Vulnerability Discovery for All: Experiences of Marginalization in Vulnerability Discovery

Kelsey R. Fulton*, Samantha Katcher†, Kevin Song‡,
Marshini Chetty‡, Michelle L. Mazurek*, Chloé Messdaghi§, Daniel Votipka†
* University of Maryland, †Tufts University, ‡University of Chicago, §Impactive Consulting

2023 IEEE Symposium on Security and Privacy (SP) | 978-1-6654-9336-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/SP46215.2023.10179478

Abstract—**Vulnerability discovery is an essential aspect of software security. Currently, the demand for security experts significantly exceeds the available vulnerability discovery workforce. Further, the existing vulnerability discovery workforce is highly homogeneous, dominated by white and Asian men. As such, one promising avenue for increasing the capacity of the vulnerability discovery community is through recruitment and retention from a broader population. Although significant prior research has explored the challenges of equity and inclusion in computing broadly, the competitive and frequently self-taught nature of vulnerability discovery work may create new variations on these challenges. This paper reports on a semi-structured interview study (N = 16) investigating how people from marginalized populations come to participate in vulnerability discovery, whether they feel welcomed by the vulnerability discovery community, and what challenges they face when joining the vulnerability discovery community. We find that members of marginalized populations face some unique challenges, while other challenges common in vulnerability discovery are exacerbated by marginalization.**

I. Introduction

As organizational reliance on technology — and incidence of cyberattacks from both criminal and nation-state attackers — continues to increase, so does demand for security review, intended to ensure early identification and mitigation of vulnerabilities. The White House's recent executive order on Improving the Nation's Cybersecurity, which emphasizes "modernizing federal government cybersecurity" and "enhancing software supply chain security" as priorities, highlights the need for improved vulnerability discovery capabilities [1].

To scale up vulnerability review, organizations adopt a variety of approaches, including review by internal security experts, hiring penetration testers, and offering bounties — in money, swag, or recognition — for responsible vulnerability disclosure [2], [3]. For simplicity, we refer to people working in any of these roles generally as the vulnerability discovery workforce and vulnerability discovery community, and individually as hackers.

Unfortunately, while the number of hackers has grown, the diversity of the vulnerability discovery workforce remains limited. In a survey of 3,493 hackers on their platform, Bugcrowd found they were almost all male (94%) and white or Asian [1] (90%), with few participants self-reporting as female (6%), Latinx (3%), or African American (3%) [4]. This is a common trend in hacker surveys [5]. Additionally, the vulnerability reports produced by the vulnerability discovery community are typically dominated by a few highly-active participants [6]–[9], meaning that in practice there is very limited diversity of perspectives in security reviews. Further, a recent hacker survey by Synack found participants from marginalized populations were less likely to feel they belong in the vulnerability discovery workforce [10], indicating there are challenges for members of marginalized populations not only in joining the vulnerability discovery workforce, but also in remaining active participants.

This lack of diversity indicates an equity problem: limited opportunities for people from marginalized populations to participate in bug bounties and/or to transition into potentially lucrative, in-demand careers in information security more broadly. The lack of diversity is also a problem for vulnerability discovery as a field: many eyes with varied perspectives are necessary to avoid blindspots and discover as many potential vulnerabilities as possible before a malicious party does [11]. With the U.S. government sponsoring initiatives to close workforce shortfalls [12], it is essential to better understand barriers to entry and continued participation faced by marginalized security experts in order to improve recruitment and retention and avoid further entrenching current demographic disparities.

Of course, struggles to diversify the workforce are not unique to vulnerability discovery; this is a long-running challenge facing science, technology, engineering, and mathematics (STEM) disciplines in general [13] and computer science in particular [14]. There has been significant effort to understand [15]–[17] and mitigate [18]–[20] barriers to entry into these fields. However, we expect that some characteristics of vulnerability discovery will lead to unique instantiations of these common challenges, making it worthwhile to study separately. The inherently competitive nature of vulnerability discovery (i.e., only the first person to identify a vulnerability is rewarded) is likely to dissuade newcomers, potentially reifying existing inequalities [13], [14], [21]–[23]. On the other hand, hackers can maintain anonymity — pseudonymously reporting vulnerabilities through bug bounty programs and participating in online discussion forums — and many useful resources (e.g., vulnerability write-ups, online wargames and capture the flag competitions (CTFs)) are freely available to the public. This theoretically could lower barriers to entry for marginalized populations.

To date, however, there is limited understanding of how these challenges play out specifically in security [24], and

[1] We define Asian broadly, as Bugcrowd did, but we recognize Asian-Americans remain marginalized in the vulnerability discovery community

DOI 10.1109/SP46215.2023.00017

particularly in the unique vulnerability discovery environment [10]. Existing research in this area has primarily measured security-education participation [25]–[27].

As a first step to address this gap in the literature, we conducted 16 semi-structured interviews with members of the vulnerability discovery community from marginalized populations. We asked participants to describe their work and personal identity and then walk us through their career in vulnerability discovery. During this walkthrough, we asked them to describe resources they used (both helpful and unhelpful), mentors they had, and their interactions within the vulnerability discovery community. Through these interviews, we aimed to answer three main research questions:

RQ1: How do people from marginalized populations come to participate in vulnerability discovery?

RQ2: Do people from marginalized populations feel accepted and supported by the broader vulnerability discovery community?

RQ3: What challenges do people from marginalized populations face in becoming a vulnerability researcher and participating in the workforce?

We find that most of our participants found the field on their own and learned about it using primarily unstructured resources, independently and outside of work hours. While our participants considered mentors critical to navigating this learning process and making community connections, many reported that without a pre-existing job in vulnerability discovery, mentors can be difficult to find.

Participants felt more welcome in the community when they saw diverse representation, including but not limited to people who shared their identity, and less welcome when they did not feel they fit in. To navigate this challenge, many choose to remain anonymous as much as possible, specifically to conceal minoritized aspects of their identities.

While not all of the challenges our participants faced were unique to members of marginalized populations, most were exacerbated by minority status and structural disadvantages (e.g., gender wage gaps). Further, we identified some challenges unique to people from marginalized groups, often related to discrimination and impostor syndrome.

Drawing from our findings, we offer recommendations for lowering barriers to entry and cultivating a more inclusive environment.

II. Background and Related Work

We define the vulnerability discovery community as body of security experts who specialize in scrutinizing software for security flaws, whether as part of a company's internal security team, contracted penetration testing, or external bug hunting. As more companies have established bug bounty programs, providing a vehicle for responsible vulnerability disclosure, the community has also grown and developed. In this section, we discuss general characteristics of vulnerability discovery and the community. We also describe related work that has investigated community dynamics, challenges faced by security experts, and challenges marginalized populations face in other STEM fields.

Vulnerability discovery is competitive and uncertain. Inherently, vulnerability disclosure is a competitive endeavor [28]. Vulnerabilities can only be reported to the software developer once. After a patch for the vulnerability is released, it is no longer viable. In the context of a bug bounty program, this means only one security expert will receive payment for their report even if others might find the same bug and report shortly after. This introduces uncertainty for any security expert investigating a program. They may find a vulnerability, but be "scooped" by an earlier report, meaning all their time and effort was wasted. A security expert's uncertainty is further compounded by the fact that there is no guarantee any vulnerability exists in the program under investigation.

The vulnerability discovery community shares resources for self-driven learning. Because of the competitiveness and uncertainty of the work, we might expect security experts to avoid sharing any information for fear it would limit an advantage. However, this is not the case. Instead, prior work has found that the community actively shares open source tools, answers questions on Q&A forums [29], and publishes thorough bug reports [30]. The vulnerability discovery community also provides a wide variety of educational exercises to students free of charge in the form of CTF challenges, wargames, and vulnerable virtual machines [31]. Of note, these resources are typically designed to support independent, self-driven learning and are not organized into any overarching course or educational thread, a common structure in hacking education since the beginning of the art [32]. This independent structure matches the typical mode of vulnerability discovery work where security experts are primarily alone searching for vulnerabilities in code [33].

A. Market behaviors in vulnerability discovery

To better understand participation and skill progression generally in the vulnerability discovery community, several papers have analyzed the behaviors of security experts in bug bounty markets [9], [34]–[39]. In each paper, the authors consider the bounty programs security experts report vulnerabilities to identify trends in the pool of participants, strategies for considering different programs, and other patterns in their behavior that might suggest motivations. Our work differs as we speak with security experts directly to understand the motivations and history behind their participation in vulnerability discovery. We also focus specifically on marginalized populations.

B. Surveys of participation and motivation

Other work has leveraged surveys to produce a broad view of the makeup and motivation of the vulnerability discovery community. At a high-level HackerOne [8] and Bugcrowd [40], two of the largest bug bounty-as-a-service platforms, perform an annual survey of security experts who contribute to their platform. These surveys collect participant demographics and general motivations for being a member of the vulnerability discovery community (e.g., money, education, challenge). These surveys have shown the limited diversity of the vulnerability discovery community, but do not provide necessary detail to indicate specific barriers for marginalized populations.

In a recent survey by Akgul et al., the authors perform a deeper analysis by asking 56 participants to indicate their motivations for participating in bug bounty programs and challenges they face [41]. Our research differs from Akgul et al.'s as they focus specifically on the decision of which programs to investigate, while we consider general community participation. Additionally, Akgul et al. consider the general security expert population and do not compare the responses between demographic groups.

Perhaps the most similar study to ours in this category is SynAck's Cybersecurity Diversity and Inclusion report [10]. In this short, informal survey, 300 participants were asked about feelings of belonging in the community and challenges faced in entry and participation. This survey showed marginalized populations were significantly more likely to feel excluded from the vulnerability discovery community and more likely to believe there was a glass ceiling on their success. Our work investigates these results in detail to understand why these feeling of otherness exist in marginalized populations and identify specific challenges faced.

C. Interviews with security experts about development and culture

Most related to our research are two hacker interview studies. First are Turkle's ethnographic studies of early hacker culture at the Massachusetts Institute of Technology in the 1980s [32, pg. 183–218]. Turkle observed how security experts in this community operated together and how new individuals joined the community. She found an insular culture of perceived differentness in this community that required others to demonstrate their worth and fit prior to joining the group. The world and vulnerability discovery itself has changed dramatically since Turkle's work. The Internet is now an integral part of many people's daily lives and vulnerability discovery itself has become more accessible and acceptable through the ever-growing adoption of bug bounty programs, possibly altering the counter-culture and insular ethos of this community. Our work investigates the impact of these changes in modern vulnerability discovery with a focus on marginalized populations.

