



---

## Graduate Theses, Dissertations, and Problem Reports

---

2017

# A system to secure websites and educate students about cyber security through crowdsourcing

Chitrangi Sameer Doshi

Follow this and additional works at: <https://researchrepository.wvu.edu/etd>

---

### Recommended Citation

Doshi, Chitrangi Sameer, "A system to secure websites and educate students about cyber security through crowdsourcing" (2017). *Graduate Theses, Dissertations, and Problem Reports*. 3976.

<https://researchrepository.wvu.edu/etd/3976>

This Problem/Project Report is protected by copyright and/or related rights. It has been brought to you by the The Research Repository @ WVU with permission from the rights-holder(s). You are free to use this Problem/Project Report in any way that is permitted by the copyright and related rights legislation that applies to your use. For other uses you must obtain permission from the rights-holder(s) directly, unless additional rights are indicated by a Creative Commons license in the record and/ or on the work itself. This Problem/Project Report has been accepted for inclusion in WVU Graduate Theses, Dissertations, and Problem Reports collection by an authorized administrator of The Research Repository @ WVU. For more information, please contact [researchrepository@mail.wvu.edu](mailto:researchrepository@mail.wvu.edu).

**A System to Secure Websites and Educate Students about Cyber  
Security through Crowdsourcing**

**Chitrangi Doshi**

**Problem Report submitted  
to the Statler College of Engineering and Mineral Resources  
at West Virginia University  
in partial fulfillment of the requirements for the degree of**

**Master of Science  
in  
Computer Science**

**Saiph Savage, Ph.D., Chair**

**Roy S. Nutter, Jr., Ph.D.**

**Elaine M. Eschen, Ph.D.**

**Lane Department of Computer Science and Electrical Engineering  
Morgantown, West Virginia**

**2017**

**Keywords: Crowdstesting, Cyber Security, Crowdsourcing, Twitter Bots, Startup  
Copyright 2017 Chitrangi Doshi**

## **ABSTRACT**

### **A System to Secure Websites and Educate Students about Cyber Security through Crowdsourcing**

**Chitrangi Doshi**

Startups are innovative companies who have ideas for the betterment of the society. But, due to limited resources, and highly expensive testing procedures, they invest less time and money in securing their website and web applications. Furthermore, cyber security education lacks integrating practical knowledge with educational theoretical materials. Recognizing, the need to educate both startups and students about cyber security, this report presents Secure Startup - a novel system, that aims to provide startups with a platform to protect their website in a cost-effective manner, while educating students about the real-world cyber skills. This system finds potential security problems in startup websites and provides them with effective solutions through a crowdtesting framework. Secure Startup, crowdsources the testers (security experts and students) of this system, through social media platforms, using Twitter Bots. The basic idea behind this report, is to understand, if such a system can help students learn the necessary cyber skills, while running successful tests and generating quality results for the startups. The results presented in this report show that, this system has a higher learning rate, and a higher task effectiveness rate, which helps in detecting and remediating maximum possible vulnerabilities. These results were generated after analyzing the performance of the testers and the learning capabilities of students, based on their feedback, trainings and task performance. These results have been promising in pursuing the system's value which lays in enhancing the security of a startup website and providing a new approach for practical cyber security education.

## **ACKNOWLEDGEMENT**

I would first like to thank my advisor Dr. Saiph Savage for her constant support and invaluable guidance in many aspects of my problem report. The door to her office was always open whenever I ran into a trouble spot or had a question about my project work. She consistently allowed this report to be my own work, but steered me in the right the direction whenever she thought I needed it.

I would like to extend my thanks to Dr. Elaine Eschen & Dr. Roy Nutter for being on the committee and supporting the project with their valuable suggestions and encouragement.

Finally, I must express my very profound gratitude to my parents for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this report. This accomplishment would not have been possible without them. Thank you.

# Table of Contents

|  |    |
|--|----|
| 1. INTRODUCTION: .....                                     | 1  |
| 2. RELATED WORK: .....                                     | 4  |
| 2.1. CYBER SECURITY EDUCATION:.....                        | 4  |
| 2.2. WEB APPLICATION SECURITY/VULNERABILITY TESTING: ..... | 7  |
| 2.2.1. SOURCE CODE REVIEW: .....                           | 8  |
| 2.2.2. PENETRATION TESTING: .....                          | 10 |
| 2.2.3. VULNERABILITY SCANNERS: .....                       | 12 |
| 2.2.4. CROWDTESTING:.....                                  | 13 |
| 2.3. SOCIAL MEDIA CHATBOTS: .....                          | 16 |
| 3. SYSTEM:.....  | 18 |
| 3.1. TESTER SELECTION: .....                               | 19 |
| 3.2. TESTING WORKFLOW:.....                                | 24 |
| 3.2.1. REGISTER: .....                                     | 24 |
| 3.2.2. TASKS AND TRAININGS FOR TESTERS:.....               | 26 |
| 3.2.3. EVALUATION: .....                                   | 28 |
| 3.2.4. REPORT GENERATION: .....                            | 29 |
| 3.2.5. FEEDBACK: .....                                     | 30 |
| 3.3. INCENTIVES: .....                                     | 31 |
| 4. SYSTEM HYPOTHESIS: .....                                | 33 |
| 5. RESULTS: .....  | 34 |
| 5.1. RESPONSE RATE: .....                                  | 34 |
| 5.2. SYSTEM HYPOTHESIS RESULTS: .....                      | 36 |
| 5.2.1. LEARNING RATE: .....                                | 36 |
| 5.2.2. TASK COMPLETION RATE: .....                         | 38 |

|   |    |
|---|----|
| 5.2.3. TASK EFFECTIVENESS RATE: .....   | 40 |
| 5.2.4. NUMBER OF FALSE NEGATIVES: ..... | 41 |
| 6. DISCUSSION: .....                    | 42 |
| 7. LIMITATIONS: .....                   | 45 |
| 8. CONCLUSION AND FUTURE WORK: .....    | 46 |
| 9. BIBLIOGRAPHY: .....                  | 47 |

## List of Figures:

|  |    |
|--|----|
| Figure 3.1: System Overview .....  | 18 |
| Figure 3.2: Tester Selection Process .....   | 19 |
| Figure 3.3: Screenshot of the Bot Streaming Twitter Users Based on #Cybersecurirty .....   | 20 |
| Figure 3.4: Excel Spreadsheet Used for Crawling.....                                       | 22 |
| Figure 3.5: Screenshot Displaying the Twitter Bot Sending Tweets to the Users.....         | 23 |
| Figure 3.6: Testing Workflow.....  | 24 |
| Figure 3.7: Screenshot of the Registration Page and Agreement Form.....                    | 25 |
| Figure 3.8: Screenshot of the Startup Space .....  | 25 |
| Figure 3.9: Screenshot of the Tasks and Trainings Posted on the Website .....              | 27 |
| Figure 3.10: Screenshot of the Task Selection Page.....                                    | 27 |
| Figure 3.11: Screenshot of the Ratings Page .....  | 28 |
| Figure 3.12: Report Generator .....  | 30 |
| Figure 3.13: Feedback Form .....   | 31 |
| Figure 5.1: Reply Rate Graph .....   | 35 |
| Figure 5.2: Graph Representing the Response Rate Generated by each Category of Tester..... | 36 |
| Figure 5.3: Graph Representing the Number of Testers Who Completed the Given Trainings...  | 37 |
| Figure 5.4: Graph Representing the Use of Secure Startup in Career Development.....        | 38 |
| Figure 5.5: Graph Representing Students Feedback on the Task Description .....             | 38 |
| Figure 5.6: Task Completion Rate Graph .....   | 39 |
| Figure 5.7: Task Effectiveness Rate Graph .....  | 40 |
| Figure 5.8: Graph Representing the False Negative Rate.....                                | 41 |

## List of Tables:

|   |    |
|---|----|
| Table 3.1: Hashtags Used for Streaming Live Tweets .....                                | 21 |
| Table 3.2: Sample Crawled Content to Determine a Potential Tester .....                 | 22 |
| Table 5.1: Twitter Bot's Account Details.....   | 34 |
| Table 5.2: Analytics on Twitter Bot's Content .....                                     | 34 |
| Table 5.3: Task Completion Rate Values based on Value Binomial Confidence Interval..... | 40 |



# 1. INTRODUCTION:

As any business endeavors to develop in today's aggressive innovation spurred world, one of the biggest challenges that they must confront and continually address is cyber security. Startups are innovative companies who have ideas for the betterment of the society. They have limited resources, and redoubtable competition, which drives them incessantly to deliver ingenious products and services. Consequently, startups dismiss other concerns and invest less time and money in cyber security. Hence, this makes new companies amazingly defenseless against digital assaults, producing the need to perceive the significance of digital security and actualizing safety efforts when the organization is as yet youthful. There are many solutions to offer, but today's vulnerability solutions have its own set of pros and cons. Some of the solutions require a large amount of investment, while others are human-centric, which are dependent on skill sets and project time constraints, and other solutions are dependent on online scanning tools which have a low coverage and higher percentage of false positives [1]. This report presents a strategy which consolidates the best of minds and machine by using social computing methods and crowdsourcing to investigate and report potential vulnerabilities. The advantage of using crowdsourcing is reduced time and cost, along with efficient results generated by diverse class of people [2]. Hence, implementing the system using crowdsourcing model is a better approach.

Wikipedia defines crowdsourcing as, a specific sourcing model in which individuals or organizations use contributions from Internet users to obtain needed services or ideas [3]. In simpler terms, an organization posts a task on the web and various people complete the task to earn incentives offered by the organization. Based on the above concept, this report presents a model for crowdsourcing cybersecurity, where best personalities and best techniques from social media platforms will be utilized to expose security flaws underlying in a startup's website and will also remediate them quickly. However, to implement crowdsourcing, additional contemplations should be taken to obtain reliable results. Section 3 provides a detailed information on the practices used to develop the crowdsourcing model that best fits the needs of this system.

On the other hand, cyber security education lacks integrating practical knowledge with educational theoretical materials. Educating students on cyber security requires profound teaching of various cyber-attacks and its consequences. But, this has merely become theoretical and lacks

thorough practical experimentation [4]. It is important that students have a hands-on experience of different security techniques. This practical experience will bear maximum benefits if the experiments were connected based on real-world problems and under the supervision of security experts. There is also a need for information sharing on cyber security [4]-[6]. Collaborations can help such information sharing as they give an opportunity to students to gain professional level experience on security activities.

