HWZ

Die Hochschule für Wirtschaft
in Zürich

From Classroom into Bug Bounty: Investigating Motivational Factors Among Swiss Students

Master's Thesis

Adrian Kress

03.02.2024

Supervisor: Bruno Wüest

Executive MBA – General Management HWZ

Abstract

This thesis explores the growing interest of Swiss students in participating in bug bounty programs, a rapidly expanding and multifaceted aspect of cyber security. With a focus on Switzerland, where a significant shortage of IT professionals is expected in the coming years, this study uses a survey to gain insights directly from students about their initial motivations for participating in bug bounty programs. The survey investigates various motivational factors, encompassing intrinsic factors such as personal interest and passion for cyber security challenges, and extrinsic factors like potential financial rewards and career advancement opportunities. Additionally, the study examines the impact of academic backgrounds in promoting interest in the realm of bug bounty and assesses whether educational institutions are effectively equipping students for this career path. The results underscore key motivators and potential gaps in academic preparation for this field. These findings are vital for educators and professionals in cyber security, as they provide a foundation for the further development of educational programs and initiatives that align more closely with student motivations and industry requirements. Ultimately, this work aims to shed light on the gap between academic learning and practical application in cyber security and to promote student engagement in bug bounty programs early in their careers. Notably, leaders of bug bounty programs in large Swiss companies and the National Center for Cybersecurity expressed their interest in this work and its results, underlining its importance and impact.

Acknowledgments

I would like to express my sincere gratitude to my advisor, Bruno Wüest, for his extensive advice and support during the writing of this thesis. Additionally, I extend my heartfelt thanks to Urs Müller for his efforts in reviewing this thesis, providing invaluable insights and contributions that significantly enhanced the quality of my work. Furthermore, my appreciation extends to all the individuals who participated in and shared the survey. Without their participation, it would not have been possible to write this thesis.

Artificial Intelligence

This thesis has incorporated the assistance of artificial intelligence tools for the drafting of certain text segments. It's important to note, however, that all interpretations, conclusions, and the overall structure of this work are solely the result of my own intellectual endeavor. The artificial intelligence was utilized purely as a supplementary aid in the writing process, helping to articulate ideas and refine language. The critical thinking, analysis, and academic rigor that underpin this thesis are entirely my own.

Contents

1 Introduction

1.1 Relevance of the Topic

Cyber security has transitioned from a niche skillset to a fundamental aspect of modern digital infrastructure. Traditionally, the task of testing software products and services for security vulnerabilities was the domain of internal security teams and external penetration testers. However, these teams often faced limitations in terms of their size and the diversity of expertise they could apply. Such constraints put them at a disadvantage against attackers who, with access to publicly available products and services, could come from a vast pool with varied skills and techniques. This imbalance in expertise between defenders and attackers highlights the need for broader and more diverse approaches to cyber security. As a result, bug bounty programs have become an integral element of the security culture in many organizations [1]. These programs harness the collective expertise of a global pool of participants, offering a more robust and diverse defense mechanism against potential cyber threats [2]. Particularly for students, bug bounty programs present an opportunity to apply their theoretical knowledge in real-world contexts, bridging the gap between academic learning and practical cyber security experience [3]. This thesis focuses on Swiss students, exploring their motivations to engage in bug bounty programs and how these motivations align with their academic experiences.

1.2 Objectives and Research Question

The central objective of this thesis is to explore and understand the factors that influence Swiss students' decision to participate in bug bounty programs. This inquiry delves into what motivates or deters them from engaging in these activities, which are becoming increasingly vital in the cyber security landscape. The primary research question guiding this study is: "What factors influence the decision of Swiss students to participate in bug bounty programs, and what could motivate them to become active in this area?" This question aims to uncover both the drivers and barriers faced by students, providing insights that could be instrumental in shaping future educational strategies and industry practices in cyber security.

1.3 Structure of the Thesis

This thesis is divided into several chapters in order to systematically address the research topic. It begins with an introduction that outlines the relevance of the topic, the objectives and the research question. Following this, Chapter 2 provides a detailed theoretical background that offers insights into the definitions and concepts of bug bounty programs, the cyber security skill gap in Switzerland and relevant motivational theories. Chapter 3 looks at the current state of research on bug bounty programs, identifies existing gaps and establishes a link between theory and research question. The methodology used for this study, including the research design, survey details, data collection and analysis procedures, is described in detail in Chapter 4. Chapter 5 presents the results of the survey, analyzing the data to provide meaningful insights. The discussion in Chapter 6 interprets these results in the context of the provided background and discusses implications for practice and future research. The thesis concludes with a summary of key findings, acknowledgement of limitations and suggestions for future research in Chapter 7, followed by a bibliography and an appendix containing the survey.

2 Theoretical Background

2.1 Definition and Concepts of Bug Bounty Program

For the sake of clarity, this section is divided into two parts. In Section 2.1.1, "What is a bug?", we define and examine software bugs in the context of cyber security. For a better understanding, it is important to know what a bug is before we can dive deeper. In 2.1.2, "What is a bug bounty program?", we then focus on the structure and purpose of bug bounty programs.

2.1.1 What is a Bug?

A software bug refers to any error, flaw, or fault found within computer software's design, development, or operational stages, leading to incorrect or unexpected results, or causing the software to act in unintended ways. In the context of software, a vulnerability is defined as a bug that has an impact on security. While it is true that all vulnerabilities stem from bugs, not every bug constitutes a security risk. For the purpose of this thesis, we define a bug as one that possesses a security impact and has the potential to lead to a vulnerability. Consequently, bugs that go undetected for an extended period of time become particularly significant security threats as they can be discovered and exploited by malicious actors. Despite advancements in software engineering, the inherent complexity of code and its interactions across multiple platforms render complete bug elimination nearly impossible, leading to the release of software with potential vulnerabilities [1]. Software companies recognize the economic and security risks posed by these bugs and employ internal teams for regular security updates [4]. Simultaneously, independent researchers and ethical hackers, understanding the value of these bugs, engage in identifying and reporting them, often expecting rewards for their findings [5]. In contrast, cybercriminals exploit these vulnerabilities for illicit access to systems [6]. Notably, in grey or black markets, such exploits can often be sold at a higher price than a bug [1].

2.1.2 What is a Bug Bounty Program?

Bug bounty programs, also known as vulnerability reward programs, motivate independent security specialists, penetration testers and ethical hackers, so-called bug hunters, to track down software vulnerabilities and report them to the operators of the program. These operators, often software companies or external entities, establish specific guidelines, including the types of vulnerabilities that qualify, technical standards, participant eligibility, and the procedures for submission and assessment of reports. The rewards in bug bounty programs can be monetary, varying from a few hundred to over USD 100,000 based on the severity of the vulnerability, or non-monetary, like branded merchandise or recognition in the program's hall of fame.

This concept is now seeing adaption in domains like e-voting systems, government operations, and autonomous vehicles [7], [8], [9]. For instance, the Swiss government initiated a program, offering up to €132,000 for discovering flaws in their e-voting system, with maximum rewards of €44,000 for undetectable vote manipulation [7]. In the United States, the Department of Defense launched the ‘Hack the Pentagon’ initiative in April 2016, aiming to evaluate the advantages of exposing vulnerability discovery to external hackers. This program identified 138 vulnerabilities within six hours [10]. Its success led to a new vulnerability disclosure policy by the Department of Defense, expanding the scope of domains accessible to hackers [8], [11]. Furthermore, there have been propositions for U.S. government departments to engage in identifying vulnerabilities in open-source projects [12].

Bug bounty programs vary in their framework and aims. They can focus on specific software products, a range of products, or the entire service infrastructure of an organization. Some programs are dedicated to commercial software, while others reward the identification of vulnerabilities in free and open-source software or third-party products. The scope of these programs encompasses a variety of software types, from operating systems and browsers to web, mobile, and embedded technologies. The objectives of bug bounty programs are not uniform, ranging from straightforward bug rectification to shaping market dynamics and hindering cybercriminals' access to sophisticated exploits on illegal markets.

2.2 The Shortage of Cyber Security Experts in Switzerland

Recent findings show a concerning rise in cyber security breaches, leading to significant financial losses for many companies, often over $1 million [13]. A notable factor contributing to this issue is the acute shortage of cyber security experts, particularly in cloud security and security operations, impacting around 68% of organizations [13]. Even though the global cyber security workforce reached 4.7 million in 2022, there remains a gap of 3.4 million needed professionals [14]. A survey further indicates that 29% of IT managers report an insufficient number of IT staff to ensure full protection of their IT infrastructure. This shortage is especially severe in certain industries, with banks and insurance companies experiencing a critical lack of IT security specialists (43% and 42%, respectively), while manufacturing and retail face lower shortages (23% and 9%, respectively) [15]. Industries dealing with sensitive data are especially at risk of sophisticated cyber-attacks, highlighting the urgent need for skilled IT security staff. The situation is similar in Switzerland, where despite the considerable presence of foreign nationals in the IT sector (32%), a shortfall of approximately 40,000 IT professionals is anticipated by 2030 in Switzerland [16].

In conclusion, the increasing cyber security breaches underline the need for more qualified IT security experts, especially in vulnerable sectors such as banking and insurance, to improve cyber defenses in Switzerland.

2.3 Motivation Theories in the Context of Bug Bounty Programs

In the context of bug bounty programs, the motivational factors influencing participation, particularly among students transitioning from academic environments to the practical realm of cyber security, are complex and multifaceted. A study from 2020 provides a comprehensive analysis, underscoring that while financial incentives are a significant draw, they are not the sole motivators. Their findings suggest that intrinsic factors such as the intellectual challenge and the opportunity for skill development play a crucial role in encouraging participation in bug bounty programs [17].

Adding to this perspective, another recent study explores the viewpoints of bug hunters themselves, revealing that rewards and learning opportunities are highly valued. This insight is particularly relevant for students who often prioritize knowledge acquisition and skill enhancement. Interestingly, the study also notes that reputation-building (e.g. by publishing bugs found or write-ups of bugs), traditionally considered a key motivator, is deemed less important among participants in bug bounty programs, indicating a shift in the motivational dynamics within these programs [5].

Furthermore, the concept of gamification in bug bounty programs, as proposed by another study, introduces an innovative dimension to motivation. By embedding game-like elements into these programs, there is potential not only to enhance engagement but also to offer alternative forms of reward that resonate with a younger audience like students. This approach could lead to a more diverse and sustained participation in bug bounty programs, fostering a richer pool of talent in cyber security [18].

In summary, the drivers of participation in bug bounty programs are not limited to monetary rewards but include a blend of intrinsic factors such as intellectual stimulation, skill development, and the novel application of gamification. These elements are crucial for engaging students and fostering a robust and dynamic cyber security community.

3 State of Research

3.1 Current State of Research on Bug Bounty Programs

In the area of bug bounty programs, researchers have investigated the motivations of bug hunters through an analysis of market behavior and direct engagement with the hunters themselves.

Studies delving into empirical data from bug bounty programs, such as vulnerability reports and payments, offer insights into hunters' program selections. These studies reveal correlations between hunter activity and factors like expected monetary rewards and program age [19], [20]. This data aligns with findings from public reporting from programs like Google Chrome and Mozilla Firefox [2], as well as HackerOne data [20].

Other publications have utilized surveys to explore hunter demographics and motivations in bug bounty programs. Notably, HackerOne [3], [21] and Bugcrowd [22] , the largest bug-bounty platforms, produce annual marketing materials that survey participants on their platforms. These surveys gather data on bug hunter demographics and offer a high-level perspective on their motivations, such as financial incentives and educational benefits. Building on previous research, another study [5] provides a deeper exploration into the motivations and experiences of bug hunters in bug bounty programs. By employing direct surveys and interviews, this study gained a more thorough understanding of the factors that drive participation in bug bounty programs, offering a richer and more detailed perspective on the priorities and incentives of bug bounty hunters.

3.2 Gaps in the Existing Research

The existing research on bug bounty programs primarily focuses on the organizational perspective [19], [20] often neglecting the individual experiences of bug hunters. There's a significant gap in studies focusing on how individuals begin their journey in bug bounty programs. While some research [5] delves into the motivations and challenges of bug hunters, these studies don't specifically focus on the initial steps or the educational pathways that guide students, particularly in Switzerland, to engage in bug bounty hunting.