Our work is also related to Votipka et al.'s interviews with software testers and security experts about their vulnerability discovery processes [30]. Specifically, Votipka et al. also consider the way security experts develop skills necessary to perform vulnerability discovery. However, they focus on these questions in the context of the skills necessary to complete particular tasks, whereas we ask about development in the context of career progress and focus on the challenges faced by marginalized populations.

D. Marginalized populations in STEM

Finally, while there is limited work considering challenges facing marginalized populations in vulnerability discovery, there has been several studies focused on other STEM fields [13]–[20]. Perhaps most famous is Margolis et al.'s ethnographic studies of the gender gap in CS, which found that woman had less coding experience than men in undergraduate CS programs, women did not want to be perceived as "geeks", and in 1999 only 15-20% of CS students were women [42]. As another example, Ko examined young adults' attitudes about technology and their journey of forming self-efficacy in computer careers through autobiographical essays [43]. This work highlighted the importance of accessible first encounters with technology. Our work builds on these prior results and focuses on the specific nuances of marginalized populations experiences in the competitive, isolated, and anonymity enabling vulnerability discovery community.

III. Method

To understand the experiences of marginalized populations in vulnerability discovery, we conducted semi-structured interviews with members from the vulnerability discovery community who also identified themselves as members of marginalized populations. In this section, we detail our recruitment, our interview protocol, our data analysis approach, ethical considerations, and limitations.

We note that our research team includes a vulnerability discovery expert who identifies as a member of a marginalized population and who is a leader in several groups promoting inclusivity and diversity in vulnerability discovery. This team member contributed key insights drawn from her knowledge and experience to the design of the study, in particular helping to ensure that we focused on the real needs of marginalized populations in the community.[2]

A. Recruitment

To recruit participants, we worked with leaders from multiple vulnerability discovery organizations and advertised the study on public (i.e., Twitter and LinkedIn) and private (e.g., Slack channels, Whatsapp groups) forums. First, we contacted the leadership of organizations that support marginalized populations in the vulnerability discovery community and bug bounty-as-a-service companies asking them to share the study details with their members. We also posted details of the study publicly on Twitter and LinkedIn and asked vulnerability discovery community leaders to promote our advertisement. Finally, several leaders of organizations supporting marginalized populations in vulnerability discovery shared our advertisement in private channels dedicated to marginalized populations, beyond their own organizations. In each advertisement, members of marginalized populations were asked to consider participating in an hour-long interview study. Those who were interested were directed to a pre-screening survey.

[2] While including members of the community being studied on the research team is not in itself sufficient to avoid harm, it is generally considered a best practice [44].

After consenting to the survey, participants answered questions about their participation in different vulnerability discovery and security groups, experiences with the vulnerability discovery community, and various demographics questions. The survey concluded by asking if participants would like to be part of our interview study, and, if so, asked for contact information in the form of an email address or Twitter handle.

From those responses, we contacted participants who indicated interest and self-identified as being a member of a marginalized population. We kept recruitment general to allow for a variety of perspectives and to reach as many community members as possible. We allowed participants to be from the United States, Canada, and Europe, as these vulnerability discovery communities typically have a lot of resources. We expect our results to generalize in part to communities in other regions, since these regions are currently the drivers of the vulnerability discovery market, but future work should expand to broader populations. To ensure potential participants were a member of the vulnerability discovery community, we asked them to send us either a resume or a link to a personal page such as LinkedIn or a personal website that indicated their credentials.

We interviewed participants until we stopped hearing substantially new ideas, resulting in a total of 16 participants [45]. This approach was validated when no new codes were created when analyzing the final 5 participants. This sample size aligns with qualitative best practices [46].

B. Interview Protocol

Between January and June 2021, we conducted 16 virtual, semi-structured interviews over various telecommunication platforms. Each session lasted about an hour. Four team members participated in the interviews. Most interviews were attended by two team members, with one asking questions and the second taking notes. To maintain consistency, only two team members asked questions, and we conducted intensive discussion and observation to ensure consistency between those two team members.

Our consent form asked permission to record audio and explicitly informed participants that we might send audio to a third party for transcription. Participants were given the consent form the morning of the day of their interview to ensure they had sufficient time to review it before the interview. Before we started the interview, participants were given plenty of time to ask questions about the consent form and the study. We confirmed with each participant that consented if it was okay for us to start recording. All interviews but one were audio recorded, with permission. One participant did not want their audio recorded, so a second team member took detailed notes while the first team member conducted the interview.

Each member of the vulnerability discovery community has a unique background, support system, personality, and intrinsic motivation, which may affect the different challenges they face and the way they respond. Because these relationships are complex and not every factor is likely to be front-of-mind for participants when discussing their development, we utilized Social Cognitive Career Theory (SCCT) as a framing structure for designing interview questions to ensure relevant concept elicitation. SCCT, which is built on Social Cognitive Theory (SCT), considers the psychological and social mechanisms driving career development [47], [48]. Specifically, SCCT was designed to study reasons for underrepresentation of particular marginalized populations in professional fields (e.g., STEM). After first using SCT to attempt to investigate these differences [49], Lent, Brown, and Hackett created SCCT by incorporating several additional personal and environmental variables [47]. Since its inception, SCCT has been one of the predominant frames used to investigate racial-ethnic and gendered career disparities in STEM [50], in contexts including middle and high school [51], [52], college [53], [54], and the workforce [55], [56]. SCCT identifies the key factors that impact career progression, and in this paper we explore how these factors manifest specifically for vulnerability discovery.

Specifically, SCCT considers the interplay of personal and contextual factors during three phases of career development: (1) initial vocational interest; (2) selection of a relevant career path, and; (3) the pursuance of academic and occupational ventures [47]. Figure 1 presents the conceptual model for SCCT. According to SCCT, self-efficacy and outcome expectations play a central role in the career development process, with self-efficacy influencing individuals' perception of different outcomes. These two factors are directly affected by the learning experiences individuals participate in and in turn affect their interests, goals, and future actions (e.g., opportunities to pursue and whether to persist in a particular career field). Also, SCCT views learning experiences as directly determined by background affordances (e.g., access to computer security courses in high school or college) and related personal antecedents like gender and race/ethnicity. Finally, SCCT acknowledges that these personal antecedents can also operate throughout career development as environmental supports and barriers directly influencing goals and persistence.

In this paper, we operationalize the SCCT model by adapting Barron's learning pathway tracing method, which asks participants to recount the stages of their development and probes particular aspects of their motivation and environment [57]. Barron developed this method to identify learning environment differences among diverse STEM students. In our modified approach, we ask participants to sequentially recount the stages of their career development and elicit concrete examples of each element in the SCCT model at each stage. That is, we first ask participants to describe the first time they were interested in vulnerability discovery and iteratively discuss stages of their development, describing how they moved from one stage to the next. At each step, we ask questions about the following items:

- Learning experiences: Any experiences (academic or occupational) through which they learned about vulnerability discovery. These could include active participation or observation.
- Environment: Initial background affordances, support structures developed throughout their career, learning re-

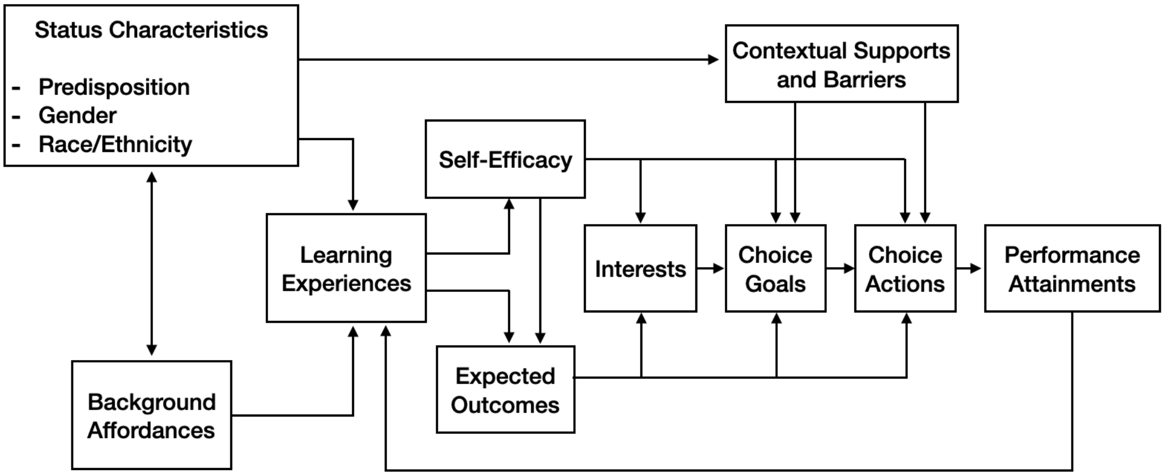

Fig. 1: The Social Cognitive Career Theory conceptual model proposed by Lent et al. [47].

sources they utilized, general hacker community support, and barriers to participation.

- Self-Efficacy: How well they believed they could perform vulnerability discovery tasks.
- Goals and expectations: What their career goals were at the time and how they believed a particular step in their development process would help them progress toward that goal.

The full interview protocol can be seen in Appendix A.

We piloted the interview protocol with four participants to ensure it elicited the desired information. Based on the pilot interviews, we implemented a few changes such as adding clarity to questions about group membership and using terminology more familiar to security experts.

C. Data Analysis

Once interviews were complete, we used an automated transcription service, Otter.ai, to transcribe the audio recordings.[3] Given that automated transcription means sending voice recordings to a third party, we made sure to get explicit participant permission prior to sending any recordings. Two researchers checked each transcript for accuracy. After transcription, two team members cooperatively coded the first eight interviews using iterative open coding [58]. The researchers were able to develop the main codebook using the first five transcripts. Then, one team member who coded the first eight interviews and a third team member coded the last eight interviews. Differences were resolved through discussion after each transcript. Because of the exploratory nature of the work, we aimed to yield themes and concepts from our data analysis rather than agreement, as "codes were the process and not the product" [59]. Each transcript was coded independently by two team members, who then met with each other and with the whole group to discuss themes, disagreements, and different interpretations of our codes. As such, we view inter-rater reliability (IRR) as inappropriate.

D. Ethical Considerations

The study was approved by University of Maryland's, Tufts University's, and University of Chicago's ethics review boards. We obtained informed consent before the pre-screening survey and again before the interview. Given the personal and sensitive nature of the questions we asked, we informed every participant that they could skip a question or stop the interview at any time. One participant withdrew their data after the completion of their interview because they felt they had shared too many details; we deleted all that participant's data and did not include it in our analysis.

