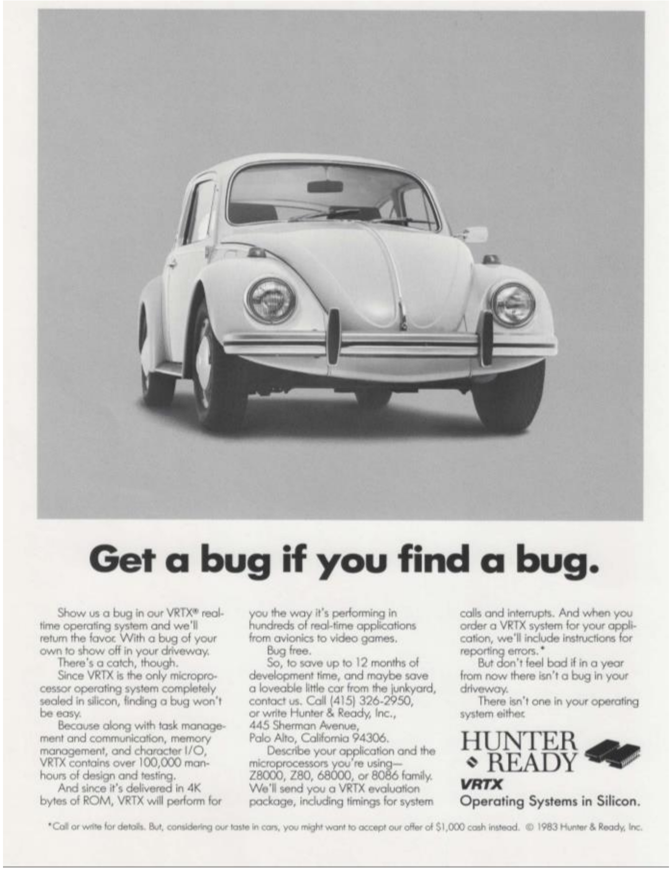
1.3 Report Plan

In Chapter 2. Literature Review, the research shows how BBPs have evolved from the time span of 1995 by Netscape to 2017 until the present. Then the research shows how different researchers analysed BBPs from the economic trade-offs to calculating the most efficient model to allocate efficiently to decrease the amount of duplicated submitted reports by hackers. Some portrayed it as a cost-effective win-win situation for organisations, but some considered this commercialised model is a big issue for the industry. Chapter 3. Objectives and research methods, illustrates how the questionnaire and interviews were conducted, and the modified technology acceptance model (TAM) framework is discussed in Chapter 4. Conceptual Framework, with an explanation of the and calculations. Then Chapter 5. Findings, shows the findings and statistics collected from questionnaire and interviews. Chapter 6. Analysis, analyses the output and research results from Chapter 5. Findings, and includes the advantages and disadvantages shared by respondents and an overall elevation, leading to a conclusion in Chapter 7. Conclusion.

Chapter 2. Literature Review

2.1 Background and recent development

Prior to the increase in the population of BBPs, finding professional security companies to do penetration tests for systems is a common methodology for companies and organisations started from the 1960s. A few decades later, the first known BBP was initiated by Hunter & Ready in 1983 for their Versatile Real-Time Executive (VRTX) operating system. They gave a Volkswagen Beetle (a.k.a. Bug) in return for anyone who finds bugs in the system (Figure 1. 1).



Show us a bug in our VRTX® real-time operating system and we'll return the favor. With a bug of your own to show off in your driveway.

There's a catch, though.

Since VRTX is the only microprocessor operating system completely sealed in silicon, finding a bug won't be easy.

Because along with task management and communication, memory management, and character I/O, VRTX contains over 100,000 man-hours of design and testing.

And since it's delivered in 4K bytes of ROM, VRTX will perform for you the way it's performing in hundreds of real-time applications from avionics to video games.

Bug free.

So, to save up to 12 months of development time, and maybe save a loveable little car from the junkyard, contact us. Call (415) 326-2950, or write Hunter & Ready, Inc., 445 Sherman Avenue, Palo Alto, California 94306.

Describe your application and the microprocessors you're using— Z8000, Z80, 68000, or 8086 family. We'll send you a VRTX evaluation package, including timings for system calls and interrupts. And when you order a VRTX system for your application, we'll include instructions for reporting errors.*

But don't feel bad if in a year from now there isn't a bug in your driveway.

There isn't one in your operating system either.

*Call or write for details. But, considering our taste in cars, you might want to accept our offer of $1,000 cash instead. © 1983 Hunter & Ready, Inc.

Figure 1. 1. First known BBP held by Hunter & Ready

According to an article about the history of BBPs written by Friis-Jensen. E, Co-Founder and Advisor at Cobalt, in 1995, Netscape held a BBP, which offered US$1000 rewards to those who were able to find security bugs in their Netscape Navigator 2.0 Beta. "By rewarding users for quickly identifying and reporting bugs back to us, this program will encourage an extensive, open review of Netscape Navigator 2.0 and will help us to continue to create products of the highest quality"[16], explained at that time by Mike Homer, former vice president of marketing at Netscape.

Then in 2005, Mozilla launched a BBP on its Firefox system offering US$500 reward for every verified bug, and the program was later expanded to cover most of the Mozilla services and products. In the 2010s, influential technology companies such as Facebook and Google kick-started the trend towards BBPs for web applications. Facebook launched a BBP in 2011, which is still receiving reports in the scope from applications like Instagram and WhatsApp to other partnerships. In addition, Google has launched an experimental program that rewards proactive security improvements to select open-source projects, with bounty rewards from US$500 up to US$20,000. A lot happened on the bug bounty scene at the time; Barracuda networks launched BBP, and Deutsche Post, the German federal postal service, launched a BBP for their secure messaging service [10].

In the same period, Bugcrowd was one of the first companies to utilize crowd-sourced security as its core business. It was founded in 2011, with the goal of helping to manage clients' penetration tests, BBPs, and vulnerability disclosure. Its bug bounty community consists of over 50 industries and 30 countries in 2020 [4].

In 2012, Jobert Abma and Michiel Prins founded HackerOne. It rapidly became one of the most successful BBP platforms with over 600,000 individuals in the hacker community and 1700 programs from companies. HackerOne has partnered with tech companies like Slack, Twitter, PayPal, and Dropbox. Four years later, the U.S. Department of Defense initiated a "Hack the Pentagon" BBP using HackerOne's platform. This program resulted in the discovery of 138 valid vulnerabilities in the department's websites and have paid over US$70,000 to the contributing hackers [13].

These third-party platforms have gradually started to take business with governments and organisations for helping them make a start for their own BBP and leverage the power of common security companies.

2.2 Related work

Despite the popularity of BBPs, Zhou and Hui (2019) shed light on the controversial questions that arise from it. The issues involved from the design and practical use of a BBP to whether the organisations can fulfil the rudimentary goals of security improvement. They developed a security game framework to analyse the economic trade-offs in BBPs. The insights they provided include: the firm will always benefit from BBPs unless they pay an excessive reward to encourage strategic hackers to participate, BBP is not a one-size-fits-all solution, the firm needs to evaluate their own in-house protection strategies with fully understand their value of the systems in a mature security environment; Zhou and Hui (2019) also showed a useful insight into law enforcement and public policies: the more the enforcement in the program, the less effective for both in-house protection and probability for identifying the bug. The model also proposed a guide for government in its extent of intervention [26].

Katie Moussouris, which is the founder and CEO of Luta Security and working at Microsoft and the Department of Defense creating their first BBPs in 2014, shared some same standpoints. "Instead of aiming to make their systems more secure, companies are viewing BBPs as a "one size fits all" solution for their business." said by her in the interview with Threat Post in 2020 [21]. In addition, Moussouris elaborated that the commercial implementation of bug bounties is failing the whole system. Several companies cannot keep up with patching the systems that they know are out of date. They believe by applying BBPs is like outsourcing to BBP platforms with everything handled. This resulted in a situation of numerous low-hanging fruit bugs in the system which should have been invested internally on finding by the developers themselves; It could also be 45 times cheaper if the bugs were identified in the design phase. This leads to another problem that since participants are rewarded in result-based when there's a lot of easy bugs to find, one should just be the first one submitting the bug report in order to get the reward. There are numbers of unpaid labour that goes into this structure and potentially leads to a poor evolution of the cybersecurity workforce [18].

Zhou and Hui (2019) also provide insights that combining "sticks" (by strengthening the punishment rules and in-house protection) and "carrots" (the rewards and incentives for participants to do penetration tests ethically) is often better than having "sticks" alone [26]. In terms of incentives and efficiency for ethical hackers in joining BBPs, Maillart et al. (2017) have a revisit to Eric Raymond's Linus's law, which is the assertion that "given enough eyeballs, all bugs are shallow" in The Cathedral and the Bazaar. They found a strong front-loading effect which indicates that newly launched programs attract many participants contributing, however, the probability of discovering bugs decays sharply after the launch. They proposed three design recommendations for organisations in their BBPs to increase the incentives of ethical hackers and the efficiency in focusing on more pressing security issues [19].

Management wise, according to Gartner analyst Dale Gardner in Gartner report (2018), he mentioned two factors that could act a stall to the potential of BBPs: trust and economics. He points out the possible trust issues occurred between buyers (firm offering programs) and vendors (ethical hackers selling the bugs). E.g. not all the participants are motivated by positive forces, hence the risks of rogue ones may disclose sensitive information or divert it to the black market. Or some of the participants have concerns over being exposed to legal jeopardies, such as being accused of violating the laws. The approach he suggests mitigating the risks is to ascertain the legal counsel, which should be consulted to examine agreements between the buyer community and vendors. A high level of transparency and clarity in terms and conditions can help alleviate misunderstandings. Then the issues of economics, both buyers and vendors should reflect a fair and economically attractive environment in order to sustain both objectives [12].

These researches did not include feedback from end-users of BBPs, including perspectives from ethical hackers, organisations, and third-party platforms. Therefore, this study aims at providing these perspectives.

Chapter 3. Objectives and research methods

3.1 Objectives

This section proposes how the quantitative survey was done, and how the questions were designed; it also shows how the qualitative interviews were conducted and brief introductions of the interviewees (Table 3. 1).

The objectives of this research are:

1. Analysis of the advantages, disadvantages from BBPs end-user perspectives.
2. Elaborate how ethical hackers, companies, government department and third-party platforms interpret BBPs, and what affects their attitude of continuing engagement in it.

3.2 Methodology

Several methods are used to achieve the stated objectives:

1. Study and review literature
2. Conduct an online questionnaire on ethical hackers
3. Conduct face-to-face interviews and email interview with managers in the IT industry and third-party platform HackerOne
4. Reviewing on multiple conference talks

3.2.1 Survey with questionnaires

The questionnaire was conducted using Google Form, which is a universal online survey tool and a user-friendly tool for organising respondents' answers. Respondents are 52 worldwide ethical hackers and IT researchers. The messages were sent through their website contacts, Twitter direct message and emails. The questions are designed base on Technology acceptance model (TAM). More details of the model are mentioned in Chapter 4. Conceptual Framework, and the demographics, findings are in 5.1 Quantitative findings from surveys. Analysis of the questionnaire are in Chapter 6.1 Quantitative analysis.

3.2.2 Empirical interviews

The interviews were conducted in face-to-face with one of them through email*; Interviewees include:

1. Mr Lee, senior security manager from Synology. Inc. headquarters
2. Mr Wu, director from the National Center for Cyber Security Technology (NCCST) in Taiwan
3. Mr Tsai, CEO, founder of Hacks in Taiwan Conference (HITCON) community and CEO of TeamT5. Inc.
4. Mr Tucker, senior director of community from HackerOne*.

Table 3. 1. Brief information of the interviewees' affiliation

Organisation	Brief Introduction	Representations in this study
Synology. Inc	An international enterprise specialising in secure network deployment and network attached storage (NAS) with the most market share in the world. It has a total asset estimated US$7.1 million and 650 employees worldwide.	Running BBPs themselves
Taiwan National Center for Cyber Security Technology (NCCST)	Taiwan top cyber-security agency established by government authority. Promote national cyber security policy and accelerate establishment of cyber security environment.	Government department that doesn't use BBP
Hacks in Taiwan Conference, HITCON/ TeamT5. Inc.	Taiwan biggest hackers' association and hacking technique forums. It aims at building hackers' community and holding international hacking competitions. / An IT security company with more than ten years of experience	Perspectives of a hacker and security company

	in malwares and Advanced persistent threat (APT). They have been invited to international conferences, such as Code Blue, Troopers, Hack in The Box and FIRST.	
HackerOne	One of the biggest and well-known BBPs platforms with over 830,000 registered hackers and 1700 programs worldwide. It offers BBPs and penetration testing solutions for government agencies and companies.	A third-party platform offers companies' BBPs

Every interviewee has signed an informed consent agreement about the disclosure of their names and titles of the organisation. The questions are focused on the satisfaction of holding BBPs or the reasons for choosing not to join, and the advantages and disadvantages based on their own experience. Important takeaways are mentioned in Chapter 5.2 Qualitative findings, and the findings are elaborated in Chapter 6.2 Qualitative analysis.

Chapter 4. Conceptual Framework

4.1 Introduction

The adoption of BBPs is an innovative technology for organisations, which is an additional method to test their software and system comparing to the old fashion way of hiring security companies. It also a revolutionary technology for ethical hackers that it is a legal and authorised platform to report bugs to companies. Questionnaire for ethical hackers and the interviewees were designed partially based on Technology Acceptance Model (TAM), which is a framework used in evaluating the acceptance process of users to a certain technology or information system.

4.2 Technology Acceptance Model (TAM)

Fred D. Davis has purposed the technology acceptance model (TAM) based on Theory of reasoned action (TRA) in 1986 [5]. TRA aims at examining the underlying motivation of an individual behaviour, and it suggests that humans are rational and able to utilise appropriate information systematically [11]. They suggested the intention to perform a behaviour is jointly determined by attitude towards the behaviour and subjective norms. The theory also purposes the greater the attitudes the more likelihood the behaviour to be performed. TAM is a special tailored adoption of TRA for better in explaining the determinants of computer acceptance and end-user behaviour. Davis (1989) initially conducted regarding acceptance of a software text editor on a survey on a group of 112 users at Canada IBM and 40 MBA students of Boston University [6].

TAM has been popularised in the research of focusing reasons of users' acceptance and reject to information technology. For instance, research on the influence on customers' use of electric vehicles [17], research on the attitude and intension of multimedia among schoolteachers [25], and predicting users' continuance intention toward e-payment system [23]. TAM is a useful and rather simple model for explaining and predicting users' intention and attitude in the acceptance of technology.

4.3 Proposed model of user behaviour of participating in BBPs

In this research, a modified model is proposed in Figure 4. 1. The survey questions are designed based on 6 parts: Trust, Perceived usefulness, Perceived ease of use, Attitude toward using, Intention to use, and Actual usage.

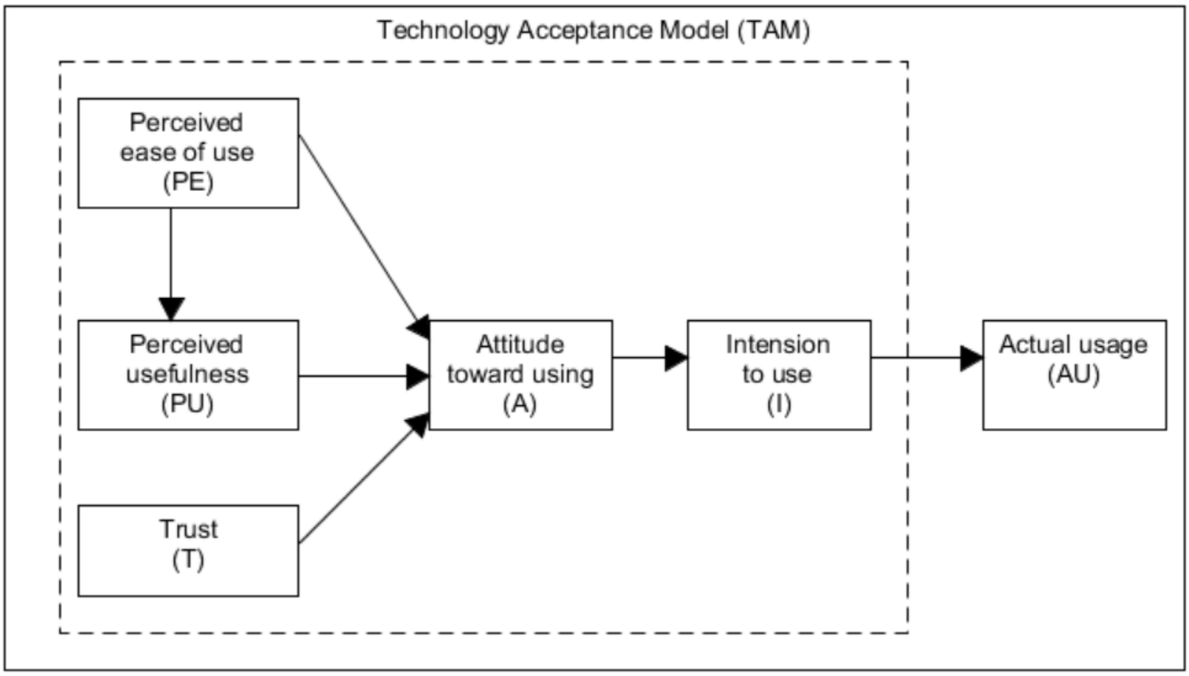

Technology Acceptance Model (TAM)
Perceived ease of use (PE)
Perceived usefulness (PU)
Trust (T)
Attitude toward using (A)
Intension to use (I)
Actual usage (AU)

Figure 4. 1. BBPs user behaviour model

Perceived ease of use (PE)

This refers as the degree an ethical hacker would be free of effort after joining BBPs. Factors including communication, reputation earning, and finding person in charge for bugs report are all critical in influencing the attitude for joining BBPs. Venkatesh and Davis (2000) has suggested that perceived ease of use has a direct effect on attitude; it also has significant effects on perceived usefulness [24].

Perceived usefulness (PU)

This refers to the degree to an ethical hacker would enhance his or her job performance or working performance by joining BBPs. This includes the skills and knowledge gained and the increase of numbers in bugs and companies he or her could find. These factors are all directly influencing the attitude of joining BBPs.

Trust (T)

This element is used as an auxiliary external variable in this study. Although perceived ease of use and perceived usefulness are the main two factors that influence user attitudes, it is also essential to maintain mutual trust between ethical hackers and BBPs provider (companies, organisations). As mentioned in Chapter 1. Introduction, before joining BBPs, some ethical hackers hesitate to report the bugs they discovered because of worries on being taken on legal actions by the companies. Furthermore, some companies are unresponsive to the bugs' reports due to the lack of trust of the reporters. Companies also hesitated to respond to the reports because of the fear of being extorted, and therefore fix the bug confidentially. The trust between ethical hackers and companies is considered one of the key factors in this study in influencing the attitude for joining BBPs.

Attitude toward using (A)

This refers to the user's feelings about joining BBPs. Amoroso and Hunsinger (2009) has hypothesised that attitude of using is positively correlated to the intentions to use [1]. In this study, the factor includes the satisfactory of financial income they have made through joining BBPs, and the general opinion on considering joining BBPs is a good idea.

Intentions to use (I)

This refers to the willingness of users to search for more information or recommend BBPs to their co-workers or other hackers. These would affect the actual behaviour of using the technology.

Actual usage (AU)

This refers to the willingness of keep participating in BBPs and increases the occurrences of joining it. These decisions are affected by their intentions to join.

Chapter 5. Findings

5.1 Quantitative findings from surveys

The online questionnaire is implemented through Google Form, which is a useful tool in receiving responses from international respondents, given that it's widely used and provides overall statistics that make responses easy to be organised. The questionnaire was sent to ethical hackers, who are from the leader boards of 5 well-known third-party BBPs platforms and other sources (3rd Nov 2020 to 4th Jan 2021).

Shown in Table 5. 1., platforms including HackerOne, YesWeHack, Intigriti, Cobalt, and Bugcrowd. Other sources: 6 researchers from HITCON community, and 4 respondents with information system background. With a total of 171 receivers through emails, website contacts and Twitter direct messages, it has collected 52 responses with the response rate around 30%. The demographics of respondents are shown in Table 5. 2.

Table 5. 1. Number of questionnaire responses

BBPs platforms	**Questionnaire receivers**
HackerOne	75
YesWeHack	21
Intigriti	40
Cobalt	24
Bugcrowd	2
Other resources	10
Total numbers sent	171
Total responses	52 (Response rate 30%)

Table 5. 2. Demographics of questionnaire respondents

Item		Frequency	Percentage (%)	Cumulative
Gender	Male	41	78.85	78.85
	Female	8	15.38	94.23
	Prefer not to say	3	5.77	100.00
Working Industry/ Status*	Information technology	31	59.62	59.62
	Freelancer	10	19.23	78.85
	Student	11	21.15	100.00
Years in the industry	Under 3 years	9	17.31	17.31
	3-8 years	24	46.15	63.46
	8 years above	13	25.00	88.46
	No working experience	6	11.54	100.00
Types of BBP joined	Directly held by companies	5	9.62	9.62
	Through third-party intermediaries	6	11.54	21.15
	Bothe of the above	34	65.38	86.54
	I haven't joined any BBPs	7	13.46	100.00
Nationality	Prefer not to say	4	7.69	7.69
	Taiwan	11	21.15	28.85
	India	7	13.46	42.31
	France	4	7.69	50.00
	Singapore	4	7.69	57.69
	Belgium	3	5.77	63.46
	United Kingdom	2	3.85	67.31
	Italy	2	3.85	71.15
	Germany	2	3.85	75.00
	Pakistan	2	3.85	78.85
	Romania	2	3.85	82.69
	**Others	9	17.31	100.00

*The options: Research Institutions, Government, and Banking and Finance are all 0, thus they are excluded from the table.
**Including countries: Australia, Greece, Nepal, Portugal, Spain, Tunisia, Turkey, Ukraine, United States, and each country has 1 respondent.

Reliability is an important factor for every questionnaire. It indicates the extent to which the questionnaire could give a same result when the measurements were taken again in the same conditions, which also means the internal consistency of the questionnaire. Cronbach's alpha is a measurement for internal consistency, which means the relatedness of the set of items are as a group. In this case, it's used to measure the consistency of the 6 elements (PE, PU, T, A, I, AU) in the questionnaire by using SPSS version 23. The alpha score above 0.7 is considered as reliable, within 0.6-0.7 is considered acceptable, 0.5-0.6 is questionable, and lower than 0.5 is unreliable. Thus, PE03, PE04 and PU03 are eliminated because of low Cronbach's alpha scores, which deleting them gives a better consistency score. Table 5. 3 shows the results of final alpha scores.

Table 5. 3. Cronbach's alpha for each element

Element	Context	Mean	Standard Deviation	Cronbach's α
Perceived ease of use (PE)	PE01 Participating in BBPs is cost-effective in communication.	4.0444	0.8516	0.689
	PE02 Participating in BBPs is easy in finding the person in charge of the program.	3.9778	0.86573	
Perceived usefulness (PU)	PU01 I believe more bugs can be found through joining BBPs.	4.3111	.94922	0.683
	PU02 I can learn new knowledge which is helpful for my job or life in BBPs' penetration testers' community.	4.2667	.8893	
Trust (T)	T01 I trust the BBPs providing companies.	4.0889	.84805	0.706
	T02 I think BBPs is a trustworthy business.	4.0889	.76343	
Attitude toward using (A)	A01 I'm satisfied with the money I make in BBPs.	3.8667	.91949	0.846
	A02 To me, joining BBPs is a good idea	4.3111	.73306	

Intentions to use (I)	I01 I would like to recommend my team or other hackers to join BBPs.	4.4222	.69048	0.698
	I02 I would like to search for other BBPs in the future.	4.6000	.57997	
Actual usage (AU)	AU01 I would like to increase the occurrences of joining BBPs.	4.0222	.65674	0.751
	AU02 I would like to keep participating in BBPs.	4.5778	.65674	

Note: The 5-point Likert Scale was used where 1 = strongly disagree to 5 = strongly agree.

5.2 Qualitative findings

This section shows important takeaways from interviewees. Further analysis is elaborated in Chapter 6.2 Qualitative analysis.

1) Senior director of community from third-party platform HackerOne: For companies, “Compared to any internal routine security testing, hackers have another distinct advantage — they can think like attackers, but act as your defenders.”

He also said HackerOne is an open platform that provides large pool of expertise. “HackerOne empowers organizations to scale security capabilities by providing ongoing access to talent, unlimited asset coverage, and assessment flexibility to enable this kind of business transformation.”

2) HITCON CEO: With both experience of hackers and companies, he talked about BBPs is a decent way to encourage ethical hackers to report bugs. He also mentioned that “Companies should have enough preparations to handle the reports with the attitude of willing to accept contributions from hackers.”

He shared that because of the time reduction in finding and fixing bugs in BBPs, the prices for bugs are skyrocketing in the black market. “Since there are more people shedding light on information security and BBPs, the bugs repairing rate of companies are getting faster than before and bugs become harder to find. This trend of bug prices in black market can be observed nowadays.”

3) Product security manager from Synology Inc.: shared his view as the company that runs their own BBPs. He said holding BBPs is low budget compared to hiring security testers. “If you hire a quality control team, you have to pay at least US$100,000 a year. However, since BBP is result-based, we only pay for valid bugs. Last year we (only) spent US$60,000 in total on BBPs”

He mentioned the difference between running BBPs themselves and through an intermediary platform. “(The benefits of) third-party platforms is credibility and reputation building to the public. The platform discloses transparently of how long it takes for a company to process a report, and how much bounty has been paid in total.” He also talked about one underlying difference is that holding BBPs offers flexibility to buy out bugs’ information or cover up bad reports, which are the things they can’t do on intermediary platforms. “It’s like cooking the books publicly, since almost any action on the platform leaves a record, and we cannot edit the record freely. Although we can choose to not disclose certain bugs, the record of reporting still exists.”

4) The general director for NCCST: standing from government’s point of view, he talked about why government department does not consider using BBPs for system testing. “The main concerns for government are the risks for finding someone unknown to test your system and whether these hackers will conceal the bugs they found.” And he also stated that “Government mainly needs to gain the trust of the people and comply with the laws and regulations for testing. I believe that BBP have a positive effect on cyber security; however, by viewing these effects we are yet convinced to try BBP.”

Chapter 6. Analysis

6.1 Quantitative analysis

6.1.1 Respondents that haven't joined any BBP

Table 6. 1 shows the demographics of the 7 respondents that haven't joined any BBP before. 4 respondents are employees and researchers from HITCON. 3 respondents are classmates with information system background and are interested in cyber security.

Table 6. 1. Demographics of survey respondents (haven't joined BBPs)

Item		Frequency	Percentage (%)
Gender	Male	3	42.86
	Female	4	57.14
Working Industry/ Status*	Information technology	4	57.14
	Student	3	42.86
Years in the industry	Under 3 years	1	14.29
	3-8 years	1	14.29
	8 years above	2	28.57
	No working experience	3	42.86
Nationality	Singapore	4	57.14
	Taiwan	2	28.57
	Portugal	1	14.29
Proportion in the whole demographics		7	13.4

*The options: Freelancer, Research Institutions, Government, and Banking and Finance are all 0, thus they are excluded from the table.

Figure 6. 1 shows the response of the question "How do you mostly deal with the bugs that you found?" It shows that 70% of them are not reporting the bugs to the companies.