Furthermore, research on bug bounty programs often takes a global perspective, overlooking the unique cultural, educational, and regulatory characteristics of the Swiss environment that may influence students' participation in these programs. This global perspective may not accurately reflect the specific dynamics in Switzerland that influence students' decision to participate in bug bounty hunting. Moreover, theses studies did not examine how Swiss educational institutions and curricula prepare or influence students to participate in bug bounty programs.

3.3 Relation of the Theory to the Research Question

Based on the information from Chapter 2, we can address the following research question: **"What factors influence the decision of Swiss students to participate in bug bounty programs, and what could motivate them to become active in this area?"**

The foundational understanding of bug bounty programs, as detailed in Section 2.1, is critical for analyzing student motivations. It is essential to not only consider what motivates students to participate in these programs but also to examine their awareness and understanding of what bug bounty programs entail. Knowing whether Swiss students can accurately describe and understand the concept of a bug bounty program is vital for this study's aim to assess their readiness and potential to engage in bug bounty programs. This includes their grasp of how bug bounty programs operate, as these perceptions could significantly influence their decision to engage with such programs.

Section 2.2 highlighted the shortage of cyber security experts in Switzerland. This workforce gap could potentially motivate students to participate in bug bounty programs, seeing them as an opportunity to address this skill shortage. The increasing demand for skilled professionals, especially in sectors such as banking and insurance, which offer lucrative career opportunities, may encourage students to view bug bounty programs as a viable pathway to develop essential skills and gain valuable experience in a high-demand field. Understanding the factors that motivate students to enter the cyber security field and how this knowledge can be used to recruit and train new talent is directly related to the research question. This understanding is pivotal to addressing the shortage of cyber security professionals in Switzerland.

Section 2.3 explored the motivational aspects of bug bounty programs, highlighting that students are attracted not just by financial rewards, but also by the intellectual challenges and opportunities for skill development that these programs provide. This understanding of intrinsic motivators, such as the pursuit of knowledge and skill enhancement, is essential in comprehending what drives Swiss students towards these programs. This insight adds to the complexity of the research question, emphasizing the multifaceted nature of student motivations in the context of bug bounty programs.

In conclusion, the theoretical background outlined in Chapter 2 provides a comprehensive perspective on the factors that could influence Swiss students' engagement in bug bounty programs. From the need to address the shortage of cyber security professionals to understanding the various motivations that drive student engagement, existing research is supportive in examining the specific factors that motivate Swiss students to participate in bug bounty programs. Consequently, it provides a solid foundation for the development of the methodology, which is detailed in the following chapter.

4 Methodology

This chapter outlines the methodology used to investigate the motivational factors that drive Swiss students to participate in bug bounty programs. This chapter is organized into four sections.

Section 4.1 outlines the overall approach and rationale behind the chosen methodology, explaining why a survey was the most appropriate tool for this investigation.

Next, Section 4.2 dives into the specific structure and content of the survey. It details the nature and format of the questions, which are designed to probe both intrinsic and extrinsic motivational factors among Swiss students. Additionally, the questions address areas such as personal interest in cyber security, passion for solving challenges, potential financial benefits, and career advancement prospects.

Section 4.3 explores the methodology for gathering research data, describe the strategies employed to contact Swiss students and the criteria for their selection. This section also addresses potential biases and limitations encountered during the sampling process.

Finally, Section 4.4 describes the methods used for analyzing the collected data. It will explain how the responses were evaluated and interpreted to draw meaningful insights about the students' motivations and the influence of academic curricula on their interest in bug bounty programs.

4.1 Research Design

The decision to use a survey to investigate the motivational factors of Swiss students in relation to bug bounty programs is supported by findings from similar studies in other fields. Most notably, [23] examined the motivational influences on architects and engineers in planning offices. In this study, a survey was effectively used to identify key motivational characteristics. This method proved valuable for thoroughly identifying and analyzing important factors and underscores the effectiveness and suitability of surveys for exploring motivational dynamics in different professional fields.

Following this model, a survey-based approach was used in this investigation. Surveys are particularly effective in capturing a broad range of viewpoints, which is essential for a comprehensive understanding of the unique motivations that might influence student participation. This methodology can be used to provide a deep understanding of the various incentives that drive student participation, ranging from monetary gains to the pursuit of increased knowledge and skill enhancement.

4.2 Description of the Survey

SurveyMonkey was used to conduct the survey. The survey begins with an introductory section, welcoming participants and explaining the purpose of the study. It assures participants of data privacy and seeks consent for data handling in accordance with SurveyMonkey's privacy policy. If participants agree to the privacy policy, they will be redirected to the main part of the survey. The main part of the survey is structured into several sections, each dedicated to different aspects. This segmentation is intended to provide a comprehensive answer to the research question by analyzing its various aspects. After the main part of the survey, it concludes with a section for additional comments and an option for participants to leave their email address for further information.

In the following chapters, we take a closer look at the individual sections of the survey and explain the rationale behind the individual questions. We will highlight some specific questions, their importance in the context of the study and the selection of available responses.

4.2.1 Overall Interest in Cyber Security

By assessing the baseline interest in cyber security, we can distinguish between intrinsic and extrinsic motivational factors. This is an essential part of answering the research question. Therefore, the initial section of the survey starts with straightforward and easy-to-answer questions to engage participants comfortably. One specific question in this section is: "On a scale of 1 to 5, how interested are you in cyber security?" This question aims to gauge the baseline interest of participants in the field of cyber security. The simplicity of this rating scale question allows for an easy start, encouraging participants to engage more deeply as the survey progresses.

Further, questions about the platforms where participants consume cyber security-related content, such as social media, online forums, or e-learning platforms, provide insights into their information-gathering habits. The survey also includes a question about participation in cyber security activities like CTF competitions or online courses, which helps to understand their practical engagement in the field.

It was a strategic choice to start the survey with simple, engaging questions, which not only facilitate a comfortable start for participants but also extract essential information regarding their involvement in the cyber security space.

4.2.2 Awareness of Bug Bounty

In this section the depth of participants' knowledge about bug bounty programs is investigated. A critical question, "From where did you first hear about bug bounty programs?" with options like university, social media, cyber security events, or friends, illuminates the channels through which bug bounty programs are most effectively reaching potential participants. This information not only sheds light on how students are introduced to these programs, but also shows which marketing channels are used effectively to promote bug bounty programs. The survey further probes the participants' confidence in explaining what a bug bounty program is, a question that gauges the depth of their understanding. A pivotal question in this section is, "Would you try out a bug bounty program?" with the possible responses being 'No,' 'Yes,' and 'Yes, but only if...'. The inclusion of the conditional "'Yes, but only if..." option allows for a sophisticated understanding of the specific factors or circumstances that might encourage or discourage students to participate in bug bounty programs. This is incredibly important for bug bounty program operators to gain insight into how they can attract more hunters.

4.2.3 Motivation to Participate in Bug Bounty

In the "Motivation to Do Bug Bounty " section, the survey focuses on uncovering the driving factors behind students' interest in participating in bug bounty programs. Key questions explore aspects such as their primary goals if they were to engage in bug bounties, with options ranging from earning money to contributing to the security of products/services. This helps in understanding the various incentives that could attract students to bug bounty activities. The survey also asks about the specific technologies or areas they would prefer to focus on in bug bounty programs, which sheds light on their areas of interest or expertise. Additionally, the importance of receiving recognition for achievements in these programs is examined, offering insights into whether external validation plays a role in their motivation.

4.2.4 Barriers to Do Bug Bounty

In this section, the survey explores the obstacles that might prevent students from participating in bug bounty programs. A key question here is, "What do you consider the primary barrier to participating in bug bounty programs?" with options like lack of skills or knowledge, time constraints, and fear of legal consequences. This question helps identify the most significant hurdles students face, which is essential for understanding why some might hesitate or abstain from participating. Such insights are crucial in tailoring strategies to lower these barriers and make bug bounty programs more accessible and appealing to potential participants.

4.2.5 How to Learn the Necessary Know-How for Doing Bug Bounty

This section, "How to Learn the Necessary Know-How for Doing Bug Bounty," investigates how students perceive their educational journey towards becoming proficient in bug bounty hunting. It includes crucial questions like whether the knowledge gained from university courses contributes to their success in bug bounties or helps in learning relevant skills faster. This question is important in understanding the perceived gap between academic learning and practical skill requirements in bug bounty programs. Additionally, the survey asks about resources that students believe would best help them gain necessary skills, such as formal coursework, online resources, practical experiences, or mentorship. These insights are key in identifying effective learning pathways that could encourage and prepares students to participate in bug bounty programs.

4.2.6 Demographic Questions

The last section of the survey gathers basic but essential demographic information from participants. This includes questions about their age, gender, current degree program, and field of study. These questions are crucial for providing context to the other responses in the survey, as they help in understanding the diversity and background of the participants. This demographic data enables a more nuanced analysis of the results, as it allows for examining how factors like age, gender, and academic background might influence attitudes towards bug bounty programs. This information is key to drawing more comprehensive conclusions from the survey data.

4.3 Data Collection and Sampling

To obtain a satisfactory number of responses for the survey, the authors personal network was utilized by approaching students and graduates and asking them to pass the survey on to suitable candidates. The survey was primarily aimed at Swiss students, as mentioned in the introduction, but was not exclusively limited to this group. Within the survey, a specific question in the demographic section served as a filter to identify respondents who were actively studying in Switzerland, which is consistent with the study's focus on the student perspective. Nevertheless, results outside of this focus group could also be interesting.

In this study, data was collected via SurveyMonkey, an online tool for creating and distributing surveys. This service enabled the creation of a survey from which a direct link was created and distributed to potential respondents via the authors' personal network. To increase reach, the survey link was also distributed via LinkedIn to reach a wider audience.

4.4 Data Analysis Procedure

The main objective of the data analysis is to put the survey data into a form that allows conclusions to be drawn in relation to the research question. The process begins with data cleansing, where all invalid entries are removed, e.g. typos or answers that are not plausible, including those from participants who completed the survey too quickly to provide meaningful data. In the analysis phase, SurveyMonkey and Microsoft Excel analysis tools are used, allowing for effective data clustering. This approach ensures a thorough and insightful analysis that aligns with the objectives of the study and sheds light on the research question.

5 Results

5.1 Survey Metadata Analysis

The survey was launched on 20 December 2023 and ended on 15 January 2024. The highest response rate was on 22 December 2023, with 31 responses. The survey contained 25 questions, including multiple-choice questions, rating scales and open-ended questions, and initially attracted 96 participants. Out of the initial 96 respondents, 68% (amounting to 65 individuals) successfully completed the survey and agreed to the data privacy terms. These participants spent an average of 6 minutes and 36 seconds on the survey, with all response times over 2 minutes, indicating that there were no invalid or rushed responses.

5.2 Demographic Overview

The average age of participants was 26.2 years, with the youngest being 20 and the oldest 44, and a median age of 25. A significant majority of the respondents, 87%, identified as male, 7% as female, and 6% preferred not to specify their gender. Regarding educational background, 69% were currently enrolled in a degree program. Of these, 29% were enrolled in a Bachelor's program, 57% in a Master's program, and 14% were pursuing a PhD. Among those not currently enrolled in a degree program (31%), 29% held a Bachelor's degree, and 62% a Master's degree. Participants predominantly represented institutions like ETH Zurich (45%), EPFL (9%), and ZHAW (8%). The field of study was heavily skewed towards Computer Science and Cyber Security (84%), with a smaller representation in Mathematics and Data Science (6%). The rest of the respondents were approximately evenly distributed across a variety of other academic disciplines.

5.3 Comprehensive Analysis

In this section, we will look at each section of the survey and analyze responses.

5.3.1 Overall Interest in Cyber Security

In the "Overall Interest in Cyber Security" section, notable enthusiasm is evident, with 52% of participants rating their interest at 5 out of 5, and an average interest level of 4.1. Figure 1 indicates that 50% frequently engage with cyber security content on YouTube. Social media platforms and cyber security blogs or websites are also popular, with 47.3% and 44.59% of respondents using them, respectively.