E. Limitations

As with most qualitative studies, the generalizability of our results is limited by our small sample size. We mitigated this limitation by recruiting a diverse cohort of participants from several regions. While our study aims to include a diverse subset of marginalized populations, we cannot claim complete representation. We strived for inclusivity by interviewing any qualified individuals who completed the screening survey and recruiting from a wide variety of platforms. We limited our recruitment to the United States (US), Canada (CA), and the European Union (EU), thus excluding marginalized communities from other locations and limiting the generalizability of our results. We expect that experiences of marginalized populations from other geographic areas in vulnerability analysis will exhibit many similarities, but also critically important differences, to the experiences of our participants; we strongly encourage further study of other geographic areas in future work.

As we recruited from platforms for vulnerability discovery and through active members in vulnerability discovery, our study was likely to only reach participants who were successful in joining the community. As such, our results likely reflect some survival bias and a focus on successful strategies. We addressed this issue by explicitly asking our participants about strategies that did not work in addition to ones that did.

[3] https://otter.ai/

However, participants are not likely to remember everything they tried that did not work, and will likely reflect on their experiences in a more positive light given their success in the field. Further work is needed to reach a population of people who have not been successful in joining the vulnerability discovery community to understand their experiences and challenges.

IV. Path to vulnerability discovery

This section describes the paths taken by our participants intovulnerability discovery. Our participants had varying identities and experience levels, shown in Table I.

A. First interest in vulnerability discovery

Our participants were first drawn to vulnerability discovery at various ages, from grade school (N = 6) to pre-teen years (N = 2), high school (N = 4), and into adulthood (N = 4). They described a variety of reasons, sometimes more than one, that drew them to vulnerability discovery.

Others introduced them to vulnerability discovery. Some participants became interested in vulnerability discovery because a family member (N = 6) or friend (N = 3) introduced them to it. P3 "*asked a friend for an idea of a new side project, and he asked if I was interested in a career change. And he said, just send me a resume, and I'm gonna pass it off to some friends of mine. I didn't know at the time that it was vulnerability research.*" P8 started exploring vulnerability discovery because their "*dad was an engineering graduate student, and he had all these books. And they ranged from math, control theory, or these highly mathematical things to more practical things.*" Similarly, P10 reflects: "*My father actually works in this industry. So growing up, I was behind the keyboard from maybe the time I was like three or four years old. And he explained so many things to me that were so over my head. And things that he knew that I had absolutely no ability to understand. But he did it anyway. And eventually, when I got older… occasionally, he would say things like, 'Oh, this is down because somebody had hacked it…' So I think that's really what got me interested.*"

Tangential activities lead to vulnerability discovery. Many of our participants found vulnerability discovery through tangentially related interests (N = 12). For example, P9's school "*had all its own stuff run on its own networks off of all its own infrastructure. And I vaguely remember me and a friend just like poking around the shared network drives. I'm stumbling into things that probably shouldn't be open to the rest of the school… just kind of that sort of playful poking at things, that maybe not everyone would poke at.*" P5 "*got really into game hacking in middle school and trying to cheat at stuff because I was super, super, super terrible at video games. And I was much better at writing hacks for them.*" This is an age-old tradition of the hacking culture, as described in Turkle's early work in the 80's studying hacker communities, "Henry's growing-up toys were machines—an old air conditioner, discarded radios, tape recorders, broken blenders—which he patiently disassembled and put back together" [32]. Our participants and the general hacking community often start similarly in this way, but our participants often face unique challenges as they try to enter the vulnerability discovery community as described in subsection VI-A.

Drawn to a specific aspect of vulnerability discovery. Some of our participants, mostly those who found vulnerability discovery in adulthood, reported being drawn to specific aspects of vulnerability discovery (N = 11), including interest in the subject matter (N = 7), monetary incentives (N =1), and community members' passion (N = 1). P1 recalls "*when I went to the office where I'm currently working, [their colleagues] were just so passionate about what they did… that was sort of what drew me in.*" P3 describes her interest stemming from "*the mystery of [vulnerability discovery], and then once I got to get a taste for what they're able to accomplish, it only drew me in more because of how interesting that was.*" P5 notes that she got into the vulnerability discovery community because "*bug bounties were really awesome incentive cause in an evening of work, I could make like $2000 or $3,000 on just the weekend.*"

B. Learning resources and tools

Participants used a variety of resources to learn the skills necessary to join the vulnerability discovery workforce.

Resources with built-in structure. Some participants reported using resources that were designed to be educational, such as hacking challenges and sites (N = 5), certifications (N = 5), online courses (N = 6), and work trainings and courses (N = 4). Participants found these especially helpful because of their inherent structure. P10 describes: "*I love hack-the-box. I think it's really cool. And it gives you a lot of opportunity to mess up. You can just mess up. You can get the question wrong a million times. It doesn't matter.*" P1 explains "*I learn best with a lot of specific instructions of do this, then do this. So the [online courses] were very beneficial for me.*"

Participants also reported learning from structured resources that were not necessarily designed to be educational, such as capture the flag competitions (N = 5), bug bounty programs (N = 2), and security internships (N = 2). P9 elaborates "*I ended up on their CTF team and took part in a couple of bigger CTFs, including some where there was more of a defense side to it. And that definitely broadened my skill set with more of a 'Blue Team' side to it.*"

Unstructured resources. Participants also reported using resources that required them to formulate their own structure, such as on the job learning (N = 7), internet groups (N = 7), YouTube (N = 5), and general hacking websites (N = 8). P17 describes learning by "*watching videos, like really old DEFCON videos, and other hacking videos.*" As described in subsection VI-B, the lack of structure in materials like these can make learning additionally challenging.

ID	Identity	Education	Skill Level	Experience (years)	CTF Participation	Bug Bounty Participation
P1	LGBTQ+, female, non-binary	Master's Degree	Basic knowledge	1	Once/year	Never
P2	Female, non-binary	Doctorate Degree	Expert	20	Never	Never
P3	Women, transgender	Associate's Degree	Expert	10	Twice/year	Twice/year
P4	BIPOC	Bachelor's Degree	Intermediate	2	N/A	N/A
P5	Woman, trans, mixed race	Some college	Intermediate	3	Once/year	Once/month
P6	BIPOC	Bachelor's Degree	Expert	21	Never	Never
P7	Asian American	Master's Degree	Intermediate	4	Once/year	Once/month
P8	African American	Some college	Intermediate	3	Once/year	Never
P9	Woman, LGBTQ+	Bachelor's degree	Intermediate	3	Twice/year	Once/month
P10	Latina, bisexual, woman	Bachelor's Degree	Novice	3	Twice/year	Never
P13	Queer woman	Some college	Intermediate	10	Twice/year	Never
P14	Woman	Doctorate Degree	Intermediate	4	Never	Twice/year
P15	Woman, African American	Bachelor's Degree	Basic knowledge	3	Never	Never
P16	Woman of color	Master's Degree	Basic knowledge	1	Once/month	Once/year
P17	Woman, Asian	Bachelor's Degree	Intermediate	3	Once/month	Once/month
P18	BIPOC	N/A	N/A	N/A	N/A	N/A

TABLE I: Participant demographics, as self-reported to us. P18 declined to provide demographic information.

V. Positive experiences

Our participants reported on several positive aspects of their participation in the vulnerability discovery community, including support and affirmation as well as finding welcoming representation within the community.

A. Support, encouragement, and affirmation

Our participants reported receiving several types of support and encouragement during their participation in the vulnerability discovery community, noting this support as a critical aspect in their success and persistence in the field.

Beneficial mentoring. Participants reported positive mentoring experiences with work colleagues, supervisors, professional organizations, and other hackers. Participants noted that mentors were essential, as described by P13: "*I probably would have failed early on. . . . if I was turned loose there on the security team, and didn't have any support, or anything like that, I would have failed.*"

Participants described three essential resources provided by good mentors: mentors provide hands-on help (N = 3), they share relevant resources (N = 3), and they have connections to programs and organizations (N = 4). P1, discussing how they found out about opportunities for career development, said, "*Primarily, it's been mentors, either sharing with me specifically, or sharing with our office in general. . . there's this opportunity.*"P1 describes a good mentors they had: "*If we're working on code, they'll, sometimes be like, oh, I'll try it too. And, we would share the screen. Sometimes they would get errors too. And that sort of made me feel more validated.*"

In fact, we observed an almost uniform dramatic increase in participant self-efficacy, activity (number of reported learning experiences participated in), and expectations for themselves when they met their first good mentor. From our interviews, it was evident these individuals' guidance was both essential and transformative.

Positive interactions with the community. Receiving affirmation from colleagues, made our participants feel welcomed by the community. As P1 describes, "*When I first asked for them to. . . use they/them pronouns, they were very kind about that. But they did say, you know, you're the first person who I've ever met who, who's asked to use they/them pronouns. And in a way, I almost feel like coming out, maybe, made them view me a little bit more as an equal?*" P10 describes receiving affirmation from colleagues: "*I told my coworkers when I was leaving work today that I was going home to do [vulnerability research]. And they're like, 'Oh, that's so fun'. . . I can honestly say that I don't feel spoken down to at all anymore.*"

Emotional support. Participants also reported that emotional support from friends (N = 4), family members (N = 5), and teachers (N = 2) was critical to their joining and persisting in the field. In particular, participants appreciated receiving encouragement to pursue vulnerability discovery; P5 recalls a teacher who "*encouraged me to do things. She really encouraged me to apply for [student funding], get the tools I needed to analyze Bluetooth stuff because that stuff is bizarrely expensive . . . she really encouraged me to take those opportunities.*" P3 describes friends who provided "*emotional support. Someone to bounce [vulnerability research] ideas off of. Someone that's willing to listen to you even though they can't provide input.*"

B. Representation and diversity in the community

Participants noted that the ability to perceive themselves within the community made them feel welcomed (N = 3). When discussing a bootcamp he attended, P4 mentions that "*the moderator was a marine captain. He got out and then started a corporate career, and he worked his way up to SVP to, you know, to deputy chief security officer. . . His message resonates with veteran students in the in the room.*"

When talking about her decision to take her first vulnerability discovery job, P10 recounts "*I definitely myself had a misconception that [the company] didn't really have women working for them. And it was nice to hear from [the team member]. And to hear that [the company] had a lot of women working for [them].*"

Participants also saw a general presence of diversity in the community as welcoming (N = 3). P13, a transgender woman, describes "*I felt very accepted. I mean, we have in the group that I'm in now, more women than men, we have a very large LGBTQ+ presence. And it's, it's very, very much accepting.*" Similarly, P4 details: "*I did feel welcome back then… because my class was very diverse. My class had African Americans. It had minorities. It had hispanic. Pretty much any race that you can name, you know, were represented in my class.*"

VI. Challenges faced by marginalized populations

This section details the challenges faced by our participants when joining and continuing in the vulnerability discovery community.