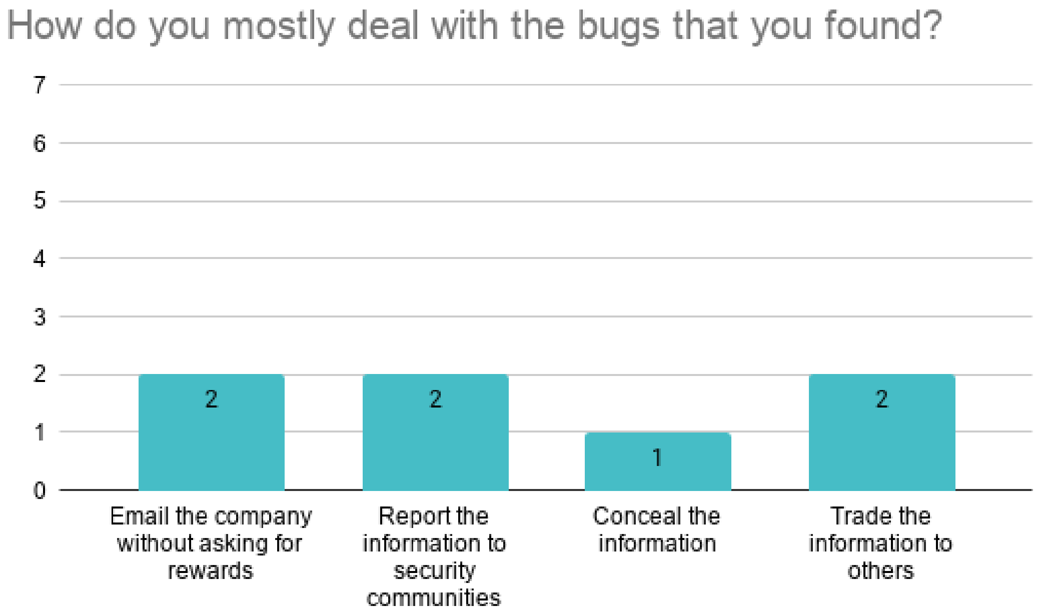


Figure 6. 1. Response to bugs by BBPs non-participants

Figure 6. 2 shows half of them have high intentions if the bug they found could be bought by the company itself.

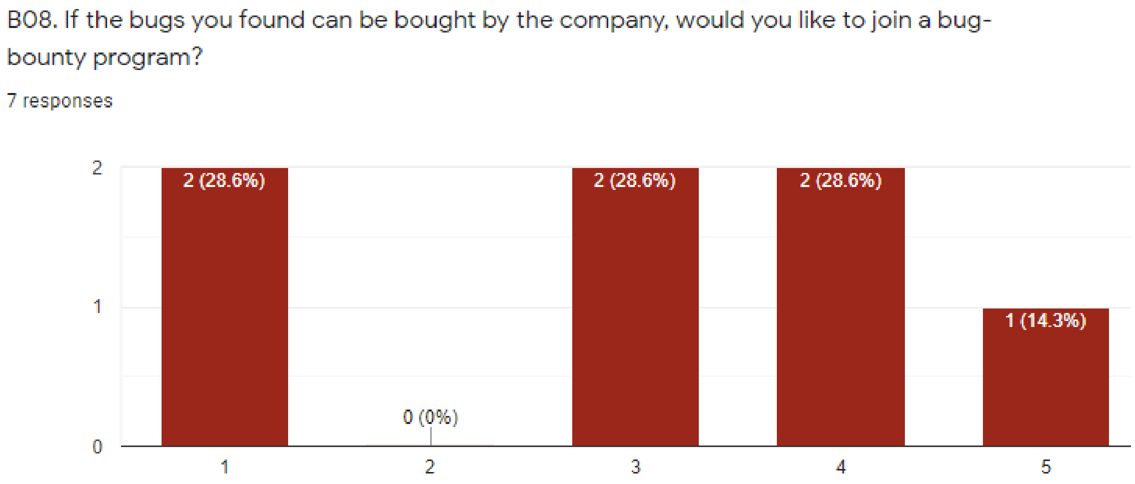
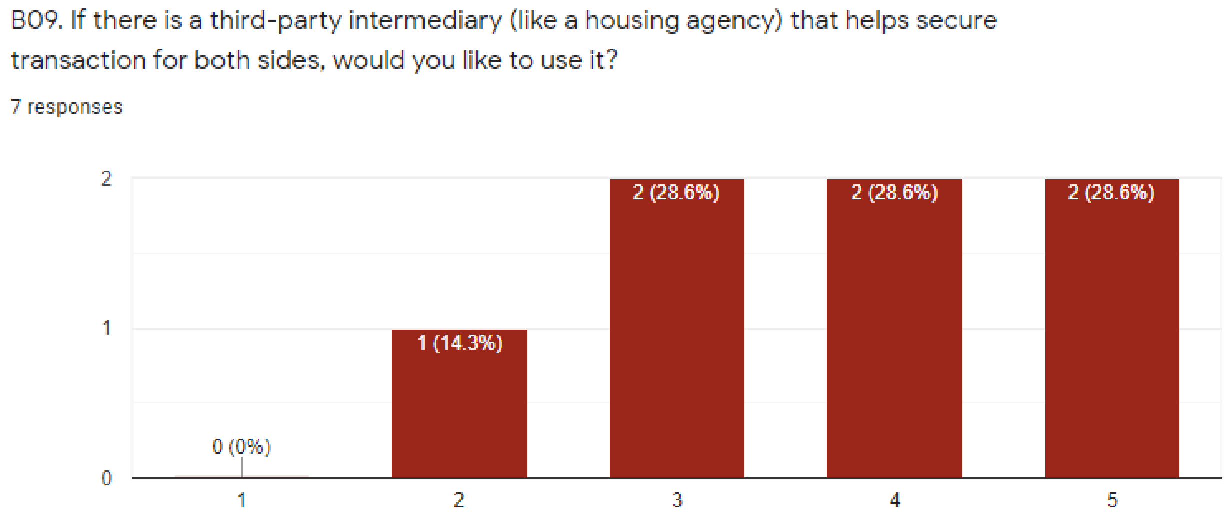


Figure 6. 2. Response to if the bugs can be bought by the company itself by BBPs non-participants (1 = strongly disagree to 5 = strongly agree)

The respondents have also answered about the attitude to third-party platforms that help bridge mutual trust between ethical hackers and companies. For example, guaranteeing participants get the rewards and companies receive trustable information. (This description was shown to the respondents along with the question) Figure 6. 3 shows that majority of them have positive attitude in joining BBPs through a third-party platform. It also presents a result of attitude change on joining BBPs when a third-party intermediary interferes in the business.



B09. If there is a third-party intermediary (like a housing agency) that helps secure transaction for both sides, would you like to use it?

7 responses

Figure 6. 3. Response to third-party platforms by BBPs non-participants
(1 = strongly disagree to 5 = strongly agree)

In addition, 5 of them also mention the main reasons they are not yet joining BBPs:

1. BBPs are a new topic to them
2. High time investment with unstable income
3. It is difficult for beginners because of a steep learning curve

6.1.2 Respondents that have joined BBPs

Reliability analysis

Table 6. 2 shows the Cronbach's alpha of the 6 elements dropped in the acceptable range after deleting PE03, PE04 and PU03 questions. This also shows that the inter consistency of the questionnaire for PE, PU, and I are Acceptable, which Cronbach's α fell between 0.6-0.7. The reliability results for T, A, and AU are Reliable, which Cronbach's α fell between 0.7-0.9.

Table 6. 2. Reliability testing results

Element	Item	Cronbach's α	Explanation
Perceived ease of use (PE)	2	0.689	Acceptable
Perceived usefulness (PU)	2	0.683	Acceptable
Trust (T)	2	0.706	Reliable
Attitude toward using (A)	2	0.846	Reliable
Intentions to use (I)	2	0.698	Acceptable
Actual usage (AU)	2	0.751	Reliable

Demographics

Table 6. 3 insicates the demographics of the respondents that have joined BBPs.

Table 6. 3. Demographics of survey respondents (joined BBPs)

Item		Frequency	Percentage (%)	Cumulative (%)
Gender	Male	38	84.44	84.44
	Female	4	8.89	93.33
	Prefer not to say	3	6.67	100.00
Working Industry/ Status*	Information technology	28	62.22	62.22
	Freelancer	10	22.22	84.44
	Student	7	15.56	100.00
Years in the industry	Under 3 years	8	17.78	17.78
	3-8 years	24	53.33	71.11
	8 years above	10	22.22	93.33
	No working experience	3	6.67	100.00

Types of BBP joined	Directly held by companies	5	11.11	11.11
	Through third-party intermediaries	6	13.33	24.44
	Bothe of the above	34	75.56	100.00
Nationality	Prefer not to say	4	8.89	8.89
	Taiwan	9	20.00	28.89
	India	7	15.56	44.44
	France	4	8.89	53.33
	Belgium	3	6.67	60.00
	United Kingdom	2	4.44	64.44
	Italy	2	4.44	68.89
	Germany	2	4.44	73.33
	Pakistan	2	4.44	77.78
	Romania	2	4.44	82.22
	**Others	8	17.78	100.00
Proportion in the whole demographic		45	86.5	

*The options: Research Institutions, Government, and Banking and Finance are all 0, thus they are excluded from the table.

**Including countries: Australia, Greece, Nepal, Spain, Tunisia, Turkey, Ukraine, United States, and each country has 1 respondent.

Gender

Table 6. 3 illustrates that nearly 85% of the respondents are males, and only 9 % are females, which shows that the hackers on these BBPs platforms are male dominant.

Types of BBPs joined

Majority of the respondents (76%) had joined both BBPs from directly held by companies and through third-party intermediaries. In Table 6. 4, estimated ratio of 88% of them consider joining BBPs through intermediary is easier in gaining reputations.

Reputations are points gained or lost based on report validity, and different platforms have their own policy on reputation counts. The higher the reputation the more exposure the hackers are on the platforms, which gives him/her an advantage on being invited to private program or the prestige in the community. Multiple leader boards on the platforms encourage hackers to engage, for instance reputation ranking calculated based on: general reputation earned, high and critical submissions that are triaged or resolved, country, and hackers that submitted their first valid report within the last 90 days, which is also a way to encourage beginners.

Nearly 80% consider third-party makes the whole business more trustworthy. The reason is that every submitted and reviewed report is recorded on the platform transparently, which means it decreases the possibility of submitted report getting ignored. Overall, nearly 80% have higher intentions to join BBPs through a third-party platform.

Table 6. 4. Preference between joining through directly and intermediary in Likert scale

		1	2	3	4	5
Comparing to BBP directly held by companies…	Using intermediaries is easier in gaining reputations.	0%	5.9%	5.9%	23.5%	64.7%
	Using intermediaries makes the business more trustworthy.	0%	2.9%	17.6%	41.2%	38.2%
	I have higher intentions to use intermediaries to join BBP.	0%	5.9%	14.7%	41.2%	38.2%

**1 = strongly disagree to 5 = strongly agree.*

Past experience on discovering bugs

In Figure 6. 4, it illustrates how they respond to bugs they discovered (through penetration tests or other situations) before knowing BBPs, and 66% of the respondents said they would email the company with or without asking for rewards. 22% of them would conceal the information without informing the company, and 11% of the bugs are being revealed publicly in the community. This shows that ethical hackers tend to not profits from the bugs, and the company are getting the bugs revealed or concealed without noticing.

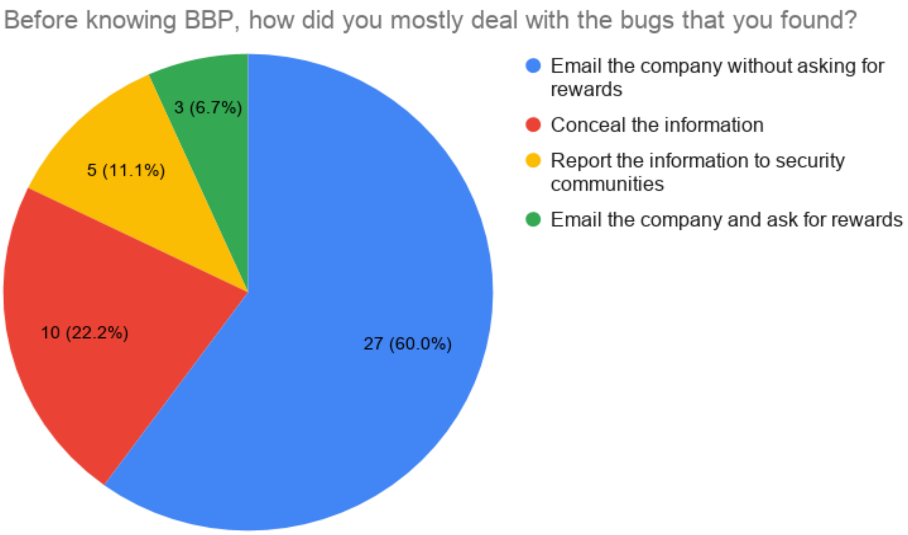


Figure 6. 4. Reaction to bugs before knowing BBPs by BBPs participants

TAM questions

Figure 6. 5 shows the stacked bar chart of responses in Likert Scale and TAM elements. It illustrates whether there is any element that generates positive or negative response. A01 "A01 I'm satisfied with the money I make in BBPs." is getting numbers of neutral responses and the least numbers in positive attitudes. For the neutrals, it may be that 63% of the respondents are doing ethical hacking as a part-time job or hobby. The income from bounties are nor satisfying and dissatisfying to them. Other elements are getting positive responses.

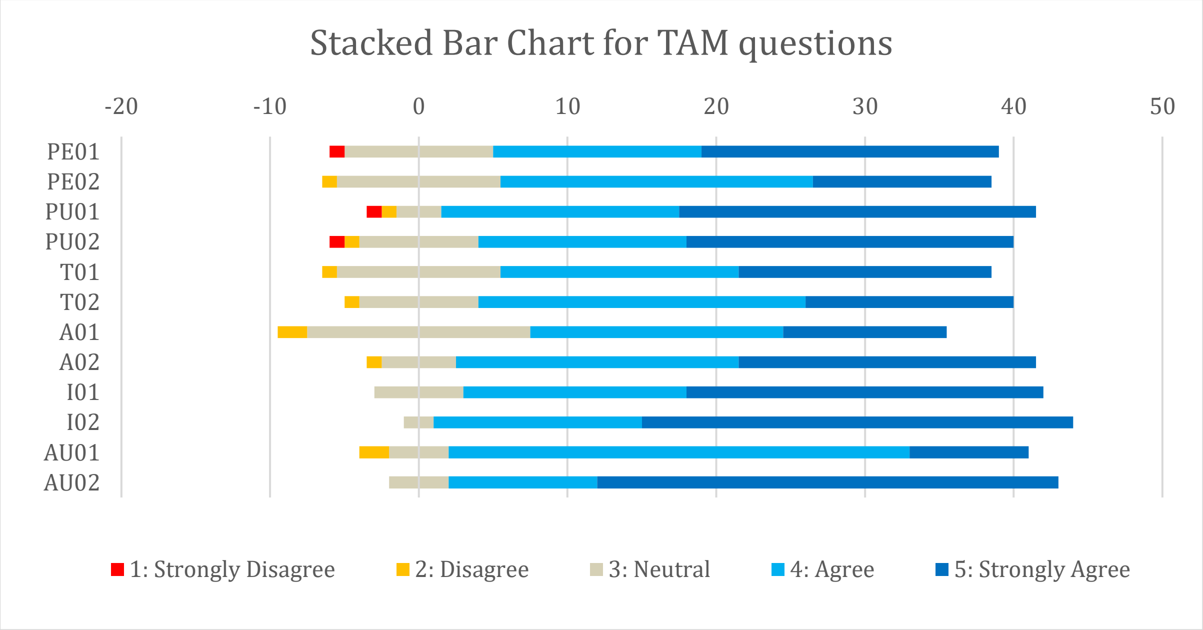


Figure 6. 5. Stacked Bar Chart for each TAM element in Likert Scale

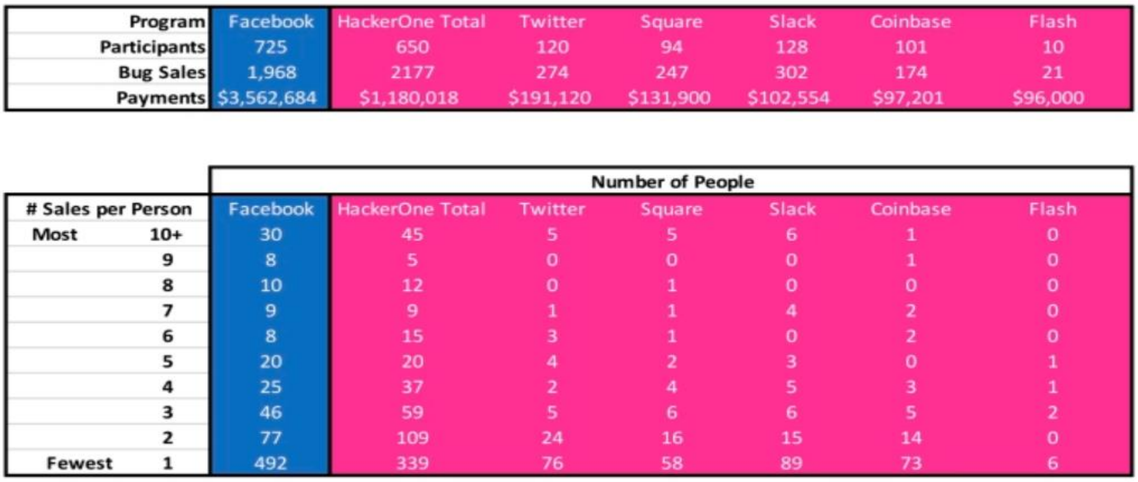
Criticism

One respondent has left a feedback about the bounties. “I wish the pay-outs were higher as it feels like our work is undervalued compared to the impact it could have on these organisations.” This study assume that this person is referring the low payment on impactful bugs.

According to the 4th hacker security report 2020, “Cross-site Scripting (XSS) continues to be the most awarded vulnerability type with US$4.2 million in total bounty awards, up 26% from the previous year.” It is a type of vulnerability that enable attackers to inject client-side scripts into web pages and impact production pipeline. This bug is accounted roughly 23% of all reported bugs with the average bounty award US$501, which is well lower than the average reward US$3650 for critical bugs [15]. This indicates that organizations are mitigating common, and potentially impactful bug on the cheap.

Parsia Hakimian, senior consultant at Synopsys, critics that BBPs is a business where the tops on the pyramid earn the majority of bounties, while others earn less than minimum wage or zero [2]. According to an data on Trail of Bits (2019) shown in Figure 6. 6, “for the entirety of the HackerOne and Facebook data sets, the 7% of participants with 10 or more bugs were paid for 1,622 bounties, while the other 93% of the population earned 2,523” [3]. This trend is getting more pronounced with bigger dataset.

Therefore, the critic from that one respondent is worth noting in terms of bounty rewards.



Program	Facebook	HackerOne Total	Twitter	Square	Slack	Coinbase	Flash
Participants	725	650	120	94	128	101	10
Bug Sales	1,968	2177	274	247	302	174	21
Payments	$3,562,684	$1,180,018	$191,120	$131,900	$102,554	$97,201	$96,000

		Number of People						
# Sales per Person		Facebook	HackerOne Total	Twitter	Square	Slack	Coinbase	Flash
Most	10+	30	45	5	5	6	1	0
	9	8	5	0	0	0	1	0
	8	10	12	0	1	0	0	0
	7	9	9	1	1	4	2	0
	6	8	15	3	1	0	2	0
	5	20	20	4	2	3	0	1
	4	25	37	2	4	5	3	1
	3	46	59	5	6	6	5	2
	2	77	109	24	16	15	14	0
Fewest	1	492	339	76	58	89	73	6

Figure 6. 6. Top: Participants, sales, and payments for Facebook (45 months) and HackerOne (23 months). Bottom: Population according to bug sales per person [3].

6.2 Qualitative analysis

6.2.1 Organisations holding BBPs themselves

Advantages

Synology, Mr Lee considered BBPs as a cost-effective way to improve product security since they have paid 40% less for doing BBPs compared to hire a whole security team, which they can buy the testing tools themselves.

Having flexibility in policy setting is one of the biggest differences for them compared to finding a third-party platform. They are able to buy out bugs information and cover up bad reports. Since every report and action on a third-party platform is transparent, that means the company itself cannot edit the record out if there's bugs that they are unwilling to disclose.

Disadvantages

The main problem that bothers Synology, Mr Lee is taxation issues in payment. Since most of their participants are foreigners, the paperwork for taxation is complicated. He said if they see BBPs as labour-relations, it is difficult to know whether they are paying meets participants' income requirements.

HITCON, Mr Tsai said that a company that can hold BBPs themselves need to prepare efficient teams to deal with the backend process, such as bugs validation, responding, marketing, budgeting, and repair tracking. These are difficult for small scale company. The disadvantages on a hackers' aspects would be the risks of report being ignored, since the report system is fully owned by the company.

Attitudes

Synology, Mr Lee has positive attitude on holding BBPs themselves, and he is willing to recommend other companies to try BBPs with sufficient preparation.

6.2.2 Having BBPs using an intermediary platform

Advantages

HackerOne, Mr Tucker said that a third-party platform provides companies a large pool of expertise available to test their system. Through the collaboration of crowdsourcing, companies can receive contributions in the view of attackers and better protect their products or systems.

Both HITCON, Mr Tsai and Synology, Mr Lee, consider a third-party platform as an efficient role to handle paperwork. Such as taxation, background checks for hackers, front-line submission reviewing, and other technical supports.

In addition, using third-party platforms are a method to gain exposure in public eye and advertising their work of responsibility in improving information security. That means, it builds the trust and reputation to the public and to the hackers.

Tsai also thinks the platform provides exposure to outstanding researchers. Companies may invite those active and top-skilled researchers listed the ranking boards to their private programs and provide salary for their contributions. This way, researchers can cover their costs in testing and earn a stable income in comparison to bounties.

Disadvantages

For Synology, Mr Lee, he thinks slotting fees to join the platform (HackerOne) are too expensive, which includes annual slotting fees US$20,000 and another 20% cash flow, and not every company can afford it.

On the other hand, except the inflexibility in editing record mentioned previously, he also raised the problem of third-party platforms in terms of cost-efficient in communication. He said that despite the platform can help deal with reports, the lack of understanding in their company's products is also increasing communication costs. Even the terminologies are correct, it takes multiple checks to get precise description of the bugs.

Attitudes

HITCON, Mr Tsai thinks joining BBPs through a third-party platform is cost-efficient for companies, and a great platform to gain reputation for both companies and ethical hackers. Synology, Mr Lee does not consider joining the platform because the fees are too expensive.

6.2.3 Organisation that doesn't use BBP

NCCST is the representation of government departments from Taiwan, and they are not yet considering using BBPs.

Director Mr Wu shared his view on the reasons: One is that unknown identities of participants and whether they would conceal the bugs they found is causing trust issues. Not only the trust between program holders and the participants, but also the trust between government and the people. They tend to hire local security companies or researchers, which test system with signed agreements and test in authorised attack environment. It's also a good way to train own specialities.

Another reason is the restrictions in laws, which regulate how government departments should do security testing for system. There are fixed processes for every procedure and a third-party's surveillance. Therefore, BBPs is not yet an option for government department in Taiwan.

Attitudes

Mr Wu agrees that BBPs is a method to de security testing. However, he thinks the challenges overweigh the benefits for government departments.

6.3 Overall evaluation

This section shows the key points of BBPs based on the opinions from questionnaire and interviewees, and the overall evaluation on the topic.

Crowdsourcing

BBPs is a method utilising crowdsourcing to find security vulnerabilities for organisations. These programs cannot prevent hackers from hiding the weaknesses they found; However, the power of crowdsourcing indicates that by accessing huge pool of expertise, the problem of hiding bugs information can be mitigated. If someone hide the information and wants to save it for malicious use, other proficient participants will find it and earn the bounty, nevertheless.

Pre-preparation

Companies doing BBPs should have their in-house protection strategies prepared. With pre-preparations arranged, it reduces the costs of fixing and paying low-hanging bugs, and it decreases the communication time to read reports back and forth between R&D department.

Companies also need teams to do paperwork for taxation, budgeting, and communicate with high-level supervisors. These are all critical in showing their efficiency and building reputation among ethical hackers and customers. Large enterprises may be able to handle the paperwork and the arrangement themselves. For small companies, some may find a third-party platform to aid the processes. Intermediaries are able to give technical supports and also the review for front-line submissions. They are also a good way to gain exposure for both researchers and companies. However, though it reduces search costs and some communication costs, it is still essential for company themselves to manage the internal communication flow.

Bounties/ Rewards

Bounties are the reason that appeal to researchers to report bugs and contribute to the good of the company. Fair and sufficient bounties are critical to encourage more reports and engagement from hackers. Although the income earn from bounties may not be as much as a penetration tester's salary, it still covers portion of hackers' costs in testing.

Policy

Clear policies play an imperative role in creating a benevolent environment for companies and ethical hackers. Policy includes safe harbour, scope to test, bounty table, disclosure policy, and disqualified rules. Policies should be precise and stringent to alleviate misunderstandings in communications. For instance, criteria for ineligible participant: Certain countries and regions that banned from laws, and contractor or vendors working with the program holder. The bounties for duplicated reports, possible criminal investigation, and out-of-scope activities are all important to be listed clearly to the participants.

Trust

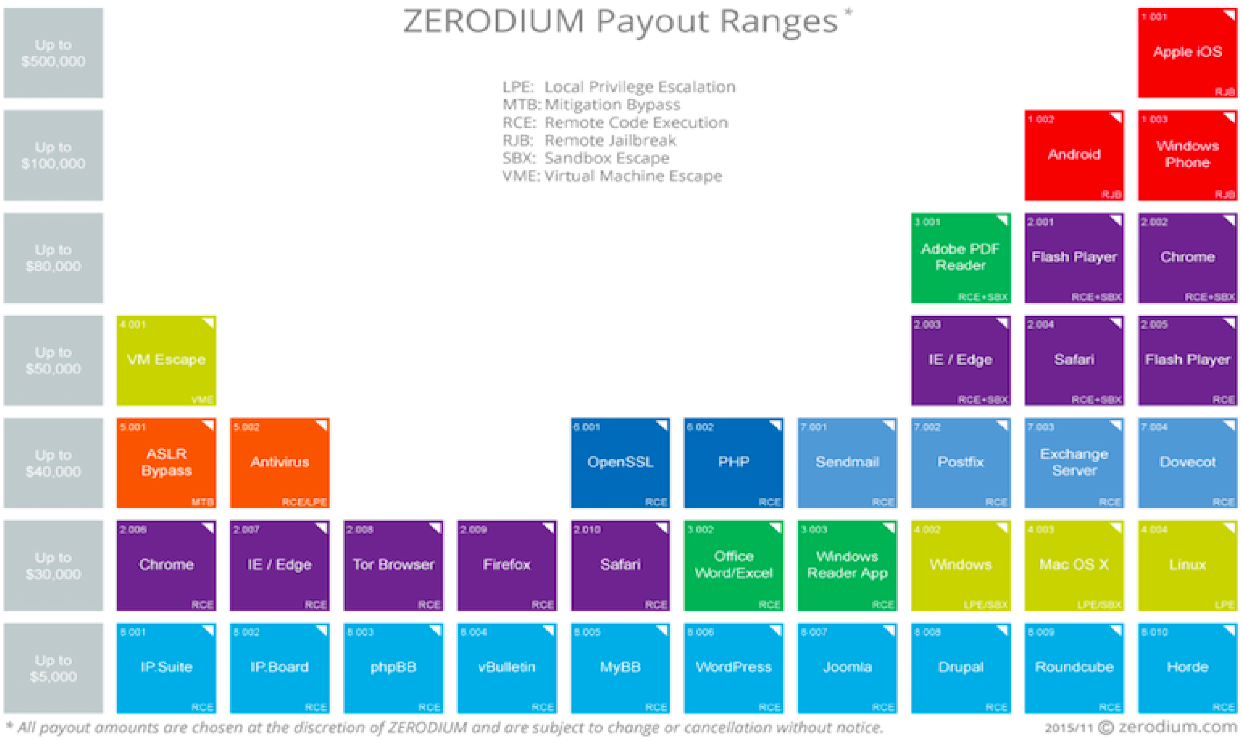
BBPs is a trust builder between companies and hackers. In the past, ethical hackers were not willing to report bugs to companies because of possible legal charges for testing websites or system without authorised. The emerge of BBPs creates an open platform held by companies that invites hackers to contribute their skills in improving information security. On the other hand, hackers' unknown identity is one of the biggest problems considered for government department to use BBPs.