This report presents a novel system called Secure Startup, that crowdsources students and security experts through learning opportunities to find vulnerabilities in startup websites and provide solutions through which website owners can protect their products. This system will not only benefit startups, but will also help students learn new techniques. Students will get an opportunity to showcase their skills by investigating the startup website and enhance their skills by learning new techniques under controlled supervision. This learning experience can act as an informal professional certification which will help students in their future careers. Figure 3.1, presents an overview of Secure Startup. The system first recruits a set of potential crowd workers on social media platforms through chatbots. The crowd workers in this system are: professional experts working in the industry, professors interested in cyber security and students majoring in computer science. Section 3.1 provides in depth explanation on the process used to recruit crowd workers while eliminating the entry of malicious workers. Once the crowdworkers are recruited, they are asked to participate in a testing platform for content sharing and completing the given tasks. The tasks are based on different security techniques that will be used to scan the website for vulnerabilities and remediate them. Experts can participate in technique sharing and monitoring the students, while students are responsible for completing the tasks. The tasks completed by students are analyzed by the experts who create a report listing all the vulnerabilities, solutions taken to resolve them and measures to be taken to avoid them in the future. This report will then be sent to the startup for mitigating their resources and understanding the concepts of cyber security that were missing from their website.

The remainder of this report is structured as follows: Section 2 gives an overview of the related work in the areas like, various security testing approaches used in the organizations, educational methods used to teach students about cyber security and crowdtesting. The working of the system is explained in detail in Section 3. It describes the method adopted to hire the most

reliable crowd workers, the methods used to generate efficient results and the design of the system. This section is followed by Section 4, which describes the metrics used to evaluate this system. Section 5 presents the results after analyzing different potential and noteworthy aspects of this system, which is followed by Section 6 that discusses the results obtained and gives a broader picture of the approaches used. Technical challenges and limitations are analyzed in Section 7. Finally, Section 8 summarizes this work and gives an outlook on important future steps for Secure Startup.

## **2. RELATED WORK:**

The related work for the proposed system can be classified into three areas: (a) cyber security education (b) web application security/vulnerability testing and (c) social media chatbots

### **2.1. CYBER SECURITY EDUCATION:**

The previous four decades have seen the computing field grow dramatically where cyber security has also found its significance in recent times. The field of cyber security is also continually extending, with more spaces to secure and more approaches to assault. Intrusions are harder to distinguish and aggressors are more equivocal. Cyber risk is now one of the highest priorities for organizations as the hackers of recent times have the capability to attack every system and service connected to the internet which can lead to disruption of the organizations' economy. These cyber-attacks will eventually have its impact on customers as attacks usually involve data breaches, which leads to the loss of user's personal information. There are experts who believe that the topic of cyber security is over-hyped and is now used as a medium to induce fear by using terms such as 'cyber-warfare' which is designed to provoke an emotional rather than a rational response [7]. But, regardless of which view one may take, clearly digital security is perceived as an undeniable point and one worthy of discussion [8]. It is worth noting that, organizations have started to realize the importance to incorporate security into every product, framework and service provided to its customers. Hence today's leading companies need skilled IT talent who can comprehend the current and developing cyberthreat condition, to successfully confront highly vulnerable cyber attackers, and help them stay competitive in the market. However, a recent research study has reported a lack of cyber-security skills within organizations [9]. The Global Information Security Workforce has predicted that over the next three years, demand for personnel with relevant security skills may rise 13 percent each year. Thus, students need to have key digital abilities to be competitive in today's workforce as no organization would hire graduates without sufficient knowledge to deal with the incoming cyber-attacks.

Apart from lack of skilled labor in this field, we need to understand that everyone is vulnerable to such threats. Each of us, in whatever part we play in life, must make decisions about digital security that will shape the future well. But, frequently, even if such decisions are made, they are managed without proper tools and technique [10]. Thus, due to the demand and intense

competition of cyber security talent, it is imperative that educational institutions include core security programs in their curriculum.

IT 2008 Model Curriculum perceives Security as a key component of IT instruction in the core and advanced curriculum [4]. Moreover, the need for security programs in the curriculum has been identified by many academicians [4], [11]-[15]. Advancing on such a curriculum will be a contributory element to the present absence of qualified experts. One of the researchers, Rowel, Dale strongly encouraged to consider progressed cyber security educational modules in establishments that offer Information Technology [4]. This new curriculum must be organized such that, it includes the latest cyber security standards, reports, and techniques that can build the students for the real cyber world. Numerous researchers have given magnificent material on instructive approaches for implementing a structured cyber security curriculum [4], [12], [15]. According to, ACM's Computing Curricula 2001, due to the advancements in technology, other computer science areas such as software safety, security and cryptography are also to be prioritized [16]. They have identified the need to incorporate an elective course related to computer crime in the Computer Science undergraduate curriculum. Through this course, students will learn techniques to combat cyber-attacks and will also learn the basis of its origin by understanding the concepts of malware. Even though cyber-crime courses are being subsumed into teaching programs, they are still being offered only as elective courses, which means, not majority of the students will sign up for this course and will graduate without a solid foundation and fundamental comprehension of cyber world. The other drawback of these elective courses is that, not sufficient practical tools and techniques are implemented during the teaching process, which leads to the lack of necessary practical exposure. As there is an expanding need of cyber security professionals in companies, an approach so static is not adequate to deal with security education. A solution to this problem is addressed by a researcher, who suggests to include security topics in all the courses and relate it to the core topics appropriately [15]. Irvine and Chin also focuses on integrating security into existing computer science programs rather than treating it separately. Examples for such an integration can be, programming classes teaching students to consider security implications in a program, that is being developed. Computer architecture classes can implement assembly language programming to build protection mechanisms. Networking courses can concentrate on latest security related protocols used by companies rather than the traditional standard protocols [12]. Another work by researchers at College of Business, Idaho State

University [11] propose the concept of the Design Reference Monitor. It is typically used for analysis and design of secure information system, during the operational maintenance and should be used in every step of design process. Introducing DRM to students will help them be acquainted with the thought of fusing security and related issues all through the framework. This will also ensure a solid foundation for students to deliver quality work at their workplace and be a useful asset to the company. Passive computer-based and web-based training is another approach that is widely used by many institutions. Such trainings prepare students for companywide standard, as the institutions have resilience to pace the training to meet different standards. The other teaching approaches include game simulations like cyber-war games [4], [17] for cyber security awareness.

The integrating teaching approach discussed above, centers the educational approaches on the real-world problems by reading and understanding the underlying concepts without any involvement of interactive tools [18]. The gaming approach has also been proven to be successful in spreading basic cyber security awareness, but it still does not solve the purpose of preparing students to deal with threats involving higher risks in computer systems and services [4]. Web based training approach becomes monotonous over time and eventually does not challenge its users and gives no exchange to further explanation [17]. All the above approaches, have a theoretical training aspect to it, and are also constructive ways to deal with cybersecurity training, but, the essential part is to develop trainings that incorporate practical and tactical skills, along with critical thinking and problem solving approaches to prepare students combat industry level threats. Moreover, industry level professionals are required to work with an assortment of tools and technologies. Hence, the specialized and operational nature of cybersecurity requires students to be involved in experiment based learning, which provides a hands-on experience along with a profound comprehension of technical topics. Lotfi ben Othmane et al. performed experiments on teaching computer security labs at two different universities and noted that teaching computer security with a hands-on approach facilitates and reinforces a students' understanding of networking and security issues [19]. There are also other studies that support the same direction [20], [21] Experiential learning approaches in the type of virtual labs, outside classroom learning activities and certifications based on interactive learning can help students gain necessary knowledge. Based on experimental based learning, Secure Startup implements another approach using crowdsourcing and crowdtesting, where students are given security related tasks, which will provide them with a hands-on experience on new tools and techniques to deal with threats

pertaining to websites. This is done under complete guidance of experts who rate student's work and provide them with constant feedback and awards. Hence, there is always an opportunity of growth and improvement for the students.

## **2.2. WEB APPLICATION SECURITY/VULNERABILITY TESTING:**

Security testing is a process intended to reveal flaws in the security mechanisms of an information system that protects data and maintains functionality as intended [22]. In simpler terms it is a set of activities conducted with the intent of finding errors in web application or software [23]. It is performed to protect the system from vulnerable attacks and to ensure that only the authorized user has the access to the system's backend and frontend functions. It involves investigation of major loopholes which can cause harm to the system by an unauthorized user [23].

Security breaches and use of malware attacks are at a rise, which directly leads to loss in economy. Apart from economic loss such attacks also damage the brand image and reputation of the organization. Organizations develop several web applications for their clients and customers, which have now become an integral part of everyone's life. These days, we use web applications on a daily basis for shopping, entertainment, chatting, video calling, and dealing with other technical activities. Most of these applications require authentication and access to a user's basic profile. This information is stored in a database which is used by the organization to construct queries [24]. Such databases, if are not protected effectively, can act as paradise for hackers who are waiting to steal and misuse this data. This is merely, one of the ways of attacking a web application. There are numerous other loopholes in a website through which attackers can entirely destroy an application and then use the data obtained from it, to fulfill their malicious purposes. Hence, every organization needs to take substantial security measures, while developing applications, to prevent any conceivable loss to its economy and to keep the customer's data safe [25].

Security testing is a crucial and complicated step, as it involves testing every part of the web application and considering every possible scenario in which the application can fail to be secure. Therefore, integrating security techniques as one of the phases of the development lifecycle is important. Security testing demands constant scrutiny and expertise of a professional. Security expert is required to have a solid understanding of the website/web application and intrusion prevention mechanism. Due to the number of tools, techniques and rapidness required to complete

this process, a team of effectual testers must be setup. Hence, organizations need to invest, enough resources that can sustain effective security testing to stay secure from data breaches or other types of cyber-attacks and to ensure confidentiality of its customer's data.