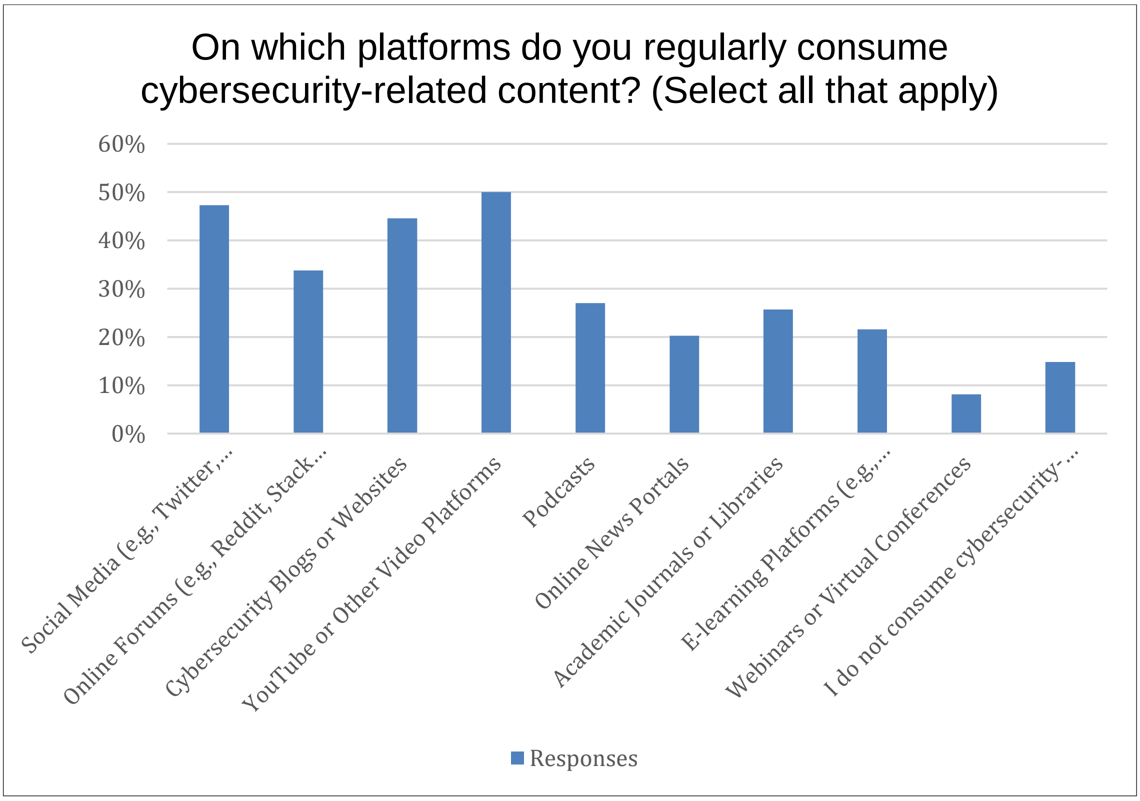

Figure 1: Question 3

In terms of practical involvement, Figure 2 shows that 45% have tried platforms such as Hack The Box or Try Hack Me, 41% have attended cyber security conferences and 38% have played CTF challenges, indicating active engagement in cyber security.

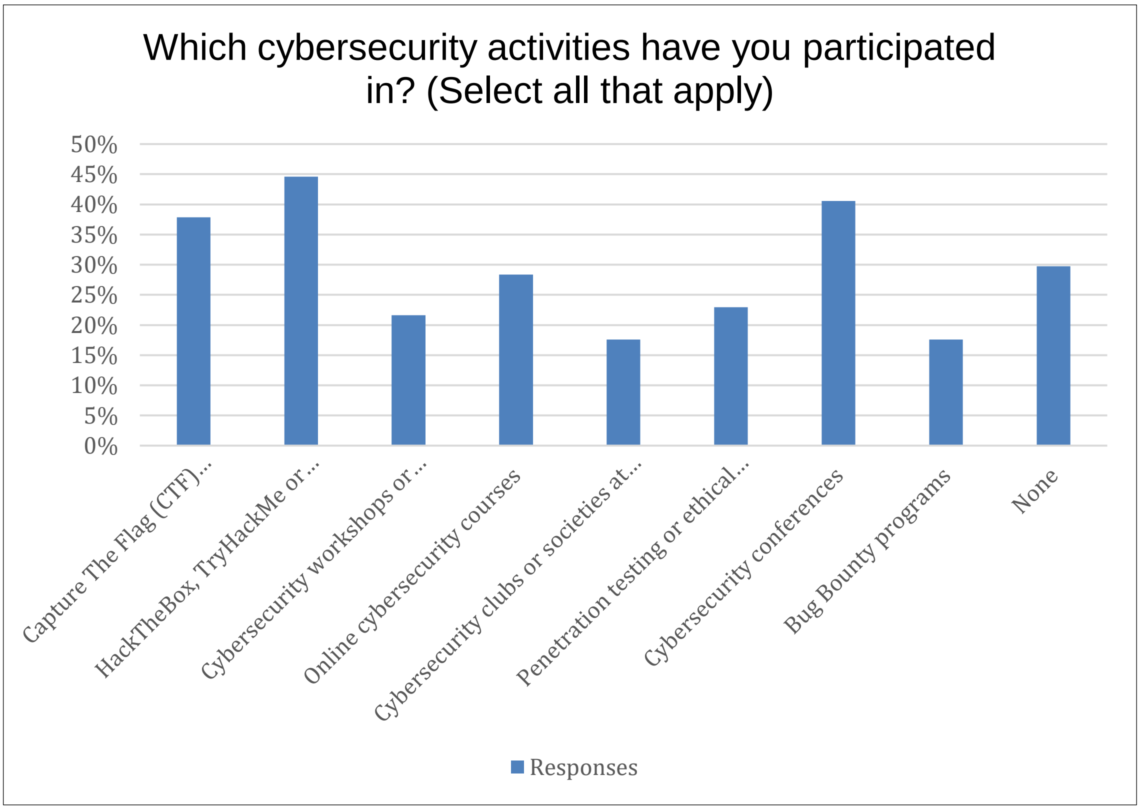

Figure 2: Question 4

5.3.2 Awareness of Bug Bounty

The results in this section show that participants rated their understanding of the concept of bug bounty as good, with an average confidence level of 3.8 out of 5 in explaining the concept to someone unfamiliar with bug bounty. A significant 82% of participants were willing to try a bug bounty program if given enough time or initial guidance. An interesting result is shown in Figure 3 below. Most of the respondents (26%) heard about bug bounties for the first time from friends or colleagues.

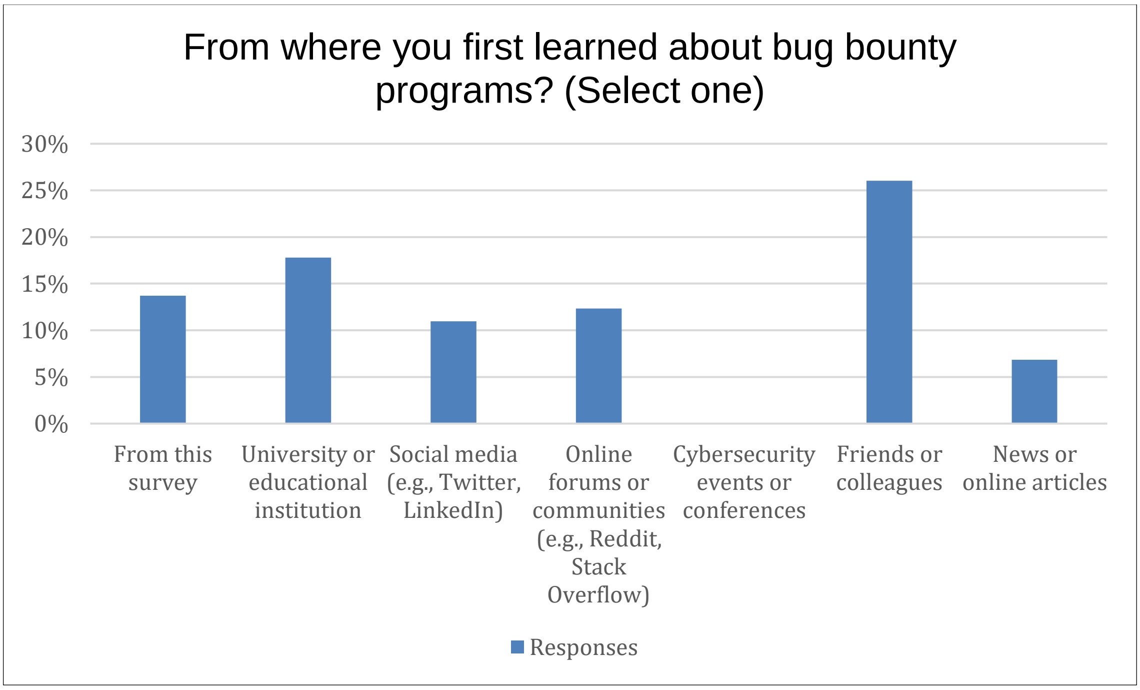

Figure 3: Question 5

5.3.3 Motivation to Do Bug Bounty

In the survey, gaining practical experience proved to be a slightly more important motivation for starting bug bounty (37%) than earning money (35%), which is consistent with previous studies [5]. The importance of receiving certificates was moderately rated at 3.0 out of 5, yet a notable 89% believe bug bounty experience would enhance their resume. In terms of focus areas, Figure 4 shows that 61% of participants prefer to start with web application security, followed by Internet of Things (IoT) at 36% and network security at 34%.

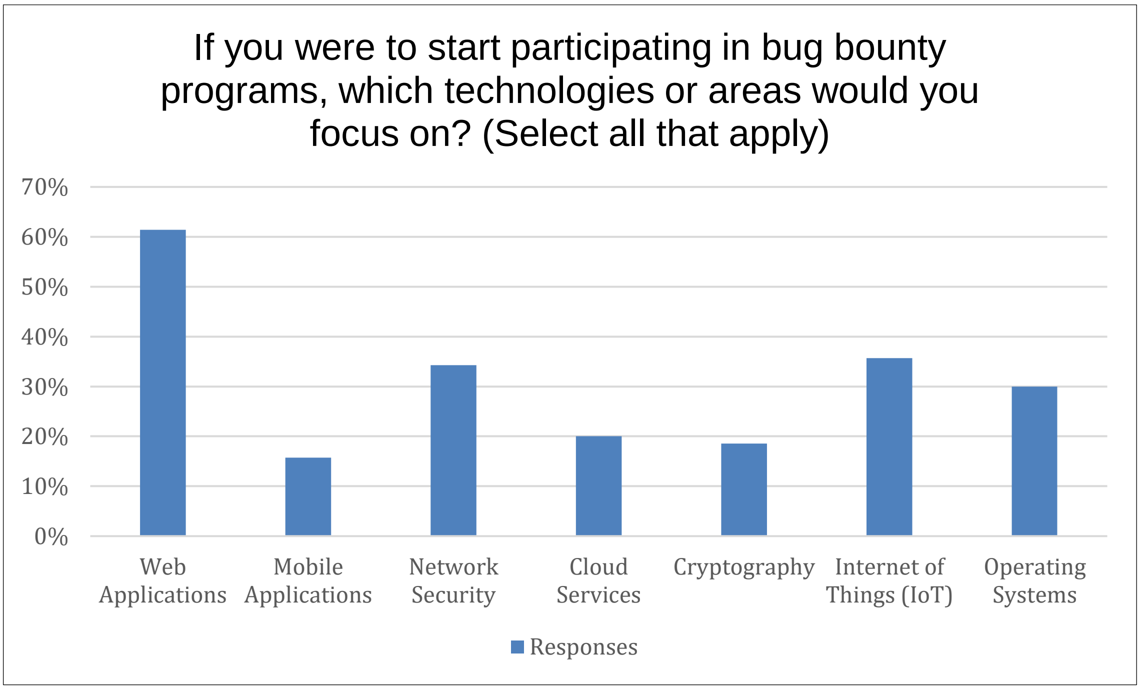

Figure 4: Question 9

5.3.4 Barriers to Do Bug Bounty

In this section, participants rated the balance between the effort required and the potential financial rewards in bug bounty programs with an average score of 2.4 out of 5. Confidence in their ability to find and report vulnerabilities was also rated moderately with an average of 2.5 out of 5. The primary barrier identified was time constraints (43%), followed by a lack of skill or knowledge (36%) as shown in the Figure 5 below.