A. Challenges unique to marginalized populations

Participants identified challenges that are unique to marginalized populations; most center on navigating the community with their marginalized identity.

Difficulty being taken seriously. Some participants felt, when interacting with other security experts, they were not taken seriously (N = 4). When discussing a hacking group meetup she attended, P5 said "*When I talked to people, I could tell they weren't taking me seriously… they saw me and were like, 'What is she doing? What's she trying to do here?'*"

Reluctance to share information. Participants also mentioned difficulty acquiring information from others in the community (N = 6). When trying to learn new things, several participants mentioned it seemed like other security experts did not want to share information. P13 mentioned that her co-workers "*weren't interested in spending the time to teach you,*" because "*they figured you should already know this. Because many of the men that are in those positions, did learn on their own.*" Our participants also felt that they often needed to be "pushy" in order to be acknowledged (N = 2). As P15 said, "*The other female was also African American. And we both sat in the same area. And then the other guys, they sat in another area, and they would forget about us. They wouldn't show us a lot of things. We had to ask all the time, like, 'What's going on today? I need some work.'*" Our participants reported working extra hard to get the training that their less marginalized colleagues were entitled to.

Relatedly, our participants were sometimes afraid to ask their colleagues questions. P15 worried that, "*If I go ask them a question, and then they're like, "Oh, did you just do this?' And they fixed it that quick, then I didn't feel good about it, because I already wasn't comfortable being there.*"

This fear of asking questions may come from the imposter syndrome [60] many participants experienced (N = 8). P9 mentions that "*there's large portions of the community that… [it's] less that I wouldn't be welcomed in and more that I don't want to risk not being welcomed. And like I won't put myself out there with lots of big groups online, because I feel like I won't belong. That's probably largely self imposed, but I don't see a reason to risk it.*"

Unwelcoming environments. While representation, and diverse work groups in general, helped our participants feel welcome, the lack thereof had the opposite effect (N = 6). For example, when asked to discuss whether she felt welcomed in the community, P13 describes "*The first time that I went to one of [this hacking organization's] networking events, I was appalled because I didn't see anybody like me, I didn't see very many women of color, or anything.*" P7 mentions, when asked whether he felt welcomed in the community, that "*there's probably 10 or 12 different women in tech groups that just kind of dominate this space of diversity … I'm just a dude, and I don't really fit into a lot of the different clubs or groups.*"

Some participants (N = 3) avoid interacting with the community altogether due to negative prior experiences and fear of rejection. As P9 explains "*Being on Twitter, being on forums and stuff and seeing like… infosec professionals just being like transphobic, or misogynistic or racist and stuff online. I don't want to work at a company where that person could be one of my coworkers on my team, something like that. Even if they're not like that in professional environments, seeing them on Twitter or elsewhere being like that. Just I don't want to be around that.*"

Deterrence from non-community members. Participants mentioned facing deterrence from people that were not in the vulnerability discovery community as well (N = 5). P7 did not join the community earlier because his "*father is a very conservative Korean guy. And he didn't want me to.*" P15 notes her husband pushed her toward other jobs: "*I know, my husband's like, 'Oh, look at these jobs for system administrators.' And I was like, 'I'm training myself to be in the cyber field. And he's like, well, 'you say you won't get promoted, so a promotion is a promotion.'*"

Discrimination. Perhaps most alarming is the discrimination faced by our participants. Our participants mentioned experiencing sexism (N = 8), racism (N = 3), sexual assault (N = 3), transphobia (N = 2), and homophobia (N = 1) either directed at themselves or someone close to them.

P3 mentions an experience where "*Once I actually transitioned, and started using all female terms, customers actually started questioning my knowledge level.*" She gives a specific example: "*Majority of the time it was other customers for new projects always assumed that when they want the smart engineer on the team is going to be a guy… So if I was doing a demo, or I was talking about some technology, they assume that I had just been taught on it. And wasn't the one that* *actually invented it. More than once, and I wasn't the only one that had this trouble.*" P18 recounts that friends told them "*about women getting sexually harassed and stalked at hotels during [security] events.*" Giving a specific example of women finding "*random hacker guys in their rooms.*" P7 describes "*I mingled with a local hacker group, club, and, I was the only minority period, you know… some of them were just outright racist to me.*"

Our participants also faced discrimination that was less explicit. P15, an African American woman describes: "*They have other interns that came in. And I felt that those interns were, they like called on them more. But I can't say for a fact that it was because they were different color.*" In a similar vein, P10 a Hispanic woman, "*had to work with all men. And I definitely noticed a big shift. And it is even some of the same people, like the same people that I would speak to in the break room, friendly or whatever, were now cutting me off in meetings and explaining things to me that I didn't need on a daily basis. So I got a lot of the mansplaining.*" These experiences caused our participants to feel a sense of otherness and rejection from the community.

Participants experienced enough discrimination that they had explicit coping mechanisms to avoid facing discrimination when joining and interacting with other hackers. Participants reported selecting online usernames to provide anonymity (N= 3) to avoid any discrimination. For example, P17 describes "*I kept myself anonymous, mainly because I didn't want people identifying me as a female.*"

B. Challenges exacerbated for marginalized populations

Not all the challenges participants faced were unique to marginalized populations. In particular, when first starting out in vulnerability discovery, they often faced challenges that many or all new members of the community face. However, these challenges are often exacerbated for marginalized populations because of the inequalities that they suffer within and outside of the vulnerability discovery community.

Structure of learning materials and resources. One example that may affect many people who are new to vulnerability discovery is that learning resources often assume students come with a technical background (N = 3). P4 said that "*part of that challenge is the technical nature of the course material. So I found myself putting more time than others simply because I did not come from a technical background.*" P1 recounts a similar experience with a CTF: "*There were definitely not very clear instructions of first do this. As someone who had never even heard of capture the flag other than the physical game before, I didn't know when it just said… SSH into here. And then enter the flag. And I'm like, 'What does SSH mean?'*" While this challenge is not unique to marginalized populations, it can be especially harmful given that this assumption can worsen members' already existing feeling of otherness. Further, underrepresentation in computing more generally means that proportionally fewer people from marginalized populations will have the technical background that is often assumed.

Our participants also noted that the inherent unstructured nature of the learning materials posed a challenge (N = 4). As P5 describes, she "*wrecked [her] little tiny laptop many times trying to install random garbage [she] found on the internet*" because the materials she used required "*a lot of trial and error.*" While these materials are unstructured for everyone, a lack of mentorship can make using these resources more difficult for marginalized populations.

Resource constraints. Participants emphasized that they had to learn and prepare on their own time (N = 5). They often were not able to pursue learning materials for vulnerability discovery on paid time. As P4 expresses, "*I rely on myself to continuously put in the time and learning on my own… when you're off the clock, everybody else is at the bar and drinking beer on a Friday night watching a movie or hanging out.*"

Participants also expressed challenges associated with the high cost of vulnerability discovery training (N = 5). P17 noted, "*I remember really wanting to do [security training]. But I couldn't really afford it. SANS Institute was also something else that I was looking to, I remember really looking forward to all of the security training, but knowing that I couldn't get into any of them. Too expensive. I couldn't afford any of it.*" When asked about challenges he faced, P8 said "*I think the biggest one was money.*"

These difficulties contribute to the larger challenges faced by our participants: the logistics of making a switch into a vulnerability discovery career (N = 3). This is exemplified by P15: "*I took a job where I was like logistics and I wasn't doing IT at all…I did that for like eight years. And there it was just every once in a while, I'd never like, let go because I was like, I want to go back to it but for my family and for money, I stayed with logistics.*" The cost of training, time commitment, and logistics of making the switch are problems faced by most new people in the community, but these are even more difficult for members of marginalized populations because of existing inequalities they face, such as pay and technology access gaps [61]–[63].

Lack of opportunities. Another challenge faced by our participants was the lack of attainable entry-level positions and opportunities (N = 3). P9 explains "*Towards the end of my college career, I was starting to look into getting a job in infosec in some way, and that definitely started to be discouraging. Seeing entry level listings, asking for eight years experience… it feels more like they want people who are less confident in themselves…to not be applying…I feel like I and many other women feel a lot less confident in doing that kind of thing, and I can't help but see job listings that do that and think they just don't want me working there.*" While finding entry level positions can be difficult for all members of the vulnerability discovery community, they are especially difficult to obtain for members of marginalized communities, as echoed in the Synack survey [10].

The lack of entry-level positions creates a secondary effect: making finding mentors harder (N = 5). Most of our participants found their mentors through a work position. As

P17 notes, "*I didn't have the resources, didn't really have the mentors. And for me, that really sucked.*" While helpful mentors are essential to the success of every member of the vulnerability discovery community, they play a pivotal role for members of marginalized populations: Our participants overwhelmingly reported that having a mentor was essential in helping them navigate imposter syndrome pertaining to their membership in the vulnerability discovery community. This imposter syndrome is often exacerbated by the discrimination they faced within the community. (Notably, in Synack's survey 71% of their white male respondents reported never experiencing bias based on their ethnicity or background, while 54% of minority respondents reported experiencing at least a moderate amount of bias [10].)

These factors interrelate and exacerbate each other in a vicious cycle: discrimination and imposter syndrome can make members of marginalized populations feel unqualified and therefore less likely to apply for an entry-level job, thus excluding them from the most likely source of mentorship, and therefore from a resource that could help to combat the discrimination and imposter syndrome.

Unhelpful mentoring. Participants also reported unhelpful and unsupportive mentors as a key challenge they faced (N = 5). P1 describes "*one [mentor] who was too blunt… to the point of it just felt like I was just not getting constructive criticism, but just sort of a one two punch… I asked a lot of questions and… he would say that he wanted me to ask questions. And it was good that I was asking questions. But whenever I would ask a question, he would say that I needed to figure it out on my own, and would sort of criticize the fact that I wasn't figuring it out on my own.*" P18 had a similar experience when their team lead told them during a performance review that "*they are too emotional… review, even though they work well with clients.*"

We expect that the presence of unhelpful mentors is not unique to members of marginalized communities and is a prevalent problem within the vulnerability discovery community. However, the encouragement to mentor minorities through special funding [64], [65], special awards [66], [67], or workplace requirements incentivizes "token mentoring" within the community and leads to an overwhelming increase of "bad" mentoring for members of marginalized communities. Our participants noted that the existence of workplace requirements to mentor new employees resulted in being mentored by unwilling mentors, thus resulting in a negative mentorship experience that further exacerbated their existing imposter syndrome and inequities. P17 notes that they were "*promised mentorship*" at a new job, but their provided mentor "*felt threatened by their presence,*" so they "*didn't quite get along quite well. So trying to work with him and trying to learn from him, it wasn't there.*" Further, research suggests that members of marginalized communities in many fields are often mentored differently, and less effectively, than their less marginalized colleagues [68].