For this issues, third-party platforms are capable of doing background checks for organisations. For instance, HackerOne has programs called "HackerOne Clear" that require proven hackers to be background-checked. These programs are mostly held by organisations with sensitive systems or private programs such as Department of Defense. These programs are also paying higher than average critical bounty pay-outs. This provides a business environment that both parties are having transparency in identity.

Cost-effective in finding and fixing bugs

BBPs allow organisations to acknowledge and fix vulnerabilities faster. Stated by Mr Tucker, HackerOne in the interview, "organizations are quickly adopting modern, transformative IT initiatives that are outpacing their security teams' capacity to keep up." The accelerated pace in bugs detecting and repairing has shown evidence in the price changes for vulnerabilities in black market and exploit brokers.

Figure 6. 7 illustrates the pay-out for zero-day exploits on Zerodium website in 2015 [27]. Zerodium is a zero-day exploit broker that connects the transaction between zero-day sellers and buyers. In Figure 6. 8 shows the change in prices and detailed descriptions for zero-days in 2019. For instance, the pay-out for Apple iOS has rose from maximum US$500,000 to US$2 million. Vulnerabilities in Chrome also rose from US$80,000 to US$500,000. The description for general Android bugs changed to Android FCP Zero click. The bugs on the site are becoming more specific and high value.



ZERODIUM Payout Ranges *

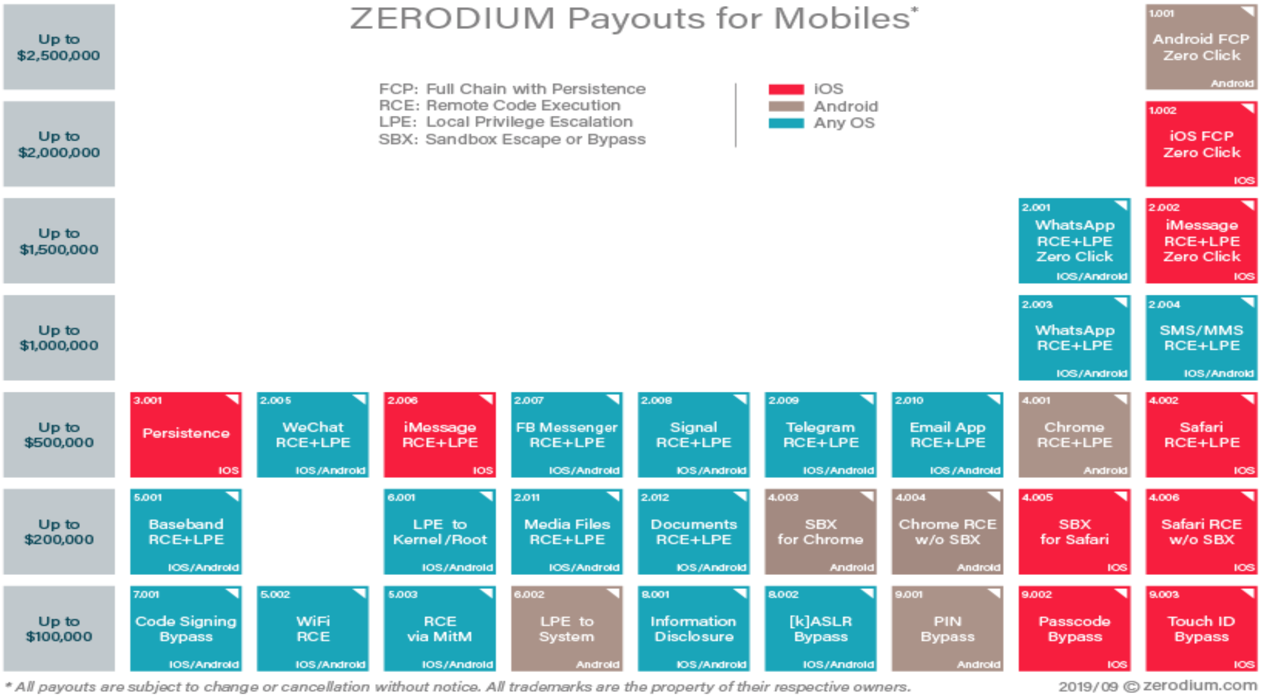
LPE: Local Privilege Escalation
MTB: Mitigation Bypass
RCE: Remote Code Execution
RJB: Remote Jailbreak
SBX: Sandbox Escape
VME: Virtual Machine Escape

Up to $500,000										1.001 Apple iOS RJB
Up to $100,000									1.002 Android RJB	1.003 Windows Phone RJB
Up to $80,000								3.001 Adobe PDF Reader RCE+SBX	2.001 Flash Player RCE+SBX	2.002 Chrome RCE+SBX
Up to $50,000	4.001 VM Escape VME							2.003 IE / Edge RCE+SBX	2.004 Safari RCE+SBX	2.005 Flash Player RCE
Up to $40,000	5.001 ASLR Bypass MTB	5.002 Antivirus RCE/LPE			6.001 OpenSSL RCE	6.002 PHP RCE	7.001 Sendmail RCE	7.002 Postfix RCE	7.003 Exchange Server RCE	7.004 Dovecot RCE
Up to $30,000	2.006 Chrome RCE	2.007 IE / Edge RCE	2.008 Tor Browser RCE	2.009 Firefox RCE	2.010 Safari RCE	3.002 Office Word/Excel RCE	3.003 Windows Reader App RCE	4.002 Windows LPE/SBX	4.003 Mac OS X LPE/SBX	4.004 Linux LPE
Up to $5,000	8.001 IP.Suite RCE	8.002 IP.Board RCE	8.003 phpBB RCE	8.004 vBulletin RCE	8.005 MyBB RCE	8.006 WordPress RCE	8.007 Joomla RCE	8.008 Drupal RCE	8.009 Roundcube RCE	8.010 Horde RCE

* All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.

2015/11 © zerodium.com

Figure 6. 7. 2015 zero-day pay-outs on Zerodium



ZERODIUM Payouts for Mobiles*

FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

🟥 iOS
🟫 Android
🟦 Any OS

Up to $2,500,000									1.001 Android FCP Zero Click Android
Up to $2,000,000									1.002 iOS FCP Zero Click iOS
Up to $1,500,000								2.001 WhatsApp RCE+LPE Zero Click iOS/Android	2.002 iMessage RCE+LPE Zero Click iOS
Up to $1,000,000								2.003 WhatsApp RCE+LPE iOS/Android	2.004 SMS/MMS RCE+LPE iOS/Android
Up to $500,000	3.001 Persistence iOS	2.005 WeChat RCE+LPE iOS/Android	2.006 iMessage RCE+LPE iOS	2.007 FB Messenger RCE+LPE iOS/Android	2.008 Signal RCE+LPE iOS/Android	2.009 Telegram RCE+LPE iOS/Android	2.010 Email App RCE+LPE iOS/Android	4.001 Chrome RCE+LPE Android	4.002 Safari RCE+LPE iOS
Up to $200,000	5.001 Baseband RCE+LPE iOS/Android		6.001 LPE to Kernel/Root iOS/Android	2.011 Media Files RCE+LPE iOS/Android	2.012 Documents RCE+LPE iOS/Android	4.003 SBX for Chrome Android	4.004 Chrome RCE w/o SBX Android	4.005 SBX for Safari iOS	4.006 Safari RCE w/o SBX iOS
Up to $100,000	7.001 Code Signing Bypass iOS/Android	5.002 WiFi RCE iOS/Android	5.003 RCE via MitM iOS/Android	6.002 LPE to System Android	8.001 Information Disclosure iOS/Android	8.002 [k]ASLR Bypass iOS/Android	9.001 PIN Bypass Android	9.002 Passcode Bypass iOS	9.003 Touch ID Bypass iOS

* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/09 © zerodium.com

Figure 6. 8. 2019 zero-day pay-outs on Zerodium

The emergence of BBPs is one of the main factors of this phenomenon. It indicates that running BBPs makes bugs in global enterprises are getting harder to find, and the fixing rate is also getting faster than before.

Chapter 7. Conclusion

7.1 Research summary

This study focused on presenting BBPs' end-user perspectives and evaluate the factors that makes them join or not join. A survey was designed based on TAM, which consisted of 6 elements (PE, PU, T, A, I, AU). It was distributed to 171 hackers from top 5 BBP platforms and hackers' community. With receiving around 30% of responses, the responses are separated into 2 groups of people. First is the one that haven't joined BBPs before, which consisted 13.4% in the demographic. They showed interest in joining BBPs with a third-party platform. The other part of respondents is the one that have joined different types of BBPs, and they are from nearly 20 different countries. They have positive attitude in joining BBPs and prefer to join through third-party platforms because of the transparency and clarity in rules.

This study also conducted 4 interviews with supervisors from company that run BBP themselves (Synology), government department that is not joining BBPs (NCCST), hackers' community association (HITCON), and a BBP third-party platform (HackerOne). They shared their experience on why or why not they choose to have BBPs. They also talked about not every companies are capable of doing BBPs. Companies without streamed line communication channel and integrated in-house protection are not suitable in doing BBPs. Pre-preparations, bounties, clarity in policies, and trust building are all important factors to work on in BBPs, and these factors also correspond to related work done by other researchers. On the other hand, third-party platforms are a role in cost reduction and creating a transparent environment for both hackers and companies.

In conclusion, BBPs is an innovative method for companies to improve information security compare to the traditional way of relying on a limited source of a IT security company. BBPs is a means of utilising crowdsourcing by incentivising skilful ethical hackers with bounties and reputations. With the access to pools of expertise and a competitive bounty-earning environment, companies are able to find bugs efficiently and fix it effectively, and at the same time mitigates the risks of participants hiding bugs for malicious use. Therefore, BBPs creates a win-win situation for companies and ethical hackers in improving information security.

7.2 Possible future research work

For interviews, this study did not include interview from company on a third-party platform, which lost insights from company that can respond to Synology's concerns on slotting fees and communication. Future work will add organisations that have BBPs through intermediary platform in order to provide more insights on the topic.

For surveys, the TAM framework is relatively simple to use, which initially only contains two core factors "Perceived Usefulness" and "Perceived Ease of Use". Future work needs to modify the framework to get better analysis of the questionnaire. In addition, the number of hackers responding are not sufficient enough to represent general opinions. Future work needs to find more numbers of respondents to have a convincing analysis.

7.3 Reflections

For questionnaire, I have several regrets when doing the online questionnaire. First, since majority of them are expertise in information security, they may think I am phishing or scamming. Thus, they mostly did not respond to me or blocked me on social media. Second, I should have studied the topic thoroughly before sending out the surveys, given that when I started to make analysis on the data, I found some questions are poorly asked or should be worded more precisely. Therefore, some questions ended up not including in the analysis. Apart from the regrets, there are also some takeaways when designing surveys. Thanks to TAM, I have learnt the basic forms of making a questionnaire, which it provides a guideline for me to know what directions I should aim for. Moreover, I have the opportunity to understand some well-known hackers' thoughts and insights, which was a whole learning experience.

For interviews, from designing questions, proofread transcripts, and collecting key points were all difficult for me at first. I have learnt time management during interviews and ability to come up with question about the additional information they mentioned but related to the topic at the same time.

Overall, this study was challenging but interesting. The topic on BBPs is new to general public but an emerging role in the information industry, and it should be study in more depth in the future.

References

[1] Amoroso, D. L., & Hunsinger, D. S. (2009). Measuring the acceptance of internet technology by consumers. A Working Paper.

[2] Armerding, T. (2019). Bug Bounties: A Good Tool, But Don't Make Them the Only Tool In Security. Forbes.

[3] Brunson, T. (2019). On Bounties and Boffins. [Blog] Trail of Bits. Available at: https://blog.trailofbits.com/2019/01/14/on-bounties-and-boffins/ [Accessed 14.11.2020].

[4] BugCrowd (2020). WE ARE THE #1CROWDSOURCED SECURITY PLATFORM [online] Available at: https://www.bugcrowd.com/about/ [Accessed 30.12.2020]

[5] Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. Management Science, 35(8), 982–1002. doi:10.1287/mnsc.35.8.982

[6] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. Management Information Systems Quarterly, 13(3), 319–340. doi:10.2307/249008

[7] Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1992), Development and Test of a Theory of Technical Learning and Usage. Human Relations, 45(7), pp.659-686

[8] FireEye, (2020). Threat Research: Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor. [online] Available at: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html [Accessed 27.10.2020].

[9] Finifter, M., Akhawe, D. and Wagner, D., (2013). An Empirical Study of Vulnerability Rewards Programs. 1st ed. [pdf] Washington, D.C., USA: 22nd USENIX Security Symposium, ISBN, pp. 274-276. Available at: https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_finifter.pdf [Accessed 28.11.2020]

[10] Friis-Jensen, E., (2014). The History of Bug Bounty Programs. [online] Available at: https://cobalt.io/blog/the-history-of-bug-bounty-programs [Accessed 24.10.2020]

[11] Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention, and behavior: An introduction to theory and research. Reading, Mass; Don Mills, Ontario: Addison-Wesley Pub. Co.

[12] Gardner, D. (2018). Emerging Technology Analysis: Bug Bounties and Crowdsourced Security Testing. Gartner, [online] pp.7-8. Available at: https://www.gartner.com/en/documents/3877467/emerging-technology-analysis-bug-bounties-and-crowdsourc [Accessed 21.11.2020].

[13] HackerOne (2020). HISTORY OF HACKER-POWERED SECURITY [online] Available at: https://www.hackerone.com/history-of-hacker-powered-security [Accessed 30.12.2020]

[14] HackerOne, (2020). The 2020 Hacker Report. [online] Available at: https://www.hackerone.com/resources/reporting/the-2020-hacker-report [Accessed 04.12.2020]

[15] HackerOne, (2020). The 4th annual hacker-powered security report. [online] Available at: https://www.hackerone.com/hacker-powered-security-report [Accessed 24.12.2020].

[16] Internet Archive, (1997). NETSCAPE ANNOUNCES, "NETSCAPE BUGS BOUNTY" WITH RELEASE OF NETSCAPE NAVIGATOR 2.0 BETA PROGRAM HARNESSES POWER OF THE INTERNET TO HELP NETSCAPE REFINE BETA VERSIONS AND ENSURE HIGHEST QUALITY SOFTWARE. [online] Available at: http://web.archive.org/web/19970501041756/www101.netscape.com/newsref/pr/newsrelease48.html [Accessed 02.11.2020].

[17] Kuo, Y. Y. (2013). A Research on The Influence on Customers' Use Intention of Electronic Vehicles with The Technology Acceptance Model, TAM. doi: 10.6844/NCKU.2013.02006

[18] Marina, A. and Moussouris, K. (2020). Verge Cast. How the commercialization of bug bounties is creating more vulnerabilities.

[19] Maillart T, Zhao M, Grossklags J, Chuang J (2017) Given enough eyeballs, all bugs are shallow? Revisiting Eric Raymond with bug bounty programs. Journal of Cybersecurity 3(2): pp. 81-90.

[20] Macfree, (2018). Economic Impact of Cybercrime - No Slowing Down. [online] Available at: https://www.mcafee.com/enterprise/en-us/forms/gated-form.html?docID=5fee1c652573999d75e4388122bf72f5&tag=ec&eid=18TL_ECGLQ1_CT_WW [Accessed 20.11.2020].

[21] O'Donnell, L. and Moussouris, K. (2020). Threat Post. Katie Moussouris: The Bug Bounty Conflict of Interest.

[22] PurpleSec, (2020). 2020 Cyber Security Statistics: The Ultimate List of Stats, Data & Trends. [online] Available at: https://purplesec.us/resources/cyber-security-statistics/ [Accessed 01.11.2020].

[23] Tella, A. and Olasina, G. (2014). Predicting Users' Continuance Intention Toward E-payment System: An Extension of the Technology Acceptance Model, In: International Journal of Information Systems and Social Change. 5(1). Available at: https://dl.acm.org/doi/10.5555/2729642.2729646 [Accessed 03.10.2020].

[24] Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management Science, 46(2), pp. 186–204. doi:10.1287/mnsc.46.2.186.11926

[25] Weng et al. (2018). A TAM-Based Study of the Attitude towards Use Intention of Multimedia among School Teachers, In: *Appl. Syst. Innov.* 1(3): 36. Available at: https://doi.org/10.3390/asi1030036 [Accessed 04.12.2020].

[26] Zhou, J., and Hui, K.L. (2019). Bug Bounty Programs, Security Investment and Law Enforcement: A Security Game Perspective. In: The 2019 Workshop on the Economics of Information Security (WEIS 2019), Boston, US, 3-4 June 2019. [online] Boston, US, pp.26. Available at: http://repository.ust.hk/ir/Record/1783.1-96436 [Accessed 03.12.2020].

[27] Greenberg, A. (2015). Here's a Spy Firm's Price List for Secret Hacker Techniques. [online] Wired. Available at: https://www.wired.com/2015/11/heres-a-spy-firms-price-list-for-secret-hacker-techniques/ [Accessed 04.12.2020].

Appendices

Table of Contents (Appendices)

Appendix I: Topic Area Proposal

Please do not exceed the **maximum** word count indicated in the various sections. A copy of this form should be included as Appendix 1 of your final report.

SECTION 1: CANDIDATE DETAILS	FILL IN THIS COLUMN
Name	Huang Pei Yu
Date	10/10/2020
Student Number	180329021
Project Working Title	Using crowdsourcing to find security bugs: The emerging role of bug- bounty programs

SECTION 2: THE BIG IDEA	FILL IN THIS COLUMN
Main theme: (A description of the general area in 50 words)	Determine and analyse the key factors that how bug-bounty business works, and how end-users think about it. Questionnaire and interviews were conducted to understand end-users' attitude on having or joining bug-bounty programs. This study also analyses on the advantages and disadvantages of bug-bounty programs.
Research ideas are drawn from the area (from 2 to 4) with possible core research questions as a focus for the research.	Bug-bounty programs, BBPs, Ethical hackers, Crowdsourcing, Information security
Idea 1	*This emerging business is changing the way organisations think of IT security protection.*
	RQ i How does bug-bounty programs change the norms and practices of security protection when adopting it?
	RQ ii what are the concerns when using bug-bounty programs?

Idea 2	*What are the success factors regarding bug-bounty programs?*
	RQ i Will this program be suitable for every organisation?
	RQ ii What are the advantages and disadvantages?

SECTION 3: CHOSEN FOCUS *(The section might be repeated for different ideas)*	FILL IN THIS COLUMN
Idea Number and core RQ	*Idea number 1* *RQ How does bug-bounty programs change the norms and practices of security protection when adopting it?*
Outline of argument or position for the chosen idea (an *initial* view – the data may change your mind, but it's good to have some early idea of what you might be able to say.	In this research, I will investigate the reasons why the end-users of bug-bounty programs keep joining and decide to join it. Aren't companies concern about the identity of the hackers? And why are hackers contributing their works to the company but not sell it to black market? This study would also research on the advantages and disadvantages of bug-bounty programs.
Links to wider Digital Innovation or Information Systems issues and themes (potential area of contribution)	IT security, security management, third-party agency problem
Links to the syllabus of other courses within the degree (useful material to draw on)	Information system management, IT security, Intermediaries, transaction costs
5 keywords or phrases for use in an online search e.g. of the Online Library or Google Scholar	Bug-bounty programs, crowdsourcing, cybersecurity, vulnerability discovery, software exploit.
Alternative ways to access the topic and to collect data: (if possible, give	The public charts from HackerOne website, hackers who submit valid reports to programs, Google

examples of other people's work and what data they have used)	Vulnerability, Research Programs, and annual hacker reports from HackerOne.
What research framework (theory or set of concepts) do you propose to use in this work?	Technology acceptance model
Required resources and issues of access:	Interviews and Questionnaire
Assessment of required skills or techniques to be applied:	Statistics 1, Math 1, information system management, Excel, and SPSS
References to 5 articles or books relevant to the topic and that you have read	1. Finifter, M., Akhawe, D. and Wagner, D., (2013). *An Empirical Study of Vulnerability Rewards Programs*. 1st ed. [pdf] Washington, D.C., USA: 22nd USENIX Security Symposium, ISBN, pp. 274-276. Available at: https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_finifter.pdf 2. Gardner, D. (2018). Emerging Technology Analysis: Bug Bounties and Crowdsourced Security Testing. *Gartner*, [online] pp.7-8. Available at: https://www.gartner.com/en/documents/3877467/emerging-technology-analysis-bug-bounties-and-crowdsourc 3. HackerOne, (2020). *THE 4TH ANNUAL HACKER-POWERED SECURITY REPORT*. [online] Available at: https://www.hackerone.com/hacker-powered-security-report 4. Kuo, Y. Y. (2013). *A Research on The Influence on Customers' Use Intention of Electronic Vehicles with The Technology Acceptance Model, TAM.* doi: 10.6844/NCKU.2013.02006 5. Zhou, J., and Hui, K.L. (2019). Bug Bounty Programs, Security Investment and Law Enforcement: A Security Game Perspective. In: *The 2019 Workshop on the Economics of Information Security (WEIS 2019), Boston, US, 3-4 June 2019.* [online] Boston, US, pp.26. Available at: http://repository.ust.hk/ir/Record/1783.1-96436

Justification of interest to others:	This topic is important because it shows the direct feedback from the end-users, including hackers, companies holding bug-bounty programs, government departments, and third-party platform. This research has showcased many perspectives. Security companies, security researchers, bug-bounty programs companies, and security managers would find the feedbacks and analysis useful to them.

Appendix II: Project Specifications

Please fill in this document and resubmit it via the VLE at the same time as you submit your final project. A copy of this form should be included as Appendix 2 of your final report.

SECTION 1: CANDIDATE DETAILS	FILL IN THIS COLUMN
Name	Huang Pei Yu
Student number	180329021
Project Title	Using crowdsourcing to find security bugs: The emerging role of bug- bounty program
Word Count (excluding Appendices)	9065 (excluding references)
Date	01/05/2021

SECTION 2: PROJECT SUMMARY	FILL IN THIS COLUMN
Brief description of the topic (50 words)	Determine and analyse the key factors that how bug-bounty business works, and how end-users think about it. Questionnaire and interviews were conducted to understand end-users' attitude on having or joining bug-bounty programs. This study also analyses on the advantages and disadvantages of bug-bounty programs.
Central Research Question (20 words) *Make sure it is a question, with a potential for an answer.*	How does bug-bounty programs change the norms and practices of security protection when organisations adopt it?
Original Research Objectives (100 words)	In this research, I will investigate the reasons how bug-bounty becomes an emerging business in the IT industry. I will argue that bug-bounty plays an imperative role in using crowded-source between its companies and hackers', and this business model will influence the decision-making process and strategies toward IT security.

Revised research objectives (and why revised) (100 words)	In this research, I will investigate the reasons why the end-users of bug-bounty programs keep joining and decide to join it. Aren't companies concern about the identity of the hackers? And why are hackers contributing their works to the company but not sell it to black market? This study would also research on the advantages and disadvantages of bug-bounty programs. The original idea was revised since the concepts were too broad and difficult even for people in the industry to answer.
Four Keywords to describe the project	Bug-bounty programs, BBPs, Ethical hackers, Crowdsourcing, Information security

SECTION 3: ANALYTICAL FRAMEWORK CHECKLIST	FILL IN THIS COLUMN			
Does your report contain a clearly expressed research question?	YES	✓	NO	
Does your report contain a review of relevant and up-to-date literature?	YES	✓	NO	
Does your report include a clearly expressed analytical framework (e.g. chosen theory, set of concepts, ways of data analysis etc.)	YES	✓	NO	
Briefly describe the framework you are using (50 words)	TAM is a useful and rather simple model for explaining users' intention and attitude in the acceptance of technology. It provides a guideline on how a user may be affected by the elements in it, and how the elements influence each other.			

SECTION 4: PRIMARY DATA COLLECTION TECHNIQUES CHECKLIST (select as appropriate)						
Questionnaire	Questions derived from a	✓	Piloted?	✓	Data analysed (more than described)?	✓

	theoretical framework					
Interviews	Interview themes given?	✓	Interviews coded?	✓	Interviews analysed?	✓
Observation	What type?	×	Participant	×	Non-Participant	×
	Methods of Analysis Used	×				
Documents	What type?	×				
	Analysis technique used	×				
Other (give brief description)	The questionnaire was conducted through online.					

SECTION 5: ETHICAL REVIEW	FILL IN THIS COLUMN			
Have all participants been told the purpose of the research and asked to consent to participate?	YES	✓	NO	
Does your research involve children or other potentially vulnerable persons?	YES		NO	✓
Does your research collect data that may be seen as sensitive or private by research participants?	YES		NO	✓
Does your research include any aspect that could be seen as deception or coercion?	YES		NO	✓
Are there any groups who may be harmed by dissemination of the results of your research?	YES		NO	✓
Does your research raise any other significant ethical concerns?	YES		NO	✓

If you have answered YES to any of these questions describe briefly what action you have taken in response. (100 words)	All participants for questionnaire and interviews are aware of the topic and where are their responses being used and used in research purposed.

SECTION 6: FINDINGS AND ANALYSIS CHECKLIST	FILL IN THIS COLUMN			
Does your report clearly express the findings from your project and relate them to an identified Information Systems theme?	YES	✓	NO	
What is the Information Systems theme your work addresses? (50 words)	Bug-bounty programs are a method for organisations to improve their information security whether on their website, systems, or products.			
What kind of a contribution do you make in this area? Who would be interested in reading your work and making use of your findings? (100 words)	Many researches have studies on this topic; however, most of them focuses on the technical or management parts of the topic. This study is based on those researches but with multiple perspectives of end-users' feedback. Security companies, security researchers, bug-bounty programs companies, and security managers would find the feedbacks and analysis useful to them.			

SECTION 7: PRESENTATION CHECKLIST	FILL IN THIS COLUMN			
Is your report printed to the guidelines given in the subject guide?	YES	✓	NO	
Does your conclusion chapter contain the essential insights of your work?	YES	✓	NO	
Are all quotations and material taken from other works properly presented and fully acknowledged?	YES	✓	NO	
Are all your references to books, articles and websites in a full and proper format (author, title,	YES	✓	NO	

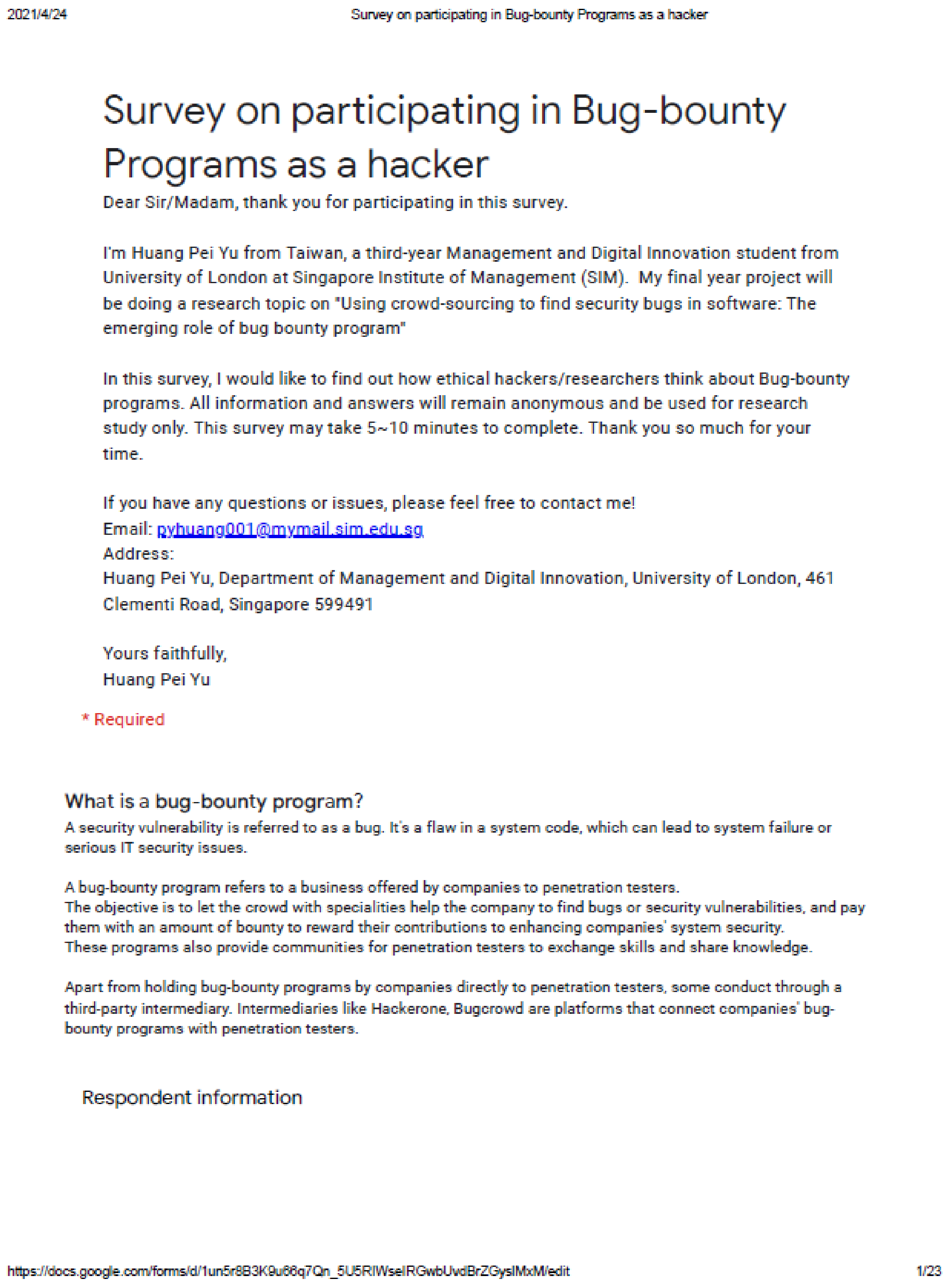
publisher, date etc.) and presented in the bibliography?				