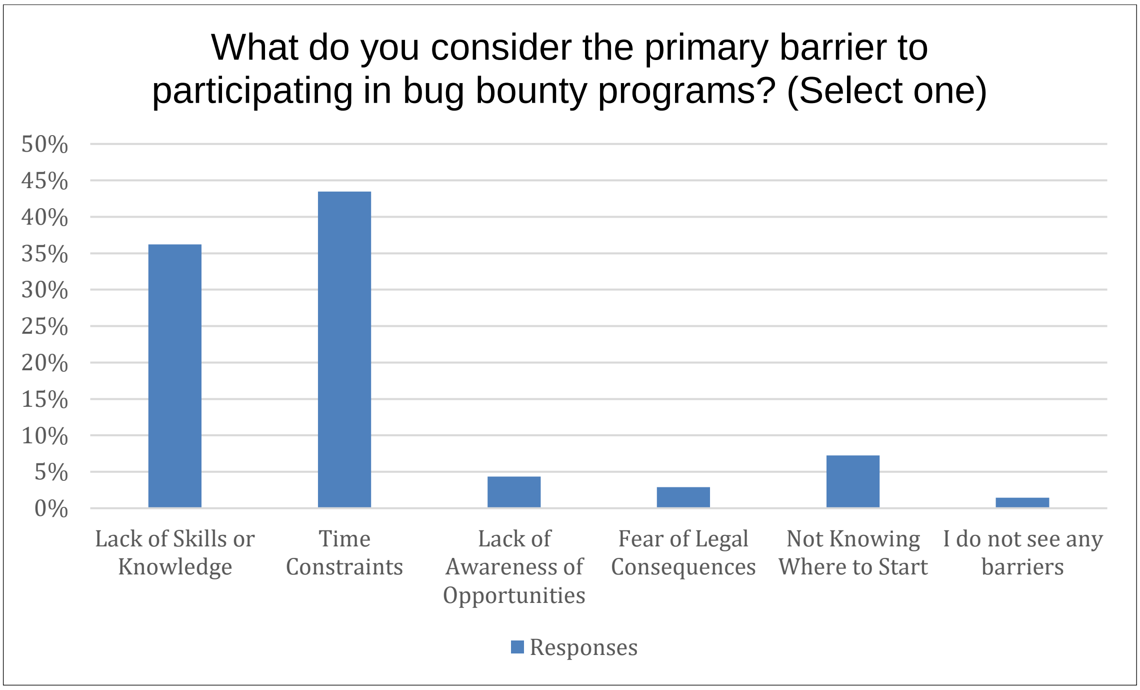

Figure 5: Question 12

5.3.5 How to Learn the Necessary Know-How for Doing Bug Bounty

In the survey, only 56% of respondents believe that their university courses provide an advantage in participating in bug bounty program or learning relevant skills more quickly. Of those who see an educational advantage, network security and cryptography were cited by 38% as areas where university courses are particularly beneficial. In addition, 28% of participants feel that their university courses provide an advantage in the area of web applications and 29% in area of operating systems. The results are illustrated in Figure 6.

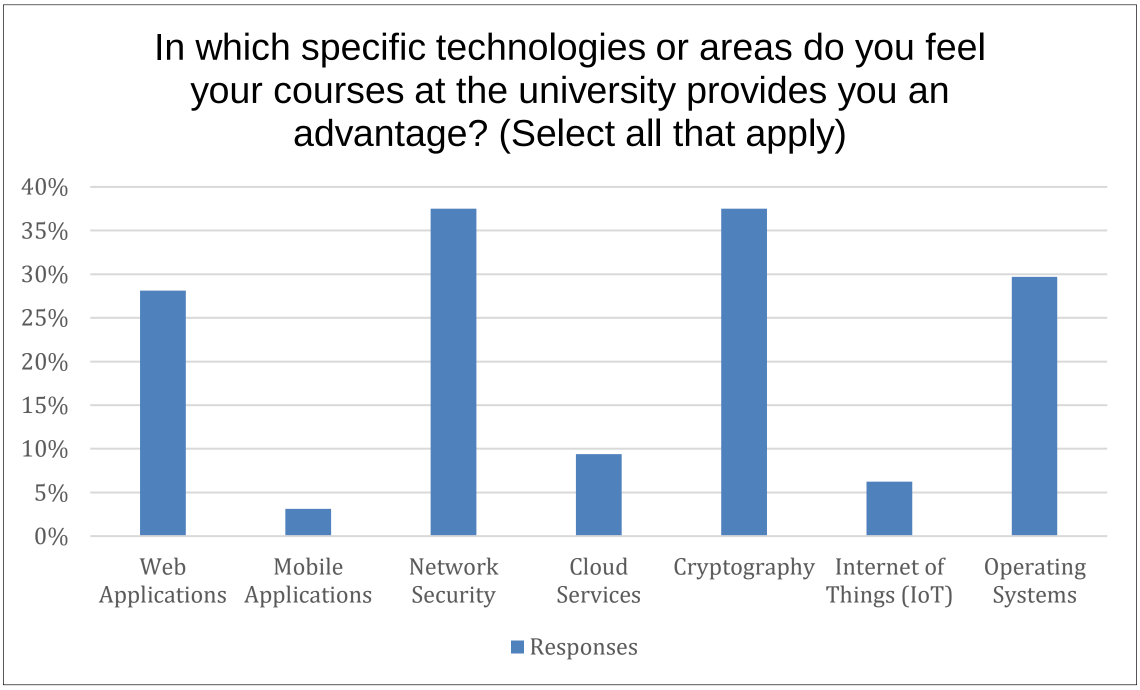

Figure 6: Question 16

As shown in Figure 7, 50% of the participants indicated that practical experiences, such as participating in Capture the Flag (CTF) events or using platforms like Hack The Box, would be the most beneficial in acquiring the skills necessary for bug bounty programs. Additionally, self-study through online resources like blogs, tutorials, and forums was ranked as the second most effective method, with 16% of respondents favoring it.

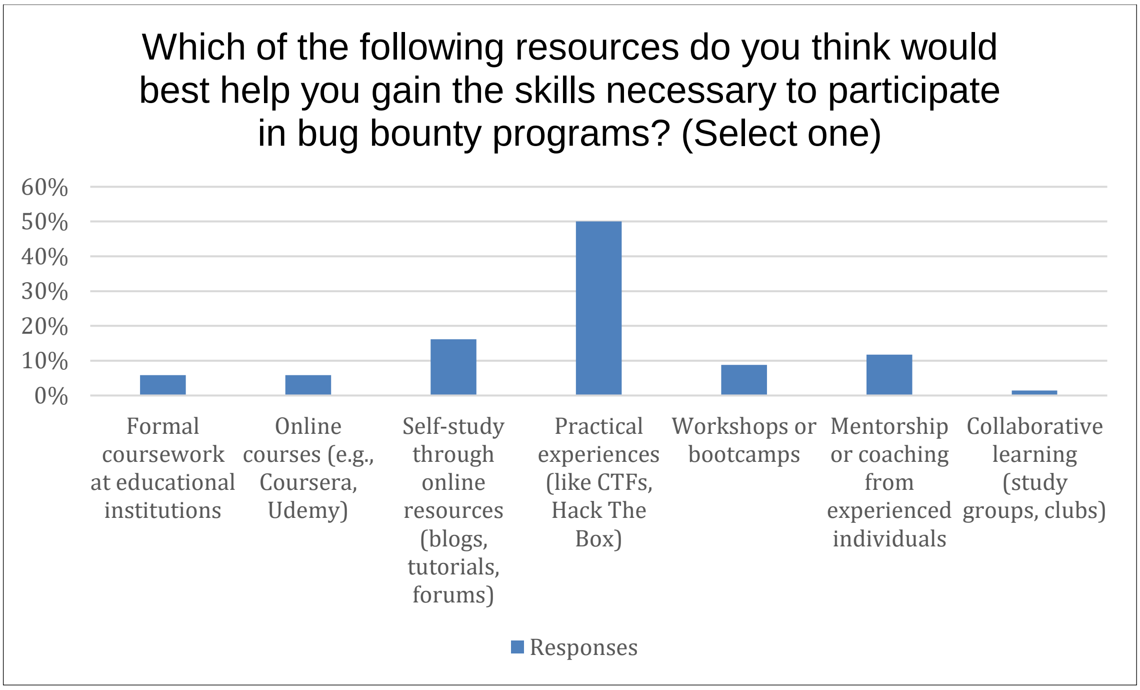

Figure 7: Question 17

5.4 Comparative Group Analysis

In this chapter we will analyze how certain groups responded to different questions and look at stand-out findings.

5.4.1 Experienced vs. Novice Perspectives

In this section, we focus on the 13 participants with experience in bug bounty programs. They exhibited a significantly higher average confidence level of 4.2 out of 5 in finding and reporting vulnerabilities, compared to the overall average of 2.5. Moreover, these experienced participants placed greater importance on recognition for achievements in bug bounty programs, with an average importance rating of 4.2, higher than the overall average of 3.0. To a certain extent, this contradicts the findings from [5]. Apart from these distinctions, their responses did not show significant differences compared to the broader participant group. For instance, in assessing the balance between effort required and potential financial rewards in bug bounty programs, their average rating was 2.7, closely aligning with the general average of 2.4.

5.4.2 Field of Study

In this chapter, we group the participants according to their field of study, which leads to different categories: Computer Science, Engineering, Mathematics and Physics, and Others (which includes fields such as Management, Law, etc.). An interesting result emerged from question 13. Participants from the fields of Computer Science, Engineering, Mathematics and Physics rated the balance between the effort required and potential financial rewards at around the overall average of 2.4 out of 5. However, participants from the "Other" category rated it significantly higher at 3.5, as shown in Figure 8.

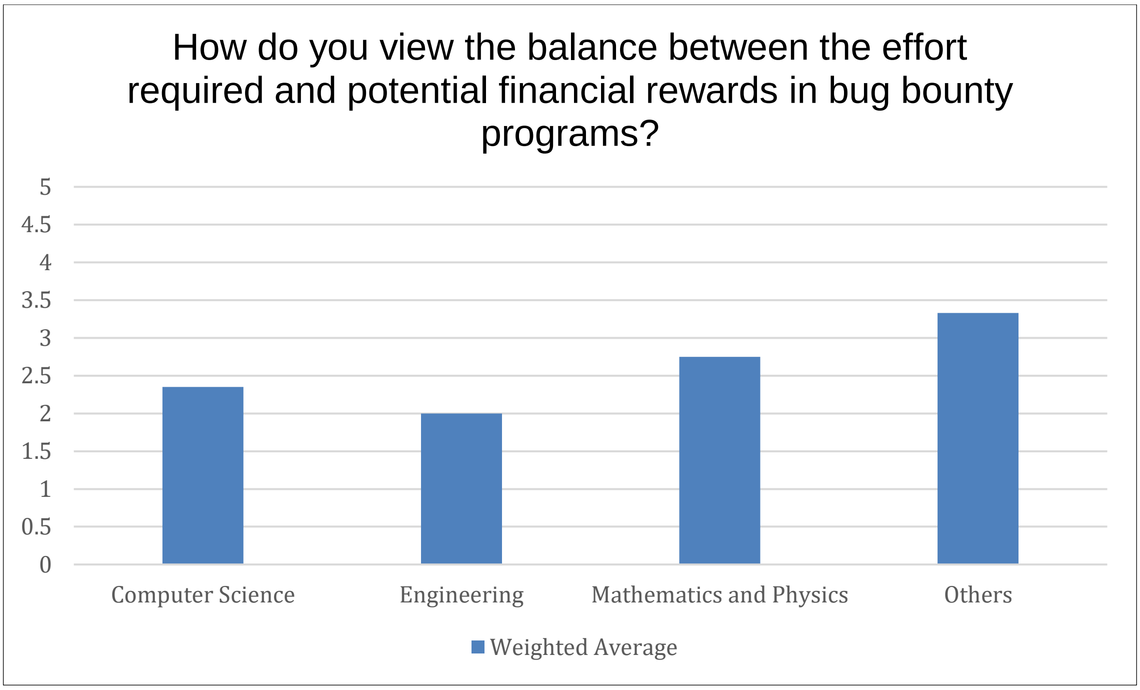

Figure 8: Question 13 Filtered by Field of Study

In addition, Figure 9 shows a notable trend among engineering students, most of whom indicated that they would prefer to start in the area of Internet of Things (IoT). This contrasts with the responses to question 16 ("In which specific technologies or areas do you feel your courses at the university provides you an advantage? (Select all that apply)") regarding the specific technologies or areas in which university courses provide an advantage. Interestingly, none of the engineering participants selected Internet of Things (IoT) in this context. 43% from engineering answered that no courses from their degree program will give them an advantage, 29% see an advantage in network security.