Security vulnerabilities are not just identified with security functionalities at the application level but are also responsive to implementation details, [26] which means vulnerabilities exist in the application code, it can also exist in the technology that is being used to develop the website, the server used to store all the information, and the command line shell used while development [27]. Several antivirus softwares, firewalls, and intrusion prevention systems are available in the market to prevent malicious attacks, but, for a definite prevention and security, constant analysis needs to be performed at every phase of network interaction [26]. There are numerous number of attacks these days, which are used to exploit an administration's data. To remediate them, it is necessary to understand the motive of the attack, the network which includes the devices attached and the access levels, and the port/part of the website that has been attacked. This involves a lot of resources of the organization. By this time, the organization must have already faced a significant amount of loss, and at the same time investing in resources needed to countermeasure the attack can be detrimental to small or newly opened businesses. Hence, the saying, "Prevention is better than cure" should be adapted by every single organization and should integrate security tests in their application development. This will ensure that the website or the web application is fully protected, avoiding any loss of sensitive data, and harm to the company's reputation.

There are different approaches used by software security practitioners to detect risks and threats pertaining to a website. Any testing method can uncover possible risks and vulnerabilities [28]. But, it is important to adapt a technique that suits the business requirements. This report discusses four approaches, commonly adapted by organizations these days for testing the security of a website.

### **2.2.1. SOURCE CODE REVIEW:**

As most universities, do not have cyber security as a core part of their curriculum, graduates hired to develop applications are not aware of the importance of implementing security in the code, which can lead to unintentional errors and vulnerabilities. Such security vulnerabilities, can lie dormant, sometimes for years, before discovery [29] and can be hard to fix after the application is ready for use. Hence, organizations require a team of security experts who can examine the code



to detect any existing flaws or vulnerabilities. Most organizations, implement manual code testing, known as Source Code Review, which is an approach that involves peer reviewing of source code of computer programs [30]. During the early development phases of web applications, a few defects and vulnerabilities are overlooked in the testing process, which can be fixed in the source code review [31]. Hence, source code review is usually performed manually by a group of testers to understand the code and fix any defects that could lead to vulnerable attacks. This is an off-line undertaking led by human analysts without compiling or executing the code [30]. The report generated after this process, is sent to the application developers, for a better guidance on the design and implementation of the web application. Code review, requires testers to have adequate experience, skills and knowledge [32] to rigorously examine the code.

There are several tools and technologies that have automated the source code review process. These tools can either perform static analysis or dynamic analysis [33]. Static analysis aims at determining, properties of programs by inspecting their code, without executing them [34], while dynamic analysis aims at finding flaws during the execution of the program [33]. There are several research works, on analyzing the effectiveness of different tools and softwares used for source code reviews [29], [33], [35], [36]. One such work by Jason Remillard, illustrates the comparison results of five different softwares [35]. He reports that, the static technique is an effective approach, but none of the softwares provide a complete solution for all kinds of inspection. An alternative solution provided in his work, is to use a software that best suits the technologies used in the application development, to detect maximum flaws, and then assign manual processing to testers, to examine the code for any other missing functionalities. Another empirical study conducted by Edmundson et al., hired 30 developers to do a manual code review of a web application. The application had seven known vulnerabilities that included, Cross-Site Scripting, Cross-Site Request Forgery, and SQL Injection. The findings of this work were:

- a) none of the subjects found all confirmed vulnerabilities,
- b) highly experienced tester does not necessarily mean that the reviewer will be more accurate or effective,
- c) reports of false vulnerabilities were significantly correlated with reports of valid vulnerabilities.

Source code Review is an effective method in establishing security in a web based application, but one cannot rely on this approach completely. The manual process is very costly and time consuming. It requires skilled labor, which is not easily available, therefore, the review process is sub-contracted to a third-party consulting agencies, which adds to the cost. Hence, we require better techniques, to conduct security testing of a website, which are not only cost-effective, but can generate results quickly and efficiently.

### **2.2.2. PENETRATION TESTING:**

Penetration testing is a comprehensive method to test the complete, integrated, operational, and trusted computing base that consists of hardware, software and people [37]. In this method, the application is stressed from the point of view of the attacker by issuing a large amount of malicious interactions [38]. The steps involved in this process, are similar to the steps taken by a hacker to attack an application. But, the penetration tester needs to have permission from the owner of the website, before conducting the test, and that differentiates him from a hacker and makes this approach ethical. At the end of the test, the tester has to submit a final report, which comprehends information on all the types of attacks that were injected into the application to detect vulnerabilities and the results obtained through these tests. This test ought to be managed without informing the employees of the company, as they are conducted to reveal the security flaws of the application. The advantage of penetration testing is that, the testers do not require access to the source code, which ensures the authenticity of the code and avoid risks of any type of code manipulations.

It is important to conduct penetration testing for various reasons:

- a) It will provide a real-time experience in dealing with an intrusion that could possibly enter the website.
- b) It helps in revealing the weak aspects of the security measures taken during the development phase.
- c) The reports generated at the end of every test process will help in organizing any future security speculations and can also be utilized in preparing programmers to commit less errors.

- d) It gives an opportunity to test out new technologies before they are used on project development. It's much easier and cost-effective to test and change new technology, while no one is depending on it.

Penetration testing involves the serial execution of automated tools and generation of technical reports, but is not restricted to these steps [39]. The testing process described by Bacudio [39] involves (1) Information Gathering Step, (2) Vulnerability Analysis Step, (3) Vulnerability Exploit Step and (4) Test Analysis Phase.

In the first step, the testers have to gather information about the website and the target network. The information gathered in this step will act as the base, for the actions to be taken in the next phase. The testers in the second phase use the information gathered from the previous phase, and examine the website to scan any existing vulnerabilities. Once the scan is completed, the testers will have a thorough knowledge of the types of vulnerabilities that exist and then will begin exploiting them in the next step. Exploiting vulnerabilities usually also help, explore other flaws of the websites. Hence, this approach involves intense detection and exploitation steps. The final step which is the test analysis phase, generates a detailed report on the types of attacks undertaken for exploitation, the list of vulnerabilities detected and the steps taken to resolve them. It also details the security measures to be taken, for future considerations.

According to Bacudio, [39] success of penetration testing depends on two important factors: the approach and the penetration team. In his work, he states that, a penetration test will be successful if a systematic and scientific approach is applied and all the tests and vulnerabilities are documented at every phase of the process. Selecting the best testers also contributes to the success of penetration testing. They should be selected based on their experience, knowledge and reputation in the industry. These efforts ensure the safety of an organization, its systems and its services.

Penetration testing can be conducted manually and can also include, use of automated tools. Manual testing is done in depth, while automated testing cannot be used to explore in depth functionalities. In manual testing exploiting one vulnerability, usually leads to exploration of other hidden vulnerabilities. This cannot be achieved by working with automated penetration tools. But, Manual pen test is time consuming and requires a team of knowledgeable testers. Automated tools

complete the job fast, but can be very costly depending on the type of tool required. Hence, to achieve best results, it is important to use both these approaches in correct context. Automated penetration tools can initially be used to fix the basic and easily detectable flaws and then testers can manually perform deep penetration tests to lock the website securely. Penetration testing is the most commonly applied mechanism, used to gauge software security, [37] but it is one of the expensive approaches as it involves the use of both man and machine. Secure Startup is a system being developed for startups, who need cost-effective testing resources and approaches. This method though being effective cannot be independently used by startups. Hence Secure Startup tries to implement other alternative testing method, which are similar to penetration testing, or black box testing, as this approaches does not require access to the source code and Secure Startup also guarantee every startup organization, that tests will be performed without having access to their source code.

### **2.2.3. VULNERABILITY SCANNERS:**

Automated Scanners are regularly utilized by organizations to test web applications against vulnerabilities, as they are viewed as the easiest approach to test web applications [1]. These scanners examine the website for vulnerabilities and report them to the organizations, so that the developers and testers can take necessary steps to resolve them. Most of the time, vulnerability scanners are considered same as automated penetration testing tools. Vulnerability scans are used to identify vulnerabilities, and document them, whereas penetration testing tools exploit vulnerabilities using custom exploit scripts and injection scripts. These tools also document vulnerabilities, but they are documented along with the solution taken to fix the defect. So, it can be said that penetration test tools are vulnerability scanners, but the vice versa is not possible. Vulnerability Scanners store different types of potential vulnerabilities in their database and scan for only those known vulnerabilities.

There are different types of scanners each with different goals [40]. Some scanners are developed to report only a certain type of vulnerability, while others claim to report all the known vulnerabilities. Scanners can easily help identify vulnerabilities in the website and the network under which the website is deployed. It also helps in tracking the devices present in the network that interact with the website/web application. This information is important to organizations, to

manage their security policies. These scanners also reduce the work load of a testing team, as the number of tests to be performed by the testers will be reduced.

The assessments of vulnerability scanners are based on signatures of operating systems used, services running, and their corresponding vulnerabilities [41]. This method leads to several false negative alarms, because the attackers these days, modify the malware, to match the signature of the operating system. There has been a lot of work done on analyzing the effectiveness of vulnerability scanners [1], [41], [42]. A study conducted by Fonseca, [1] analyzed 3 different leading scanners based on a method of, injecting realistic software faults in web applications in order to compare the efficiency of different tools. The results obtained from this study, shows that all the three scanners were not successful in detecting a considerable percentage of vulnerabilities, and the reports generated by these scanners were also completely different. Another study by Holm, studied seven different scanners, and concluded that, though scanners are useful and important, but organizations cannot rely on them completely, as they are capable of detecting only a subset of vulnerabilities present in the website and the network. There was another study conducted by Concordia University College of Alberta, Edmonton, Canada, [42] which examined three scanners used for detecting only SQL injections. They observed that, all the three scanners were poor at their tasks, because the attack codes used to exploit SQL injections vulnerabilities were very weak. The scanner was not even aware whether the first step of the attack was successful.

Most of the studies, do not encourage the use of vulnerability scanners due to its incapability of detecting all the vulnerabilities existing in the network. They include modules that guide them in the scanning process. A website is scanned against these modules and results are generated, without considering false positives and false negative values. Hence, a human is required to examine the results again which is going to take extra time. In addition to this, scanners can only detect those vulnerabilities that can be verified by its built-in plugins, which limits its application purpose. Hence it is necessary to plan and perform a website testing carefully, and should not be dependent on the results generated by a vulnerability scanner.