SECTION 8: SUBMISSION CHECKLIST	FILL IN THIS COLUMN			
Have you included the Topic Area Proposal and a Project Specification as the first two appendices of your written report?	YES	✓	NO	
Have you completed and signed the submission cover sheet?	YES	✓	NO	
Have you prepared a file of your project report for uploading?	YES	✓	NO	

SECTION 9: Personal reflections FILL IN THIS BOX
Working on this topic is challenging and interesting for me. I was not familiar with designing a questionnaire. It would be difficult to ask reasonable and meaningful questions if not understanding the topic well. Some of my questions are poorly asked and therefore were deleted after doing Cronbach’s alpha. I also learnt the importance of deciding framework to use for the whole project. Since my questionnaire questions were designed based on my framework, insufficient understandings on the topic leads to poor questions and leads to ineffective survey responses, and then leads to poor analysis. Therefore, I have spent extra time on evaluating the results. Other reflections would be to change the way I distribute my questionnaire. Because the topic of bug-bounty programs is not really common to general public, I have a hard time finding sufficient number of respondents. Even I have contacted them, through social media messaging was mostly ended up being blocked or ignored. I have also learnt to organise large amount of data and context; Since the interviews were mostly conducted nearly 1 hour, the information in each transcript is enormous. I needed to collect useful information and eliminate unrelated context.

Appendix III: Survey Questionnaires

This section shows the pdf version of the whole questionnaire. The respondents were being directed to questions based on their answers in Google Form. Page 4 to 8 are excluded since they are all country options.



2021/4/24 Survey on participating in Bug-bounty Programs as a hacker

Survey on participating in Bug-bounty Programs as a hacker

Dear Sir/Madam, thank you for participating in this survey.

I'm Huang Pei Yu from Taiwan, a third-year Management and Digital Innovation student from University of London at Singapore Institute of Management (SIM). My final year project will be doing a research topic on "Using crowd-sourcing to find security bugs in software: The emerging role of bug bounty program"

In this survey, I would like to find out how ethical hackers/researchers think about Bug-bounty programs. All information and answers will remain anonymous and be used for research study only. This survey may take 5~10 minutes to complete. Thank you so much for your time.

If you have any questions or issues, please feel free to contact me!
Email: pyhuang001@mymail.sim.edu.sg
Address:
Huang Pei Yu, Department of Management and Digital Innovation, University of London, 461 Clementi Road, Singapore 599491

Yours faithfully,
Huang Pei Yu

* Required

What is a bug-bounty program?

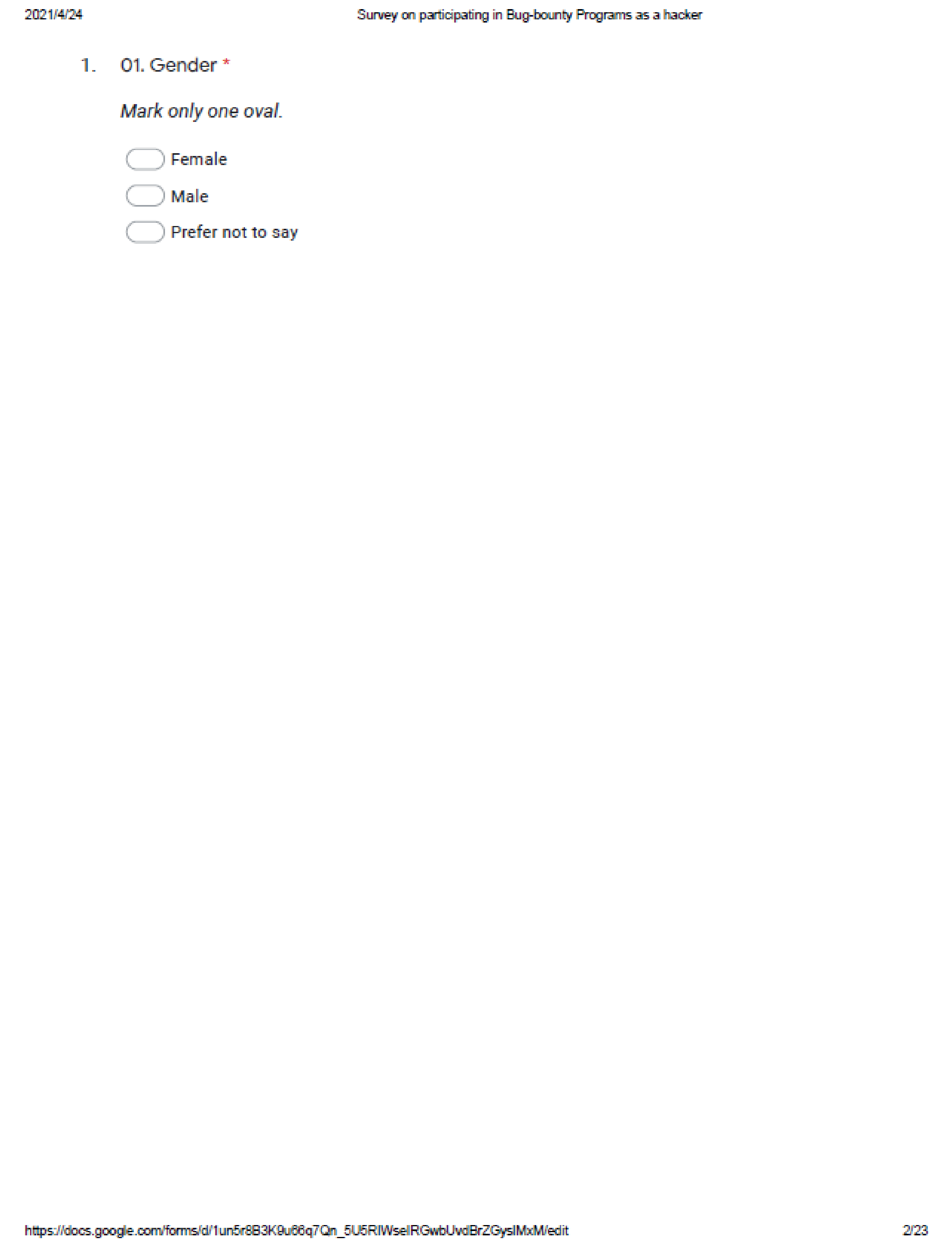
A security vulnerability is referred to as a bug. It's a flaw in a system code, which can lead to system failure or serious IT security issues.

A bug-bounty program refers to a business offered by companies to penetration testers.
The objective is to let the crowd with specialities help the company to find bugs or security vulnerabilities, and pay them with an amount of bounty to reward their contributions to enhancing companies' system security.
These programs also provide communities for penetration testers to exchange skills and share knowledge.

Apart from holding bug-bounty programs by companies directly to penetration testers, some conduct through a third-party intermediary. Intermediaries like Hackerone, Bugcrowd are platforms that connect companies' bug-bounty programs with penetration testers.

Respondent information

https://docs.google.com/forms/d/1un5r8B3K9u66q7Qn_5U5RIWselRGwbUvdBrZGysIMxM/edit 1/23



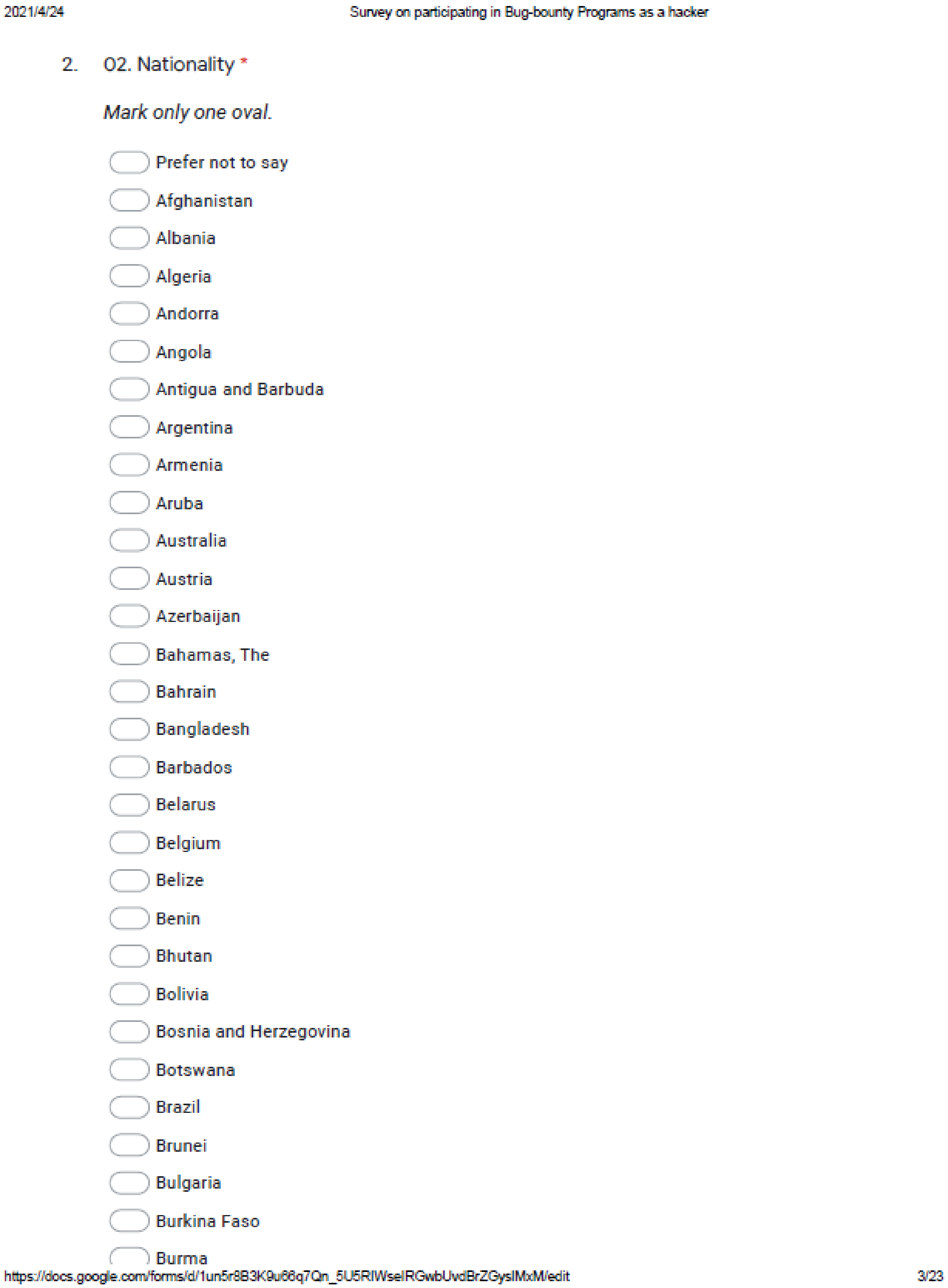
1. 01. Gender *

Mark only one oval.

○ Female

○ Male

○ Prefer not to say



2. 02. Nationality *

Mark only one oval.

○ Prefer not to say

○ Afghanistan

○ Albania

○ Algeria

○ Andorra

○ Angola

○ Antigua and Barbuda

○ Argentina

○ Armenia

○ Aruba

○ Australia

○ Austria

○ Azerbaijan

○ Bahamas, The

○ Bahrain

○ Bangladesh

○ Barbados

○ Belarus

○ Belgium

○ Belize

○ Benin

○ Bhutan

○ Bolivia

○ Bosnia and Herzegovina

○ Botswana

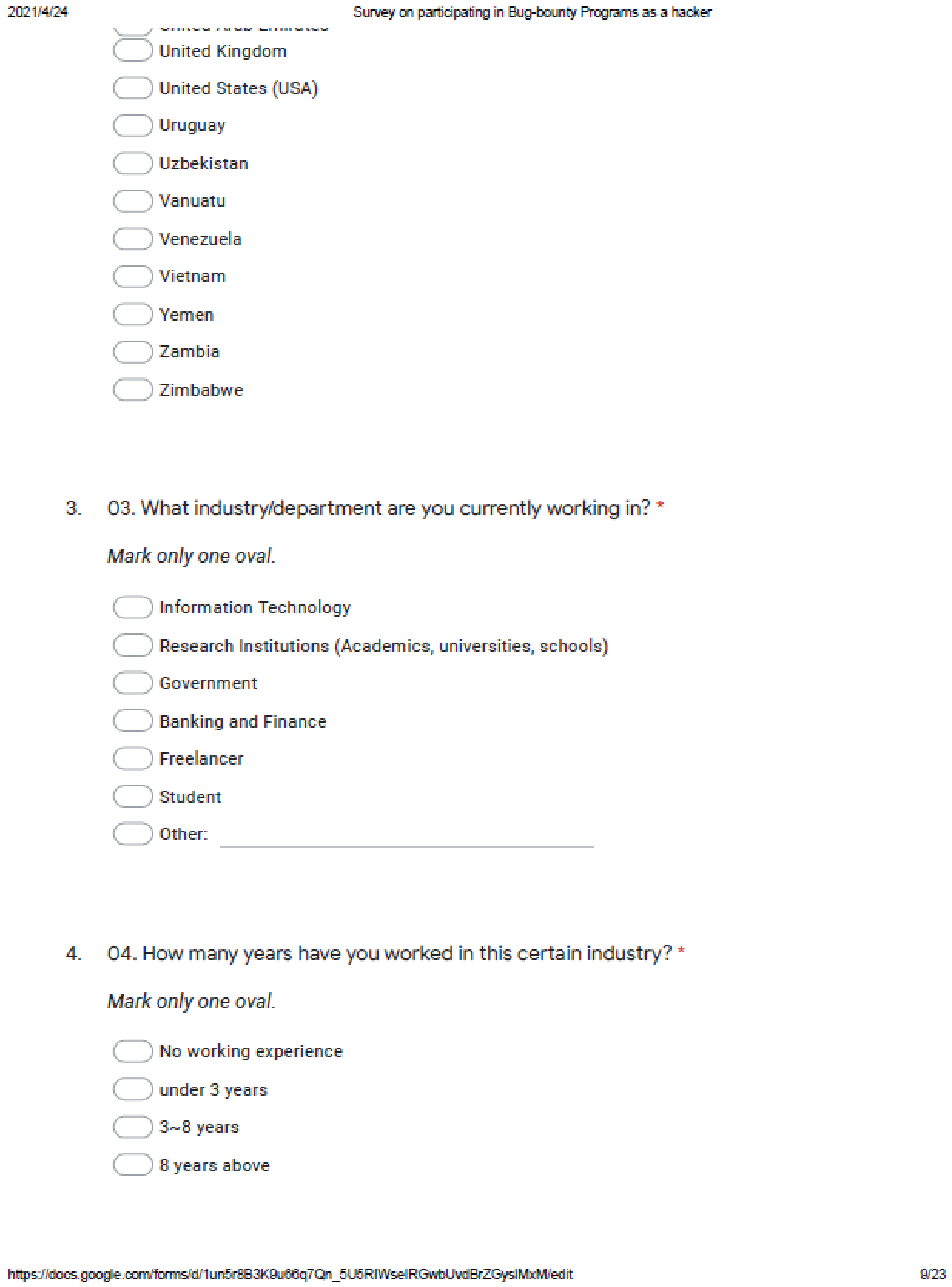
○ Brazil

○ Brunei

○ Bulgaria

○ Burkina Faso

○ Burma



○ United Arab Emirates

○ United Kingdom

○ United States (USA)

○ Uruguay

○ Uzbekistan

○ Vanuatu

○ Venezuela

○ Vietnam

○ Yemen

○ Zambia

○ Zimbabwe

3. 03. What industry/department are you currently working in? *

Mark only one oval.

○ Information Technology

○ Research Institutions (Academics, universities, schools)

○ Government

○ Banking and Finance

○ Freelancer

○ Student

○ Other: ______________________

4. 04. How many years have you worked in this certain industry? *

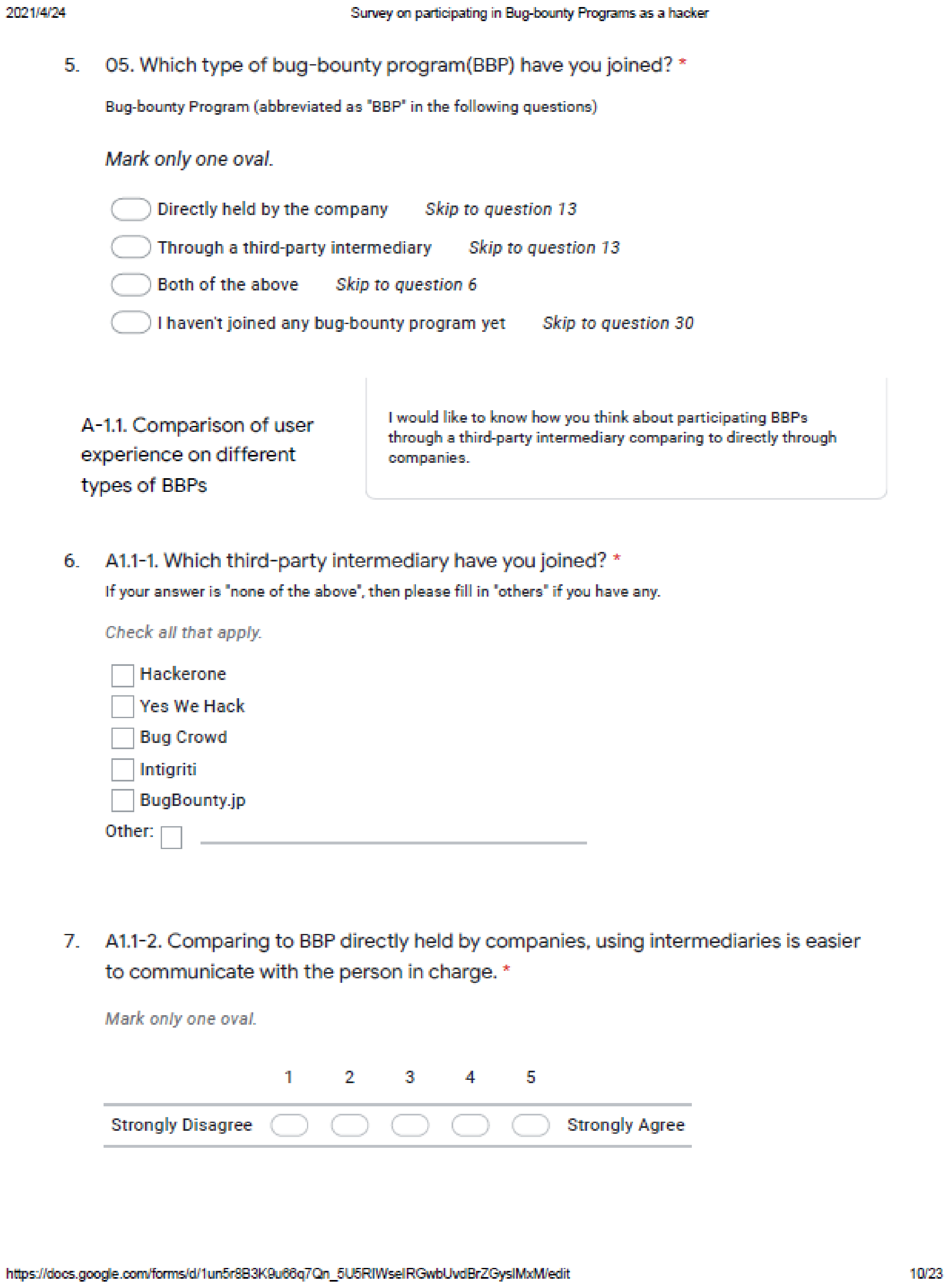
Mark only one oval.

○ No working experience

○ under 3 years

○ 3~8 years

○ 8 years above



5. 05. Which type of bug-bounty program(BBP) have you joined? *

Bug-bounty Program (abbreviated as "BBP" in the following questions)

Mark only one oval.

○ Directly held by the company *Skip to question 13*
○ Through a third-party intermediary *Skip to question 13*
○ Both of the above *Skip to question 6*
○ I haven't joined any bug-bounty program yet *Skip to question 30*

A-1.1. Comparison of user experience on different types of BBPs

I would like to know how you think about participating BBPs through a third-party intermediary comparing to directly through companies.

6. A1.1-1. Which third-party intermediary have you joined? *

If your answer is "none of the above", then please fill in "others" if you have any.

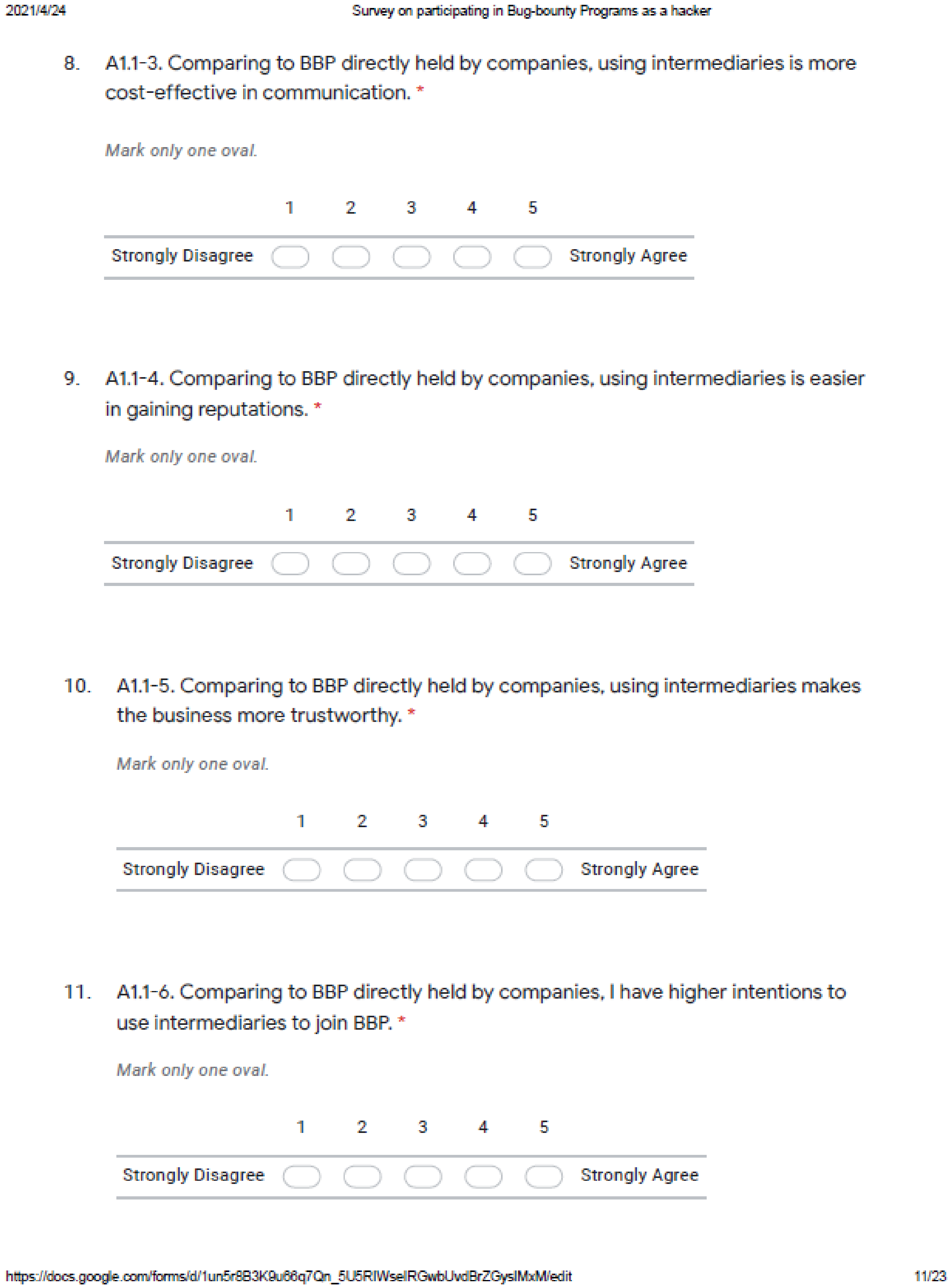
Check all that apply.

□ Hackerone
□ Yes We Hack
□ Bug Crowd
□ Intigriti
□ BugBounty.jp
Other: □ ____________________

7. A1.1-2. Comparing to BBP directly held by companies, using intermediaries is easier to communicate with the person in charge. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree



8. A1.1-3. Comparing to BBP directly held by companies, using intermediaries is more cost-effective in communication. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

9. A1.1-4. Comparing to BBP directly held by companies, using intermediaries is easier in gaining reputations. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

10. A1.1-5. Comparing to BBP directly held by companies, using intermediaries makes the business more trustworthy. *

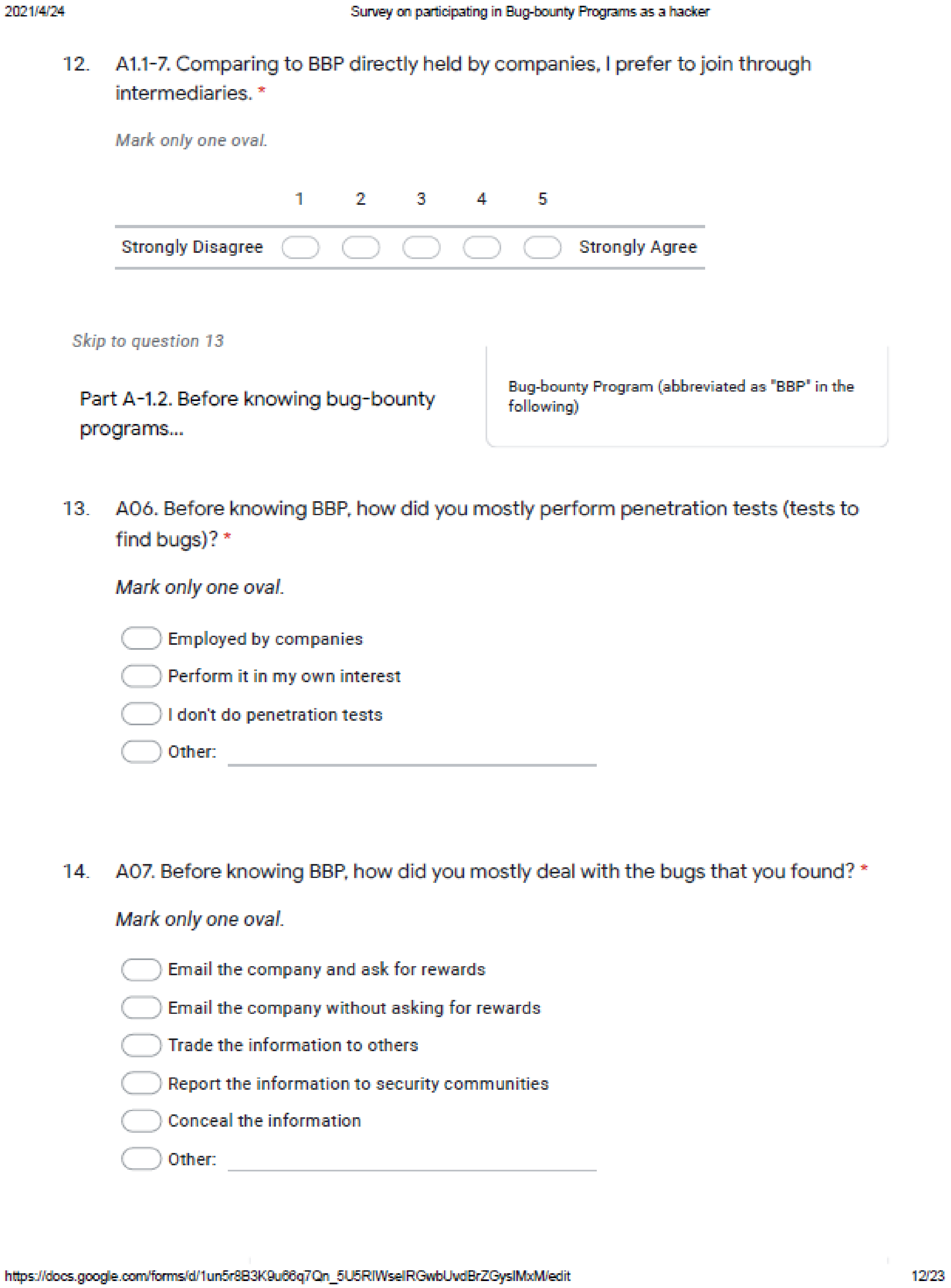
Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

11. A1.1-6. Comparing to BBP directly held by companies, I have higher intentions to use intermediaries to join BBP. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree



12. A1.1-7. Comparing to BBP directly held by companies, I prefer to join through intermediaries. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Skip to question 13

Part A-1.2. Before knowing bug-bounty programs...