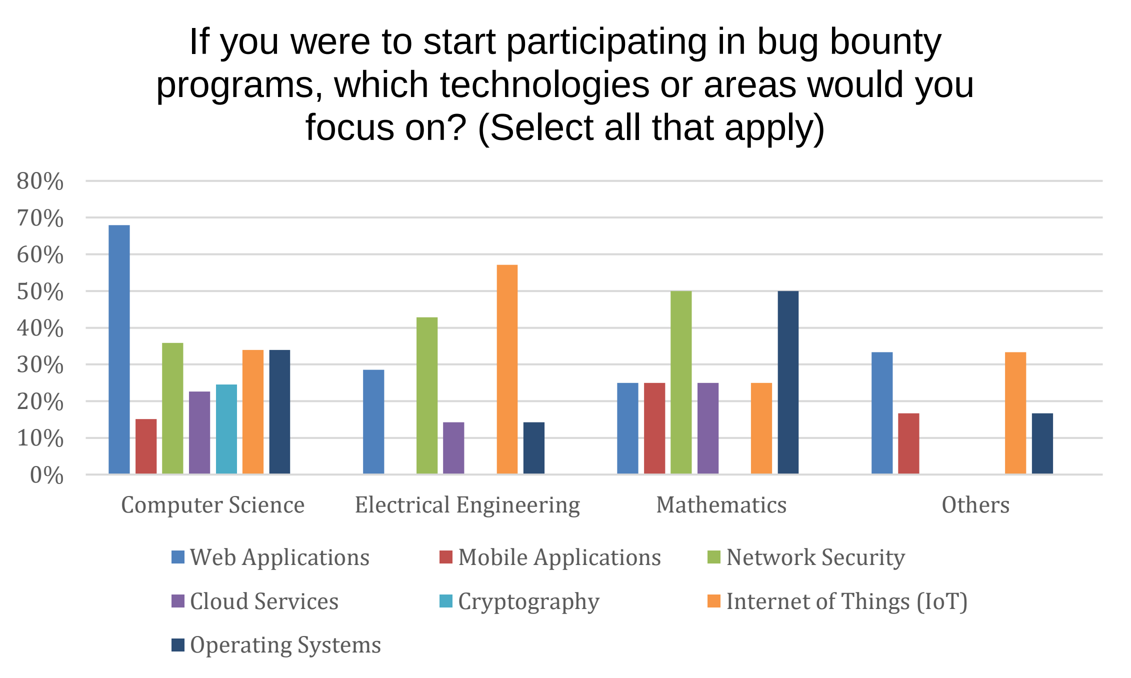

Figure 9: Question 9 Filtered by Field of Study

5.4.3 Type of University

In this subsection, we group the participants from ETHZ and EPFL as representatives of the traditional universities and compare them with the participants from the group of universities of applied sciences (ZHAW, OST, HSLU). Overall, the differences between these groups are not particularly pronounced. However, a noteworthy observation emerges from question 16 regarding the perceived advantages in certain technologies or areas due to university courses. In chapter 205.3.3, as illustrated in Figure 4, we saw that 61% of all participants prefer to start with web applications in bug bounty programs. In this analysis, similar trends are observed: 54% of the participants from ETHZ and EPFL, and 67% of the participants from ZHAW, OST and HSLU expressed a preference to start with web applications. Given this, only 17% of ETHZ and EPFL students believe that they have an advantage in this area, as shown in Figure 10.

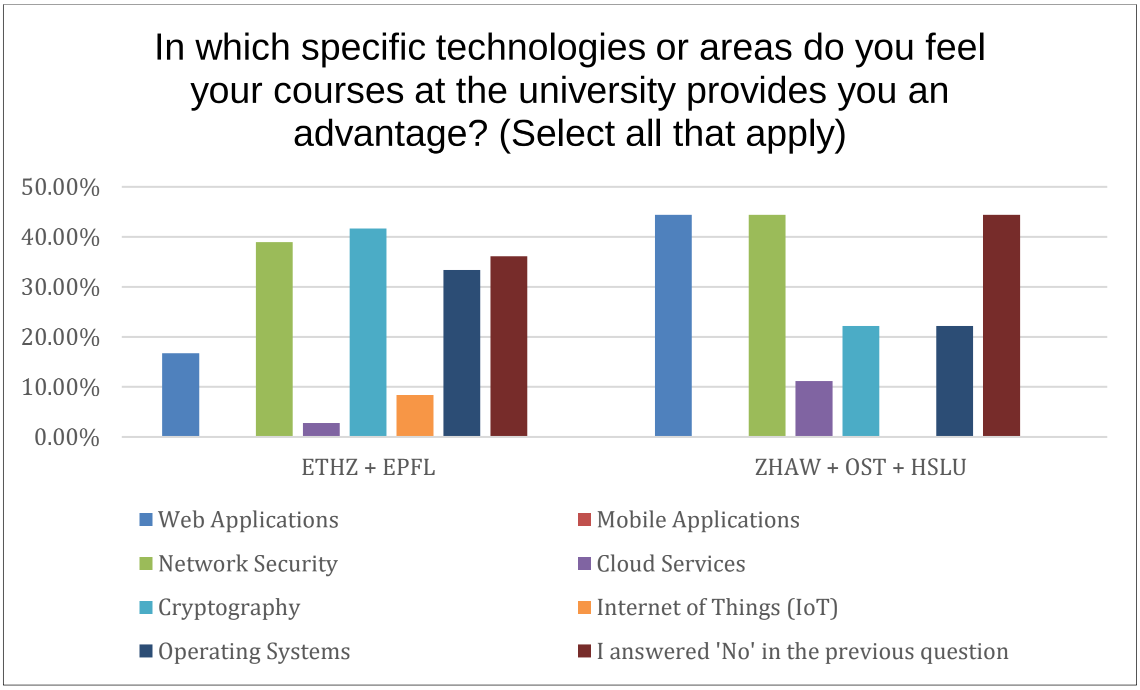

Figure 10: Question 16 Filtered by Type of University

Another interesting observation from question 12, relating to the main barriers to participation in bug bounty programs, shows that 41% of ETHZ and EPFL students cited a lack of skills or knowledge as the main barrier. This percentage is slightly lower than the 43% who stated a lack of time. In comparison, 56% of ZHAW, OST and HSLU students cited lack of skills or knowledge as the main barrier, followed by lack of time and not knowing where to start (both 22%), as shown in Figure 11. This finding is interesting, especially considering that 44% of the students from university of applied science stated that their university courses gave them an advantage in the area of web applications (Figure 10).

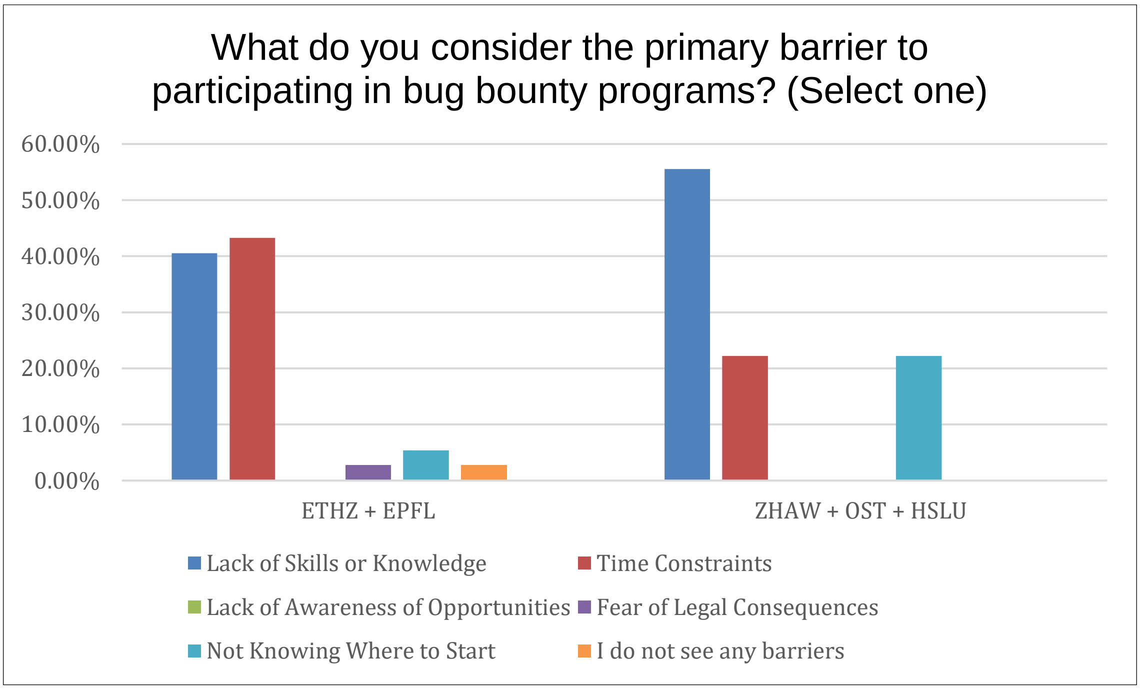

Figure 11: Question 12 Filtered by Type of University

Similar to this observation, the results from question 14 "How confident are you in your ability to find and report vulnerabilities in a bug bounty program?" reveal a noteworthy contrast in self-assessed confidence between different groups of students. Participants from ETHZ and EPFL rated their confidence at 2.7 out of 5, which is a significant amount higher than the average of the universities of applied sciences group, with a confidence rating of 1.7.

Another notable difference was found in attitudes towards recognizing bug bounty achievements (e.g. certificates or recognition) between these groups. Participants from ETHZ and EPFL rated the importance of recognition at an average of 3.2 out of 5. In contrast, participants from the universities of applied sciences (ZHAW, OST, HSLU) rated the importance of recognition lower, with an average score of 2.6.

5.4.4 Type of Degree

In this analysis, we compare the survey results of Bachelor, Master, and PhD students. Question 15 " Do you think the knowledge you gained from the courses at the university will give you an advantage when participating in bug bounty programs or help you learn the relevant skills faster?" shows a clear tendency. The results in Figure 12 show that the higher the degree, the more participants believe in the advantage of their university courses for bug bounty activities. Specifically, 38% of Bachelor students, 48% of Master students and 83% of PhD students see their education as beneficial for participating in bug bounty programs.