Lack of awareness. Participants felt their lack of knowledge about vulnerability discovery as a career option contributed to their difficulty in getting involved (N = 6). P2 mentioned they "*did [vulnerability research] as a hobby" because they had "no notion that there existed a career option. Other than if you successfully hacked some big company, they might hire you to become a security person. Which I didn't think was that likely to work out.*" This lack of awareness can be further aggravated by the fact that members of marginalized populations are actively dissuaded from joining vulnerability discovery as described in subsection VI-A. P1 experienced this: "*They were trying to push me towards 'Oh, but wouldn't you rather be a teacher?'*"

Uncertainty and resilience. Uncertainty is inherent in vulnerability discovery. Effort analyzing a target may not pay off, as the security expert may not find a bug, or another security expert may "scoop" a bug before it is submitted. Ambiguity in bug bounty programs also contributes uncertainty, as the security expert may have to argue with bounty managers about the bug's existence or value. Participants cited frustration with this uncertainty about bug acknowledgement as one factor dissuading them from participation in the field (N = 5). P7, for example, joined a bug bounty program, but "*then I realized they don't really want to pay for it. You know, it's like, oh, we'll give you this much money. Just kidding [they backed out]. It was informational.*"

This level of uncertainty creates pressure: "*So you got to have that mental toughness to go. But even when people are talking to you saying that maybe you should move on… tough it out. It can work out for you.*" While this need for resilience applies throughout the vulnerability discovery community, it may be particularly challenging for members of marginalized populations who have less community support and face frequently hostile environments, as described above. Further, bugs that go unacknowledged and unpaid may be especially challenging for people from marginalized populations, given pre-existing pay gaps and less frequent opportunities [62], [63].

VII. Discussion and Recommendations

Our results demonstrate the unique and exacerbated challenges faced by members of marginalized populations in vulnerability discovery, but these challenges can be lessened through active changes within the community. We observed in our results that the general relationships between factors hypothesized by SCCT held. For example, the introduction of participant support through good mentors dramatically improved development and career progress. This section starts by comparing our results to prior work and concludes by recommending steps towards improving the vulnerability discovery community's inclusivity and equity by more systematically improving marginalized populations' support through mentoring and resource restructuring.

A. Comparing our results to prior findings

As we discussed in Section II, Turkle's early work offers a similar investigation into the way hackers join and participate in the community, but how much has changed over the past 40 years as the field has professionalized and become less stigmatized. Our results suggest vulnerability discovery has grown without significant changes to the insular nature of the community. Access to educational resources have become more widely available, but they remain relatively difficult to parse. Additionally, the community continues to be exclusionary toward those who cannot first prove their worth, most often aided by the support of a mentor, which disadvantages people from marginalized populations's without similar support. One participant (P2) who began her career in the early days of the Internet (shortly after Turkle's work) described similar othering related to her gender both at the start of her career up until more recently when she decided to stop participating in the broader security community because of these interactions.

Most relevant to our study is SynAck's 300-person Diversity and Inclusion white paper [10]. Our work builds on an extends the SynAck findings by digging into specific instances and patterns of discrimination and how they are perceived, understood, and overcome. SynAck reports that more than half of minority respondents experienced at least a moderate amount of bias based on their ethnicity or background (54%). Our results support this: all 16 of our participants experienced some type of bias based on their ethnicity, sexual orientation, or gender identity. However, we expand on this result by illuminating specific examples and patterns of how this discrimination manifests such as a difficulty being taken seriously, deterrence from non-community members, and direct examples of racism, sexism, transphobia, homophobia, and sexual assault. Uncovering direct examples of these challenges allows us to better design interventions to the overwhelming discrimination problems faced in the vulnerability discovery community.

Additionally, the Synack report suggests more mentoring for marginalized community members but does not ask any questions about mentoring or put forth recommendations to improve mentoring. Our work underlines the need for high-quality mentoring while identifying specific aspects of mentoring that are (not) valuable and effective. Specifically, we find that the current mentoring system in vulnerability discovery community encourages "token mentoring" and thus points to a need for different methods of mentoring that are not currently found within the community (i.e. anonymous mentoring, mentoring matching system, etc).

B. Comparing to other STEM fields

We found evidence that the vulnerability discovery community is sometimes hostile to members of marginalized populations, with many examples of both overt discrimination and micro-aggressions. Many participants report experiencing imposter syndrome. These issues mirror problems in other STEM fields, but we also found important differences.

As hypothesized, the ability to remain anonymous enables members of marginalized populations to participate without revealing their marginalized identities. While hiding one's identity is no substitute for full inclusion, some of our participants did find it a successful strategy for making inroads in the community. It also creates an opportunity for partially anonymous mentoring, in ways that may not be as possible in other areas of STEM. To be clear, taking advantage of anonymity is a short-term strategy that must be paired with larger structural changes that will allow everyone to participate fully, without fear of being "discovered."

Another key difference is that unlike many STEM fields, vulnerability discovery is dominated by learning from online resources, peer mentors, and on the job, rather than a standardized curriculum or educational path [30]. This can have both positive and negative effects for members of marginalized populations. It may allow some people to work around well-known barriers that can limit access to formal educational paths. However, trying to make sense of large amounts of information of varying quality is often overwhelming for beginners, as our participants explained and prior work in software development has shown [69]. Therefore, successful vulnerability discovery experts are often apprenticed into the community, relying on elder members to guide them in choosing the right resources and providing important learning structures [31]. This strong dependence on a mentor figure to make progress can be particularly challenging for underrepresented or marginalized people, who may have less access to this guidance and accordingly have a harder time breaking into the field.

Relatedly, another difference we note is the inherently competitive and individualistic nature of vulnerability discovery. In vulnerability discovery, one member of the community identifying and submitting a vulnerability directly affects the ability of another member to do the same [28]. This can lead to a resistance to share knowledge, as seen in our participants' experiences. This general resistance may be exacerbated by marginalization and by the aforementioned difficulty obtaining mentors.

We recommend the vulnerability discovery community invest in creating more structured resources that can be useful to beginners and intermediate learners from any background. Some progress has been made on this front with the development of vulnerability discovery educational platforms targeted at supporting beginners [70]–[73] and bug bounty platform curated resource libraries [74]–[76]. However, these resources continue to have some educational limitations [31], and further work is needed.

C. Aligning our results with SCCT

Based on its usefulness in prior work, we adopted SCCT as a guiding structure for building our interview materials, to ensure we would elicit an appropriate breadth of factors influencing participant development and motivation.

Our findings align well with the relationships described by the model, for example, when comparing marginalized participants' negative (Section VI) and positive (Section V) experiences in vulnerability discovery. Participants reported limited or negative background affordances (e.g., poor mentoring and limited resources) inhibiting their ability to identify and take advantage of the available poorly structured learning experiences, which led to lowered self-efficacy and made them consider not continuing in vulnerability discovery. Similarly, negative contextual supports, such as non-representativeness of the community, made participants less likely to pursue a vulnerability discovery career. However, when one of these factors changed, primarily by finding a good mentor, participants reported a dramatic shift in self-efficacy and vulnerability discovery education and career pursuit, as is suggested by the SCCT model. Our results also match the SCCT model, as participant gender and race/ethnicity played a key role in whether the participant faced different challenges or did not have the same background affordances as others (e.g., lacking access to good mentors or being discouraged from pursuing a vulnerability discovery career), causing the negative trend. Additionally, participant gender and race/ethnicity increased the effect of identified barriers that were generic to all members of the vulnerability discovery community. This suggests future studies could use this model as a guide for work that expands on our initial results. Specifically, researchers could use SCCT to guide questions asked in future investigations to ensure relevant factors are measured, SCCT could be used as a frame for interpreting participant behaviors and responses in qualitative work, and it could inspire possible interventions that focus on improving particular parts of the model which are expected to influence increased career participation.

D. *Mentoring members of marginalized populations*

Our results suggest mentoring can be critical to help members of marginalized populations succeed in vulnerability discovery, but quality mentoring is not always simple to achieve. Simply creating programs to encourage mentoring for marginalized populations can lead to instances of unhelpful, even "token" mentoring.

This accords with prior work finding that members of marginalized populations, specifically women, are often mentored differently than less marginalized populations. In their work, Ibarra et al. find women are often over-mentored and under-sponsored: sponsors not only provide advice but actively work to advocate for their mentees and recommend them for new opportunities [68]. Mentors in the vulnerability discovery community should keep this distinction in mind; many of our participants indicated that their most successful mentoring experiences involve this kind of sponsorship. We recommend that programs designed to promote mentoring explicitly consider how to incorporate sponsorship.

Other prior work distinguishes among *collectors*, *nightlights*, and *allies* as mentors: collectors mentor in part to benefit themselves or demonstrate their own magnanimity, nightlights illuminate unspoken rules and show mentees how to navigate in a community, and allies go further to become full partners and advocates for their mentees [77]. Among the participants in our study, we did not see much evidence of mentors-as-collectors. Our participants benefited from nightlights, but did not provide many examples of full-blown allyship; senior members of the vulnerability discovery community should consider expanding their mentorship in this direction, at least for the mentees to whom they can devote the most time and energy. Overall, we argue that for mentoring programs to realize their intended benefits, they must carefully account for these potential pitfalls.

E. *Helping mentees reach mentors*

Our results suggest that success in the vulnerability discovery community, particularly for marginalized populations, can be positively influenced by the assistance of a mentor. However, finding a mentor and building a relationship over time is not always easy. We suggest that the vulnerability discovery community invest in creating systems that help facilitate mentoring for members of marginalized populations. Mentoring systems could take a number of forms reflecting the different needs of participants as they join and, subsequently, become active members of the vulnerability discovery community. For instance, not all members of marginalized populations feel comfortable disclosing that they are from a marginalized or under-served group, as discussed in subsection VI-A. Systems that allow for anonymous mentoring may help in this regard. While this would not allow for sponsorship, anonymous mentoring would allow new members of the community to ask technical questions without the fear of being discriminated against. This could be done easily via Discord or other means that allow users to interact without revealing personally identifiable information. More research into what would work best is required.