Bug-bounty Program (abbreviated as "BBP" in the following)

13. A06. Before knowing BBP, how did you mostly perform penetration tests (tests to find bugs)? *

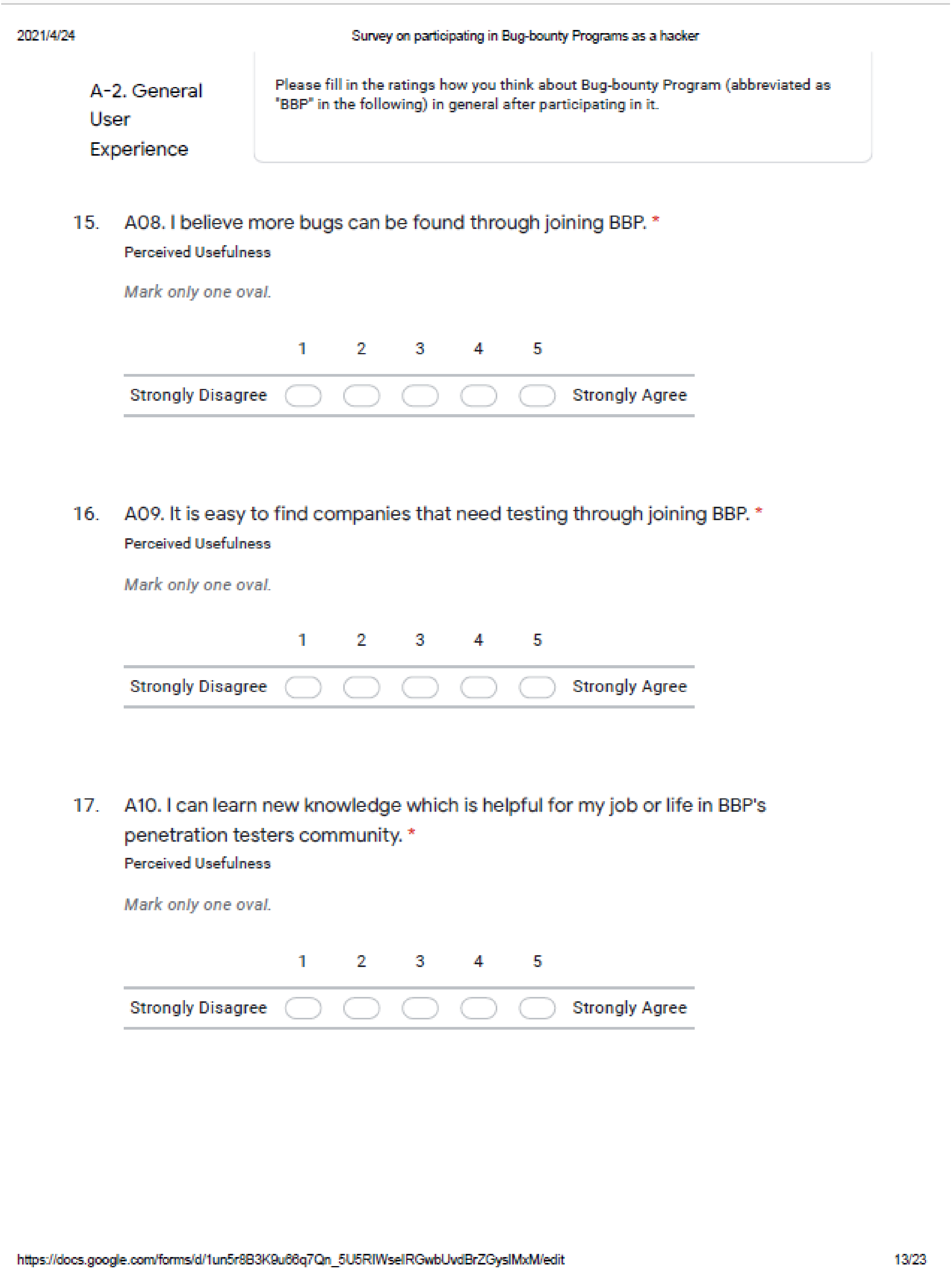
Mark only one oval.

○ Employed by companies
○ Perform it in my own interest
○ I don't do penetration tests
○ Other: ______________________

14. A07. Before knowing BBP, how did you mostly deal with the bugs that you found? *

Mark only one oval.

○ Email the company and ask for rewards
○ Email the company without asking for rewards
○ Trade the information to others
○ Report the information to security communities
○ Conceal the information
○ Other: ______________________



A-2. General User Experience

Please fill in the ratings how you think about Bug-bounty Program (abbreviated as "BBP" in the following) in general after participating in it.

15. A08. I believe more bugs can be found through joining BBP. *

Perceived Usefulness

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

16. A09. It is easy to find companies that need testing through joining BBP. *

Perceived Usefulness

Mark only one oval.

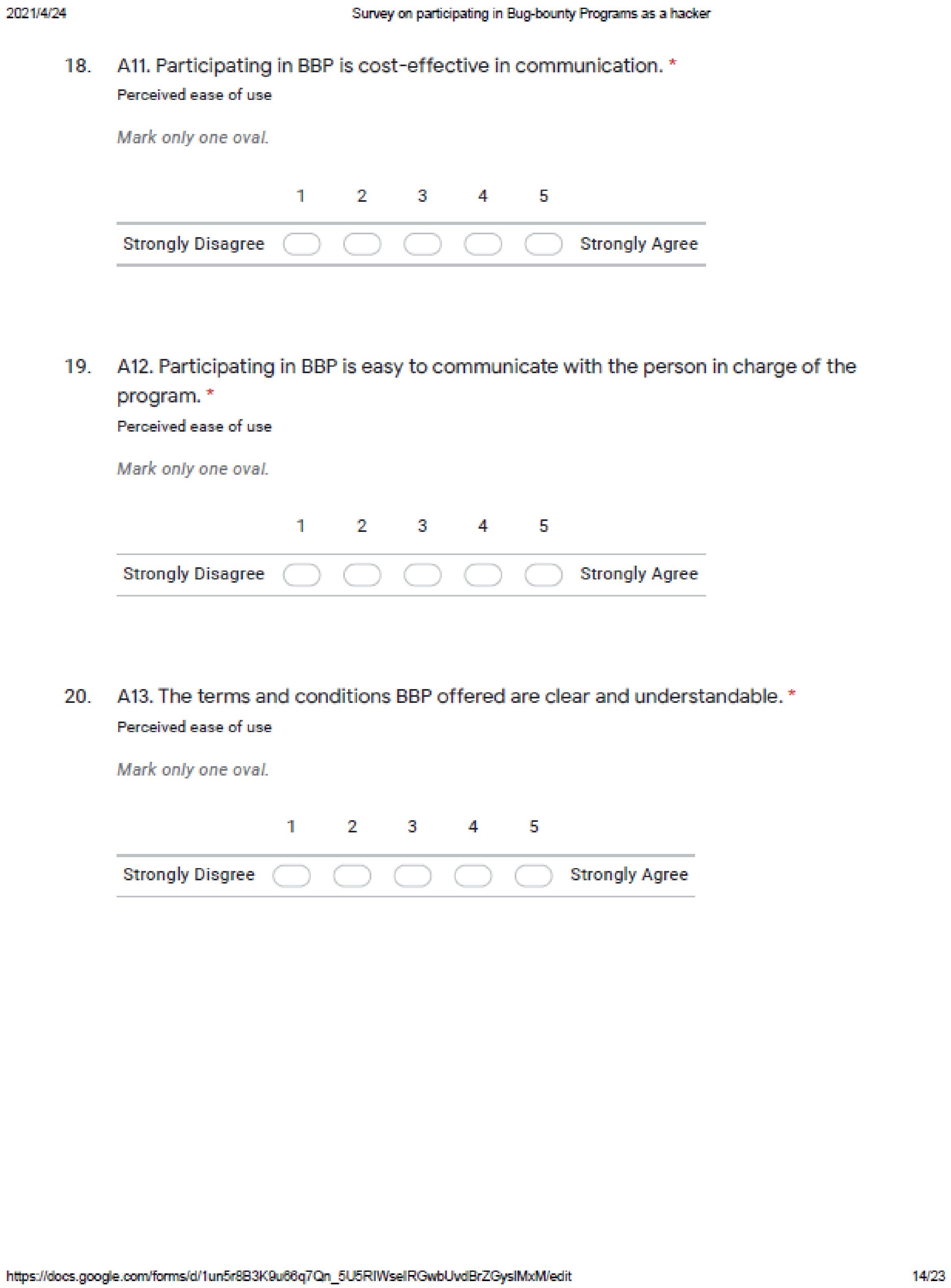
	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

17. A10. I can learn new knowledge which is helpful for my job or life in BBP's penetration testers community. *

Perceived Usefulness

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree



2021/4/24 Survey on participating in Bug-bounty Programs as a hacker

18. A11. Participating in BBP is cost-effective in communication. *

Perceived ease of use

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

19. A12. Participating in BBP is easy to communicate with the person in charge of the program. *

Perceived ease of use

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

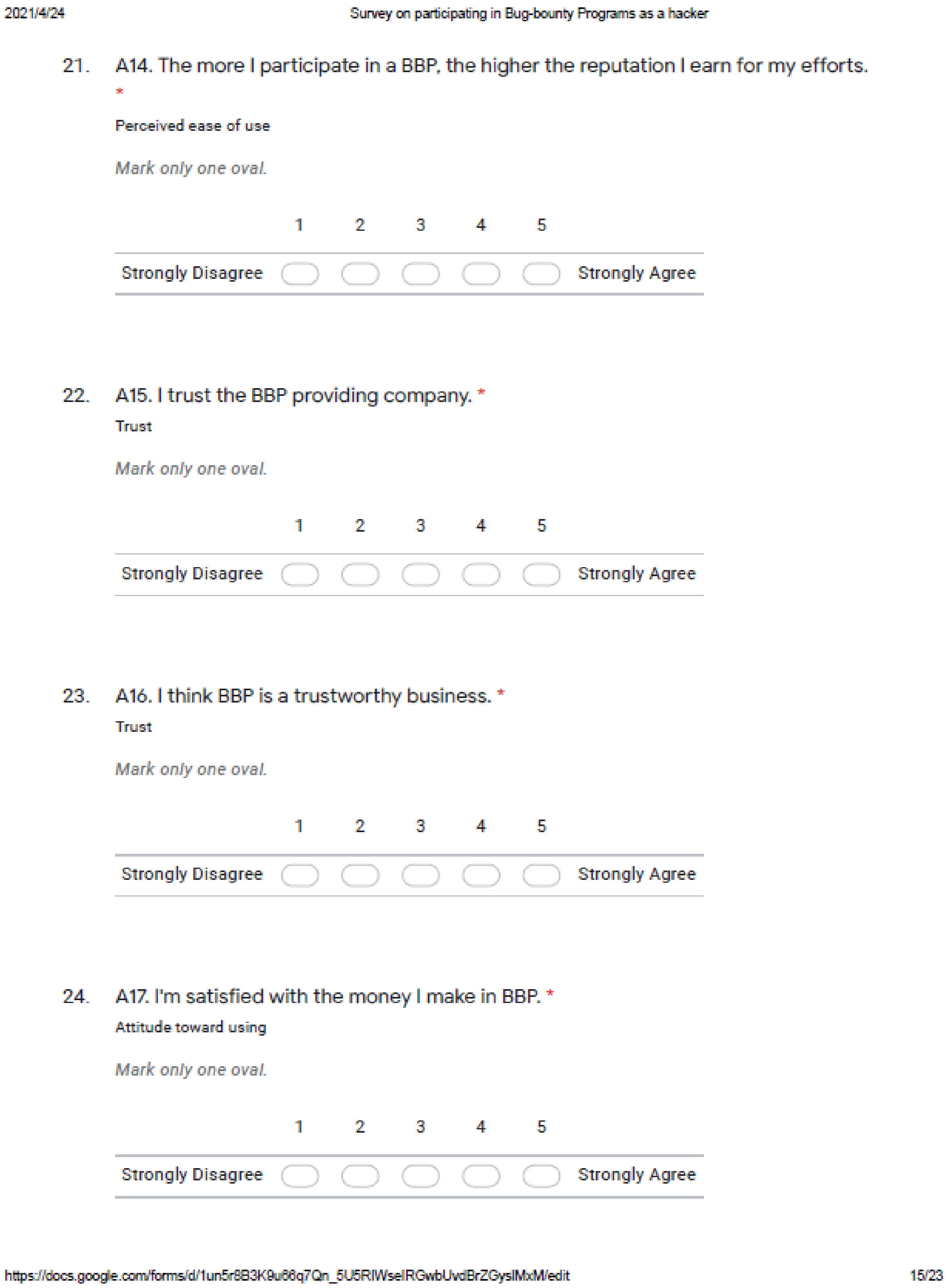
20. A13. The terms and conditions BBP offered are clear and understandable. *

Perceived ease of use

Mark only one oval.

	1	2	3	4	5	
Strongly Disgree	○	○	○	○	○	Strongly Agree

https://docs.google.com/forms/d/1un5r8B3K9u66q7Qn_5U5RIWselRGwbUvdBrZGysIMxM/edit 14/23



2021/4/24 Survey on participating in Bug-bounty Programs as a hacker

21. A14. The more I participate in a BBP, the higher the reputation I earn for my efforts. *

Perceived ease of use

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

22. A15. I trust the BBP providing company. *

Trust

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

23. A16. I think BBP is a trustworthy business. *

Trust

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

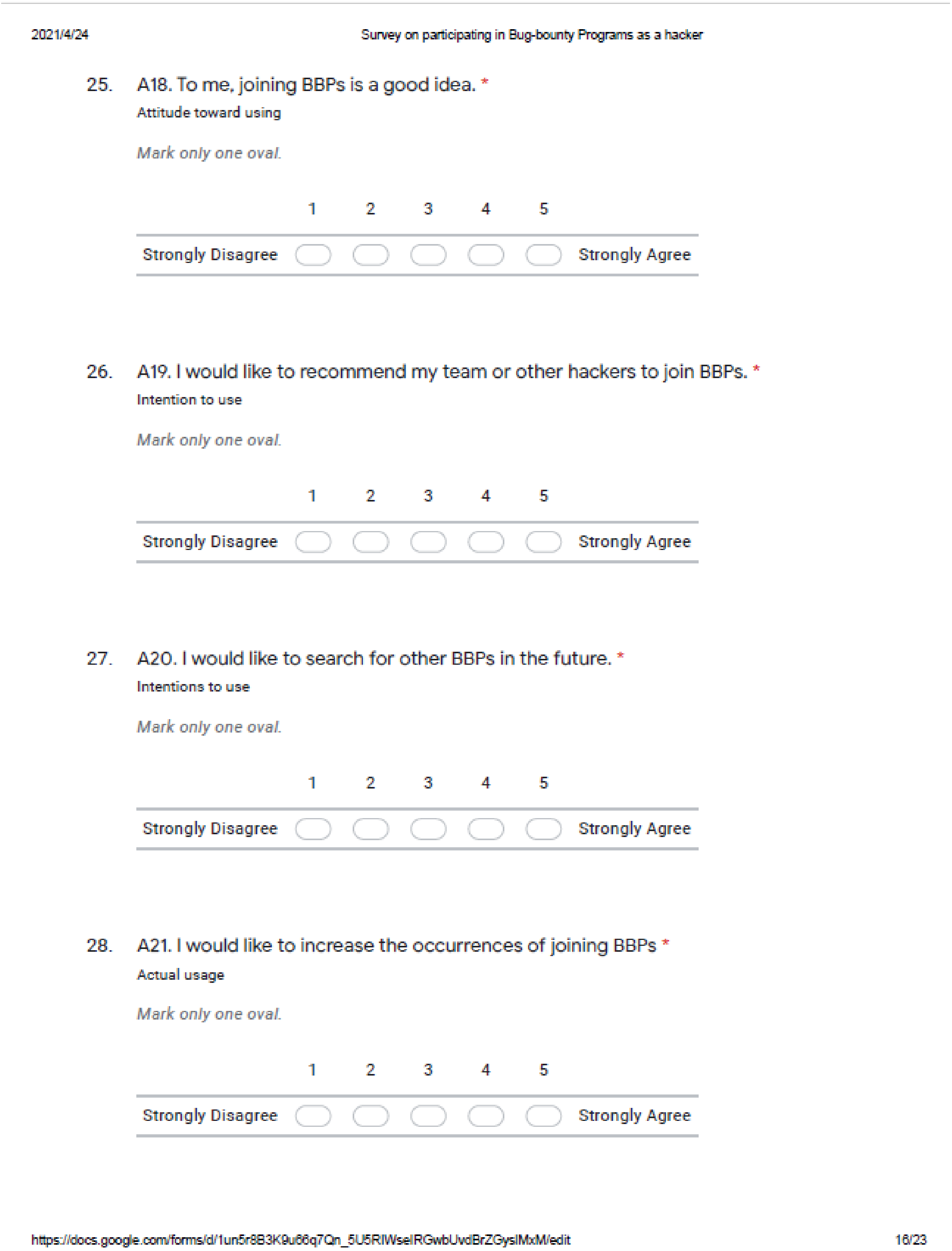
24. A17. I'm satisfied with the money I make in BBP. *

Attitude toward using

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

https://docs.google.com/forms/d/1un5r8B3K9u66q7Qn_5U5RIWselRGwbUvdBrZGysIMxM/edit 15/23



2021/4/24 Survey on participating in Bug-bounty Programs as a hacker

25. A18. To me, joining BBPs is a good idea. *

Attitude toward using

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

26. A19. I would like to recommend my team or other hackers to join BBPs. *

Intention to use

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

27. A20. I would like to search for other BBPs in the future. *

Intentions to use

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

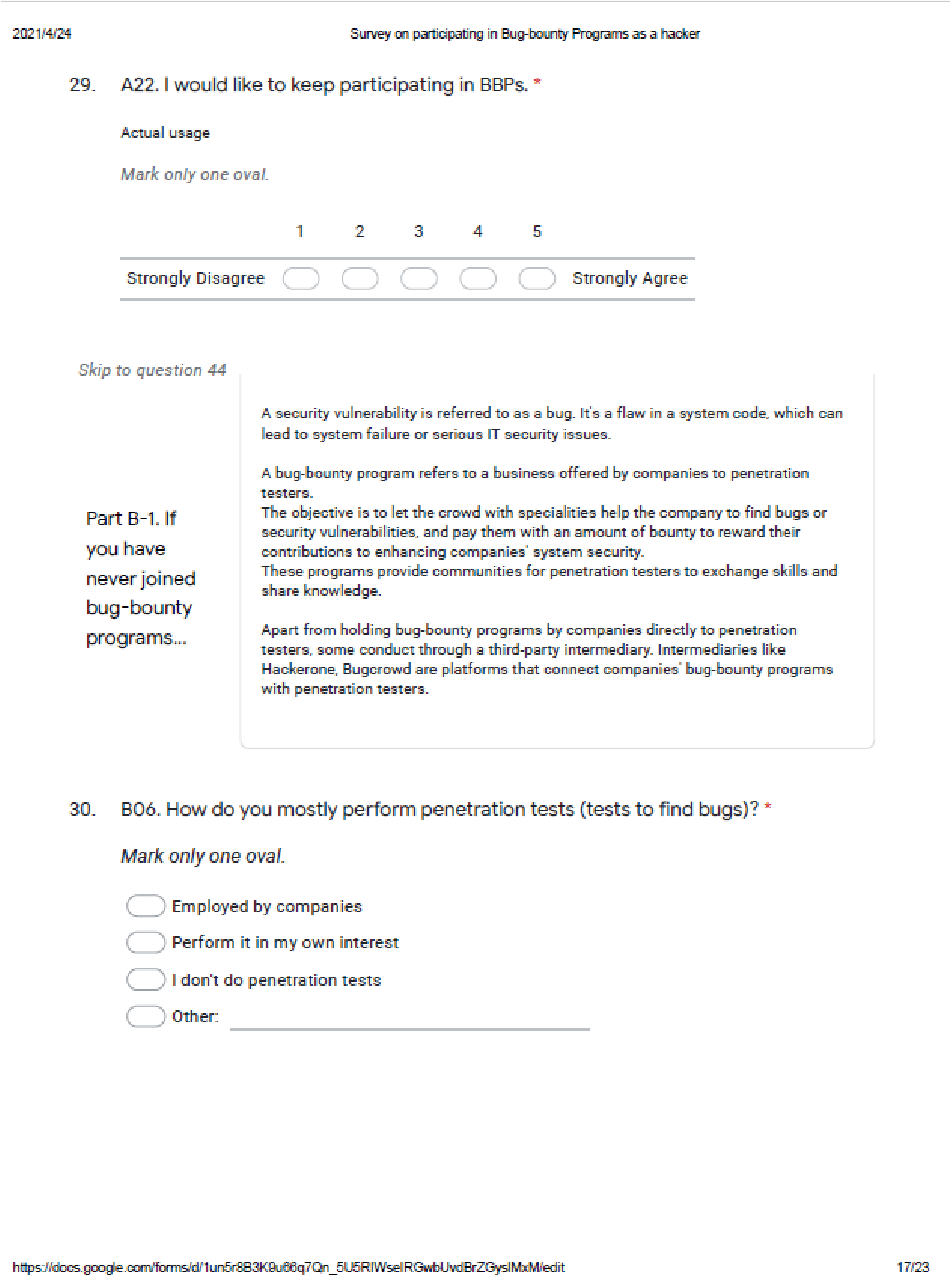
28. A21. I would like to increase the occurrences of joining BBPs *

Actual usage

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

https://docs.google.com/forms/d/1un5r8B3K9u66q7Qn_5U5RIWselRGwbUvdBrZGysIMxM/edit 16/23



2021/4/24 Survey on participating in Bug-bounty Programs as a hacker

29. A22. I would like to keep participating in BBPs. *

Actual usage

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Skip to question 44

Part B-1. If you have never joined bug-bounty programs...

A security vulnerability is referred to as a bug. It's a flaw in a system code, which can lead to system failure or serious IT security issues.

A bug-bounty program refers to a business offered by companies to penetration testers.
The objective is to let the crowd with specialities help the company to find bugs or security vulnerabilities, and pay them with an amount of bounty to reward their contributions to enhancing companies' system security.
These programs provide communities for penetration testers to exchange skills and share knowledge.

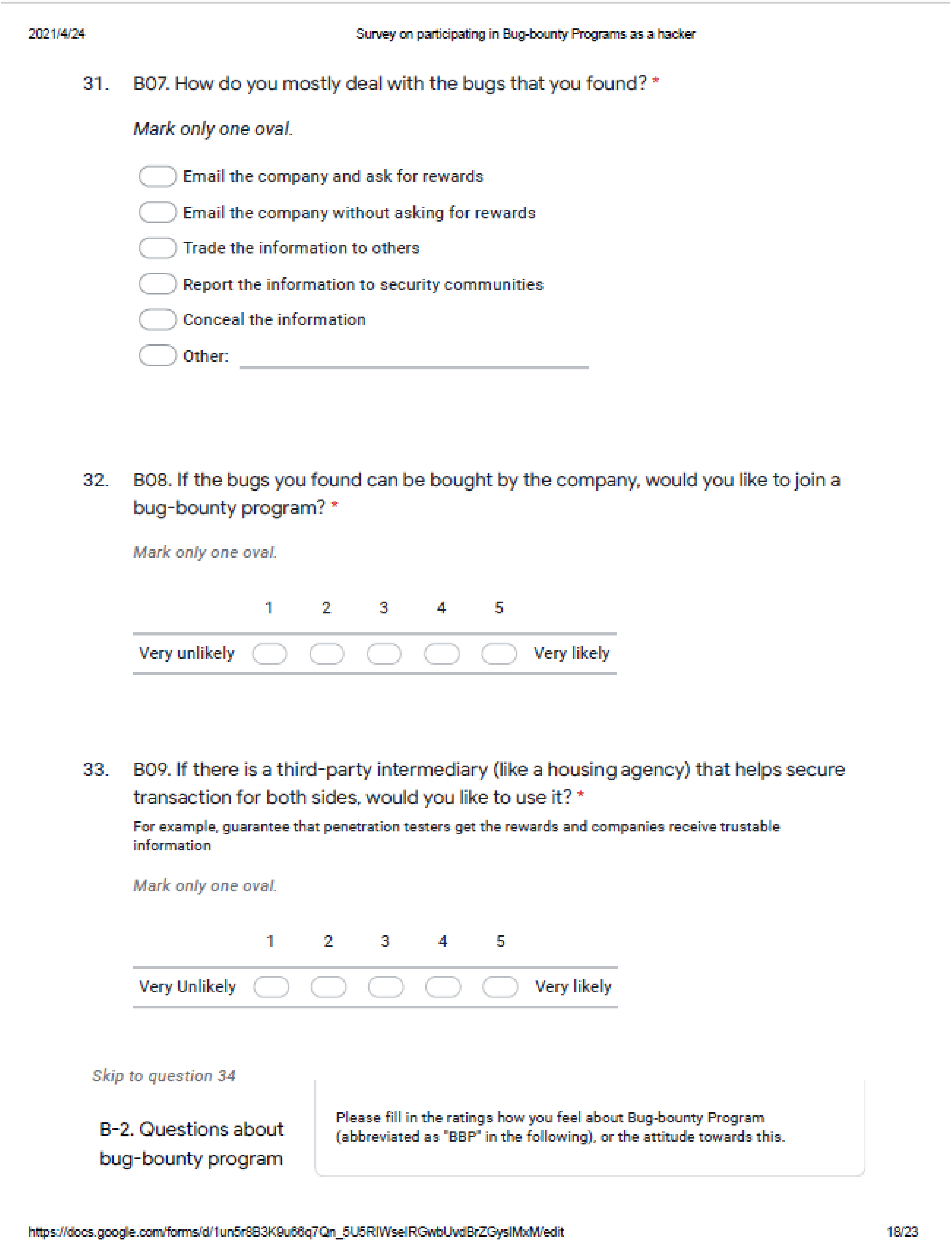
Apart from holding bug-bounty programs by companies directly to penetration testers, some conduct through a third-party intermediary. Intermediaries like Hackerone, Bugcrowd are platforms that connect companies' bug-bounty programs with penetration testers.