#### **2.2.4. CROWDTESTING:**

Crowdtesting, or crowdsourced testing, has gained a lot attention in recent years because of the value achieved by the crowd which cannot be accomplished by the interior testing team [43].

It is a specific application of crowdsourcing in the domain of software development [44]. In crowdtesting, the security procedure followed, to test a system, is crowdsourced to different people in the form of tasks, using the social media platforms, crowdsourcing platforms, emails, or organization's website. Testing can be quick, with quick ramp-up and ramp-down, in different environments and situations [45]. These tasks are completed by crowdworkers to earn incentives. This means, that the organization does not have to hire a team of specialists to complete the security or vulnerability tests for their products, as these tests are being performed by a varying and a much larger group of professionals for a lesser disbursement. There are several crowdtesting platforms that help deliver bug reports, run tests on the functionalities of web application and secure it against cyber threats.

With the advances in technology, securing a product or a service can be challenging. Any website or web application that is developed will encompass different skills and disciplines [46]. So, the security tests also should be performed in all disciplines, involved in the website development, which makes the testing process quite complex, involving several aspects and scenarios to be considered. Hence, it, is vital to hire testers, who possess expertise in wide-ranging areas, to focus on multiple branches of the application/website. While it is possible to have professionals, learned in numerous territories of data security, it is hard to hold staff who are specialists in more than a couple branches of technology [47]. Also, the expenses involved in setting up a lab, that has diverse devices to support the testing process on every technology is extremely high. Crowdtesting enables organizations to get their products tested on all major platforms, devices, system configurations and country or region-specific aspects under real-world conditions as, the tasks are performed by a large group people possessing diverse skills and knowledge [48]. So, crowdtesting is a great opportunity for generating efficient results by being able to test all the areas of the website /web application.

Crowdtesting is an approach where the testers are located in different horizons and time zones, and they are also intellectually dissimilar, which makes, synchronizing the entire testing process extremely difficult for the organization. Therefore, organizations usually build a common platform or use the existing crowdtesting platforms to distribute tasks, monitor the workflow, and provide constant feedback to its testers and manage the working of huge pool of testers [49]. These platforms also act as medium for testers to interact, share their knowledge and hold discussions. So, the crowdsourcing platform should also have necessary tools and channels, for direct

communication. The testers are usually anonymous and the tasks are independently performed [50]. So, the testing platform should be able to screen test, the crowdworkers for safety drives, before assigning them on the security testing project. This will help reduce the number of cheating cases, and will also ensure that the testers are trustworthy and will not try to misuse any information of the website.

Crowd testing is not a replacement for traditional testing, but it provides good value when the right crowd is chosen [43]. Crowdworkers or testers are individuals who should be selected based on their profile, experience and knowledge on the subject of testing. Diversity of the crowd is also beneficial for the system, as testers with different capabilities and experiences will have a different approach to solving a problem. This difference in approach can help discover maximum number of flaws and vulnerabilities. Hence, the crowdsourcing platform should rightly select the crowd for obtaining effective test results.

#### ADVANTAGES:

Crowd testing brings diversity to testing techniques, works with low-cost testing devices, and ensures better test coverage across multiple geographic regions [51]. The crowdworkers belong to different geographical regions, which can make cost of labor less expensive, as cost of living varies from region to region, causing a difference in wages.

The testing process is faster with crowdtesting. As there are numerous testers working on the investigation process, the speed significantly increases when compared to the test speed of an organization's testing group which consists of a small batch of people. But, more number of people always does not imply to resourceful results. Apart from, hiring more number of crowd workers, hiring efficient and experienced workers with solid understanding of testing can help improve the output of the testing process. There are various other ways of motivating workers to perform well and meet the standards expected by the customer. Hence crowdtesting is not only a fast testing process but can also produce resourceful outputs.

Crowdtesting model is endlessly flexible [52]. It provides a massive pool of testers, with diverse background. But it is necessary to select the right crowd, based on the type of system to be tested. This can be done by building or using the right platform, that can provide its customers the flexibility to choose the testers based on their desired characteristics.

It is an effective way to get boots on the ground to test the app in the real world [52]. On a wide scale, virtualized testing is used to create real world scenarios. But crowdtesting, provides an

opportunity to test the app in the real world, which will help the developers have a better understanding on the shortcomings.

Along with the benefits offered by crowdtesting, there are also certain risks and challenges associated with it. The biggest concern is testing the integrity of a crowd-worker. It is difficult to predict if a crowd tester will not indulge in malicious practices to harm the system under test. It is also important to use a well-designed platform for effective communication with the crowd. Most of the crowdtesting platforms available in the market today, pay their workers for the tasks completed by them and they usually have hundreds of testers participating in their crowdtesting platform. Hence, this method can still not be entirely cost-effective for startups as their resources are very limited, and they would not want to indulge in security projects that involves extra expenditures.

Crowdtesting has several advantages over traditional testing methods, but it also cannot be used without understanding its shortcomings. Before using any platform, all the challenges should be considered to obtain flexible and varied solutions. Secure Startup builds on this approach to develop a platform that can help startups, test their website effectively, understand the challenges faced by crowdtesting, and use techniques to overcome them.

### **2.3. SOCIAL MEDIA CHATBOTS:**

Chatbots are algorithms designed to hold conversations with a human. Based on this same design, social media bots were created which is also a computer algorithm that automatically creates content and connects with people on social media platforms [53]. These bots are being developed to provide useful services like, responding to business enquiries, providing customer care services, and posting news feeds for different companies. There are many research works that explore different possibilities of utilizing social bots for different causes [54], [55]. One of the previous social experiments conducted by Aiello [55] aimed to explore the influence of a social bot in the dynamics of online social media. His investigations uncover that an unreliable individual, like a bot can turn out to be extremely important and persuasive through extremely straightforward automated activity. Another research work, aimed to use online bots to call volunteers to action [54]. They present a real-world possibility of utilizing online bots by making use of different strategies. This work also shows that strategies known to be viable when utilized by people were not as powerful at the point when embraced by online bots. This suggests that



social bots, are more effective in conveying messages to a very large group of people and helping them realize their social responsibilities and call them to action. Secure Startups, advances on these findings to use social bots in hiring testers, on one of the social media platforms, Twitter. Section 6.1 discusses, different methods adopted by Secure Startup to hire maximum testers, from different technical backgrounds and knowledge.

Based on the literature survey, we understand that,

- a) Students need more practical awareness on cybersecurity.
- b) Source code Review is a costly and time consuming approach.
- c) The use of a vulnerability scanner cannot reveal all the vulnerabilities, as there is lack of comprehensive scanner that can detect all kinds of vulnerabilities.
- d) Crowdfunding is an effective way, to test websites for vulnerabilities, but it is difficult to trust an unknown crowd, to not harm the system under test.
- e) Students interested in learning cyber security, need to have practical exercises along with the theoretical knowledge to advance their understanding.

To the best of our knowledge, there is no system, that is particularly developed to help startups test their websites securely in an inexpensive way, and simultaneously help students learn practical and real world cyber skills.

### 3. SYSTEM:

Secure Startup is a web based platform that startups can use to test the security of their website and it can also be used by students to learn new cyber skills. It is based on the concept of crowdtesting, where security experts and students are crowdsourced to complete tasks related to testing a website for vulnerabilities. This system makes it simple to setup explorative tests while allowing startups to specify special and confidential test related instructions and setting up a budget for the test process. This system is designed:

- a) to provide a crowdtesting platform, for better test coverage in a cost-effective manner.
- b) to make use of OWASP Web Application Testing Methodology, to test startup website,
- c) to provide an educational experience with hands-on component for students and,
- d) to utilize the expertise of security experts, who can maximize the quality of solutions suggested by students.

Figure 1 shows the overview of the system, where chatbots play a major role in crowdsourcing the testers. Chat bots use social media platforms to search for potential security experts and students, and encourage them to participate in this system. They also direct interested users to register for Secure Startups where they get an opportunity to learn cyber skills and showcase their skills to secure a startup’s website.

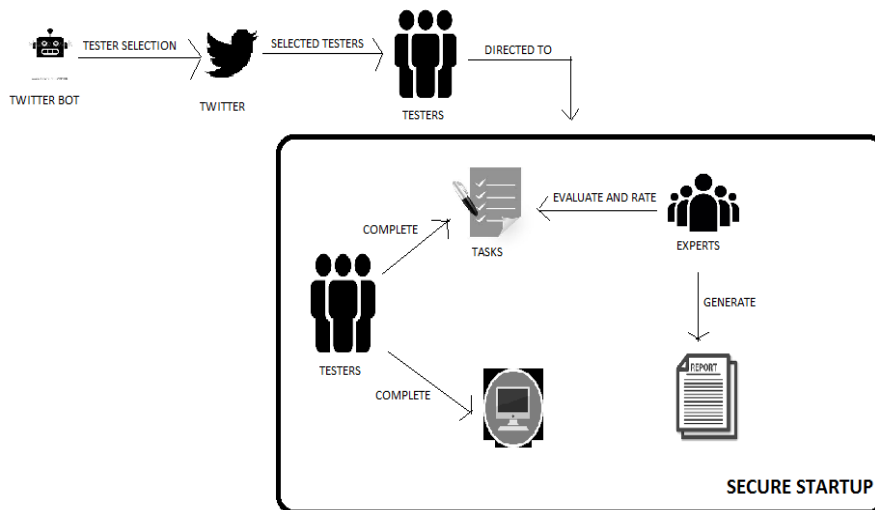


Figure 3.1: System Overview

This section describes how Secure Startup works, by describing the procedure of selecting testers and the testing workflow used to detect vulnerabilities in the website.

### 3.1. TESTER SELECTION:

Selecting testers is a critical process, as their skills and values determine the success of this system. Hence, the goal of tester selection is to ensure that each test task, is taken by the right tester [48] who can complete it with utmost sincerity and without indulging into malicious activities. Testers are selected through social media platforms. Social media is now an integral part of everyone’s life and is one of the prime mediums for mass communication. Such platforms have a crowd with different background, goals and expertise. Everyone is constantly active and is engaged in different campaigns, causes, groups, etc. This social nature of social media platforms, aids the task of conveying messages and selecting crowd workers in an easy manner. Hence, this makes social media an ideal online space to select crowd workers [56]. There are different social media platforms that can be used to select diverse testers. Twitter is one such platform that has been constantly used by different crowdsourcing groups. Deploying online chat bots on social media platforms makes the entire selection process automated and hassle free. Secure Startup uses Twitter bots to select testers who can chat with different users and identifies potential testers for this system. Twitter API allows creation of interesting chatbots with very limited set of restricting policies. Discoverability of this bot is also easy with Twitter, when compared to other social media platforms.