Another issue may be that although there are senior members of the vulnerability discovery community who are willing to mentor, some marginalized populations may find it hard to know who will be welcoming, or daunting to approach them uninvited. One way that some members of the security community have tried to lower the barrier to mentoring and open the doors for people is to hold 'open office hours' on a regular basis. In these 'open office hours,' the senior member of the community typically advertises a video chat link or another way to get in touch, with the express purpose of answering questions and mentoring newcomers. This may be fraught with privacy and security challenges for both the mentor and mentee, but with sign-ups ahead of time and some vetting procedures, 'open office hours' could allow more people to benefit from senior members' experience. If several senior mentors pair up or hold group office hours, this could ensure safety from the mentor side and similarly, meetings could be arranged with groups of mentees if preferred. We note that while this approach can help to identify potentially welcoming mentors to approach, it will not necessarily be enough to overcome a fear of asking questions arising from impostor syndrome.

A mentor matching system, in which people who are comfortable disclosing demographic information that identifies them as a member of marginalized populations self-select interests or needs could also be beneficial. This system could be used to match willing mentors to mentees in general. This one-on-one mentoring could allow new members to be matched with willing mentors and allow for sponsorship.

Further, if both parties opt in, such a system could specifically match mentors and mentees who are both from marginalized populations, with the goal of offering a mentor who understands some of the specific challenges the mentee is likely to face. We note here this does not mean the mentor and mentee have to be from the same marginalized population, as our results suggest mentees feel welcomed when a broad diversity is represented in the community.

F. Forming affinity groups with care

One strategy that has been used to help marginalized populations in STEM generally has been to create various affinity groups, such as Women in Cybersecurity. These groups are often helpful for people to find others who are facing similar challenges. However, our results suggest this approach needs to be undertaken with care. First, it is hard to get sufficient representation to cover every marginalized population, which may leave members of some populations feeling left out. Further, it is important not to rely on affinity groups to solve structural problems that must be tackled by people who already have representation and power.

G. Clear rules of engagement

One key aspect of improving retention of marginalized people in vulnerability discovery may be improving the environment that — as reported by our participants — is often hostile. Senior and authoritative people and organizations in the community could start by making clear what behaviors, such as discriminatory conduct, are unacceptable and responding accordingly to violations. For platforms, programs, forums, and other organizations, this could mean a tiered approach in which first offenses generate warnings (including an explanation of the problem), while later offenses escalate to temporary and then permanent bans.

H. Improving entry-level opportunities

Our participants highlighted the lack of available entry-level and beginner opportunities within the vulnerability discovery community, and specifically how discouraging advertisement for purportedly entry-level positions can be. This points to an area of improvement for the vulnerability discovery community. Businesses should consider how to best frame security job advertisements to highlight necessary skills without excluding potential candidates. This may require carefully crafting the ad, or even being willing to train high-potential candidates who do not yet possess all the "required" skills. For the later, businesses could consider using Saner et al.'s cyber operations aptitude assessment to help them evaluate candidates without long resumes or the "required years of experience" [78].

I. Intersectionality

Intersectionality — in which multiple facets of identity contribute to discrimination and marginalization in ways that are not simply the sum of the parts — is likely an important factor in how marginalized populations experience the vulnerability discovery community. Perhaps unsurprisingly, our small dataset did not clearly reveal patterns of intersectionality that might be visible in a larger sample. We advocate for future work explicitly targeting issues of intersectionality in the vulnerability discovery context.

VIII. Conclusion

Vulnerability discovery is an essential aspect of software security. Currently, the demand for security experts significantly exceeds the available vulnerability discovery workforce, but the existing vulnerability discovery workforce is highly homogeneous, dominated by white and Asian men. As such, one promising avenue for increasing the capacity of the vulnerability discovery community is through recruitment and retention from a broader population. Therefore, it is important to understand the challenges faced by and experiences of marginalized populations when joining the vulnerability discovery workforce. As a step towards understanding this, we conducted semi-structured interviews with 16 members of the vulnerability discovery community who identified as being from a marginalized population.

We found varying paths taken and resources used by our participants as they begin and continue in vulnerability discovery careers. Further, members of marginalized populations face some unique challenges, while other challenges common in vulnerability discovery are exacerbated by marginalization. Future work is needed with participants from other regions of the world and larger samples to allow for the study of intersectionality in detail.

With the obvious challenges faced by members of marginalized populations, there is a clear need for strong and inclusive mentorship. To address this challenge, we recommend new forms of mentorship that includes a system that allows mentees to remain anonymous and a matching system for mentors and mentees that helps promote strong mentor and mentee pairings. Additionally, we distill recommendations to help mentors become better sponsors and allies for mentees from marginalized populations.

Acknowledgments

We thank the anonymous reviewers who provided helpful comments on drafts of this paper, WISP [79], #ShareTheMicInCyber [80], and Jordan Wiens for help with recruitment, and Rachel Tobac for valuable insights on the design of our study. This project was supported by NSF grants CNS-1943215 and CNS-1801545 and gifts from Google.

References

[1] J. Biden, "Executive order on improving the nation's cybersecurity," Office of the United States President, May 2021. [Online]. Available: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[2] J. Marcil, "Building an application security team," 2017. [Online]. Available: https://adam.shostack.org/blog/2017/10/application-security-team/

[3] Hackerone, "2019 hacker-powered security report," Hackerone, San Francisco, California, Tech. Rep., December 2019. [Online]. Available: https://www.hackerone.com/resources/reporting/the-hacker-powered-security-report-2019

[4] BugCrowd, "Inside the mind of a hacker 2020," BugCrowd, 2020. [Online]. Available: https://itmoah.bugcrowd.com

[5] HackerOne, "The 2020 hacker report," HackerOne, Tech. Rep., 2020. [Online]. Available: https://www.hackerone.com/sites/default/files/2020-04/the-2020-hacker-report.pdf

[6] Bugcrowd, "The state of bug bounty," Bugcrowd, Tech. Rep., 2016. [Online]. Available: https://pages.bugcrowd.com/2016-state-of-bug-bounty-report

[7] A. Mein and C. Evans, "Dosh4vulns: Google's vulnerability reward programs," https://docs.google.com/presentation/d/1REYDohHohDhGAUfUq_Pyz5XFQL44Z3nfH9FnOvvTKBQ/htmlpresent, Google, 2011.

[8] Hackerone, "2016 bug bounty hacker report," Hackerone, San Francisco, California, Tech. Rep., September 2016. [Online]. Available: https://hackerone.com/blog/bug-bounty-hacker-report-2016

[9] M. Finifter, D. Akhawe, and D. Wagner, "An empirical study of vulnerability rewards programs," in *Proceedings of the 22nd USENIX Security Symposium*, ser. USENIX Security '13, 2013, pp. 273–288.

[10] Synack, "Synack cybersecurity diversity and inclusion report," Synack, Tech. Rep., 2020. [Online]. Available: https://www.synack.com/diversity-report/

[11] T. Maillart, M. Zhao, J. Grossklags, and J. Chuang, "Given enough eyeballs, all bugs are shallow? revisiting eric raymond with bug bounty programs," in *Proceedings of the 15th Workshop on the Economics of Information Security*, ser. WEIS '16, 2016.

[12] U. D. of Homeland Security, "Secretary mayorkas announces most successful cybersecurity hiring initiative in dhs history," US Department of Homeland Security, 2021. [Online]. Available: https://www.dhs.gov/news/2021/07/01/secretary-mayorkas-announces-most-successful-cybersecurity-hiring-initiative-dhs

[13] E. Seymour and N. M. Hewitt, *Talking About Leaving: Why Undergraduates Leave the Sciences*. Westview Press, 2000.

[14] J. Margolis and A. Fisher, *Unlocking the clubhouse: Women in computing*. Cambridge, MA: MIT press, 2002.

[15] S. Cheryan, V. C. Plaut, P. G. Davies, and C. M. Steele, "Ambient belonging: how stereotypical cues impact gender participation in computer science." *Journal of personality and social psychology*, vol. 97, no. 6, p. 1045, 2009.

[16] J. Margolis, R. Estrella, J. Goode, J. J. Holme, and K. Nao, *Stuck in the shallow end: Education, race, and computing*. MIT press, 2017.

[17] S. Cheryan, J. O. Siy, M. Vichayapai, B. J. Drury, and S. Kim, "Do female and male role models who embody stem stereotypes hinder women's anticipated success in stem?" *Social Psychological and Personality Science*, vol. 2, no. 6, pp. 656–664, 2011.

[18] D. G. Smith, *Diversity's promise for higher education: Making it work*. JHU Press, 2020.

[19] S. Cheryan, A. Master, and A. N. Meltzoff, "Cultural stereotypes as gatekeepers: Increasing girls' interest in computer science and engineering by diversifying stereotypes," *Frontiers in psychology*, vol. 6, p. 49, 2015.

[20] C. E. Foor, S. E. Walden, and D. A. Trytten, ""i wish that i belonged more in this whole engineering group:" achieving individual diversity," *Journal of Engineering Education*, vol. 96, no. 2, pp. 103–115, 2007.

[21] L. J. Barker, K. Garvin-Doxas, and M. Jackson, "Defensive climate in the computer science classroom," in *Proceedings of the 33rd SIGCSE Technical Symposium on Computer Science Education*, ser. SIGCSE '02. New York, NY, USA: Association for Computing Machinery, 2002, pp. 43–47.

[22] K. Garvin-Doxas and L. J. Barker, "Communication in computer science classrooms: Understanding defensive climates as a means of creating supportive behaviors," *J. Educ. Resour. Comput.*, vol. 4, no. 1, p. 2?es, Mar. 2004.

[23] C. M. Lewis, K. Yasuhara, and R. E. Anderson, "Deciding to major in computer science: A grounded theory of students? self-assessment of ability," in *Proceedings of the Seventh International Workshop on Computing Education Research*, ser. ICER '11. New York, NY, USA: Association for Computing Machinery, 2011, pp. 3–10.

[24] (ICS2)^2, "Cybersecurity workforce study," (ICS2)^2, Tech. Rep., 2018. [Online]. Available: www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx

[25] D. H. Tobey, P. Pusey, and D. L. Burley, "Engaging learners in cybersecurity careers: Lessons from the launch of the national cyber league," *ACM Inroads*, vol. 5, no. 1, pp. 53–56, 2014.

[26] P. Pusey, M. Gondree, and Z. Peterson, "The outcomes of cybersecurity competitions and implications for underrepresented populations," *IEEE Security Privacy*, vol. 14, no. 6, pp. 90–95, 2016.