30. B06. How do you mostly perform penetration tests (tests to find bugs)? *

Mark only one oval.

○ Employed by companies
○ Perform it in my own interest
○ I don't do penetration tests
○ Other: ____________________

https://docs.google.com/forms/d/1un5r8B3K9u66q7Qn_5U5RIWselRGwbUvdBrZGysIMxM/edit 17/23



31. B07. How do you mostly deal with the bugs that you found? *

Mark only one oval.

○ Email the company and ask for rewards
○ Email the company without asking for rewards
○ Trade the information to others
○ Report the information to security communities
○ Conceal the information
○ Other: ________________

32. B08. If the bugs you found can be bought by the company, would you like to join a bug-bounty program? *

Mark only one oval.

	1	2	3	4	5	
Very unlikely	○	○	○	○	○	Very likely

33. B09. If there is a third-party intermediary (like a housing agency) that helps secure transaction for both sides, would you like to use it? *

For example, guarantee that penetration testers get the rewards and companies receive trustable information

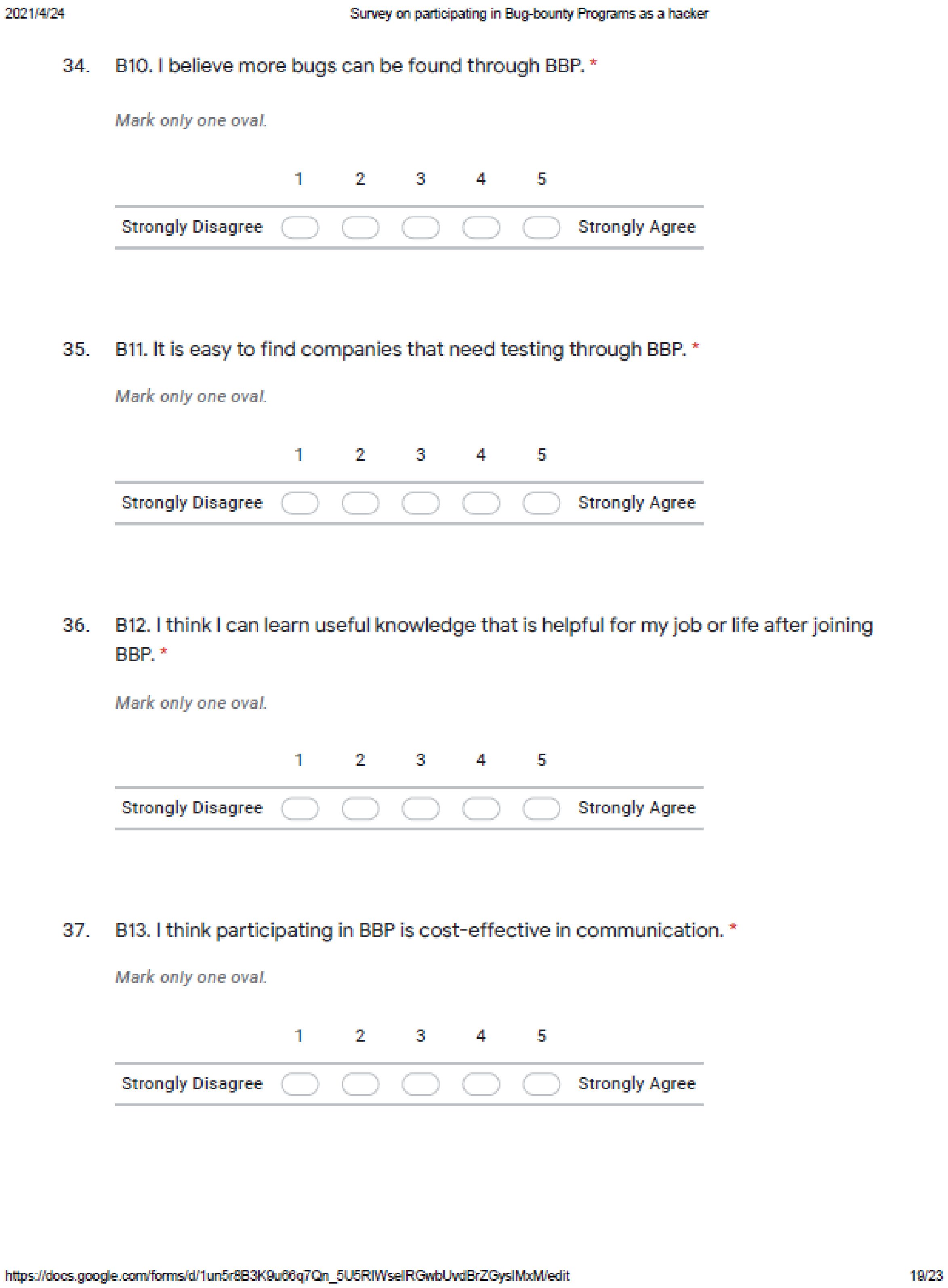
Mark only one oval.

	1	2	3	4	5	
Very Unlikely	○	○	○	○	○	Very likely

Skip to question 34

B-2. Questions about bug-bounty program

Please fill in the ratings how you feel about Bug-bounty Program (abbreviated as "BBP" in the following), or the attitude towards this.



34. B10. I believe more bugs can be found through BBP. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

35. B11. It is easy to find companies that need testing through BBP. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

36. B12. I think I can learn useful knowledge that is helpful for my job or life after joining BBP. *

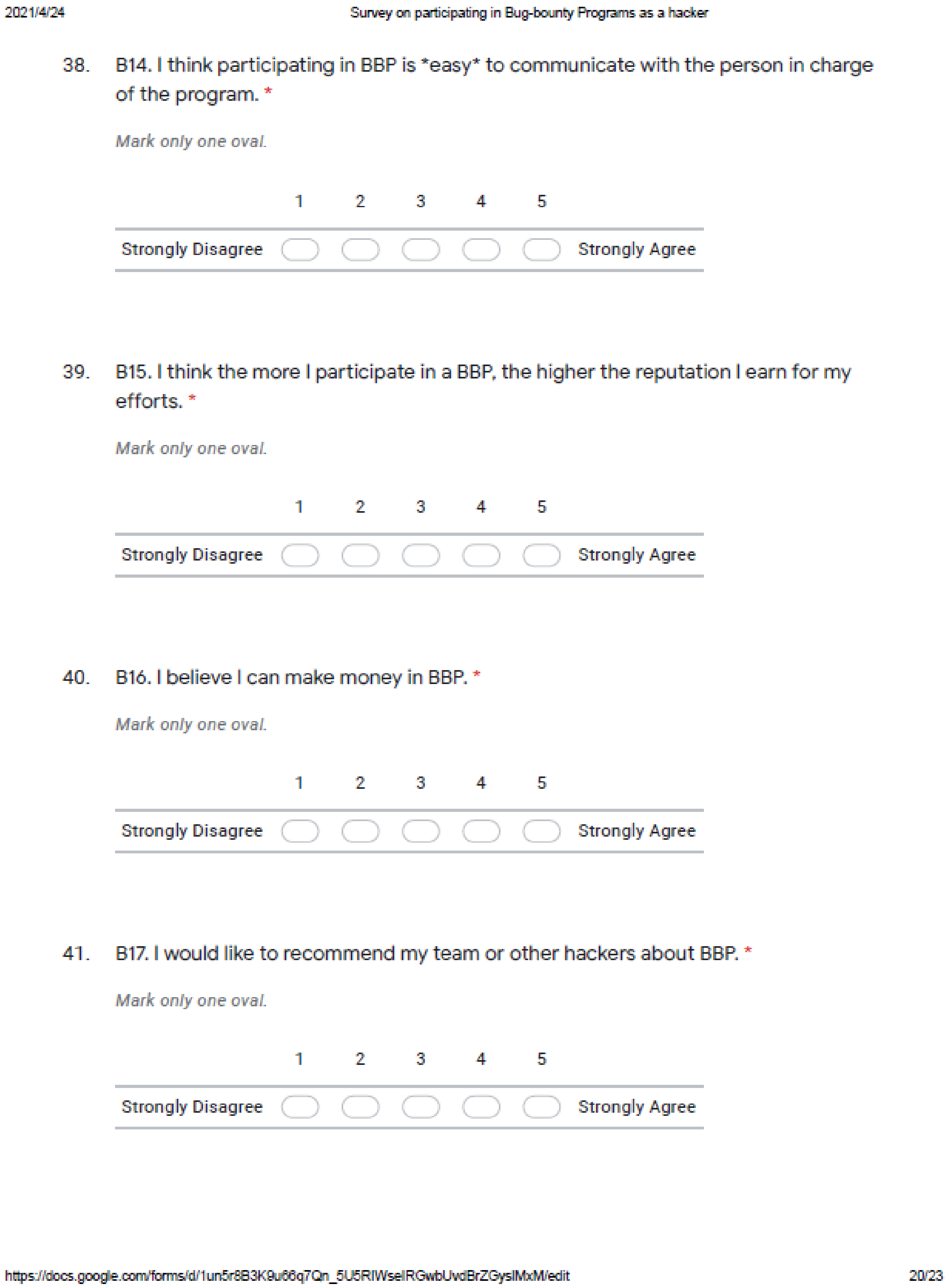
Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

37. B13. I think participating in BBP is cost-effective in communication. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree



38. B14. I think participating in BBP is *easy* to communicate with the person in charge of the program. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

39. B15. I think the more I participate in a BBP, the higher the reputation I earn for my efforts. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

40. B16. I believe I can make money in BBP. *

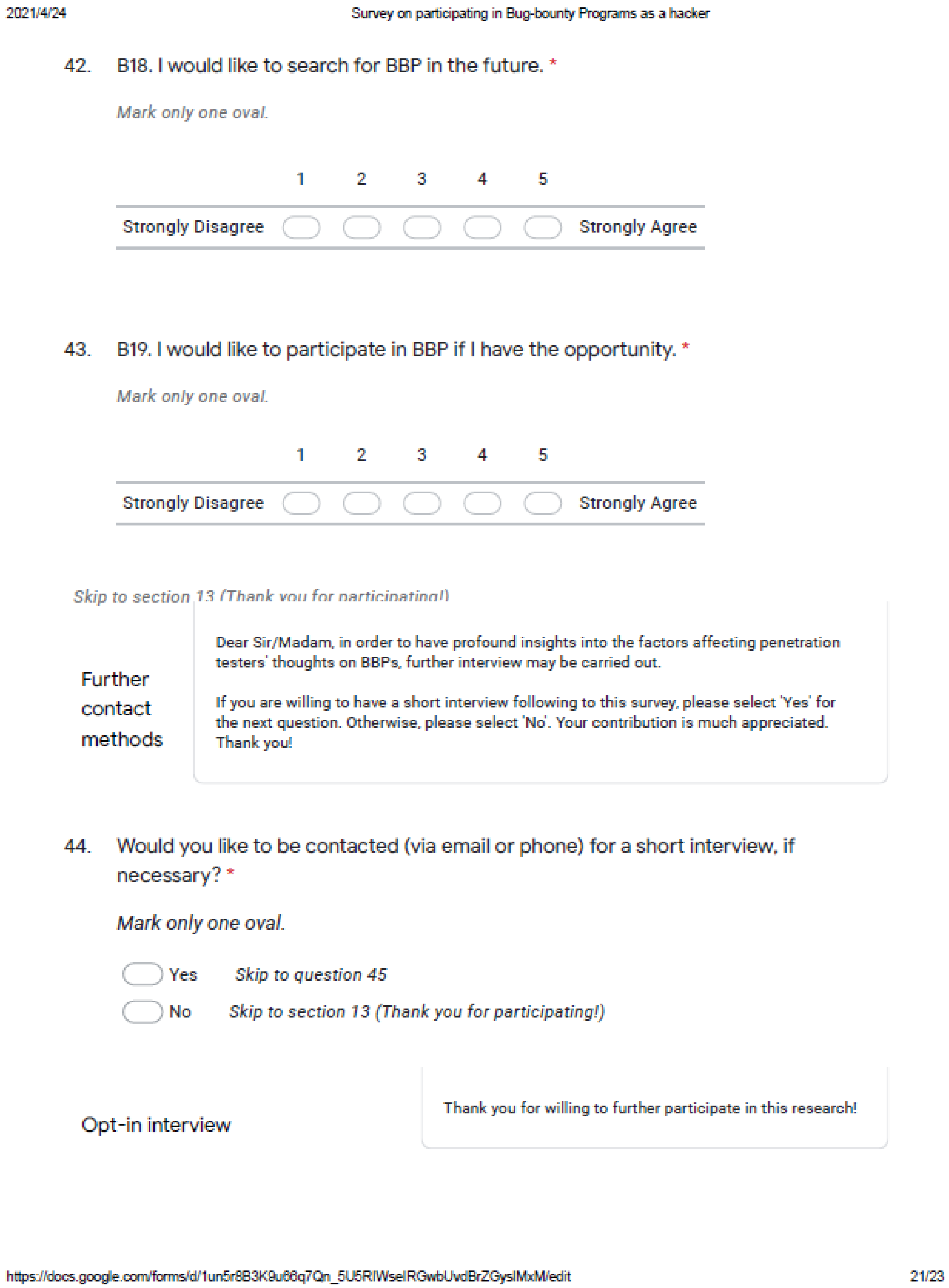
Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

41. B17. I would like to recommend my team or other hackers about BBP. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree



2021/4/24 Survey on participating in Bug-bounty Programs as a hacker

42. B18. I would like to search for BBP in the future. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

43. B19. I would like to participate in BBP if I have the opportunity. *

Mark only one oval.

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Skip to section 13 (Thank you for participating!)

Further contact methods

Dear Sir/Madam, in order to have profound insights into the factors affecting penetration testers' thoughts on BBPs, further interview may be carried out.

If you are willing to have a short interview following to this survey, please select 'Yes' for the next question. Otherwise, please select 'No'. Your contribution is much appreciated. Thank you!

44. Would you like to be contacted (via email or phone) for a short interview, if necessary? *

Mark only one oval.

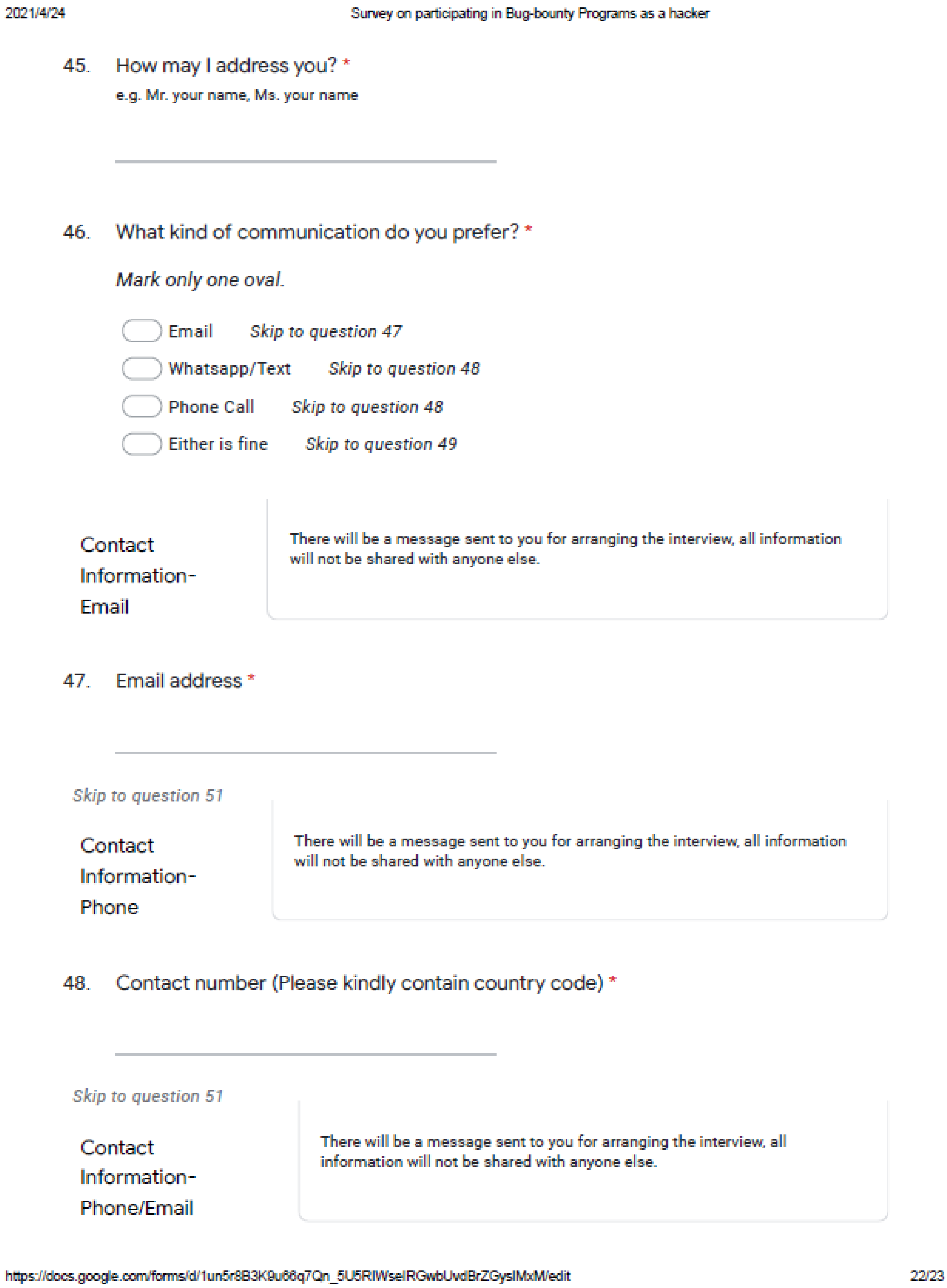
○ Yes *Skip to question 45*

○ No *Skip to section 13 (Thank you for participating!)*

Opt-in interview

Thank you for willing to further participate in this research!

https://docs.google.com/forms/d/1un5r8B3K9u66q7Qn_5U5RIWselRGwbUvdBrZGysIMxM/edit 21/23



45. How may I address you? *

e.g. Mr. your name, Ms. your name

46. What kind of communication do you prefer? *

Mark only one oval.

○ Email *Skip to question 47*

○ Whatsapp/Text *Skip to question 48*

○ Phone Call *Skip to question 48*

○ Either is fine *Skip to question 49*

Contact Information-Email

There will be a message sent to you for arranging the interview, all information will not be shared with anyone else.

47. Email address *

Skip to question 51

Contact Information-Phone

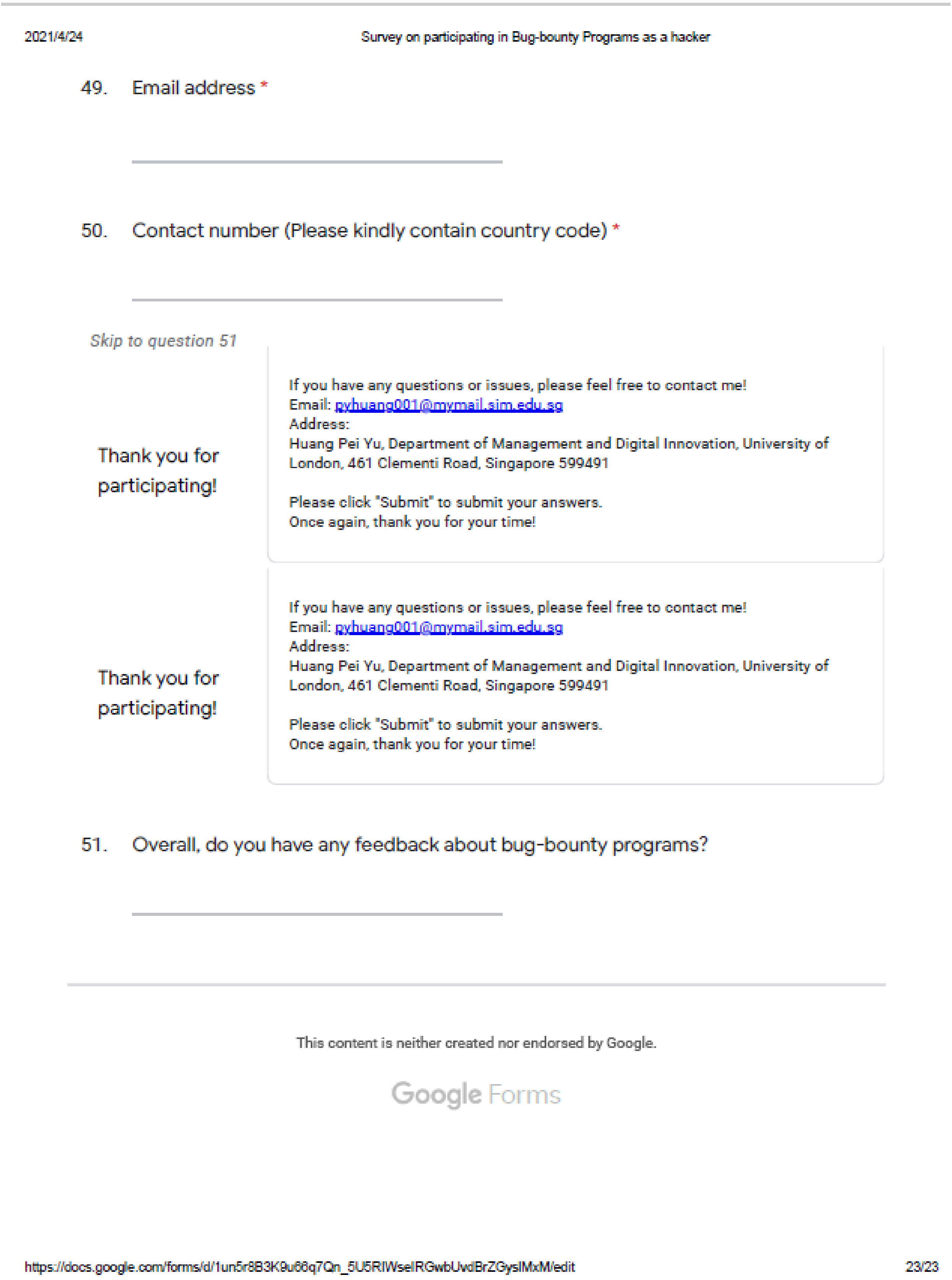
There will be a message sent to you for arranging the interview, all information will not be shared with anyone else.

48. Contact number (Please kindly contain country code) *

Skip to question 51

Contact Information-Phone/Email

There will be a message sent to you for arranging the interview, all information will not be shared with anyone else.



49. Email address *

50. Contact number (Please kindly contain country code) *

Skip to question 51

Thank you for participating!

If you have any questions or issues, please feel free to contact me!
Email: pyhuang001@mymail.sim.edu.sg
Address:
Huang Pei Yu, Department of Management and Digital Innovation, University of London, 461 Clementi Road, Singapore 599491

Please click "Submit" to submit your answers.
Once again, thank you for your time!

Thank you for participating!

If you have any questions or issues, please feel free to contact me!
Email: pyhuang001@mymail.sim.edu.sg
Address:
Huang Pei Yu, Department of Management and Digital Innovation, University of London, 461 Clementi Road, Singapore 599491

Please click "Submit" to submit your answers.
Once again, thank you for your time!

51. Overall, do you have any feedback about bug-bounty programs?

Appendix IV: Raw Survey Results

BBPs participants:

TAM elements	1: Strongly Disagree	2: Disagree	3: Neutral	4: Agree	5: Strongly Agree
PE01 Participating in BBPs is cost-effective in communication.	1	0	10	14	20
PE02 Participating in BBPs is easy in finding the person in charge of the program.	0	1	11	21	12
PE03* The terms and conditions BBPs offered are clear and understandable.	0	3	10	18	14
PE04* The more I participate in BBPs, the higher the reputation I earn for my efforts.	0	0	8	16	21
PU01 I believe more bugs can be found through joining BBP.	1	1	3	16	24
PU02 I can learn new knowledge which is helpful for my job or life in BBPs' penetration testers' community.	1	1	8	14	22
PU03* It is easy to find companies that need testing through joining BBP.	0	2	9	14	19
T01 I trust the BBPs providing companies.	0	1	11	16	17
T02 I trust the BBPs providing companies.	0	1	8	22	14
A01 I'm satisfied with the money I make in BBPs.	0	2	15	17	11
A02 To me, joining BBPs is a good idea	0	1	5	19	20
I01 I would like to recommend my team or other hackers to join BBPs.	0	0	6	15	24
I02 I would like to search for other BBPs in the future.	0	0	2	14	29
AU01 I would like to increase the occurrences of joining BBPs.	0	2	4	31	8

AU02 I would like to keep participating in BBPs.	0	0	4	10	31

*The ones being deleted

Comparing to BBP directly held by companies...	1: Strongly Disagree	2: Disagree	3: Neutral	4: Agree	5: Strongly Agree
using intermediaries is easier to communicate with the person in charge.	0	4	9	14	7
using intermediaries is more cost-effective in communication.	1	2	13	15	3
using intermediaries is easier in gaining reputations.	0	2	2	8	22
using intermediaries makes the business more trustworthy.	0	1	6	14	13
I have higher intentions to use intermediaries to join BBP.	0	2	5	14	13
I prefer to join through intermediaries.	0	1	9	15	9

Individual feedback:

BBP changed my life. It gave me a stable career and financial freedom.
I think the charge of bug bounty platforms, like hackerone, bugcrowd, is too expensive for companies.
Try Harder!
a legal way for hackers, good jobs!
BBP are totally different when it comes to comparing it with traditional Pentests. The resources available online are enough for Starts to kick off if directed in right direction. I've rarely disagreed or raised dispute with BBP response or resolution which was just in one of the BBP. I prefer Hunting on Yes We Hack rather H1 or etc.
They're a good way to increase a company's security, but there's still a long way to go to make the concept of bug bounty mainstream.
Overall, bug bounties provide an effective way to report security issues to companies and be rewarded for it. I wish the pay outs were higher as it feels like our work is undervalued compared to the impact it could have on these organisations.

Very good. They offer flexibility, freedom, and good monetary rewards. On the other hand, it has a very steep learning curve, so it is pretty hard in the beginning.
Bug bounty program are revolutionizing the whole security industry. They have become big source of income for hacker's and allows them to use their knowledge and skills for good. It helps companies finding vulnerabilities before the bad guys.
Bug Bounty programs are a great way to expand knowledge for hackers while great way to security infrastructure for companies.
Creating a BBP always results in having a way more secured company.

BBP non-participants:

	1: Strongly Disagree	2: Disagree	3: Neutral	4: Agree	5: Strongly Agree
If the bugs you found can be bought by the company, would you like to join a bug-bounty program?	2	0	2	2	1
If there is a third-party intermediary (like a housing agency) that helps secure transaction for both sides, would you like to use it?	0	1	2	2	2
I believe more bugs can be found through BBP.	0	0	1	4	2
It is easy to find companies that need testing through BBP.	0	2	2	3	0
I think I can learn useful knowledge that is helpful for my job or life after joining BBP.	0	1	2	3	1
I think participating in BBP is cost-effective in communication.	1	0	0	5	1
I think participating in BBP is easy to communicate with the person in charge of the program.	0	0	4	3	0
I think the more I participate in a BBP, the higher the reputation I earn for my efforts.	0	1	3	2	1
I believe I can make money in BBP.	1	0	3	3	0

I would like to recommend my team or other hackers about BBP.	1	0	2	4	0
I would like to search for BBP in the future.	1	1	2	2	1
I would like to participate in BBP if I have the opportunity.	1	1	1	3	1

Appendix V: Interview Questions/ Transcripts

All Transcripts were proofread.