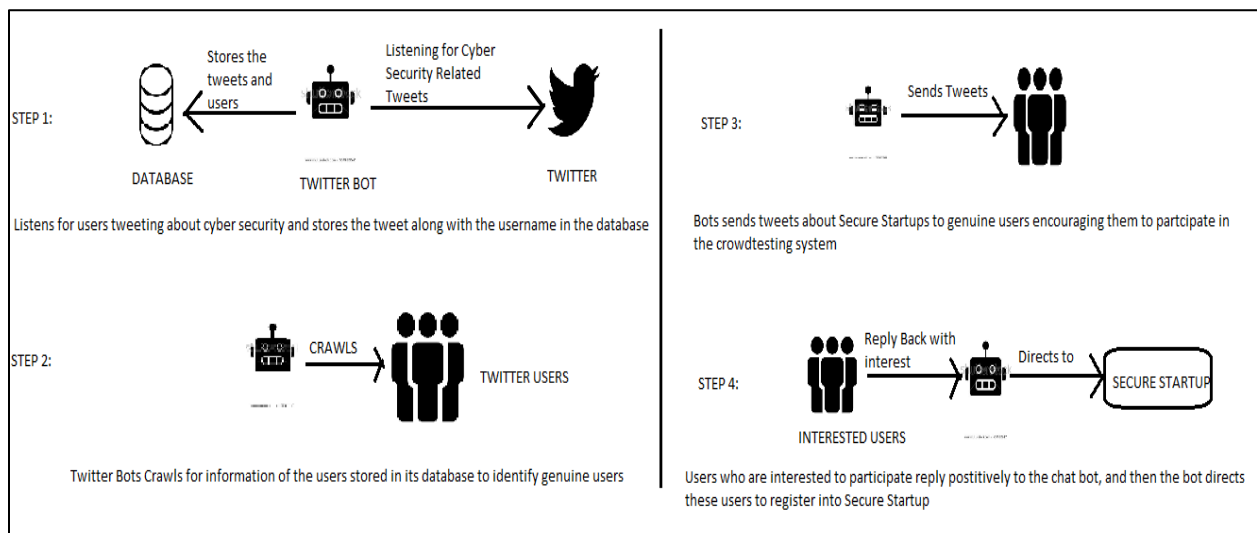


Figure 3.2: Tester Selection Process

Figure 3.2, explains the tester selection process using twitter bots. Testers for this system, are broadly classified into two main categories: (a) Security Experts, (b) Computer Science Students. Security Experts can be industry professionals who have a greater experience and knowledge on different cyber-attacks and remediation methods. They can also be educational professors and researchers who have thorough understanding of cyber security. It is important to include security experts in this system, as their expertise will ensure professionalism and quality of work. Students mostly comprise of undergraduate and graduate level students who are studying in the field of computer science or any other related field.

In the tester selection process, twitter bots, streams for live tweets related to a given hashtag. The hashtags used for streaming are strict cyber security terms [see Table 3.1] which are usually used by cyber professionals or people interested in the field of technology. As the bot streams for cyber security tweets, it simultaneously stores the tweet and the username in an Excel spreadsheet. This information will later be used to contact these twitter users. Figure 3.3 displays a screenshot of the bot streaming different twitter users based on the hashtag #cybersecurity.

```
Node.js command prompt - node stream1.js
user:
{ id: 831448779731656700,
  id_str: '831448779731656700',
  name: 'cybersecnews',
  screen_name: 'Cyb_Sec_News',
  location: 'New York, NY',
  url: 'https://cyber-sec-news.blogspot.it/',
  description: 'Cyber Security News collector for professionals, geeks, security addicted and enthusiasts!',
  protected: false,
  verified: false,
  followers_count: 3480,
  friends_count: 452,
  listed_count: 3,
  favourites_count: 0,
  statuses_count: 13754,
  created_at: 'Tue Feb 14 10:23:31 +0000 2017',
  utc_offset: 7200,
  time_zone: 'Rome',
  geo_enabled: false,
  lang: 'it',
  contributors_enabled: false,
  is_translator: false,
  profile_background_color: '000000',
  profile_background_image_url: 'http://abs.twimg.com/images/themes/theme1/bg.png',
  profile_background_image_url_https: 'https://abs.twimg.com/images/themes/theme1/bg.png',
  profile_background_tile: false,
  profile_link_color: '1895E0',
  profile_sidebar_border_color: '000000',
  profile_sidebar_fill_color: '000000',
  profile_text_color: '000000',
  profile_use_background_image: false,
  profile_image_url: 'http://pbs.twimg.com/profile_images/831451289351548928/eSXoNVFV_normal.jpg',
  profile_image_url_https: 'https://pbs.twimg.com/profile_images/831451289351548928/eSXoNVFV_normal.jpg',
  profile_banner_url: 'https://pbs.twimg.com/profile_banners/831448779731656700/1487068856',
  default_profile: false,
  default_profile_image: false,
  following: null,
  follow_request_sent: null,
  notifications: null },
geo: null,
coordinates: null,
place: null,
contributors: null,
```

Figure 3.3: Screenshot of the Bot Streaming Twitter Users Based on #Cybersecurity

| S. No. | HASHTAGS        |
|--------|-----------------|
| 1      | #Encryption     |
| 2      | #SSLInjection   |
| 3      | #Server         |
| 4      | #Crypgraphy     |
| 5      | #DataStructures |

Table 3.1: Hashtags Used for Streaming Live Tweets

We then, extract each username from the excel spreadsheet, and manually crawl the descriptions of their twitter accounts and their tweets. First, the information on the spreadsheet is crawled to identify genuine users. If a user’s information does not provide necessary details from the spreadsheet, then we crawl through the twitter feed of that particular user. This is done to filter all the twitter users, based on their qualifications, interests and knowledge. This step also ensures that the twitter bot does not tweet about the system to any malicious user. Upon crawling and going through the user’s twitter account, we were clearly able to identify, different security experts, students with computer background, malicious users, and spam accounts. Figure 3.4 shows a screenshot of an Excel sheet, that contains a descriptive user information for crawling their data. Every user that matches the standards, required by Secure Startup, is stored in a separate excel sheet. These users will later be contacted by the online bot to participate in the system. Table 3.2 shows examples of different Twitter bio’s that has been used to understand a user’s interest and if the account belongs to a genuine person or not. This crawling activity acts as a background check, to determine genuine users, their expertise and knowledge, which can be used to perform effective testing.

The excel sheet which stores the usernames after the crawling step, is divided into two lists, the first list consists of usernames of security experts, and the second list contains usernames of students. Creating such lists, makes it easier for the bot to explain the role that the user can play in this system, based on the category they belong to. For example, if a user is selected from the list of security experts, the bot will send tweets which explains their role as an expert for this system, which is managing the system and creating reports. If the bot selects a user from the students list, then tweets will be based on the explanation of a student’s role, which is completing micro tasks.

CATEGORY

BIO DESCRIPTION

|                 |   |
|-----------------|---|
| Security Expert | <p>Julio Cesar Melo</p> <p>@JulioCyberSec</p> <p>Tweeting about #CyberSecurity, #CyberDefense, #Forensics, #Privacy, #Pentesting, and sharing #InfoSec news</p> <p>Specialist: Security Operations Center(SOC)</p> <p>Ca.linkedin.com/in/jcmelo</p> |
| Student         | <p>Amanda Mitchell</p> <p>@mandamarie20</p> <p>I'm just your red ray of sunshine, Fire Princess, I love Aaron B. Taylor, makeup, and fried chicken. CS Major, VSU '18</p> <p>m.youtube.com/channel/UCZRJR...</p>                                    |