[27] P. Pusey, S. David Tobey, and R. Soule, "An argument for game balance: Improving student engagement by matching difficulty level with learner readiness," in *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*. San Diego, CA: USENIX Association, 2014.

[28] R. Ellis and Y. Stevens, "Bounty everything: Hackers and the making of the global bug marketplace," *Available at SSRN 4009275*, 2022.

[29] D. Votipka, M. N. Punzalan, S. M. Rabin, Y. Tausczik, and M. L. Mazurek, "An investigation of online reverse engineering community discussions in the context of ghidra," in *2021 IEEE European Symposium on Security and Privacy (EuroS P)*, 2021, pp. 1–20.

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

[31] D. Votipka, E. Zhang, and M. L. Mazurek, "Hacked: A pedagogical analysis of online vulnerability discovery exercises," in *2021 IEEE Symposium on Security and Privacy (SP)*, 2021, pp. 1268–1285.

[32] S. Turkle, *The second self: Computers and the human spirit*. Mit Press, 1984.

[33] D. Votipka, S. Rabin, K. Micinski, J. S. Foster, and M. L. Mazurek, "An observational investigation of reverse Engineers' processes," in *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, 2020, pp. 1875–1892.

[34] K. Sridhar and M. Ng, "Hacking for good: Leveraging HackerOne data to develop an economic model of Bug Bounties," *Journal of Cybersecurity*, vol. 7, no. 1, 03 2021.

[35] M. Zhao, A. Laszka, T. Maillart, and J. Grossklags, "Crowdsourced security vulnerability discovery: Modeling and organizing bug-bounty programs," in *Proceedings of the 4th AAAI Workshop on Mathematical Foundations of Human Computation*, ser. HCOMP '16, November 2016.

[36] K. Huang, M. Siegel, S. Madnick, X. Li, and Z. Feng, "Poster: Diversity or concentration? hackers' strategy for working across multiple bug bounty programs," in *Proceedings of the 37th IEEE Symposium on Security and Privacy*, ser. IEEE S&P '16, 2016.

[37] A. Magazinius, N. Mellegård, and L. Olsson, "What we know about bug bounty programs - an exploratory systematic mapping study," in *Socio-Technical Aspects in Security and Trust*, T. Groß and T. Tryfonas, Eds. Cham: Springer International Publishing, 2021, pp. 89–106.

[38] J. Ruohonen and L. Allodi, "A bug bounty perspective on the disclosure of web vulnerabilities," *CoRR*, vol. abs/1805.09850, 2018.

[39] N. Alexopoulos, A. Meneely, D. Arnouts, and M. Mühlhäuser, "Who are vulnerability reporters? a large-scale empirical study on floss," in *Proceedings of the 15th ACM / IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)*, ser. ESEM '21. New York, NY, USA: Association for Computing Machinery, 2021. [Online]. Available: https://doi.org/10.1145/3475716.3475783

[40] BugCrowd, "Inside the mind of a hacker," BugCrowd, 2016. [Online]. Available: https://pages.bugcrowd.com/inside-the-mind-of-a-hacker-2016

[41] O. Akgul, T. Eghtesad, A. Elazari, O. Gnawali, J. Grossklags, D. Votipka, and A. Laszka, "The hackers' viewpoint: Exploring challenges and benefits of bug-bounty programs," in *Proceedings of the 2020 Workshop on Security Information Workers*, ser. WSIW '20. USENIX Association, 2020.

[42] J. Margolis, A. Fisher, and F. Miller, "Caring about connections: Gender and computing," *IEEE technology and society magazine*, vol. 18, no. 4, pp. 13–20, 1999.

[43] A. J. Ko, "Attitudes and self-efficacy in young adults' computing autobiographies," in *2009 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*. IEEE, 2009, pp. 67–74.

[44] C. A. Liang, S. A. Munson, and J. A. Kientz, "Embracing four tensions in human-computer interaction research with marginalized people," *ACM Transactions on Computer-Human Interaction (TOCHI)*, vol. 28, no. 2, pp. 1–47, 2021.

[45] K. Charmaz, *Constructing grounded theory: A practical guide through qualitative analysis*. sage, 2006.

[46] G. Guest, A. Bunce, and L. Johnson, "How many interviews are enough? an experiment with data saturation and variability," *Field Methods*, vol. 18, no. 1, pp. 59–82, 2006.

[47] R. W. Lent, S. D. Brown, and G. Hackett, "Toward a unifying social cognitive theory of career and academic interest, choice, and performance," *Journal of Vocational Behavior*, vol. 45, no. 1, pp. 79 – 122, 1994.

[48] A. Bandura, "Human agency in social cognitive theory." *American psychologist*, vol. 44, no. 9, p. 1175, 1989.

[49] N. E. Betz and G. Hackett, "The relationship of career-related self-efficacy expectations to perceived career options in college women and men." *Journal of counseling psychology*, vol. 28, no. 5, p. 399, 1981.

[50] N. A. Fouad and M. C. Santana, "Scct and underrepresented populations in stem fields: Moving the needle," *Journal of Career Assessment*, vol. 25, no. 1, pp. 24–39, 2017.

[51] R. L. Navarro, L. Y. Flores, H.-S. Lee, and R. Gonzalez, "Testing a longitudinal social cognitive model of intended persistence with engineering students across gender and race/ethnicity," *Journal of Vocational Behavior*, vol. 85, no. 1, pp. 146–155, 2014.

[52] L. Y. Flores, R. L. Navarro, and S. J. DeWitz, "Mexican american high school students' postsecondary educational goals: Applying social cognitive career theory," *Journal of Career Assessment*, vol. 16, no. 4, pp. 489–501, 2008.

[53] R. W. Lent, S. D. Brown, H.-B. Sheu, J. Schmidt, B. R. Brenner, C. S. Gloster, G. Wilkins, L. C. Schmidt, H. Lyons, and D. Treistman, "Social cognitive predictors of academic interests and goals in engineering: Utility for women and students at historically black universities." *Journal of counseling psychology*, vol. 52, no. 1, p. 84, 2005.

[54] L. Y. Flores, R. L. Navarro, H. S. Lee, D. A. Addae, R. Gonzalez, L. L. Luna, R. Jacquez, S. Cooper, and M. Mitchell, "Academic satisfaction among latino/a and white men and women engineering students." *Journal of Counseling Psychology*, vol. 61, no. 1, p. 81, 2014.

[55] K. Buse, D. Bilimoria, and S. Perelli, "Why they stay: Women persisting in us engineering careers," *Career Development International*, 2013.

[56] R. Singh, N. A. Fouad, M. E. Fitzpatrick, J. P. Liu, K. J. Cappaert, and C. Figuereido, "Stemming the tide: Predicting women engineers' intentions to leave," *Journal of Vocational Behavior*, vol. 83, no. 3, pp. 281–294, 2013.

[57] B. Barron, "Conceptualizing and tracing learning pathways over time and setting," *Yearbook of the National Society for the Study of Education*, vol. 109, no. 1, pp. 113–127, 2010.

[58] J. Corbin and A. Strauss, *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications, 2014.

[59] N. McDonald, S. Schoenebeck, and A. Forte, "Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice," *Proceedings of the ACM on Human-Computer Interaction*, vol. 3, no. CSCW, pp. 1–23, 2019.

[60] M. Haber, "Do you suffer from imposter syndrome?" https://www.forbes.com/sites/forbestechcouncil/2021/10/28/do-you-suffer-from-imposter-syndrome/?sh=760dc87d8f57, Forbes, 2021.

[61] E. A. Vogels, "Digital divide persists even as americans with lower incomes make gains in tech adoption," https://www.pewresearch.org/fact-tank/2021/06/22/digital-divide-persists-even-as-americans-with-lower-incomes-make-gains-in-tech-adoption/, Pew Research Center, 2021.

[62] A. Barroso and A. Brown, "Gender pay gap in u.s. held steady in 2020," https://www.pewresearch.org/fact-tank/2021/05/25/gender-pay-gap-facts/, Pew Research Center, 2021.

[63] R. Fry, J. Bennett, and A. Barroso, "Racial and ethnic gaps in the u.s. persist on key demographic indicators," https://www.pewresearch.org/interactives/racial-and-ethnic-gaps-in-the-u-s-persist-on-key-demographic-indicators/, Pew Research Center, 2021.

[64] S. Mintz, "Boston cyber training company gets $1 million from dhs for diversity efforts," The Business Journals. [Online]. Available: https://www.bizjournals.com/boston/inno/stories/news/2021/11/01/boston-cyber-training-company-gets-1m-from-dhs.html

[65] CISA, "Cisa awards $2 million to bring cybersecurity training to rural communities and diverse populations," CISA. [Online]. Available: https://www.cisa.gov/news/2021/10/20/cisa-awards-2-million-bring-cybersecurity-training-rural-communities-and-diverse

[66] (ISC)^2, "(ISC)^2 diversity award," (ISC)^2. [Online]. Available: https://www.isc2.org/About/Award-Programs/Diversity-Award#

[67] A. Dietsch, "Winner of the at&t diversity and inclusion champion award 2021," AT&T. [Online]. Available: https://cybersecurity.att.com/blogs/security-essentials/winner-of-the-att-diversity-and-inclusion-champion-award-2021

[68] H. Ibarra, N. M. Carter, C. Silva *et al.*, "Why men still get more promotions than women," *Harvard business review*, vol. 88, no. 9, pp. 80–85, 2010.

[69] M.-A. Storey, A. Zagalsky, F. Figueira Filho, L. Singer, and D. M. German, "How social and communication channels shape and challenge a participatory culture in software development," *IEEE Transactions on Software Engineering*, vol. 43, no. 2, pp. 185–204, 2016.

[70] P. P. of Pwning, "picoctf," Carnegie Mellon University. [Online]. Available: https://picoctf.com/

[71] Y. Shoshitaishvili and C. Nelson, "pwn.college," Arizona State University. [Online]. Available: https://pwn.college/

[72] Google, "Learn cybersecurity with google," Google. [Online]. Available: https://learncybersecurity.withgoogle.com/

[73] S. C. Institute, "Girls go cyberstart," SANS Cybersecurity Institute. [Online]. Available: https://girlsgocyberstart.org/

[74] HackerOne, "Home — hacker 101," HackerOne. [Online]. Available: https://www.hacker101.com/

[75] Bugcrowd, "Bugcrowd university," Bugcrowd. [Online]. Available: https://www.bugcrowd.com/hackers/bugcrowd-university/

[76] Google, "Learn - google bug hunters," Google. [Online]. Available: https://bughunters.google.com/learn

[77] M. Martinez-Cola, "Collectors, nightlights, and allies, oh my! White mentors in the academy," *Understanding and Dismantling Privilege*, vol. 10, no. 1, pp. 25–57, 2020.