Interview with HackerOne

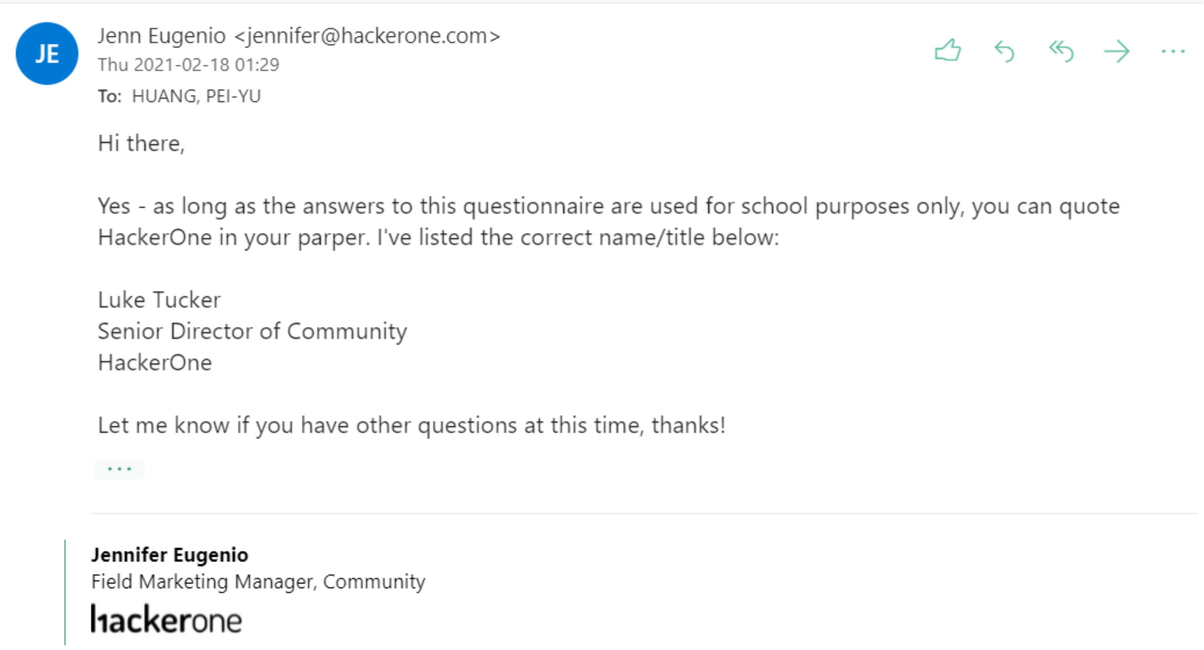
Hi, I'm Huang Pei Yu from Taiwan, a third-year Management and Digital Innovation student from the University of London at the Singapore Institute of Management (SIM). My final year project will be doing a research topic on "Using crowd-sourcing to find security bugs: The emerging role of bug bounty program". I will be doing the following for my research:

1) Analysis of the advantages, disadvantages from BBPs end-user perspectives.

2) Highlight how ethical hackers, companies and third-party platforms think about bug bounty programs, and how it affects their attitude of continuing engagement in it.

Thank you for answering this email interview, if it's possible to do an online interview with you please contact me through this email: pyhuang001@mymail.sim.edu.sg

Email of consent to disclose interviwee's name and title:



JE

Jenn Eugenio <jennifer@hackerone.com>
Thu 2021-02-18 01:29
To: HUANG, PEI-YU

Hi there,

Yes - as long as the answers to this questionnaire are used for school purposes only, you can quote HackerOne in your parper. I've listed the correct name/title below:

Luke Tucker
Senior Director of Community
HackerOne

Let me know if you have other questions at this time, thanks!

...

Jennifer Eugenio
Field Marketing Manager, Community
hackerone

Interviewee: Luke Tucker

Interviewee Designation: HackerOne, Senior Director of Community

Interview Method: Email interview

Date: 18th February 2020

Interview Questions and Answers:

No.	Question/ Answer
1.	**What profession are you in HackerOne?** Ans: Sr. Director of Community
2.	**Please briefly describe HackerOne's main business, and what are the security issues HackerOne trying to solve for companies?** Ans: HackerOne empowers the world to build a safer internet. As the world's most trusted hacker-powered security platform, HackerOne gives organizations access to the largest community of hackers on the planet. Armed with the most robust database of vulnerability trends and industry benchmarks, the hacker community mitigates cyber risk by searching, finding, and safely reporting real-world security weaknesses for organizations across all industries and attack surfaces. Customers include The U.S. Department of Defense, Dropbox, General Motors, GitHub, Goldman Sachs, Google, Hyatt, Intel, Lufthansa, Microsoft, MINDEF Singapore, Nintendo, PayPal, Slack, Starbucks, Twitter, and Verizon Media. HackerOne was ranked fifth on the Fast Company World's Most Innovative Companies list for 2020. Headquartered in San Francisco, HackerOne has a presence in London, New York, the Netherlands, France, Singapore, and over 70 other locations across the globe.

3.	**Except for your business, what are the common methodologies other companies use to solve the issues you've mentioned in Question 2?** Ans: There are many mechanisms used to find vulnerabilities, including scanners, traditional point-in-time penetration tests, and other SaaS solutions.
4.	**Can you talk about the advantages and edges HackerOne has, compared to the common methodologies used you've mentioned in Question 3?** Ans: Collaboration isn't a new concept. Scientists and academics live and breathe peer review. You can get the biggest brains in the world together in one room, but there is nothing like opening up your work to the rest of the brains in the world: You are guaranteed to learn something. That's why a company invites hackers in — to get the best and brightest minds and as many perspectives as possible looking at their infrastructure. While SaaS solutions like scanners can find frequent, uncomplicated vulnerabilities, they lack creativity — a distinctly human trait — needed to find complex vulnerabilities that can be incredibly impactful. Compared to any internal routine security testing, hackers have another distinct advantage — they can think like attackers, but act as your defenders.
5.	**How do you find companies to engage in bug bounty programs on your platform?** Ans: In short, everywhere — inbound, outbound, and referrals. Everyone should have a Vulnerability Disclosure Policy (VDP). Often referred to as the "see something, say something" of the internet, a VDP is the first step in helping protect your company from an attack or premature vulnerability

	release to the public. This is oftentimes an organization's entry point to working with HackerOne.
6.	**How do you evaluate the satisfaction rate of the company on the platform?** Ans: All companies have different success metrics but the most common would be valid vulnerabilities and high/critical impactful bugs.
7.	**Do most of the joined companies continue to stay on your platform? Why?** Ans: Working with hackers is an industry best practice, and adoption is growing year over year. More than $44.75 million in bounties were awarded to hackers across the globe over the past year according to our annual Hacker-Powered Security Report. That's a year-over- year increase of 87% in total bounties paid and helped drive total bounties past $100 million in May 2020.
8.	**How do you find hackers to join bug bounty programs through HackerOne?** Ans: Hackers find HackerOne in a variety of ways. Most often, they find us! They hear about us through word of mouth or on social media and are interested in hacking. We also actively find and recruit hackers to engage with.
9.	**Do you have any professional criteria when selecting hackers?** Ans: Anyone can be a hacker on HackerOne!

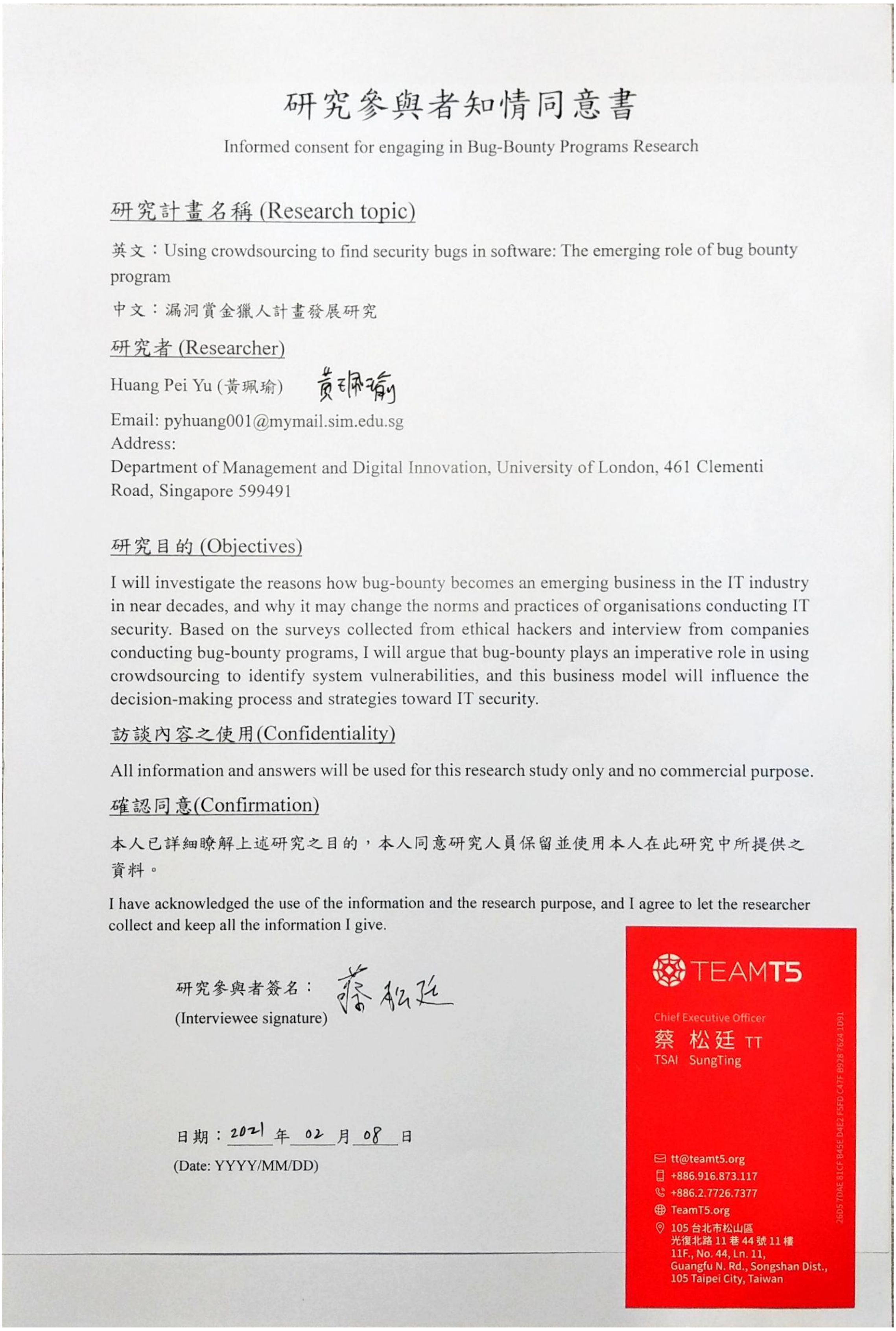
10.	**Do you do background checks on hackers?** Ans: For the majority of our programs, background checks are not required as hackers get no special access to company infrastructure. For more sensitive programs or assets, we have HackerOne Clear, which requires background checks.
11.	**How is the bounty price being set?** Ans: Bounty tables are determined by each individual customer for their respective program.
12.	**What factors make hackers and companies choose to join bug bounty programs through third-party platforms, but not joining or holding it on their own (ex. Synology)?** Ans: While the reasons to adopt HackerOne may vary from staffing restrictions to policy requirements, HackerOne provides companies of all sizes with services and products that fit their needs. One reason we hear often is organizations are quickly adopting modern, transformative IT initiatives that are outpacing their security teams' capacity to keep up. For security teams, this means constant change, disruptions with unknown consequences, increased risk, competing priorities, and a growing, disparate, and diverse IT ecosystem to protect. The challenge for cybersecurity teams is finding effective ways to deliver and scale security at the speed of digital transformation, ensuring that every new technology, digital process, customer, and partner interaction is protected.

	HackerOne empowers organizations to scale security capabilities by providing ongoing access to talent, unlimited asset coverage, and assessment flexibility to enable this kind of business transformation.
13.	**There are several competitors (ex. Bugcrowd, YesWeHack) in the market providing similar services as HackerOne, what factors make HackerOne stand out?** Ans: Looking solely from a hacker perspective, HackerOne has the most programs resulting in larger financial opportunities.
14.	**How do you manage the quality of the submitted report from hackers, for instance, scams and invalid reports?** Ans: Not applicable and invalid reports happen often but our security analyst team is fully equipped to review and handle these large volume reports.
15.	**How do you build mutual trust between companies and hackers?** Ans: HackerOne is dedicated to ensuring the trust between companies and hackers, with the Customer Success team and Community team fulfilling this mission every day. The Customer Success team is comprised of program managers, technical program managers and security analysts to ensure the success of the company while addressing hacker questions and needs.
16.	**What are some of the top bug bounty trends in future?** Ans: It's constantly changing but the most recent trends have been recon to specific vulnerability types and new techniques presented at large

	conferences like Black Hat and DEFCON. For a list of the top vulnerabilities hackers find through bug bounty, vulnerability disclosure, and hacker-powered penetration tests, check out our latest research: https://www.hackerone.com/top-ten-vulnerabilities

Interview with HITCON/ TeamT5

Consent letter:



研究參與者知情同意書

Informed consent for engaging in Bug-Bounty Programs Research

研究計畫名稱 (Research topic)

英文：Using crowdsourcing to find security bugs in software: The emerging role of bug bounty program

中文：漏洞賞金獵人計畫發展研究

研究者 (Researcher)

Huang Pei Yu (黃珮瑜) 黃珮瑜

Email: pyhuang001@mymail.sim.edu.sg
Address:
Department of Management and Digital Innovation, University of London, 461 Clementi Road, Singapore 599491

研究目的 (Objectives)

I will investigate the reasons how bug-bounty becomes an emerging business in the IT industry in near decades, and why it may change the norms and practices of organisations conducting IT security. Based on the surveys collected from ethical hackers and interview from companies conducting bug-bounty programs, I will argue that bug-bounty plays an imperative role in using crowdsourcing to identify system vulnerabilities, and this business model will influence the decision-making process and strategies toward IT security.

訪談內容之使用(Confidentiality)

All information and answers will be used for this research study only and no commercial purpose.

確認同意(Confirmation)

本人已詳細瞭解上述研究之目的，本人同意研究人員保留並使用本人在此研究中所提供之資料。

I have acknowledged the use of the information and the research purpose, and I agree to let the researcher collect and keep all the information I give.

研究參與者簽名：蔡松廷
(Interviewee signature)

日期：2021 年 02 月 08 日
(Date: YYYY/MM/DD)

TEAMT5

Chief Executive Officer
蔡 松廷 TT
TSAI SungTing

tt@teamt5.org
+886.916.873.117
+886.2.7726.7377
TeamT5.org
105 台北市松山區
光復北路 11 巷 44 號 11 樓
11F., No. 44, Ln. 11,
Guangfu N. Rd., Songshan Dist.,
105 Taipei City, Taiwan

26D5 7DAE 81CF B45E D4E2 F5FD CA7F B928 7624 1D91

Interviewee: Sung Ting, Tsai

Interviewee Designation: TeamT5, Chief Executive Officer. HITCON CEO and founder

Interview Method: face-to-face interview

Date: 8th February 2021

**A* is additional question asked based on interviewee's answers.

1. Tell us about your experience in HITCON Association.

HITCON Association is mainly building hackers community and promoting information security. We have held various information security activities every year, and we organize and encourage young researchers to participate in competitions. Competitions like the capture the flag (CTF) world competitions. We also cooperate with many government institutes and as consultants. From the National Security Council to the Information Security Office, the Ministry of Economic Affairs, the Bureau of Industry, the Ministry of Education, and other government units. They also ask us to help their programs and carry out activities to support their information security. We have seen a lot of positive energy and influence in the industry in past 16 years. Many contents published on HITCON is competent compared to the content I heard in the Black Hat conference. Thus, we also help many young people to submit their research works to international journals, which is one of the reasons why I want to start a business.

A: What kind of people are your members?

HITCON Association is divided into several different levels. First, there are ten plus core members: directors and supervisors who are responsible for decision-making, budgeting, and planning. Then, there are HITCON volunteers. These staffs help HITCON organise activities. Next, the HITCON community, which includes thousands of people, or even 10,000 people. They are mainly the participants of activities every year.

2. What do you think about the connection between hackers and information security?

Our definition of hackers is different from the definition in the media. We think that hackers are people that like challenges, brave to challenge, and are expertise in technology. For example, some companies claim that their encryption algorithm or system is unbreakable and secure. Then hackers would want to challenge it, because they have a deep understanding of the mechanism of systems. They aim at challenging themselves and enhance their skills. It is the enthusiasm for technical research, not the matter of crime.

Hence, although we are called the Hacker Association, we certainly do not support crime. “Pure technology” is the way we say in the field, which means there is no distinction between black and white (hat) in technology. It’s the way how people utilise the technology that matters. This is our definition of hackers.

You asked that what connection between hackers and information security is. I think hackers are the driving force for the development of information security. Whether it is offensive and defensive, it is a double-edges sword. If you are defencing your system, someone will attack it. If you are being attack, you will start to think about how to defence.

The underlying motivations are the cause of offense and defence; However, the motivation is not purely in technical discussions. Our association is focusing in the technical field. If the motivation involves interests and benefits relationships, it may cross the illegal line. That is not what we encourage.

3. Based on your knowledge of hackers, how do they use their research results?

I know a lot of people who are expertise and enthusiastic. Most of them are keen to exchange knowledge, and what they want is a sense of accomplishment. He/r has put so much effort in the research, of course s/he wants to show off to the community. Since hacking technology is difficult for others to understand. Hackers want to participate in discussion forums and communities to gain recognitions. That’s to say, HITCON is a very suitable place for this type of discussions. The discussions enable hackers’ research to be more in-depth, because of other people giving them opinions. The sense of recognitions is also the source of inspirations.

A: Will they report the bugs they found to the company?

It depends on the situation and people. We certainly encourage to use appropriate methods to report the bugs to the company. But this is actually very complicated. In the early days, if I find any bugs, I'll just go show off to the community, and that's all. However, nowadays, if you have shared some critical bugs in the community, units from the dark web may contact you to trade the bug details to them. Some secret service agents would ask you to not disclose the information. These are all part of the information security industry. Whether it's about money or political factors, it's really complicated. Therefore, HITCON only focus on researching bugs, we cannot manage how hackers do to the bugs.

4. If these research results are being used to help companies' information security, what method do you think is more suitable?

We encourage them to use appropriate channels to report bugs to the company that makes the product or website. But to be honest, from the researcher's point of view, these processes are often very frustrating. For example, there are researchers that wrote emails to the company to inform the bugs they found. It didn't take too long for them to receive a demand letter. Even though they kindly reported back and didn't ask for any money. The company asked why they were looking for bugs on their website and whether they had bad intentions. This is the most negative results for researchers.

Most of the cases getting no response from the company. Therefore, an unobstructed channel is the key factor for this report process to work. Start from encouraging researchers to report the bugs, and the company side should have enough preparations to handle the reports with the attitude of willing to accept the contributions from hackers.

5. From the perspective of a hacker, what are your thoughts on BBP as a way of protecting information security? Do you think it can solve some of the problems you mentioned earlier?

I think BBP can solve the reporting problem for researchers. It ensures a clear channel to report, and a transparent disclosure policy. Plus, it encourages hackers to use the bugs in a good way, and researchers can receive bounty for reporting valid bugs. Therefore, we are supportive in the idea of joining BBP.

Before introducing BBP, researchers have two ways. One is selling the bugs to the black market and earn money or report it to the company and take the risks of being sued. Some hackers found 10 bugs, then 7 are sold in black market, rest of the 3 are for building reputation in the community. We would not recommend researchers to sell the bugs for malicious behaviour. Therefore, the company must give a reasonable bounty to encourage hackers to report bugs to them but not the black market. Many hackers would be satisfied to keep joining BBP when their efforts and costs in testing is being covered. They feel sense of accomplishments in helping the company to improve their information security. I think this is a positive thing in this business.

A: You mean that as the disclosure policy becomes more transparent, benevolent environment is established, and satisfactory bounties are provided, more hackers are willing to join BBP?

Yes, these are the incentives for hackers to join BBP. In fact, we have observed that in past few years, the bugs price in the black market has soared, which means the bugs are getting harder to purchase. Even if you buy a zero-day (the number of days that the software vendor has known about the bug) successfully, the time you are able to use it are getting shorter. In the past, the zero-day you bought might not be fixed for a year, because no one knows about that bug. But now the bug may be repaired in three months, and I often hear that some researchers' zero-day has expired immediately when they bought it.

Since there are more people shedding light on information security and BBP, the fix rate for bugs are also getting faster than before. Therefore, this trend of bug price in the black market can be observed nowadays. For example, the website Zerodium, which is an online broker for buying loopholes. If you can find zero-days in iOS systems, the price last time I saw was US$1.5 million. Bugs like Android CLICK worth up to US$250 million. Thus, this shows how hard to invade newest version of Android phones. Google have invested a lot of money and effort in doing information security. They are willing to pay any valid bugs reported to them, and they will fix it immediately. Moreover, Zerodium has an open table of multiple kind of zero-days with details on what system or device it can be used. Cloud service on Windows costs US$100 million while antivirus RC costs only $50 thousand. That means antivirus is relatively easy to be found. By seeing this table, you can tell that Android is really putting effort in their system security.

A: Is this website staying in the grey area of the law?

They are not illegal but only a broker. They buy your research results, but you don't know who they will sell to after and for what. In the governments' point of view, they cannot ban the transactions, instead they can control it. You can think of it as a piece of unlocking technology. Your current lock is a very ordinary lock. But for very complex locks, you need special or advance unlocking technology. There are people researching and developing for more unlocking skills, and even selling the tool. However, this can be regulated by the government. These technical materials and tools are regulated, and not everyone can acquire this technology. Zero-day is actually being regulated. It is considered as a weapon now.

The Wassenaar Arrangement is an international agreement that regulated exported weapons to certain countries and region, and Zero-day is also included in the agreement. Country that has no legislation about this means you cannot use a Zero-day, but you can study and exchange it.

7. Why do you think some hackers want to participate in BBP, but some do not?

Most of hackers I know are joining it because they can gain reputation and make money. For the ones that aren't joining, I think they are keeping the bugs for own use, or they have other channels to sell it for higher prices.

8. We have interviewed a company that runs BBP themselves, and they said that the biggest problem is that they need a lot of manpower to read reports. What are your thoughts on this?

I think it is an execution problem. The process of verifying a report is complicated. For example, whether a loophole is “useful” or not is very important. If the loophole I reported can only be triggered once every ten times. Then is that really a loophole? Yes, it is. But it’s not really an “effective” bug for the company, thus the bounty for it may be low. There are lots of cases that the bugs can only be triggered in rare conditions, and these technical difficulties in verification are for both companies and researchers.

Therefore, the policy for the bounty table is getting more precise and detailed to decrease the possibility of having disagreement in payment.

8. You have mentioned the advantages for BBP, then how about the disadvantages?

I cannot think of any right now.

The main concern is that the company must prepare itself fully before doing BBP. After the product or system is developed, you should have a red team (with knowledge of the product) to test the vulnerability first. Once you have done the testing yourself, then you can release it to BBP hackers. This preparation includes the back-end execution for reports, the budget, and the ability to verify and fix the bugs immediately. The communication with R&D department is also important. It’s unacceptable if R&D is only able to fix the bugs six months later.

A: Will some companies worry about financing terrorism because of unknown participants?

I don’t think so. Since those bounties are not much comparing to the salaries paid to full-time professional testers.

A: Some hackers feel that their contributions are being underestimated.

Yes, this is actually a problem currently, which the bounty is not enough. Companies that really value information security will increase their bounty prices, and because critical loopholes are becoming harder to find.

9. What is the difference between company holding their own BBP and having through a third-party platform?

I think the difference lies in the organizational structure. For long-term BBP you must have a marketing team, a verification team, and a repair tracking team. The resource management is no joke. The companies I know that are running their own BBP are international enterprises. Most companies will find a third-party platform to help them handle all or part of those paper works.

If you entrust a third-party platform to handle your BBP, you can actually save a lot of money and save a lot of time in communication and verifying. So, I think this is the biggest difference. This is the value of the third-party platforms.

10. What do you think are the advantages and disadvantages for participating in BBP through a third-party platform,?

I didn't think of any shortcomings. If you are the people who uses the loopholes, of course it is a bad thing since the loopholes have been fixed fairly quickly.

A: Can having BBP on third-party platforms increase the company's reputation and exposure?

Yes. Being able to join the BBP website also means that you are recognised and ready.

Then this can indeed enhance customer trust and image.

11. Do you think hackers can increase mutual trust with the company by participating in BBP through a third-party platform?

Yes.

12. Do you think hackers can gain reputation faster by participating in BBP?

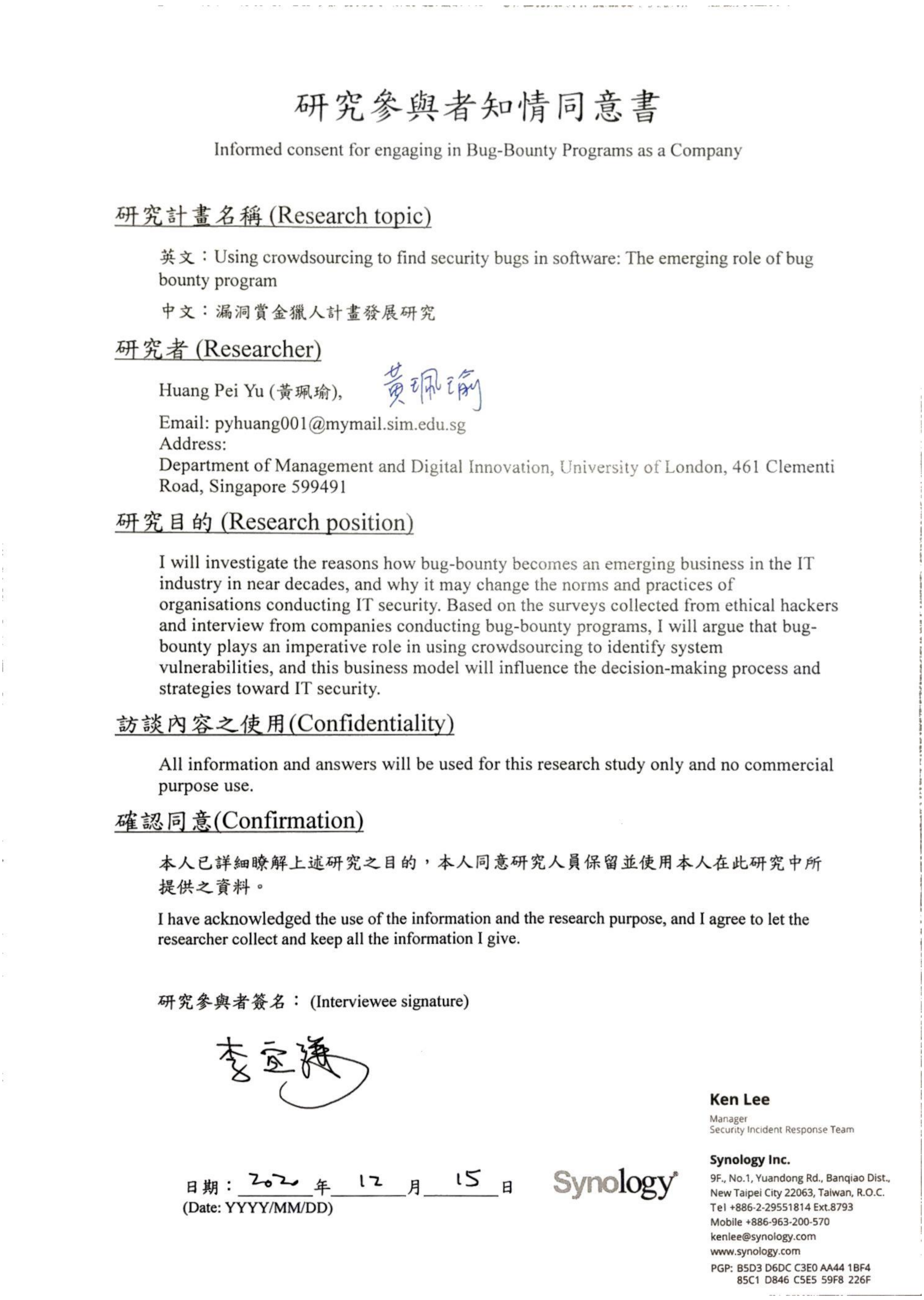
Yes.