Table 3.2: Sample Crawled Content to Determine a Potential Tester

| Twitter URL                         | Username        | First Name | Last Name | Bio   | Location                  | Personal URL                   | Tweet   | Follow  | Followi | Last Tweet T | Last Tweet Text                       |
|-------------------------------------|-----------------|------------|-----------|---|---------------------------|--------------------------------|---------|---------|---------|--------------|---------------------------------------|
| http://www.twitter.com/chrismakara  | chrismakara     | Chris      |           | Digital Marketing Strategist & @Bulky Founder           | Houston, TX               | chrismakara.com/about          | 45,900  | 66,100  | 23,800  | 1h           | Processes To Supercharge Yo           |
| https://twitter.com/Secure_Startup  | Secure_Startup  | Secure     | Startup   | Let's start sharing the responsibility of securing cybe | New Delhi, India          |                                | 116     | 49      | 246     | 11h          | #Security #startup @synack raise      |
| https://twitter.com/sharifkhan      | sharifkhan      | Sharif     | Khan      | #dlir #malware hunter. Director of Engineering @Inf     | San Antonio, TX           | linkedin.com/in/sharifkhan     | 2,220   | 919     | 892     |              | Opportunity to work in #cybersec      |
| https://twitter.com/CyberSecPicki   | CyberSecPicki   | Ricki      | Burke     | Founder of @CyberSec_People, a global Informatio        | Melbourne, Victoria       | au.linkedin.com/in/cybersecpic | 1,165   | 2,263   | 3,122   | 1h           | The #Cybersecurity skills shortage    |
| https://twitter.com/Ellen_Timmer    | Ellen_Timmer    | Ellen      | Timmer    | Advocaat ondernemingsrecht / attorney-at-lav bus        | Rotterdam                 | nl.linkedin.com/in/ellentimmer | 28,200  | 900     | 421     | 10h          | % maak me er mee! zorgen over d       |
| https://twitter.com/RemiAlon        | RemiAlon        | Remi       | Alon      | #CyberSecurity and #Information Assurance Consu         | Nigeria   United Kingdom  | lussec.com                     | 1,071   | 411     | 332     | 10h          | Be part of the future of #cybersec    |
| https://twitter.com/PadraigMcGowan  | PadraigMcGowan  | Padraig    | McGowan   | As the saying goes, a re-tweet is not necessarily a     | Ireland                   |                                | 14,500  | 257     | 538     | 43m          | #UK #Payday loan firm #Wonga          |
| https://twitter.com/UrvashiPrakash  | UrvashiPrakash  | Urvashi    | Prakash   | Love Numbers, Tea, Football and F1. I tweet about       | Fri   Boardroom           |                                | 13,100  | 730     | 380     | 1h           | Use #UPI for banking. Be wary of c    |
| https://twitter.com/GillesHerard    | GillesHerard    | Gilles     | jk        | Businessman, merchant banker, private equity inve       |                           | gillesherard.com               | 21,100  | 1,134   | 1,566   | 10m          | Retail #sales drop as #consumers      |
| https://twitter.com/KestutisG       | KestutisG       | Kestutis   | Gardvilis | Co-founder @ETRONKA, passionate about #FinTe            | Vilnius                   | li.linkedin.com/in/gardvilis   | 7,288   | 449     | 638     | 2h           | How the ideal #challenger (#ne)       |
| https://twitter.com/evankirstel     | evankirstel     | Evan       | Kirstel   | #Solopreneur #Influencer #ThoughtLeader Helpi           | Boston, MA                | evankirstel.com                | 481,000 | 113,000 | 93,100  | 55s          | The iceberg illusion... via @evank    |
| https://twitter.com/pernyalevka     | pernyalevka     | Perry      | Malevka   | Tweets about #Startup #Cloud, #VoIP, #Security          | in Israel                 | li.linkedin.com/in/pernyalevka | 32,100  | 25,400  | 22,500  | 1m           | Why #AI #cloud technology and n       |
| https://twitter.com/alphabetsuccess | alphabetsuccess | Tim        | Fargo     | CEO of Social Juicebox. #socialhood #Quotes, in         | terax. 2x Inc. 500 winner | socialjuicebox.com             | 584,000 | 470,000 | 419,000 | 19h          | In order to be irreplaceable one m    |
| https://twitter.com/Oscharlie       | Oscharlie       | Charlie    | Miller    | I'm that 0day guy                                       | St. Louis, MO             |                                | 13,000  | 61,500  | 90      | 14m          | Doing tons of quiet step practice. Pe |
| https://twitter.com/bex0n           | bex0n           | Stephan    | Schmitz   | hacking stuff... software engineer at @sunzinet.        | opik Köln, Deutschland    | github.com/eyecatchup          | 925     | 154     | 443     | 21h          | #Vault7 linked #Longhorn group i      |
| https://twitter.com/WolfSec_ch      | WolfSec_ch      | Stephan    | Wolf      | Cyber Security Expert / Senior Security Engineer        | / Air Zürich              | wolfsec.ch                     | 6,051   | 368     | 527     | 30m          | FlashpointIntel Featuring great c     |
| https://twitter.com/hiramcoop       | hiramcoop       | Hiram      | Alejandro | Magician of 1s & 0s since 5670675001 @Seekint           | CDMX - GDL - MTY          | Seekint.com                    | 34,500  | 1,178   | 1,349   | 20m          | #Emergencias, #Phishing, #Malw        |

Figure 3.4: Excel Spreadsheet Used for Crawling

The next step is to send tweets to the identified genuine users. The twitter bot, selects one user at a time from each category and sends a tweet, about Secure Startup, which explains the system, the role the user can play and the incentives that can be earned. But, Twitter imposes a character limit of 140 characters on each tweet. This makes it difficult for the bot to explain everything in detail. Hence, the bot attaches a MS Word file which describes the entire system in detail, along with each tweet. It is easier to build trust between the bot and a twitter user, by providing detailed explanations of the system, as this gives an opportunity to the user, to understand the system and its deliverables, and the contribution that he can make to improve the testing scenario and his own skills and intellect. If the user is interested in participating in Secure Startup as a tester, he replies back to the bot with a positive message. The bot then directs the interested user to register into Secure Startup, which is a web based platform for testing. Figure 3.5 presents a screenshot of the bot sending tweets to the twitter users.

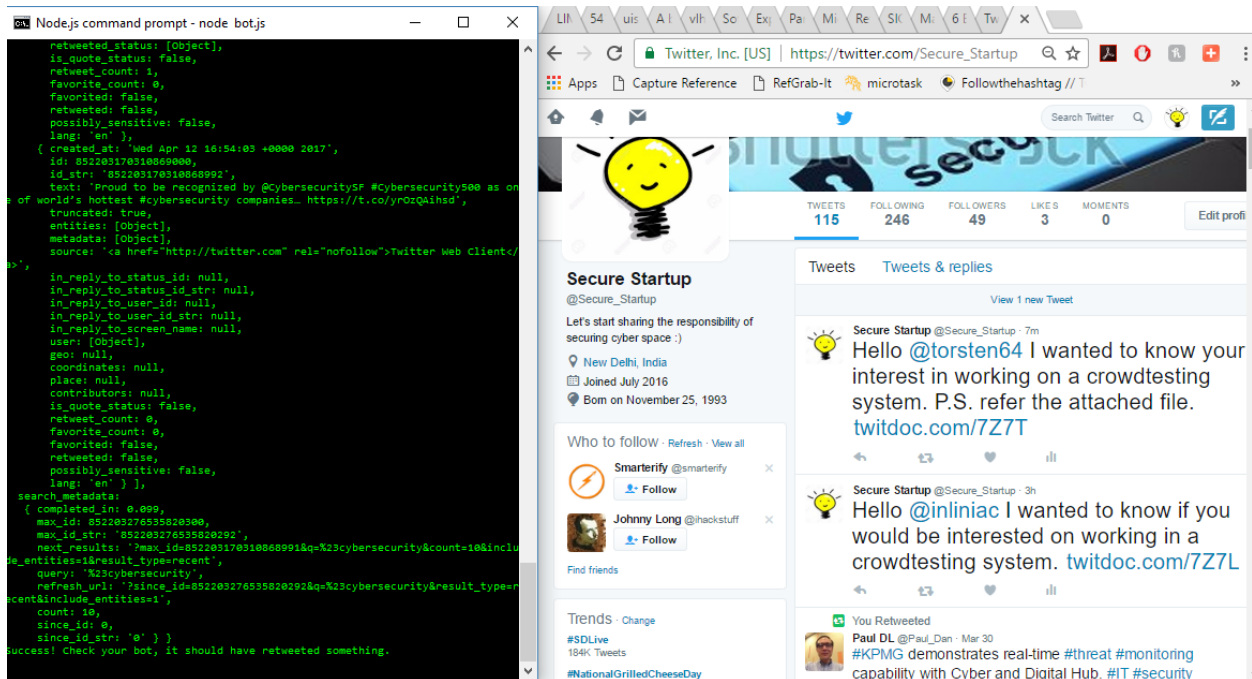


Figure 3.5: Screenshot Displaying the Twitter Bot Sending Tweets to the Users

### 3.2. TESTING WORKFLOW:

Figure 3.6 gives an overview of the testing workflow followed by Secure Startup, which has five basic steps and is entirely managed by an administrator.

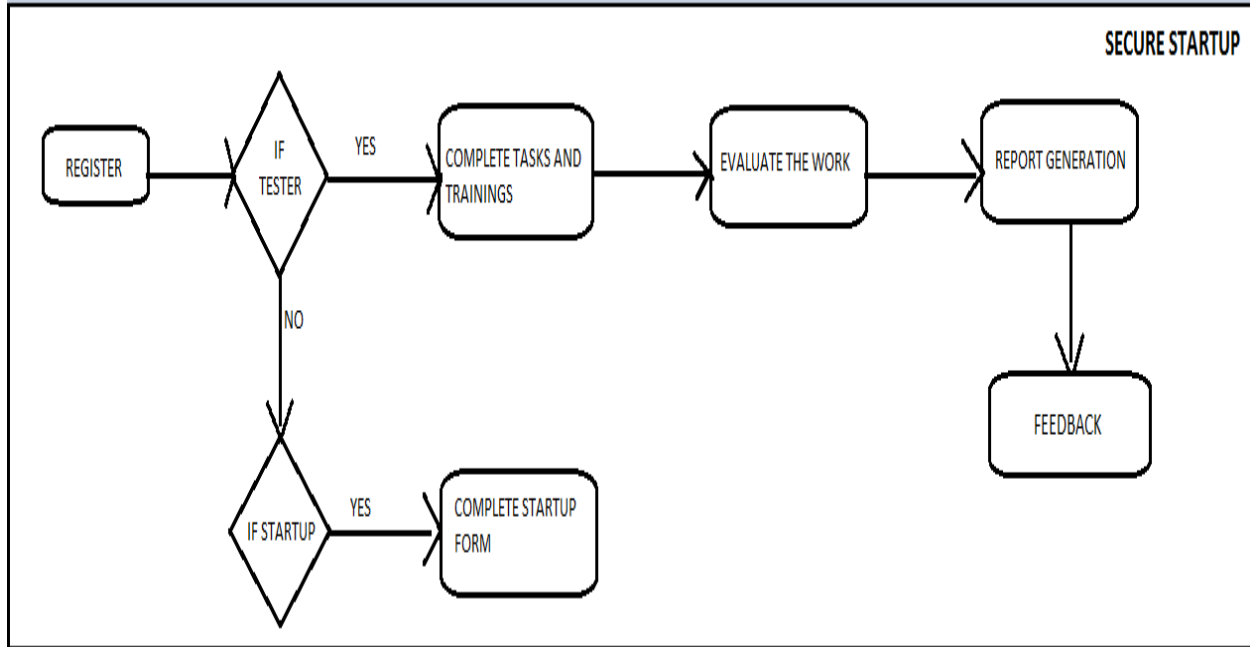


Figure 3.6: Testing Workflow

#### 3.2.1. REGISTER:

All the testers selected by the bot, must register into Secure Startup using a valid email address. When the testers click on “Register”, which is the registration button on the website, they are required to sign a non-disclosure agreement [Figure3.7] which prohibits them from using the content of the website elsewhere outside this platform. This limits the effect of security breaches and guarantees security as testers comply to non-misusage of sensitive information. [57] Captchas are also included into the registration process, to filter out unreliable users and any automated system that tries to misuse this system. Once the users are successfully registered, they have to fill in their profile and join groups. Initially Secure Startup has only two groups: Experts and Students, which are used by the new testers registering into the system. As the testers complete the tasks and trainings, they move onto the advanced level groups, based on their performance, ratings and learning capabilities. This process keeps the testers motivated to work efficiently. User groups also provide different access privileges to testers, which ensures the testing integrity. Figure 3.7 is a screenshot of the registration page and the non-disclosure agreement of Secure Startup.