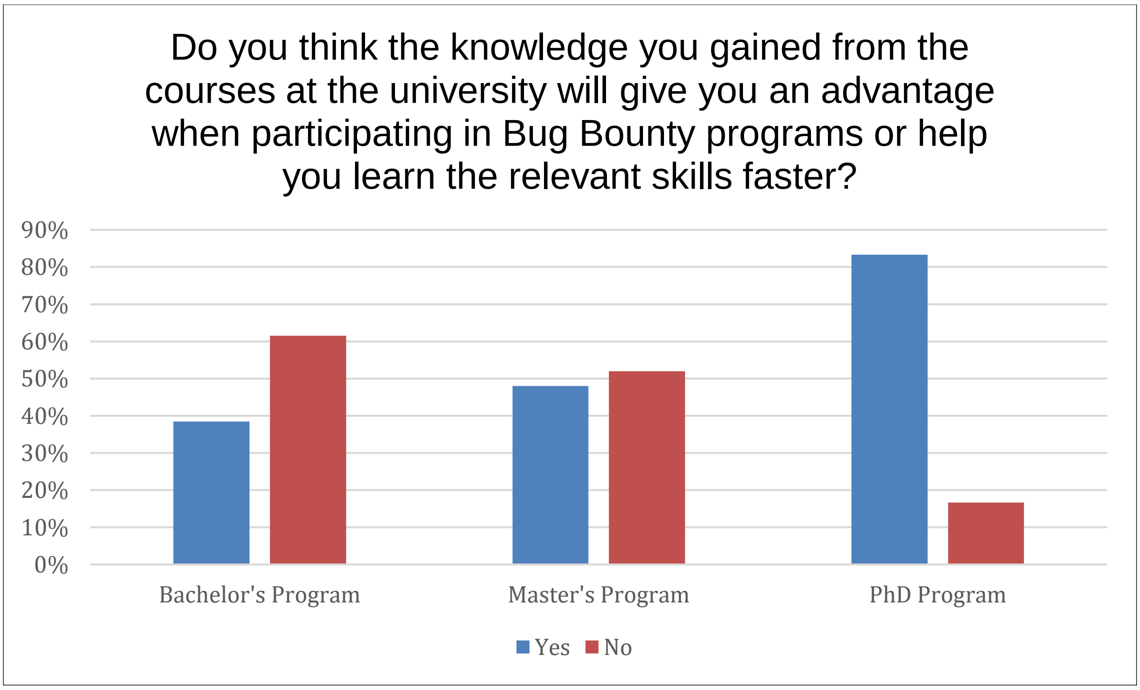

Figure 12: Question 15 Filtered by Type of Degree

This trend is further reflected in the responses to Question 14, where participants rated their confidence in finding and reporting vulnerabilities in a bug bounty program on a scale of 1 to 5 stars. A clear correlation is evident: the higher the degree, the greater the confidence. Bachelor students averaged at a confidence level of 2.2 out of 5, master's students at 2.5, and PhD students at 2.8.

The findings from question 13 regarding the perceived relationship between effort and potential financial reward for bug bounty programs also show a trend. The participants rated this ratio on a scale of 1 to 5, with Bachelor's students averaging at 2.7, Master's students at 2.4 and doctoral students significantly lower at 1.7. This is illustrated in Figure 13.

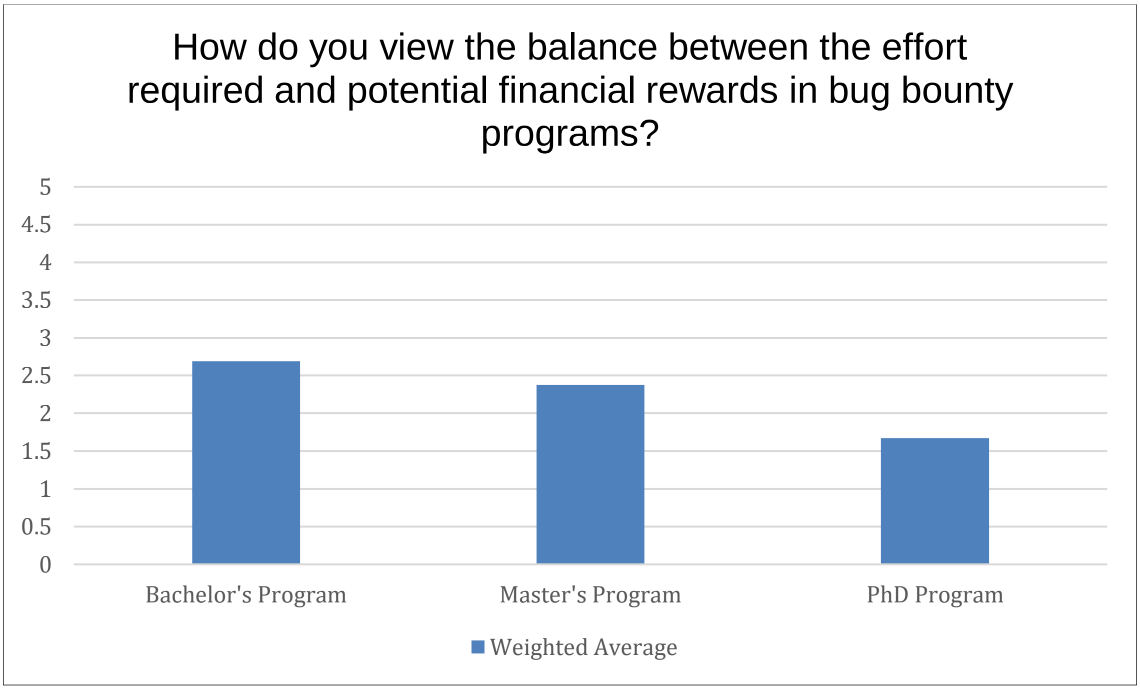

Figure 13: Filtered by Type of Degree

6 Discussion

6.1 Key Findings

The survey, which aimed to understand the motivating factors of Swiss students to participate in a bug bounty program, was opened by 96 participants, 65 of whom completed the survey in full. Demographic analysis revealed that the average participant was a 25-year-old male, predominantly enrolled in a master's program at ETH Zurich, majoring in computer science. This demographic distribution aligns well with the trends observed in ETH Zurich's Equality Monitoring 2022 report [24]. In the study, we conducted a comprehensive analysis and a comparative group analysis of the survey results. This approach allowed for a deeper understanding of how different demographic factors interact and influence Swiss students' participation in bug bounty programs. The comprehensive analysis delved into the overall interest in cyber security, awareness of bug bounty programs, and motivational factors, while the comparative group analysis focused on contrasting these elements across various demographic groups.

6.1.1 Key Findings of the Comprehensive Analysis

The survey revealed a high level of interest in cyber security among participants. A significant number of them regularly consumed security-related content on platforms such as YouTube and other video platforms. In addition, many participants were actively involved in cyber security-related activities and actively engaged in platforms such as Hack The Box and Try Hack Me.

Most participants feel that they have a good understanding of the bug bounty concept, and the majority are willing to try bug bounty programs. Interestingly, the study revealed that most of the participants heard about bug bounty for the first time from their friends or colleagues.

Furthermore, the findings showed that participants prioritize gaining practical experience over earning money when engaging in bug bounty programs. This aligns with previous research trends indicating similar preferences [5]. The survey showed that the importance of certifications is rated as medium, but most respondents believe that bug bounty experience would enhance their resumes. In terms of specific focus areas in which to begin bug bounty, web applications were most frequently cited, followed by Internet of Things (IoT) and network security.

In this survey, the effort-to-reward ratio for bug bounty programs was rated as medium, as was confidence in finding and reporting vulnerabilities. Lack of time and lack of skills or knowledge were cited as the main challenges by the respondents.

More than half of participants believe that their university courses provide an advantage when participating in bug bounty programs or learning relevant skills more quickly. The greatest benefits were seen in the areas of network security and cryptography, followed by web applications. The majority of participants emphasized the value of hands-on experience, such as Capture the Flag events or using platforms such as Hack The Box for acquiring skills. Self-study using online resources was also stated as an effective learning method.

6.1.2 Key Findings of the Comparative Group Analysis

The survey was completed by 13 participants with bug bounty experience. It was found that these experienced individuals placed more importance on recognition for their achievements in bug bounty programs. Despite these differences, their views on the balance between effort and reward in bug bounty programs were like those of the wider participant group and closely aligned with the overall average rating.

In a group analysis, participants were categorized into groups such as Computer Science, Engineering, Mathematics and Physics, and Other (including Management, Law, etc.) based on their field of study. Interestingly, participants from the first three categories rated the ratio of effort to potential financial reward for bug bounty programs as lower than participants from the "Others" category, representing non-technical areas, who rated this ratio much more positively.

Furthermore, a notable trend was revealed that shows that engineering students prefer to start in the area of Internet of Things (IoT). However, when asked about the advantages provided by their university courses in specific technologies or areas, none of the engineering students identified IoT as an area of advantage. Furthermore, a significant portion of engineering students felt that their degree program did not offer any advantages for bug bounty activities, while some recognized benefits in network security.

In a further analysis, the students from ETH Zurich and EPFL were grouped together as representatives of the traditional universities and those from ZHAW, OST and HSLU as representing the universities of applied sciences. The analysis showed that the differences in perspectives between these groups were small overall. As we saw in the comprehensive analysis, the majority of participants stated that they would start in the area of web applications if they were to begin with bug bounty. This result was also reflected in this analysis, with students from universities of applied sciences seeing a greater benefit in their university courses for this area than their peers from traditional universities. In a way, this contradicts the result of the question of where participants see the main barrier to participating in bug bounty programs. A considerably large proportion of participants from universities of applied sciences stated, "Lack of Skills or Knowledge" and "Not Knowing where to start" as the main barrier to enter bug bounty. Students from ETH Zurich and EPFL mainly cited lack of time as the main barrier, closely followed by "Lack of Skills or Knowledge" and " Not Knowing Where to Start". This observation is also reflected in the self-assessed confidence levels of students from universities of applied sciences. These students generally reported lower confidence in their ability to find and report bugs in bug bounty programs compared to their peers from traditional universities.

Furthermore, a significant difference was observed in how much value was placed on recognition for bug bounty activities. Participants from ETH Zurich and EPFL showed a higher appreciation for recognition, such as certificates, compared to their counterparts from universities of applied sciences.

In Section 5.4.4, we analyzed the survey responses from Bachelor, Master, and PhD students, revealing two significant trends. Firstly, there seems to be a correlation between the level of academic degree and the perceived benefit of university courses in acquiring bug bounty skills. The higher the academic degree, the greater the benefit participants see from their university education in acquiring the skills necessary for bug bounty activities. This result is also reflected in the question " How confident are you in your ability to find and report vulnerabilities in a bug bounty program?" where participants with a higher degree returned a higher score.

On the other hand, the second trend can be observed in the answers to the question about the balance between effort and potential financial reward in bug bounty programs. Bachelor's students rated this ratio as the most profitable, Master's students as moderate and doctoral students as the least favorable.

6.2 Interpretations of Findings

This chapter focuses on the interpretation of the results of the study. It aims to draw conclusions on some outstanding results, as well as contradictory or divergent results shown in the findings.

6.2.1 Misalignment in the Marketing Strategies

The comprehensive analysis of our survey revealed a popular trend: most participants actively engage with cyber security-related content on platforms such as YouTube, Twitter or LinkedIn. This behavior not only indicates a keen interest in cyber security, as also reflected in the survey results, but also uncovers a crucial insight. The initial awareness of bug bounty programs seems to have come predominantly from personal and academic sources, rather than from these digital platforms. Most participants discovered bug bounty opportunities through interactions with friends, colleagues, or university channels. This result could indicate that the marketing strategies of bug bounty programs are non-existent or misaligned. Despite the popularity of online platforms as sources of cyber security information, it appears that bug bounty programs are not utilizing these spaces effectively for outreach.

6.2.2 Average to Low Effort to Financial Reward Ratio

The results of our survey clearly showed in Section 5.3.4 that most participants rate the effort to financial reward ratio as medium. Considering that the median reward for a bug on the HackerOne platform is $500 [25], which is relatively modest given Switzerland's high cost of living, this perception is understandable. The participants' confidence in their ability to find and report vulnerabilities was also rated at an average of 2.5 out of 5, further suggesting that the financial compensation, balanced against the likelihood of finding a bug and its potential financial reward, is seen as low.

Participants with a technical field of study rate the relationship between effort and financial reward in bug bounty programs lower than their non-technical colleagues as shown in the results of Section 5.4.2. This is in line with information from the employer review platform Kununu, which lists software architect as the profession with the highest average salary in Switzerland at the time of writing [26]. This would suggest that people with technical skills are finding more stable and better paid opportunities in the job market than participating in bug bounty activities. Adding to this, Section 5.4.4 shows a parallel trend among participants with higher degrees, who also rate the effort to financial reward ratio in bug bounty lower. This reflects the general market trend in Switzerland, where higher degrees generally go hand in hand with higher average salaries, according to survey results [27].