[78] L. D. Saner, S. Campbell, P. Bradley, E. Michael, N. Pandza, and M. Bunting, "Assessing aptitude and talent for cyber operations," in *Advances in Human Factors in Cybersecurity*. Springer, 2016, pp. 431–437.

[79] "Women in security and privacy," https://www.wisporg.com/, 2022.

[80] C. Stewart, L. Zabierek, and K. Ringrose, "#sharethemicincyber," https://www.sharethemicincyber.com/, 2021.

APPENDIX A
INTERVIEW PROTOCOL

A. *Introduction*

- Hello. My name is [INSERT NAME] and this is [INTRODUCE OTHER PERSON]. Today we will be asking you several questions with the goal of understanding your career path, the steps you've taken to develop the necessary expertise to search for and identify vulnerabilities, and any challenges or difficulties you have faced along the way and how you've overcome them. We are specifically interviewing individuals from marginalized populations in the vulnerability discovery community with the goal of identifying challenges which may limit diversity in this community so that we can push for improvements by relevant organizations (e.g., educational entities, bug bounty platforms, companies hiring security experts, and community groups).
- First, let's quickly go over how the interview is going to work. The interview will be organized around a discussion of your history of expertise development in vulnerability discovery. I will ask you to start by discussing the first time you remember being interested in vulnerability discovery and ask you to recount the path taken to your current position in the vulnerability discovery community. As we go through your story, I ask more specific questions about why you decided to follow specific paths, support and resources available to you, and any challenges you faced. If you would like to mention another person during this journey, please only share their first name. This will help protect confidentiality while

allowing you to still discuss them with us. I expect that the interview will take approximately an hour.

- Describe everything in the consent form
- Although I do not expect this to occur, if you become uncomfortable at any time during the study, please let me know. Do you have any questions at this point?
- Review previously provided consent form
- We sent a consent form to your email address. It tells you whom to contact if you want to report any objections. [POINT OUT BOXES TO CHECK.]

B. *Self-Identification*

- Please indicate how you identify in your personal and work life (ex: mother, security pro, teacher, mentor, LGBTQ, etc.)
  - Do you identify as a person of color?
- Do you specialize in any particular area of vulnerability discovery? (e.g., crypto, web, mobile, social engineering)

C. *Biographical Sketch*

- Next, we would like you to walk through how you developed the skills necessary to search for and identify vulnerabilities in software. Note, as we discuss your personal history in vulnerability discovery, I will be drawing a diagram to represent what you tell me for our records. If you would like to reference it at any point to help jog your memory or you need to correct anything, please let me know and I can display it on my camera. I will also ask you at the end of this section of the interview to review the diagram and confirm its accuracy.
- To begin, when was the first time you remember being interested in vulnerability discovery?
  - What sparked your interest?
  - What did you do to develop this interest (i.e., procure skills necessary to identify vulnerabilities)? Why? These could be through active participation or observation.
    - Were there any other options you considered? Why not those? [Cost expectancy]
  - What did you expect to get out of this learning experience? How did this change after participation?
  - At this time, was there anyone supporting you? (i.e., someone who believed in your ability to learn or perform vulnerability discovery and provide feedback and/or encouragement)
    - Who was most helpful in guiding you to your current career? How? (Cultural capital and social capital theory)
    - If not, Did you reach out to anyone unsuccessfully?
  - At this time, did you feel part of/welcomed by the vuln discovery community? How so?
    - Which peer relationships and interactions were most beneficial? Why?
  - What resources did you draw on?
    - What compelled you to take advantage of these resources and how did you find them? (Cultural capital and social capital theory)
  - How did you activate the knowledge you developed? (i.e., how did you actually use education/training you participated in)
    - What do you think you gained from this activation of knowledge (including things beyond just getting more practice)?
  - Did you face any challenges in participating in the vulnerability discovery community at this point?
    - (for each challenge they list) do you think this challenge is unique to you or does the larger community experience it as well?
  - Did you face any additional challenges at this time in your development beyond what we have already discussed?
  - At this point in time, how would you rate your level of skill as in vulnerability discovery on a scale from 0 (novice) to 10 (expert)? [Self-efficacy theory]
  - At this point in time, what goals were you pursuing with respect to vulnerability discovery and did you believe you would achieve them? [Possible selves theory]
- Where did you go from there? What was the next step in your development? (continue until you reach current point in their career)
  - Repeat the same questions as above about the next step in their trajectory.
- Were there any other things you tried to develop your vuln discovery skill that we did not cover?
  - Were they useful? If not, why?
  - Why did you try them?
- Was there anyone else you haven't already discussed who you relied on for support throughout this process (educationally or emotionally)?

D. *General questions about the vulnerability discovery market*

- Optional, depending on responses through bio sketch section
  - You have identified as being from a marginalized group - how has that shaped your experiences in the bug bounty community, are there specific challenges you faced/overcame/what would help to broaden participation/increase representation. Please give examples. (R1)
    - How did you negotiate the "onliness" and underrepresentation in vulnerability discovery? [Campus ecology theory]
    - If you met racial or sexist stereotypes, what were productive responses? [Stereotype threat theory]
  - Have you observed challenges faced by anyone else from an underrepresented population? Please give examples.

- (optional, usually we don't have time) Where do you see yourself going from here with vulnerability discovery?

Appendix B
Screening Survey

A. Intro

This survey consists of three parts:

1) Your experience being a vulnerability discovery professional
2) Your professional background
3) Demographics

In the next section, you will be asked questions about your experience being a vulnerability discovery professional.

B. Community

1) Are you a member of (or associate with) any professional cybersecurity organizations (e.g., WiCyS, BIC, OWASP, including NGO's and informal groups)?
[Yes, No, Prefer not to answer]
2) **[If yes to 1]** Please list each professional cybersecurity organization that you are a member of or associate with. (e.g., WiCyS, BIC, OWASP, NGO's and informal groups)
[Text box]
3) Do you identify as a member of an underrepresented population in cybersecurity (e.g., woman, Black, Indigenous, person of color, LGTBQ+)?
[Yes, No, Prefer not to answer]
4) **[If yes to 3]** Please list each underrepresented population in cybersecurity you identify as a member of. **[Text box]**

C. Belonging uncertainty

1) Think about how you feel about yourself at different times. Some people pretty much always feel the same way about themselves. Other people feel differently about themselves at different times. Please indicate your level of agreement with the questions below about how you feel about yourself at different times.
[Disagree, Moderately disagree, Neutral, Moderately agree, Agree, Strongly agree]
2) Sometimes I feel that I belong in the vulnerability discovery community, and sometimes I feel that I don't belong.
3) When something bad happens, I feel that maybe I don't belong in the vulnerability discovery community.
4) When something good happens, I feel that I really belong in the vulnerability discovery community.

D. Background

1) What is the highest degree or level of school you have completed?
[Less than 9th grade, 9th to 12th grade, no diploma, High school graduate, Some college, no degree, Associate's degree, Bachelor's degree, Master's degree, Professional degree (e.g., MD, JD), Doctorate degree, Other [text box], Prefer not to answer]
2) What is/was your field of study?
[Text box]
3) Choose the letter grade that corresponds with your cumulative grade point average (GPA) for all subjects in high school.
[A, B, C, D, E/F, Prefer not to answer]
4) Choose the letter grade that corresponds with your cumulative grade point average (GPA) for all courses taken during your undergraduate degree (i.e., Associate's and Batchelor's).
[A, B, C, D, E/F, Prefer not to answer]
5) What is the highest degree or level of school completed by your parents or guardians?
[Less than 9th grade, 9th to 12th grade, no diploma, High school graduate, Some college, no degree, Associate's degree, Bachelor's degree, Master's degree, Professional degree (e.g., MD, JD), Doctorate degree, Other [text box], Prefer not to answer]
6) Which option describes your current employment status best?
[Employed working 40 hours per week or more, Employed working less than 40 hours per week, Unemployed looking for work, Unemployed not looking for work, Retired, Other [Text box], Prefer not to answer]
7) What is your current job title?
[Text box]
8) How frequently do you participate in bug bounty programs?
[Once a day, Once a week, Once a month, Once every 6 months, Once a year, Never]
9) How frequently do you participate in security CTF (Capture The Flag) competitions?
[Once a day, Once a week, Once a month, Once every 6 months, Once a year, Never]
10) How would you assess your skill level as a vulnerability discovery professional on the following scale?
[Fundamental awareness (basic knowledge), Novice (limited experience), Intermediate (practical application), Advanced (applied theory), Expert (recognized authority)]
11) For how many years have you been involved in vulnerability discovery?
[Sliding scale]
12) Growing up (prior to your 18th birthday), did you know any people (in your close surroundings—family and friends) who held jobs in vulnerability discovery or computer security?
[Yes, No, Do not know]

E. Demographics

1) What is your gender?
[Female, Male, Non-binary, Prefer to self describe, Prefer not to answer]
2) Please use the slider to enter your age.
3) In which country do you currently reside?
[USA, India, Russia, Germany, Canada, United King-

dom, Sweden, Netherlands, China, Australia, Other [Text box]]

4) **[USA not selected]** Which of the following describe your race and ethnicity, if any? (select all that apply)
   [White or of European descent, South Asian, Hispanic or Latino/a/x, Middle Eastern, East Asian, Black or of African descent, Southeast Asian, Indigenous (such as Native American, Pacific Islander, or Indigenous Australian, Prefer to self describe [Text box], Prefer not to answer]
5) **[USA selected]** Are you of Hispanic, Latino, or Spanish origin?
   [Yes, No, Prefer not to answer]
6) **[USA selected]** Which of the following best describes your ethnicity? (select all that apply)
   [White, Black or African American, American Indian or Alaska Native, Asian, Native Hawaiian or other Pacific Islander, Prefer to self describe [Text box], Prefer not to answer]
7) Which range matches most closely your total, pre-tax household income in 2019?
   [<$29,000, $30,000 - $49,999, $50,000 - $74,999, $75,000 - $99,999, $100,000 - $124,999, $125,000 - $149,999, $150,000 - $174,999, $175,000 - $199,999, >$200,000, Prefer not to answer]
8) Growing up (prior to your 18th birthday), which range matches most closely to your family's average total, pre-tax household income?
   [<$29,000, $30,000 - $49,999, $50,000 - $74,999, $75,000 - $99,999, $100,000 - $124,999, $125,000 - $149,999, $150,000 - $174,999, $175,000 - $199,999, >$200,000, Prefer not to answer]