SECURE STARTUP

**SECURE STARTUP - Registration Agreement Terms**

**Forum Terms of service**

The moderators of this forum will try hard to edit or remove reprehensible messages as soon as possible. However, it is impossible for them to review all the messages. You thus admit that all the messages posted on this forum express the sight and opinion of their respective authors and not those of the moderators or the Webmaster (except messages posted by them) and consequently, they cannot be held responsible of the discussions.

This forum uses cookies to store information on your computer. These cookies will not contain any personal information; they are only used to improve comfort while browsing. The address e-mail is only used in order to confirm the details of your registration as your password (and also to send you back your password if you forget it).

- Aggressive or slanderous messages, as well as personal insults and critics, the coarseness and vulgarities, and more generally any message contravening the French laws are prohibited.
- Messages who promote - or evoke - illegal practices are prohibited.
- If you post informations which come from another site, look first if the site in question doesn't forbid it. Show the address of the site in question in order to respect the work of their administrators!
- Please post your messages only once. The repetitions are unpleasant and useless!
- Please make an effort on grammar and spelling. SMS-style language (ex: r u sking?) is not advised!

Any message contravening the listing above will be edited or removed without additional notice or justification within deadlines which will depend on the availability of the moderators. Any abuse will involve the cancellation of the registration. Internet is neither an anonymous space, nor a space of no-right! We reserve ourselves the possibility of informing your access provider and/or the legal authorities of any malevolent behavior. An IP address of each poster is recorded in order to help us to make you respect these conditions.

By clicking on " I agree to these terms " below:

- You acknowledge to have fully read these current rules;
- You commit yourself to respect unreservedly these current rules;
- You grant the moderators of this forum the right to delete, move or edit any discussion subject at any moment.

I Agree to these terms  
 I do not agree to these terms.

SECURE STARTUP

**Registration Information**

Items marked with a \* are required.


Username : \*

E-mail address : \*

Password : \*

Figure 3.7: Screenshot of the Registration Page and Agreement Form

Startups are also required to register onto this platform. Once they register, they need to provide details about their website, instructions on testing, preference of operating system, browser preference, and budget. This helps Secure Startups manage the testing process easily, while conforming to the startup's needs. Figure 3.8 displays a screenshot of the startup space, where the startups can provide information on testing.

 **SECURE STARTUP :: STARTUPS**









|   | Topics  | Replies | Author | Views |
|---|---|---------|--------|-------|
|  |  PREFERRED BUDGET            | 0       | Admin  | 1     |
|  |  OPERATING SYSTEM PREFERENCE | 0       | Admin  | 2     |
|  |  BROWSER PREFERENCE          | 0       | Admin  | 1     |
|  |  INSTRUCTIONS                | 0       | Admin  | 1     |

Figure 3.8: Screenshot of the Startup Space

### **3.2.2. TASKS AND TRAININGS FOR TESTERS:**

The crowdsourced testers are responsible for testing the startup's website for vulnerabilities, and suggesting measures to remediate them. Secure Startup uses the OWASP Web Application Testing Methodology to test a website for vulnerabilities. The solutions are then provided by the experts to remediate any detected defect. The OWASP penetration testing method, does not require access to the source code of the website. Therefore, this method works best for this system, as no tester can manipulate the source code, which reduces the chances of security breaches. OWASP testing methodology, is an entire testing framework, which presents a high-level overview on evaluating the security of a web application [58]. This testing method is very long and consists of different techniques, to perform 9 active tests for a total of 66 controls, so, the testers have to try all the techniques to safeguard the website. Scanning a website for vulnerabilities is complex and time consuming, as it involves processing a large volume of data, hence, it is important to divide all the steps into micro tasks, to manage crowdtesting effectively. This also helps in easy task distribution, and enables parallel execution, which makes this system much faster [59].

Secure Startup, also provides trainings to testers, to ensure that the testers are well-prepared to complete the security tasks, expected of them. These trainings also help testers gain incentives and master different concepts. Completing the assigned trainings can be a fun way of learning new cyber skills, for students. These trainings are also designed to ensure that testers learn configuring different tools, and browser settings that will be used in the testing process. It is recommended that testers complete the trainings before attempting the online tasks.

As shown in Figure 3.9, Tasks and trainings are posted on the website, which can be easily accessed by testers, who can then select their preferred tasks as shown in Figure 3.10 for completion. A student must complete maximum number of tasks, to learn various skills. The more number of tasks a student completes, the maximum skills can be learned. The tasks posted on the website are related to the techniques used to detect flaws. Hence, every task provides an approximate background and detailed explanation, on the security content delivered by the task, and the steps needed to be taken, to complete the task. This helps students to better understand the importance of the technique and generate correct results.







| Forum   |           | Topics | Posts | Last Posts  |
|---|-----------|--------|-------|---|
|  | TRAININGS | 1      | 54    | <a href="#">TRAINING #1</a><br>Mon Mar 27, 2017 5:02 pm<br>abha3091          |
| <b>FORUM</b>  |           |        |       |   |
|  | TASKS     | 5      | 108   | <a href="#">TASK 3 - SQL INJ...</a><br>Mon Mar 27, 2017 5:00 pm<br>abha3091  |
|  | FEEDBACK  | 1      | 12    | <a href="#">Feedback Form</a><br>Wed Mar 22, 2017 12:16 pm<br>khalid123      |

Figure 3.9: Screenshot of the Tasks and Trainings Posted on the Website

|  SECURE STARTUP :: FORUM :: TASKS |   |         |        |       |
|--|---|---------|--------|-------|
| Topics   |   | Replies | Author | Views |
|                                  |  [ Poll ] TASK 1-SPF Enable  | 18      | Admin  | 230   |
|                                 |  TASK 3 - SQL INJECTION<br>[  Go to page: <a href="#">1</a> , <a href="#">2</a> , <a href="#">3</a> ] | 69      | Admin  | 228   |
|                                 |  [ Poll ] TASK #2 - Steal my Login   | 8       | Admin  | 230   |
|                                 |  [ Poll ] TASK 4 - Safe Browsing   | 9       | Admin  | 191   |
|                                 |  Your first subject  | 0       | Admin  | 27    |

Figure 3.10: Screenshot of the Task Selection Page

All the tasks have to be managed by an administrator, as Secure Startup requires generation of new tasks constantly, depending on the number of vulnerabilities detected and the solution chosen to deal with such weaknesses. Once the vulnerabilities are detected, new tasks are created, for the experts, to offer solutions to remediate the detected vulnerabilities. Once all the solutions are obtained, another set of tasks are created, where testers try to implement the given solutions to

fix the flaw. This chain of task creation is continued, until all the vulnerabilities are detected and fixed.

### 3.2.3. EVALUATION:

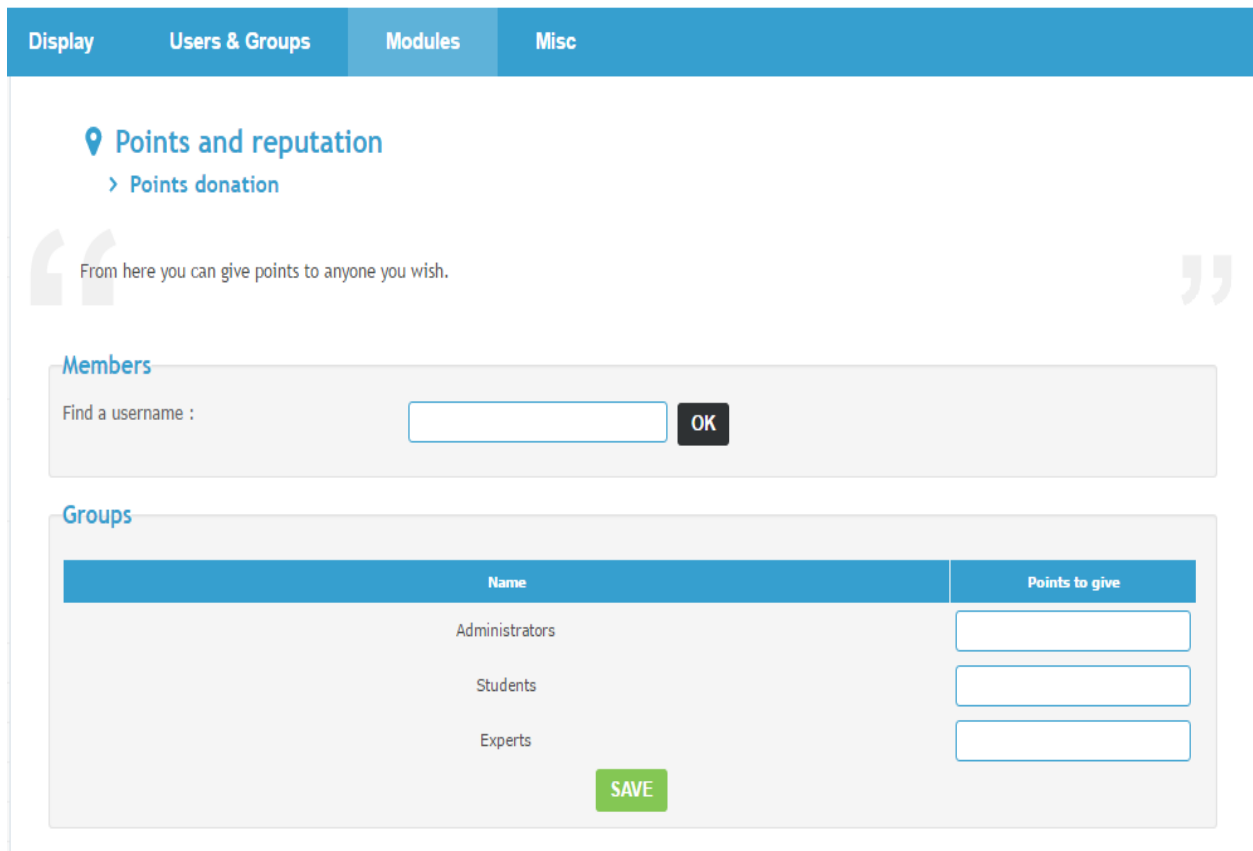


Figure 3.11: Screenshot of the Ratings Page

As the tasks are being completed by the testers, security experts provide constant feedback and rate another tester's work. This improves a testers performance, and helps them easily alleviate to advanced levels. Figure 3.11 provides a screenshot of the ratings page used by experts who can evaluate and rate a testers performance. Every tester, who executes a task, will receive 10 Yash point, and a tester, who correctly executes the task, generating accurate result, receives 20 Yash points. A tester receives 50 Yash points if he provides further explanation, on his results. Yash is a term used to award points. It is derived from an Indian language called Hindi. This is one of the criteria, used by the experts to rate the performance. Security experts also rate each other's performance by analyzing their task performance and feedback content. Experts receive 10 points