6.2.3 Importance of Recognition

Previous studies have found that monetary incentives are not the only motivators for students to participate in bug bounty programs [5]. This finding is consistent with the empirical data collected in this study, which emphasizes the importance of gaining practical experience. The majority of students even stated that such experience would be beneficial for their resume.

Particularly revealing is the observation in Section 5.4.3 that students from traditional universities such as ETH and EPFL place more value on recognition than their peers from universities of applied sciences. This trend could be due to the more theoretical nature of the programs at traditional universities, which encourages students to seek recognition as proof of their practical skills.

Interestingly, the 13 participants who already had experience with bug bounty did not consider the relationship between effort and potential financial reward to be particularly worthwhile. However, these participants rated the importance of recognition quite highly. This suggests that for these individuals' participation in bug bounty is less of a financial venture and more of an opportunity to gain practical experience and recognition that may serve as a form of credential to enhance their professional profile.

6.2.4 Entry Difficulties for Student from University of Applied Sciences

The transition from the academic world to practical engagement in bug bounty programs appears to pose a particular challenge for students at universities of applied sciences. Unlike students from traditional universities, who primarily cite "Time Constraints" as the main obstacle to participating in bug bounty programs, universities of applied sciences students identify "Lack of Skills or Knowledge" and " Not Knowing Where to Start" as their primary barrier. This result is somewhat intriguing, especially when you consider that a relatively high proportion of universities of applied sciences students see their degree program as useful for the area of web application security.

Although they recognize the knowledge acquired in their courses, these students show a relatively low level of confidence in finding and reporting vulnerabilities compared to the responses of participants from traditional universities. This paradox highlights a potential gap: despite having a solid knowledge of theory, universities of applied sciences students appear to have difficulty translating this knowledge into practical applications in the field of bug bounty.

6.3 Implications for Best Practices

In this section, we draw on findings from Section 6.2 to outline best practices for bug bounty program owners, platform operators, and educators.

6.3.1 Align Marketing

In this section, we focus on the importance of aligning marketing strategies for bug bounty programs and platform providers in Switzerland with the media consumption habits of potential participants. Given that most participants regularly consume cyber security content through platforms like YouTube and other social media, yet primarily hear about bug bounty programs through personal networks like friends and family, there is a clear opportunity for targeted marketing on these digital channels. Given that, it is highly recommended to increase the marketing presence on YouTube and other social media platforms to engage potential bug bounty participants. This can be effectively accomplished by collaborating with influencers or streamers within the cyber security community, or through direct marketing campaigns on these channels. Such strategies will not only enhance visibility but also foster active participation in bug bounty programs.

Additionally, considering that monetary rewards are not the primary attractor for most participants in this survey, it may be beneficial to focus the marketing message more on the educational aspects of bug bounty programs. Emphasizing how participants can learn and gain practical experience would likely resonate more with the target audience, aligning with their interests in skill development and career advancement in the field of cyber security. This shift in marketing focus can further enhance the effectiveness of the programs in attracting and engaging potential participants.

6.3.2 Alternative Forms of Acknowledgement

As highlighted in Section 5.3.3, gaining practical experience emerged as a slightly more significant motivational factor for beginning bug bounty activities compared to earning money. Additionally, Section 5.4.1 revealed that experienced bug bounty hunters place a greater emphasis on receiving recognition for their achievements. These insights underscore the need for alternative forms of acknowledgement in bug bounty programs, beyond just financial incentives. Here are some potential ideas which could help to diversify a bug bounty's reward system:

Bug discovery certificates: Awarded as formal recognition for identifying security vulnerabilities, enhancing a participant's professional standing in the cyber security field.

Public recognition: Featuring contributors on websites and social media boosts their professional reputation and community standing.

Tickets to cyber security training programs and conferences: These initiatives provide a twofold advantage by not only rewarding bug hunters with valuable educational opportunities but also serving as effective marketing and sponsorship channels for the training providers and conference organizers. They enhance participants' technical skills while promoting the respective events and programs within the cyber security community.

Customized swag and merchandise: Branded items can create a sense of belonging and appreciation for the bug bounty hunter.

Recognition in product updates: Crediting contributors in updates where their findings were crucial underlines their impact on improving product security.

Recognition hierarchy with gamification: Incorporating a tiered system based on contribution levels alongside gamification elements can greatly boost participant engagement. This approach is supported by previous research, highlighting the effectiveness of gamification in enhancing involvement [18].

Job offers: Potential bug hunters could be offered job opportunities, such as part-time security testing roles or full-time positions. Furthermore, this could also help reduce the shortage of cyber security experts in Switzerland, as discussed in Section 2.2.

In the end, including different forms of rewards can significantly increase the appeal of bug bounty programs as they are tailored to the different motivations of hunters and so attracting a wider range of participants. These incentives can also serve as effective marketing platforms for courses or conferences, while providing a unique opportunity to recruit motivated cyber security talents in the market.

6.3.3 Tailored Courses

Given the different motivations and barriers identified in Section 5.3 across the different student demographics, this subchapter proposes tailored educational approaches for designing courses and delivering the necessary knowledge for successful participation in bug bounty programs.

Bridging knowledge gaps: According to the survey results, students from universities of applied sciences seem to have difficulties applying their academic knowledge in the bug bounty world. Customized courses for these students should therefore focus on bridging this gap between the theoretical understanding of a technology and its practical application in bug bounty activities.

Time management strategy courses: Participants from ETH Zurich and EPFL in this survey identified the primary barrier to entering bug bounty programs as a lack of time. To mitigate this, tailored courses should focus on time-efficient methodologies in bug hunting. This includes techniques for efficient scanning of bug bounty programs for specific vulnerabilities and the ability to swiftly switch to the next target if no vulnerabilities are found within a predetermined timeframe. These strategies align with findings from HackerOne [3], which reveal that the largest segment of bug hunters dedicate between 1-9 hours weekly to their activities, underscoring the importance of maximizing the impact of limited time.

Internet of Things (IoT) as a gateway: As shown in Section 5.4.2, engineering students seem to have an interest in starting their bug bounty journey in the Internet of Things (IoT) domain. Courses tailored to engineers could capitalize on this interest by presenting Internet of Things (IoT) security challenges as a gateway into the cyber security landscape.

A preferred learning method: Section 5.3.5 underscores a significant preference among participants for acquiring bug bounty skills through practical experience. Popular platforms like Hack The Box and Try Hack Me emerge as favored learning tools. Integrating these or comparable hands-on platforms into the curriculum can offer invaluable practical exposure.

In conclusion, these tailored educational approaches aim to address the unique needs and barriers faced by different student demographics. By aligning educational content with the specific interests and challenges of each group, these courses can more effectively prepare students for active and successful participation in bug bounty programs.

7 Conclusion and Outlook

7.1 Conclusion

Bug bounty programs have become increasingly popular in recent times; in fact, this concept is now also being implemented in various areas such as e-voting systems or autonomous vehicles [7], [9]. This trend could be due to the critical shortage of cyber security experts worldwide, as highlighted in a recent study [14]. Switzerland is not spared from this either, as experts predict that there will be a considerable shortage of IT specialists in Switzerland in the coming years [16]. In this context, it is becoming increasingly important to explore how to effectively attract and motivate young people into the cyber security field in order to close this cyber security talent gap.

While existing research has delved into the motivational factors of bug hunters [5] and the program-specific elements that enhance the efficacy of bug bounty programs [18], a critical gap remains. The specific motivations that lead individuals to initiate their journey in bug bounty hunting have not been extensively researched. As studies in the field of bug bounty predominantly take a global perspective rather than a specific educational background of bug hunters, this thesis focuses on the Swiss landscape and examines how students in particular are drawn into the world of bug bounty programs. It therefore attempts to answer the related research question: "What factors influence Swiss students' decision to participate in bug bounty programs and what might motivate them to become active in this field?".

To find answers to the research question, a survey method was chosen as it can capture a wide range of perspectives. The survey explored various aspects, including initial interest in cyber security, awareness of bug bounty programs, specific motivating factors, and perceived barriers to participation in bug bounty programs. Crucially, detailed demographic information was also collected, including participants' degree programs and university affiliations. This demographic data is key to identifying trends across different groups and provides a more nuanced understanding of how different educational and cultural backgrounds influence motivation to participate in bug bounty activities.

The survey revealed some interesting insights. Although most of the participants regularly consume cyber security related content on YouTube or other social media platforms, most of the participants heard about bug bounty for the first time from friends and colleagues. The study showed that the relationship between the effort involved in discovering and reporting vulnerabilities and the potential financial reward is perceived as only moderately rewarding. Nevertheless, a significant majority in the survey expressed a willingness to try participating in a bug bounty program. As the data suggests, this willingness is driven less by the financial aspect and more to the desire to gain practical experience in the field of cyber security. In particular, the participants in this survey who had already gained experience with bug bounty programs not only valued the practical skills they had acquired, but also placed more value on the recognition they received when hunting for bugs. There were also clear differences between the different fields of study. Where, for example, computer science students would rather focus on web applications in a bug bounty program, engineering students would prefer the Internet of Things (IoT) area. The answers also varied between the different types of universities. For example, students from traditional universities were more likely to cite lack of time as the main barrier to participating in bug bounty programs, while students from universities of applied sciences were more likely to cite a lack of skills or knowledge as the main barrier. Furthermore, the answers to several questions showed that the higher the academic degree, the less attractive the relationship between effort and financial reward appears to be.

Best practices have now been derived from these findings, such as more targeted marketing on YouTube or other social media platforms, with the inclusion of cyber security influencers, for example. Alternative rewards, such as certificates for vulnerabilities found and reported, can be implemented alongside financial rewards in a bug bounty program to recognize the work of the bug hunter with a token of appreciation. Advice has been developed for bug bounty course providers on how to tailor their courses to the specific needs of different demographic groups. Ultimately, the results of this work provide insights for various stakeholders involved in bug bounty programs, offering guidance on making their programs or courses more attractive to Swiss students. The findings may also have parallels outside Switzerland.

7.2 Limitations and Improvements

Although the study attracted many interested participants that provided sufficient data for a thorough analysis, there are some limitations. The majority of respondents were ETH students (47%). Overall, 79% of participants were studying computer science. This may have led to biased responses and may not accurately represent Swiss students in general. This bias is likely due to the network effect, as the survey was primarily shared and then disseminated among ETH colleagues. Furthermore, the survey was also shared on LinkedIn, and so it could not be guaranteed that it would be filled out exclusively by students or recent graduates. Surprisingly, it also attracted a few interested people who had completed their studies some years ago. A comparison between participants who graduated some time ago and current students could also have led to interesting results but was not investigated in this study.

In addition, questions about the ethical aspects of bug bounty programs could have been included. In discussions with some participants, the opinion was expressed that bug bounties are more advantageous for companies than for hunters, as they can access expensive knowledge more cheaply.

Furthermore, question 11, which asked whether success in bug bounty programs improves one's professional profile, could have been removed from the survey. An overwhelming majority of 89% of respondents answered yes to this question, an answer that seems quite predictable. Similarly, question 15, asking if university course knowledge contributes to a quicker acquisition of relevant bug bounty skills, might also have been redundant. This aspect is indirectly addressed in question 16, which asks about the specific technologies or areas in which university courses offer an advantage for bug bounty activities. With an additional answer option in question 16: "I don't see any benefits from my courses", the same findings could have been obtained with just one question.

Finally, the study is time-limited as the survey responses reflect the situation in late 2023 and early 2024, which may no longer be relevant in a few years in the rapidly evolving field of bug bounty programs.

7.3 Recommendations for Future Research

This study has revealed interesting aspects of the motivational factors for students in Switzerland to participate in bug bounty. Some of the results of this work could serve as an inspiration for further research in this direction. The fact that the survey in this study was mainly completed by ETH computer science students emphasizes the need for broader research that includes a wider range of participants. For example, this study could also be conducted at other universities in Switzerland or even in other countries to show parallels or differences to this study. Moreover, future research could benefit from including high school students in the study to gain insight into early cyber security education and its impact. Furthermore, a comparison between students and non-students would enrich our understanding of the motivating factors for participating in bug bounty activities. Building on this work, the best practices proposed in this thesis could be analyzed for their efficiency and effectiveness. Finally, as the field of bug bounty is rapidly evolving, continued research is essential to keep up with the latest developments and understand the changing dynamics within the cyber security landscape.