13. Do you think BBP is hard for beginners?

I think it depends on people. It may be hard for beginners because of low-hanging bugs are all being fixed already. So, the beginners need to be fast once the program is released.
14. Related reports has pointed out that BBP often results in a lot of unpaid labor in the long run. Do you think this will have a negative impact in the long-term?
This is inevitable. For researchers, it may take a lot of time and find nothing at all. I do know that some companies will invite researchers that has good rankings and reputation to test their private BBP. They will pay them salaries through the whole term, so the researchers will not work for nothing.
15. Do you think BBP can improve company's information security compared to other information security methods?
Yes, but you must be prepared. It's not a pill that can cure anything.
16. Will you recommend other hackers to join BBP?
Yes, and this is one of HITCON's goals.

Interview with Synology. Inc

Consent letter:



研究參與者知情同意書

Informed consent for engaging in Bug-Bounty Programs as a Company

研究計畫名稱 (Research topic)

英文：Using crowdsourcing to find security bugs in software: The emerging role of bug bounty program

中文：漏洞賞金獵人計畫發展研究

研究者 (Researcher)

Huang Pei Yu (黃珮瑜), 黃珮瑜

Email: pyhuang001@mymail.sim.edu.sg
Address:
Department of Management and Digital Innovation, University of London, 461 Clementi Road, Singapore 599491

研究目的 (Research position)

I will investigate the reasons how bug-bounty becomes an emerging business in the IT industry in near decades, and why it may change the norms and practices of organisations conducting IT security. Based on the surveys collected from ethical hackers and interview from companies conducting bug-bounty programs, I will argue that bug-bounty plays an imperative role in using crowdsourcing to identify system vulnerabilities, and this business model will influence the decision-making process and strategies toward IT security.

訪談內容之使用(Confidentiality)

All information and answers will be used for this research study only and no commercial purpose use.

確認同意(Confirmation)

本人已詳細瞭解上述研究之目的，本人同意研究人員保留並使用本人在此研究中所提供之資料。

I have acknowledged the use of the information and the research purpose, and I agree to let the researcher collect and keep all the information I give.

研究參與者簽名： (Interviewee signature)

Ken Lee
Manager
Security Incident Response Team

Synology Inc.
9F., No.1, Yuandong Rd., Banqiao Dist.,
New Taipei City 22063, Taiwan, R.O.C.
Tel +886-2-29551814 Ext.8793
Mobile +886-963-200-570
kenlee@synology.com
www.synology.com
PGP: B5D3 D6DC C3E0 AA44 1BF4
85C1 D846 C5E5 59F8 226F

日期：2020 年 12 月 15 日
(Date: YYYY/MM/DD)

Synology

Interviewee: Ken Lee

Interviewee Designation: Synology Inc. Headquarters, product security manager

Interview Method: face-to-face interview

Date: 15th December 2020

**A* is additional question asked based on interviewee's answers.

1. **Tell us what business Synology Inc. is mainly in?**

Our mission is to centralize data storage and secure network deployment.

2. **How does Synology perform penetration tests to protect system security?**

One of general security controls is internal quality control. We do not use internal quality control since there are no product security assessments and cyber security assessments in internal quality control. It only focuses on testing functions but not finding security flaws or bugs. Therefore, we use BBP to execute low budget rating assessment and vulnerability assessment.

A: BBP is considered low budget to you?

Yes. If you hire a quality control team, you have to pay at least US$100 thousand a year. However, since BBP is result-based, we only pay for valid bugs. Last year we spent US$60 thousand in total on BBP so BBP is low cost for us.

A: How do you test the products?

We only provide hardware for testers that have good cooperate experience with us.

A: Why don't you find security companies that do penetration testing?

We can buy those testing tools ourselves.

3. **Has your company received any letters or messages to report system vulnerabilities in your company? How do you deal with it?**

We have a security email address, which is specially managed by the support team. After we started BBP, we have another email address bugbounty@synology.com. These two are working simultaneously.

In the past, researchers contacted us through security address. But if it is stuck in the customer service, the email will be ignored. The message can be delivered successfully only if our security team receive it. Therefore, an organization basically must have an external channel, and with cyber-security professionals to deal with reports.

A: Would these reporters ask for money?

There was less monetary exchange in the past. Those researchers only wanted to put research results on their websites, and any kind of acknowledge and recognition is enough for them. The disclosure policy is the main purpose for us to have BBP, which is a mutually beneficial between us and researchers. In program holder's point of view, we want to fix the bugs and update our clients' system as soon as possible. Disclosure means that we have bought your reports, and you cannot disclose it unless enough clients have updated the latest version.

4. **Have you thought about using third-party platforms to launch your BBP? What are the advantages and disadvantages?**

We have considered using an intermediate platform, but the cost of "slotting fee" (the fee to launch programs on the website) is too expensive. Last year, we had talked to HackerOne about slotting, but the slotting fee costs US$20 thousand annually, and the cash flow is another 20% calculated separately. For us, self-holding BBP is relatively cheaper.

The main problem for us is taxation. If we consider BBP as labour relations, we don't know the standard taxation of the researcher's country and whether it meets their income requirement since we are simply paying them the bounty. If the researcher is from the same country, we can help them deal with taxation. But we are not sure about the taxation part if they are foreigners.

Then through an intermediary platform, this problem will be solved. That's because we only need to report operating cost, and the remaining risks and responsibilities are handled by the platform.

The more common difficulties are the process making and paperwork, but what really bothers me is the taxation issue.

A: Are those hackers using their legal name?

We don't care whether they are using their real name, or even the bank account is a dummy account. The risk is that we may be financing terrorists' activities, since we don't have any control on participants' identities. This is another task for third-party platforms to handle. If we bought the service from the intermediaries, then they should do the background checks for us.

A: Will HackerOne help you verify technical details of reports?

It depends on what service you buy, the more advanced you buy the more interference they will have. But my question is, will those companies who can afford the slotting fee on HackerOne platform not be able to support in-house penetration testers? The other benefit of third-party platform is credibility and reputation building to the public. The platform discloses transparently how long it takes for a company to process a report and how much bounty has been paid in total. Without the intervention of a third party, no one can verify the numbers.

A: What is the advantage to hold BBP yourself?

Absolute flexibility, flexibility in execution. For example, the flexibility to buy out bugs' information or cover up bad reports.

A: You are not able to do it on intermediaries?

If we do that, it will look weird in the record. It's like cooking the books publicly, since almost any action on the platform leaves a record, and we cannot edit the record freely. Although we can choose to not disclose certain bugs, the record of reporting still exists. Trust issues may arise if some undisclosed reports earned huge bounties.

Therefore, the transparency policy on the platform is a double-edged sword for BBP companies.
5. Does BBP make you find bugs more efficiently?
Definitely. Because no one in the company was doing security testing in the past.
6. After adopting BBP, how accurate is the bugs found?
The bugs on website are easier to find so bounty for websites are lower compared to products. Therefore, the spam rate for websites are also higher and inevitable. The reports for products are often more valuable.
7. How does your company determine the bounties?
Based on heuristics or look at how HackerOne pays. Since the person in charge is me, I would talk to product managers about the maximum payment for a single case. For example, per bug for operating system is maximum US$10 thousand, application is $5 thousand, and website is around $2 thousand. The final decisions like severity ratings are based on my heuristics.
8. After adopting BBP, has the communication cost between your company and hackers reduced?

The cost of communication is quite high. I oversaw front line responding in the past, but now my boss assigned the work to product manager. Since product manager is not a technical position. They don't quite understand what BBP is, and the message delivered to us may not be accurate and precise. The difference in communication or understanding of technical terms increases the cost of communication. We still cannot solve this problem yet.

A: Can a third-party platform solve this issue?

If you're talking about HackerOne, then it depends on what service you buy from them. They can send in technical staffs to help with front line submissions, and this makes communication process smoother.

A: What if the bugs found are too many?

We expect bugs convergence to happen, thus after convergence, we won't be paying the same amount of bounty anymore.

9. **After adopting BBP, how can your company prevent the bugs discovered from being concealed or abused?**

Then the disclosure policy should be clear and strict. We would refuse to pay if anything went wrong before payment.

10. **How do you keep and maintain the mutual trust between your company and hackers?**

We do regular meetings or community forums. Let researchers know that we are not just a company paying money but also people doing research. I also bridge the gap between conservative supervisors and researchers for letting external people know what we are requesting and rejecting, and the supervisors know what external people are providing.

A: Will hackers worry about their reports being ignored?

If we did not pay you the money for the report, that means we are not disclosing this information. Paying bounties means that we are buying the time to fix the bugs, and if you did not get our response after 14 days then you can do anything with that bug. So hackers should also make concessions to the disclosure policy. Most of the hackers want Common Vulnerabilities and Exposures (CVE) as rewards, and it sometimes is more important than bounties.

11. After adopting BBP, is it effective as initially expected?

Yes.

12. What are the advantages and disadvantages of BBP?

The paperwork and strategy planning are not easy for small companies. Paperwork such as security/disclosure policy setting, the qualification to give CVE, and internal structure that communicates well.

13. Do you recommend other companies to have BBP?

I do recommend, but you need to get the support of high-level supervisors.

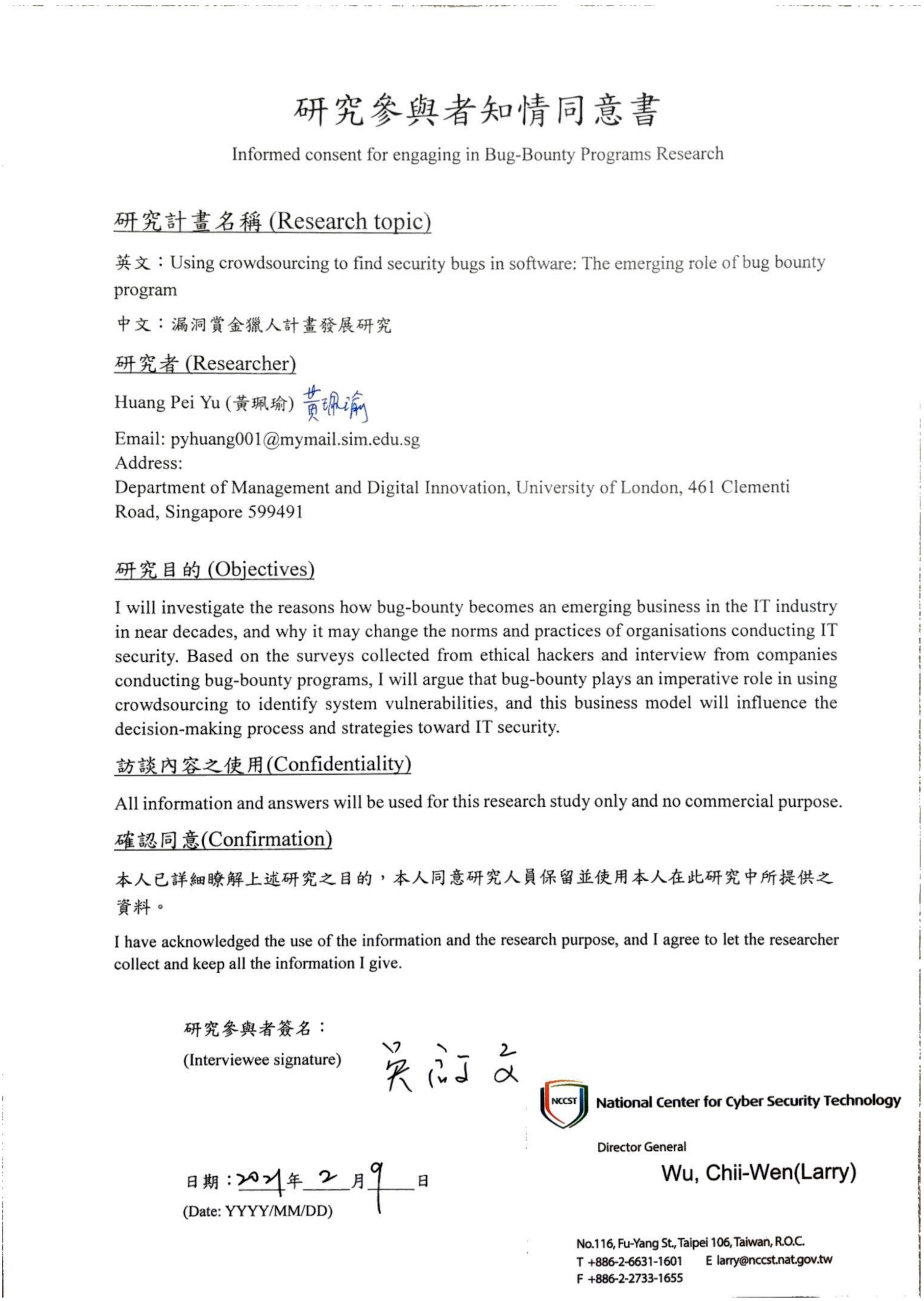
The ability to have a professional team to read reports is really critical for having BBP. Third-party platforms may be ineffective if they don't understand your product, which means they cannot fully deliver and translate the information for you. Although the terminology they used is correct, the detailed product features are still going to be inaccurate. We have a team in charge of reading reports, and this hugely affects the quality and rating consistency. These are all service quality to researchers and image building to the public, thus are important and difficult for company.

14. Do you want to continue to use BBP?

Definitely. It costs less.

Interview with NCCST

Consent letter:



研究參與者知情同意書

Informed consent for engaging in Bug-Bounty Programs Research

研究計畫名稱 (Research topic)

英文：Using crowdsourcing to find security bugs in software: The emerging role of bug bounty program

中文：漏洞賞金獵人計畫發展研究

研究者 (Researcher)

Huang Pei Yu (黃珮瑜) 黃珮瑜

Email: pyhuang001@mymail.sim.edu.sg
Address:
Department of Management and Digital Innovation, University of London, 461 Clementi Road, Singapore 599491

研究目的 (Objectives)

I will investigate the reasons how bug-bounty becomes an emerging business in the IT industry in near decades, and why it may change the norms and practices of organisations conducting IT security. Based on the surveys collected from ethical hackers and interview from companies conducting bug-bounty programs, I will argue that bug-bounty plays an imperative role in using crowdsourcing to identify system vulnerabilities, and this business model will influence the decision-making process and strategies toward IT security.

訪談內容之使用(Confidentiality)

All information and answers will be used for this research study only and no commercial purpose.

確認同意(Confirmation)

本人已詳細瞭解上述研究之目的，本人同意研究人員保留並使用本人在此研究中所提供之資料。

I have acknowledged the use of the information and the research purpose, and I agree to let the researcher collect and keep all the information I give.

研究參與者簽名：
(Interviewee signature) 吳啟文

NCCST National Center for Cyber Security Technology

Director General

Wu, Chii-Wen(Larry)

日期：2021年 2 月 9 日
(Date: YYYY/MM/DD)

No.116, Fu-Yang St., Taipei 106, Taiwan, R.O.C.
T +886-2-6631-1601 E larry@nccst.nat.gov.tw
F +886-2-2733-1655

Interviewee: Larry, Wu

Interviewee Designation: National Center for Cyber Security Technology (NCCST), Director General

Interview Method: face-to-face interview

Date: 9th February 2021

**A* is additional question asked based on interviewee's answers.

1. Tell us about your experience in NCCST, and what are you in charge of?

I was in Research, Development and Evaluation Commission (RDEC) in 1995 and I oversaw the business with NCCST. Then, I transferred to NCCST in few years later. Our mission in NCCST is to provide technical supports for central government to enhance cyber security protection, including prior-incident security protection, during-incident early warning and responses, and post-incident recoveries and forensics. Our institute are gaining more attention from the government and has become more visible in public eye. We are planning to expand our cyber security assessment services to the whole nation. In order to achieve this, we have established serval sharing platforms such as: National- Information Sharing and Analysis Center (N-ISAC), National- Computer Emergency Response Team (N-CERT), and National-Security Operation Center (N-SOC). These platforms are all maintain and operate by NCCST.

2. Tell us how government institutes address to cyber security issues?

We have divided our business in multiple areas. As previous mentioned, we take in charge of the government cyber security affairs, and we are integrating the channels to achieve the vision of a safe and reliable digital nation. We use a standardised language called STIX, (Structured Threat Information eXpression), which is a standardised format for transforming security information. These transforming processes are all automatically operated. For example, N-ISAC is able to share and deal with the information with other institutes in real time. Whenever there are cyber security related issues happen, every institute and related companies can react to it quickly and act in protection. Last year in May, CPC cooperation was attacked by the ransomware virus. We contacted them to share their Indicators of compromise (IOCs) with us, which is the blacklist and overall strategic information. Therefore, by combining and connecting this information from the victim company to security companies and related industry, we can prevent the damage from spreading.

We have the Information Security Law, which is regulating one type of institute in the early days, and now it is slowly implemented in other public institutes. There are two main requirements. One is that you must do a self-maintenance plan. The other is prescribed procedures for the response of information communication security. In fact, the maintenance plan in this section is somewhat like the ISO27001 system. We first classify the institutes into five levels: A, B, C, D, and E. The higher the level, the stricter the to-do list is. We will require A and B-level institutes to implement EDR (Endpoint Detection and Response). If these requirements are met, they must submit security strategy plans. We will depend on the actual situation. Generally, we will check whether he has complied with the regulations through an audit.

Therefore, the current information security law is relatively strict, unlike in the past, the information security incidents were not reported because of the fear of losing reputation. Now there are penalties for not reporting the incidents.

3. Is the government implementing BBP? What are the actual practices and ideas? It's been reported that the government is considering using BBP on digital ID card (NewID)?

Yes, the government have mentioned the idea of using BBP for NewID. However, to be honest, we haven't seen this thing happening so far.

The National Development Council were pushing the idea of digital government or smart government in the early days. From the concept of big data to open data and now Mydata. Mydata means customisation. The implementation of NewID was being challenged, and the main worries were about the variety of data it can access. For example, through NewID, citizens can search for their own private bank information. It feels convenient from the user's point of view, but it is relatively risky from the information security point of view.

We know that there is a BBP as a method for cyber security, but it is not yet specific about which related areas to use in the government. In fact, earning trust from the people is the core for government when implementing anything new. The public will not trust us completely if we said we are doing BBP by opening channels to let outsiders test whether there are loopholes in the NewID system.

Not to mention, information security laws have requirements for government's systems. Once the system is developed, it must be scanned looking for weaknesses and do penetration testing before it can be launched. These assessments are tested by a third-party agency, and this is different from BBP. BBP is a testing program open to outsiders, which is uncertain and risky in government's point of view. We have done surveys in the attitude of pushing such a mechanism, but still, we haven't considered to do BBP in our present and near future. I have only seen cases among private enterprises.

A: If you decide whether to use BBP or not, what factors will be considered?

The current nature of the government is mainly because of the law, it requires the information system to be tested before released. It not that easy to set a new strategy and change the usual way of doing security assessments. I think BBP are seen common in the organisations that are constantly involved and interacting with the public. The communication process with the public is important and letting them trust and understand BBP is the key.

4. How did you deal with the letters informing the vulnerabilities in government systems or websites? Is there a channel to deal with it?

There are two types of hackers I've encountered, one is for money, for example, attackers using ransomware viruses. The other is keeping quiet about the bugs and aim for stealing the data. Most of them is doing Advanced persistent threat (APT) attack, or some will send phishing emails. Once the fake links are being clicked, they can create a route to the system and steal valuable data.

A: So, you have not encountered ethical hackers that inform you vulnerabilities in a good faith?

I would say rarely, or most of them do inform you the bugs but they want money for providing more detailed information, otherwise they would disclose it. Therefore, we don't rely on external researchers to inform us. It is more common for us to do the assessments ourselves. Once we found problems in the product, IP cameras, printers, and mitres, we will inform it to the manufacturer and let them revise it within a time limit. On the other hand, we do regular offensive and defensive drills for system assessments every year. A group of researchers from Ministry of National Defense, Ministry of Justice Investigation Bureau, Criminal Investigation Bureau, and students from security laboratory will attack the systems and websites in the attack laboratory. All attacks are authorised. That's is to say, any cyber-attacks without authorised is illegal. That is the reason why it's controversial for those hackers informing us the bugs, since not only their actions are illegal but also most of them are asking for money and would disclose the information if you ignore them.

A: Can I also say that's because the lack of a benevolent environment for BBP so you cannot do anything when receiving these kinds of reports?

Yes, so most of the researchers in Taiwan contribute their skills to those international BBP. They can earn bounties in a legal way. I think those international companies have a more complete mechanism in responding to the reports.

5. What do you think are BBP's advantages and disadvantages, and what's the difficulties in implementation?

The positive side is that it is operating on an open platform, so the testing process is transparent, but not like some companies keep the process in-house.

For the negative side, the main concerns for government are the risks for finding someone unknown to test your system and whether these hackers will conceal the bugs they found. Especially, because of the sensitive political relationships between Taiwan and China, we cannot afford the risk of inviting unknown or external hackers to test governmental systems. Government has an enormous amount of people’s data; every information security incident and breach will be reviewed by the Investigation Bureau and the public. It will be tricky if any incidents happened.

6. The company I have interviewed mentioned that one of the difficulties in holding a BBP is to deal with the taxation of paying foreign hackers, and they have concerns about funding terrorists (because of unknown participants). What are your thoughts on this?

If the government are going to use BBP, then the regulations should be detailed and stringent. Background check is a must for government BBP, however, by doing this we may lost some elites and top skilled hackers.

7. How do you usually build the foundation of trust with hackers to prevent discovered vulnerabilities from not being reported or even being abused?

When we do drills, we will track the penetration test activities and keep all the records. All tests are carried out in the attack laboratory to prevent any suspicious behaviour, and a confidentiality agreement must be signed. In fact, it is also a good way to train our technical staffs when we do test in-house.

8. Do you think that using BBP can effectively improve the information security for government departments?

The government mainly needs to gain the trust of the people and comply with the laws and regulations for testing. I believe that BBP have a positive effect on cyber security; however, by viewing these effects we are yet convinced to try BBP.

9. Would you recommend government departments to use or continue to use BBP?

I will not recommend implementing it in a full-scale, but I will not disagree using it for individual cases.

Appendix VI: Project Summary

Please fill it this document and resubmit it via the VLE at the same time as you submit your final project. It is a basic Microsoft word table. Boxes will expand as you type and where you are asked a "yes"/"no" question please type "X" next to the appropriate answer. Please do not exceed the maximum word count indicated in the various sections

SECTION 1: CANDIDATE DETAILS	FILL IN THIS COLUMN
Name	Huang Pei Yu
Student number	180329021
Project Title	Using crowdsourcing to find security bugs: The emerging role of bug- bounty program
Word Count (excluding Appendices)	9065 (excluding references)
Date	01/05/2021

SECTION 2: PROJECT SUMMARY	FILL IN THIS COLUMN
Brief description of the topic (50 words)	Determine and analyse the key factors that how bug-bounty business works, and how end-users think about it. Questionnaire and interviews were conducted to understand end-users' attitude on having or joining bug-bounty programs. This study also analyses on the advantages and disadvantages of bug-bounty programs.
Central Research Question (20 words) *Make sure it is a question, with a potential for an answer.*	How does bug-bounty programs change the norms and practices of security protection when organisations adopt it?
Original Research Objectives (100 words)	In this research, I will investigate the reasons how bug-bounty becomes an emerging business in the IT industry. I will argue that bug-bounty plays an imperative role in using crowded-source between its companies and hackers', and this business model will

	influence the decision-making process and strategies toward IT security.
Revised research objectives (and why revised) (100 words)	In this research, I will investigate the reasons why the end-users of bug-bounty programs keep joining and decide to join it. Aren't companies concern about the identity of the hackers? And why are hackers contributing their works to the company but not sell it to black market? This study would also research on the advantages and disadvantages of bug-bounty programs. The original idea was revised since the concepts were too broad and difficult even for people in the industry to answer.
Four Keywords to describe the project	Bug-bounty programs, BBPs, Ethical hackers, Crowdsourcing, Information security

SECTION 3: ANALYTICAL FRAMEWORK CHECKLIST	FILL IN THIS COLUMN			
Does your report contain a clearly expressed research question?	YES	✓	NO	
Does your report contain a review of relevant and up-to-date literature?	YES	✓	NO	
Does your report include a clearly expressed analytical framework (e.g. chosen theory, set of concepts, ways of data analysis etc.)	YES	✓	NO	
Briefly describe the framework you are using (50 words)	TAM is a useful and rather simple model for explaining users' intention and attitude in the acceptance of technology. It provides a guideline on how a user may be affected by the elements in it, and how the elements influence each other.			

SECTION 4: PRIMARY DATA COLLECTION TECHNIQUES CHECKLIST (select as appropriate)

Questionnaire	Questions derived from a theoretical framework	✓	Piloted?	✓	Data analysed (more than described)?	✓
Interviews	Interview themes given?	✓	Interviews coded?	✓	Interviews analysed?	✓
Observation	What type?	×	Participant	×	Non-Participant	×
	Methods of Analysis Used	×				
Documents	What type?	×				
	Analysis technique used	×				
Other (give brief description)	The questionnaire was conducted through online.					

SECTION 5: ETHICAL REVIEW	FILL IN THIS COLUMN			
Have all participants been told the purpose of the research and asked to consent to participate?	YES	✓	NO	
Does your research involve children or other potentially vulnerable persons?	YES		NO	✓
Does your research collect data that may be seen as sensitive or private by research participants?	YES		NO	✓
Does your research include any aspect that could be seen as deception or coercion?	YES		NO	✓
Are there any groups who may be harmed by dissemination of the results of your research?	YES		NO	✓
Does your research raise any other significant ethical concerns?	YES		NO	✓

If you have answered YES to any of these questions describe briefly what action you have taken in response. (100 words)	All participants for questionnaire and interviews are aware of the topic and where are their responses being used and used in research purposed.

SECTION 6: FINDINGS AND ANALYSIS CHECKLIST	FILL IN THIS COLUMN			
Does your report clearly express the findings from your project and relate them to an identified Information Systems theme?	YES	✓	NO	
What is the Information Systems theme your work addresses? (50 words)	Bug-bounty programs are a method for organisations to improve their information security whether on their website, systems, or products.			
What kind of a contribution do you make in this area? Who would be interested in reading your work and making use of your findings? (100 words)	Many researches have studies on this topic; however, most of them focuses on the technical or management parts of the topic. This study is based on those researches but with multiple perspectives of end-users' feedback. Security companies, security researchers, bug-bounty programs companies, and security managers would find the feedbacks and analysis useful to them.			

SECTION 7: PRESENTATION CHECKLIST	FILL IN THIS COLUMN			
Is your report printed to the guidelines given in the subject guide?	YES	✓	NO	
Does your conclusion chapter contain the essential insights of your work?	YES	✓	NO	
Are all quotations and material taken from other works properly presented and fully acknowledged?	YES	✓	NO	
Are all your references to books, articles and websites in a full and proper format (author, title,	YES	✓	NO	

publisher, date etc.) and presented in the bibliography?				

SECTION 8: SUBMISSION CHECKLIST	FILL IN THIS COLUMN			
Have you included the Topic Area Proposal and a Project Specification as the first two appendices of your written report?	YES	✓	NO	
Have you completed and signed the submission cover sheet?	YES	✓	NO	
Have you prepared a file of your project report for uploading?	YES	✓	NO	

SECTION 9: Personal reflections FILL IN THIS BOX
Working on this topic is challenging and interesting for me. I was not familiar with designing a questionnaire. It would be difficult to ask reasonable and meaningful questions if not understanding the topic well. Some of my questions are poorly asked and therefore were deleted after doing Cronbach's alpha. I also learnt the importance of deciding framework to use for the whole project. Since my questionnaire questions were designed based on my framework, insufficient understandings on the topic leads to poor questions and leads to ineffective survey responses, and then leads to poor analysis. Therefore, I have spent extra time on evaluating the results. Other reflections would be to change the way I distribute my questionnaire. Because the topic of bug-bounty programs is not really common to general public, I have a hard time finding sufficient number of respondents. Even I have contacted them, through social media messaging was mostly ended up being blocked or ignored. I have also learnt to organise large amount of data and context; Since the interviews were mostly conducted nearly 1 hour, the information in each transcript is enormous. I needed to collect useful information and eliminate unrelated context.

-END-