8 Bibliography

[1] A. Kuehn and M. Mueller, "Analyzing bug bounty programs: An institutional perspective on the economics of software vulnerabilities.," in *The 42nd Research Conference on Communication, Information and Internet Policy*, 2014.

[2] M. Finifter, D. Akhawe and D. Wagner, "An empirical study of vulnerability rewards programs," *22nd USENIX Security Symposium (USENIX Security),* pp. 273-288, 2013.

[3] HackerOne, "https://www.hackerone.com," 04 2020. [Online]. Available: https://www.hackerone.com/sites/default/files/2020-04/the-2020-hacker-report.pdf. [Accessed 08 12 2023].

[4] M. Zhao, J. Grossklags and P. Liu, "An Empirical Study of Web Vulnerability Discovery Ecosystems," in *22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15)*, 2015.

[5] O. Akgul, T. Eghtesad, A. Elazari, O. Gnawali, J. Grossklags, M. L. Mazurek, D. Votipka and A. Laszka, "Bug hunters' perspectives on the challenges and benefits of the bug bounty ecosystem," in *32nd USENIX Security Symposium (USENIX Security)*, 2023.

[6] J. Radianti, E. Rich and J. J. Gonzalez, "Vulnerability Black Markets: Empirical Evidence and Scenario Simulation," in *System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on*, 2009.

[7] E. News, "Switzerland offers cash to hackers who can crack its e-voting system," 13 02 2019. [Online]. Available: https://www.euronews.com/2019/02/13/. [Accessed 03 01 2024].

[8] D. o. Defense, "Department of Defense Expands 'Hack the Pentagon' Crowdsourced Digital Defense Program," 24 10 2018. [Online]. Available: https://www.defense.gov/News/Releases/Release/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/. [Accessed 03 01 2024].

[9] TESLA, "Product Security," TESLA, [Online]. Available: https://www.tesla.com/legal/security. [Accessed 3 1 2024].

[10] HackerOne, "Hackers Wanted: Hack the Army & Pentagon!," 21 11 2016. [Online]. Available: https://www.hackerone.com/ethical-hacker/hackers-wanted-hack-army-pentagon. [Accessed 3 1 2024].

[11] A. Chatfield and C. Reddick, "Cybersecurity Innovation in Government: A Case Study of U.S. Pentagon's Vulnerability Reward Program.," pp. 64-73, 2017.

[12] A. Schwartz, R. Knake and B. C. f. S. a. I. Affairs, "Government's Role in Vulnerability

Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process," *Belfer Center discussion paper,* p. 18, 2016.

[13] Fortinet, "Cybersecurity Skills Gap," Fortinet, 2023.

[14] ISC2, "Cybersecurity Workforce Study," ISC2, 2022.

[15] J. Schindler, "Umfrage: IT-Fachkräftemangel bezieht sich zu 71% auf den Bereich Cybersecurity," 5 12 2023. [Online]. Available: https://news.sophos.com/de-de/2023/12/05/umfrage-it-fachkraeftemangel-bezieht-sich-zu-71-auf-den-bereich-cybersecurity/. [Accessed 4 1 2024].

[16] Schweizer Eidgenossenschaft, "Bis 2030 werden in der Schweiz rund 40'000 Informatiker fehlen," 7 12 2022. [Online]. Available: https://www.kmu.admin.ch/kmu/de/home/aktuell/interviews/2022/bis-2030-werden-in-der-schweiz-rund-40000-informatiker-fehlen.html. [Accessed 5 1 2024].

[17] H. Subramanian and S. Malladi, "Bug Bounty Marketplaces and Enabling Responsible Vulnerability Disclosure: An Empirical Analysis," *J. Database Manag.,* vol. 31, pp. 38-63, 2020.

[18] J. O'Hare and L. A. Shepherd, "Proposal of a Novel Bug Bounty Implementation Using Gamification," *ArXiv,* vol. abs/2009.10158, 2020.

[19] A. Laszka, M. Zhao, A. Malbari and J. Grossklags, "The rules of engagement for bug bounty," in *22nd International Conference on Financial*, 2018.

[20] T. Maillart, M. Zhao, J. Grossklags and J. Chuang, "Given enough eyeballs, all bugs are shallow?," *Journal of Cybersecurity,* 2017.

[21] HackerOne, "The 2021 hacker report," 2021. [Online]. Available: https://www.hackerone.com/resources/reporting/the-2021-hacker-report. [Accessed 5 1 2024].

[22] Bugcrowd, "Inside the mind of a hacker," 2020. [Online]. Available: https://www.bugcrowd.com/resources/guides/inside-the-mind-of-a-hacker/. [Accessed 5 1 2024].

[23] L. O. Oyedele, "Sustaining architects' and engineers' motivation in design firms: An investigation of critical success factors," *Engineering, Construction and Architectural Management,* vol. 17, pp. 180-196, 2010.

[24] E. Zurich, "Equality Monitoring," ETH Zurich, [Online]. Available: https://ethz.ch/staffnet/en/employment-and-work/working-environment/diversity/strategy-and-numbers/equality-monitoring.html. [Accessed 23 01 2024].

[25] HackerOne, "7th Annual Hacker Powered Security Report," 25 10 2023.

[26] kununu, "Bestbezahlte Berufe der Schweiz," kununu, 27 1 2024. [Online]. Available: https://news.kununu.com/bestbezahlte-berufe-schweiz/. [Accessed 27 1 2024].

[27] C. Services, "Lohnentwicklung nach Studienabschluss," Universität Zürich, Zürich, 2013.

9 Appendix

9.1 Survey

9.1.1 Welcome

Dear Participant

Welcome and thank you for taking the time to participate in this survey. I am Adrian Kress, a penetration tester with over three years of experience at Compass Security https://www.compass-security.com/. I am currently enrolled in the EMBA General Management program at the HWZ, and this survey is an integral part of my Master's thesis. The aim is to investigate the motivational factors of Swiss students in relation to bug bounty programs. The completion of this survey takes between 8-10 minutes. If you know a potential candidate for this survey, please share it with them: https://de.surveymonkey.com/r/bug_bounty.

Data privacy: This survey is conducted anonymously. I do not collect any personal information that can identify participants. I am using SurveyMonkey as a feedback platform. By completing the survey, you consent to the data you enter being transferred to SurveyMonkey for processing in accordance with their privacy policy (https://www.surveymonkey.com/mp/legal/privacy/).

I have read and understood the points on data privacy, and I agree with the privacy notice of SurveyMonkey.
Yes
No

9.1.2 Overall Interest in Cyber Security

On a scale of 1 to 5, how interested are you in cyber security?
[1 (Not Interested) - 5 (Very Interested)]

On which platforms do you regularly consume cyber security-related content? (Select all that apply)
Social Media (e.g., Twitter, LinkedIn, Facebook)
Online Forums (e.g., Reddit, Stack Overflow)
Cyber security Blogs or Websites
YouTube or Other Video Platforms
Podcasts
Online News Portals
Academic Journals or Libraries
E-learning Platforms (e.g., Coursera, Udemy)
Webinars or Virtual Conferences
I do not consume cyber security-related content regularly
Other: [Please Specify]

Which cyber security activities have you participated in? (Select all that apply)
Capture The Flag (CTF) competitions
HackTheBox, TryHackMe or similar challenges
Cyber security workshops or bootcamps
Online cyber security courses
Cyber security clubs or societies at school/university
Penetration testing or ethical hacking projects
Cyber security conferences
Bug Bounty programs
None
Other: [Please specify]

9.1.3 Awareness of Bug Bounty

From where you first learned about bug bounty programs? (Select one)
From this questionnaire
University or educational institution
Social media (e.g., Twitter, LinkedIn)
Online forums or communities (e.g., Reddit, Stack Overflow)
Cyber security events or conferences
Friends or colleagues
News or online articles
Other: [Please specify]

On a scale of 1 to 5, how confidently could you explain what a bug bounty program is to someone who is unfamiliar with the concept?
[1 (Not Confident at All) - 5 (Extremely Confident)]

Would you try out a bug bounty program?
Yes
No
Yes, but only if… [Please specify]

9.1.4 Motivation to Do Bug Bounty

If you were to participate in a bug bounty program, what would be your primary goal? (Select one)
Earning money
Gaining practical experience
Building a professional network
Contributing to the security of products/services
Other: [Please Specify]

If you were to start participating in bug bounty programs, which technologies or areas would you focus on? (Select all that apply)
Web Applications
Mobile Applications
Network Security
Cloud Services
Cryptography
Internet of Things (IoT)
Operating Systems
Other: [Please Specify]

How important is receiving recognition (like certificates, acknowledgments) for your achievements in bug bounty programs?
[1 (Not Important) - 5 (Very Important)]

Do you feel that success in bug bounty programs would enhance your resume or professional profile?
Yes
No

9.1.5 Barriers to Do Bug Bounty

What do you consider the primary barrier to participating in bug bounty programs? (Select one)
Lack of Skills or Knowledge
Time Constraints
Lack of Awareness of Opportunities
Fear of Legal Consequences
Not Knowing Where to Start
I do not see any barriers
Other: [Please Specify]

How do you view the balance between the effort required and potential financial rewards in bug bounty programs?
[1 (Not Worth the Effort) - 5 (Highly Worthwhile)]

How confident are you in your ability to find and report vulnerabilities in a bug bounty program?
[1 (Not Confident At All) - 5 (Extremely Confident)]

9.1.6 How to Learn the Necessary Know-How for Doing Bug Bounty

Do you think the knowledge you gained from the courses at the university will give you an advantage when participating in Bug Bounty programs or help you learn the relevant skills faster?
Yes
No

If you answered 'Yes' to the previous question, in which specific technologies or areas do you feel your courses at the university provides you an advantage? (Select all that apply)
Web Applications
Mobile Applications
Network Security
Cloud Services
Cryptography
Internet of Things (IoT)
Operating Systems
I answered 'No' in the previous question.
Other: [Please Specify]

Which of the following resources do you think would best help you gain the skills necessary to participate in bug bounty programs? (Select one)
Formal coursework at educational institutions
Online courses (e.g., Coursera, Udemy)
Self-study through online resources (blogs, tutorials, forums)
Practical experiences (like CTFs, Hack The Box)
Workshops or bootcamps
Mentorship or coaching from experienced individuals
Collaborative learning (study groups, clubs)
Other: [Please Specify]

9.1.7 Demographic Questions

What is your age?

[________]

Please specify your gender. (Select all that apply)

Male
Female
Non-Binary
Prefer Not to Say
Other: [Please Specify]]

Which degree program are you currently enrolled in? (Select one)

Bachelor's Program
Master's Program
PhD Program
Not Currently Enrolled in Any Program
Other: [Please Specify]

If you selected 'Not Currently Enrolled in Any Program,' in the previous question, what is the highest degree of education you have completed? (Select one)

High School Diploma
Bachelor's Degree
Master's Degree
PhD or Equivalent
I answered 'Yes' in the previous question.
Other: [Please Specify]

Which university or college are you currently attending? (Select all that apply)

ETHZ
UZH
EPFL
ZHAW
OST
HSLU
I am not currently attending a university or college
Other: [Please Specify]

What is your current field of study? (Select all that apply)
Computer Science
Electrical Engineering
Mathematics
Physics
Mechanical Engineering
Other: [Please Specify]

9.1.8 End of the survey

You have now reached the end of the survey. Thank you for your valuable participation. If you have any additional comments, thoughts, or insights regarding bug bounty programs or any other related topic we may not have covered, please feel free to share them here. Your perspectives are greatly appreciated.
[________]

As we conclude the survey, we'd like to offer you the opportunity to stay informed. If you are interested in receiving more information about the results of this survey, or if you would like to learn more about bug bounty programs and potential opportunities with Compass Security https://www.compass-security.com/, please leave your email address below. Your contact information will be used solely to provide updates about this survey and will not be shared for any other purpose.
[________]