for giving feedback, and 50 Yash point for providing a detailed feedback. They also receive 50 Yash points, for filling in each part of the report. These ratings provided by the experts, to their peers, help all the group of testers in advancing to the next levels. This means that every student has possible chances of becoming an expert in near future. As the ratings of the tester increases, the opportunity to advance on further levels also increases. Every tester will require to earn 5000 Yash points, to advance to the next level. Such rating and evaluation systems, keep all the testers motivated to work hard, and gain expert skills.

#### **3.2.4. REPORT GENERATION:**

Generating Reports, is one of the most critical aspects, of Secure Startups. It is important to record every detail about the detected vulnerability, so that the startups can take necessary steps to implement security policies, and can reuse the document to ensure safety in their future projects. As soon as a task is completed on the website, and a vulnerability is detected, the expert has to describe the vulnerability and fill in the necessary details present in the report. Other experts, can go through the report at any point of time, to make necessary changes. The Reports page can only be accessed by the experts and not by students, to ensure correctness. The details included in the report are maintained to be completely accurate, as startups follow the report to make necessary changes to their website and use the same concepts to strengthen their security policies. There are certain vulnerabilities, that can cannot be fixed by the testers, because the testers require access to the source code to make certain modifications or additions. Such vulnerabilities are listed on the report, along with the process to fix them. These vulnerabilities are then handled by the startups, who make necessary modifications to their source code to exterminate the defect. The report is maintained in an Excel worksheet, which can be accessed by the Experts through link available on the website.

Figure 3.12 presents a screenshot of different items in the report, which helps in storing every detail of the vulnerability. The report stores a vulnerability ID, the tester's name who describes the vulnerability, the date of posting, the status of the defect, which shows if the vulnerability is fixed or not, and summary which is used to describe the behavior of the defect, and the measures taken to eradicate the vulnerability. If the vulnerability is not fixed, then the summary section is used to explain the process of eradicating the defect. The report also contains an extra

sheet, named as “About this Report”, which explains how to use the report effectively, for documenting every single detected vulnerability in detail

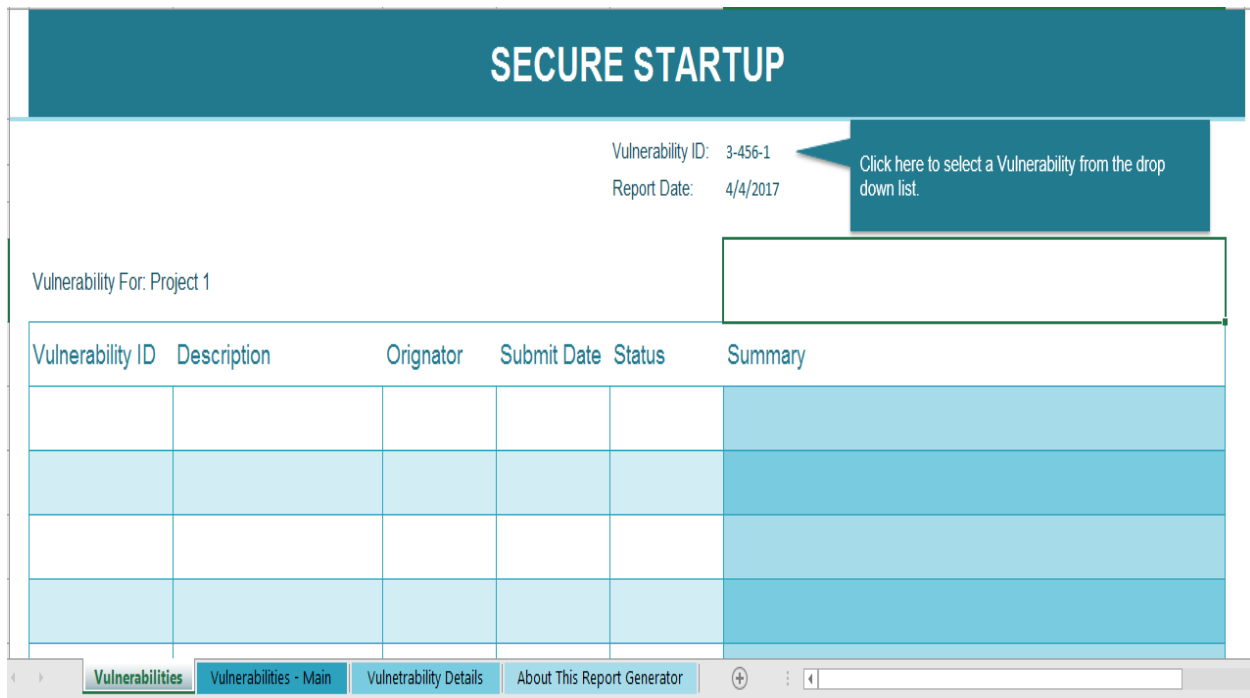


Figure 3.12: Report Generator

### 3.2.5. FEEDBACK:

Secure Startup provides a feedback channel to its testers, for providing quality feedback on this system. Figure 3.13 illustrates a screenshot of the feedback form used by Secure Startup. This feedback is used to analyze the effectiveness of this system, and understand its downsides. It helps in improving the quality of the system, for active testing. Once the testers complete their testing tasks and report generation, they are asked to fill out the feedback form for Secure Startup. As discussed previously, Secure Startup not only provides an opportunity to startups, to test their website in a cost-effective manner, but also helps students in learning, real-world cyber skills. So, the feedback channel is also used in analyzing the learning capabilities of students, and considering their needs to incorporate or delete any part of the training material. It also helps in understanding, that this system is being used and the results generated through it are accurate, while providing a real insight, on the system’s quality. Therefore, the feedback channel is necessary for constant

improvement, as it has helped in analyzing the learning capability of students and quality of the system, which is further discussed in Section 6.

The image shows a web-based feedback form titled "FEEDBACK FORM". At the top left, there is a blue header bar. Below the title, a red asterisk indicates that the following fields are required. The form contains four input sections: 1. "Email address \*": A text input field with the placeholder "Your email". 2. "Name \*": A text input field with the placeholder "Your answer". 3. "Username on 'Secure Startup' \*": A text input field with the placeholder "Your answer". 4. "Rate the overall difficulty level of the tasks \*": A horizontal scale with five radio buttons labeled 1, 2, 3, 4, and 5. The radio button for '1' is currently selected.

Figure 3.13: Feedback Form

### 3.3. INCENTIVES:

Incentives play a key role in the effective utilization of crowdtesting, [2] as it important to keep the testers highly motivated throughout the testing process. To build the incentive structure for this system, it is important to understand, the different motivating factors that can help testers perform better. One regular approach with regards to motivation is to make a refinement amongst intrinsic and extrinsic motivation [60]. Intrinsic motivation occurs when an individual engages in an activity, such as a hobby, that is initiated without obvious outside motivators, whereas, Extrinsic motivation is activated by external incentives, such as direct or indirect monetary compensation, or recognition by others [61]. Security experts are highly motivated to conduct tests, as they enjoy testing and treat it as a hobby. But, at the same time students require some monetary incentives to conduct tests, since they treat crowdtesting as a part time job, where they can learn certain skills and also earn some extra cash. Moreover, a survey conducted by Zogaj [44] also showed that

crowd testing is a part-time work and a hobby at the same time for most of the crowdworkers. Hence, Secure Startups provides its testers, with both, extrinsic and intrinsic incentives. While tester selection, it was observed that, security experts were highly motivated and were always willing to help as they truly understand the need of cybersecurity education. They also want to help startups create a highly secure website which is a safe place for its targeted users. So, experts don't necessarily require monetary incentives for their work. Moreover, due to the limited budget, it is not possible to provide money to all the students. Hence, Secure startup will reward a cash price to one expert and one student, who completes all the tasks, with remarkable performance. This can lead to an increase in creativity, information sharing and active engagement when hunting for bugs. This also helps Secure Startup in being cost effective to all the small organizations. Secure Startups also includes, ranking and reward system for all its testers as an extrinsic motivation, where every expert provides constant feedback and ratings to all its peers. The rating system is explained in detail in Section 3.2.3. In a previous work by LaToza, it is revealed that the motivational power of the points system and leaderboard, leads to an increase in the performance of the crowdworkers [62].



## 4. SYSTEM HYPOTHESIS:

The hypothesis of this system is that, crowdtesting platform, that includes educating students, leads to:

a) Higher Learning Rate:

- i. Students complete higher number of trainings.
- ii. Students feel that by completing the tasks and trainings they can gain necessary skills for their career development.
- iii. Students learn better when the theoretical concepts are explained as the task description.

b) Higher Task Completion Rate:

- i. Testers complete maximum number of tasks.
- ii. There is no task left unattended.

c) Higher Task Effectiveness: To calculate the effectiveness of each task that is completed,

$$\text{Effectiveness: } \frac{\text{Number of Tasks Completed Successfully}}{\text{Total Number of Tasks Undertaken}} * 100$$

d) Lower Number of False Negatives: A False negative can occur when testers do not detect a vulnerability that exists in the website.

The results obtained after analyzing these metrics are discussed in the next section (Section 5.2 and Section 6)

## 5. RESULTS:

The goal of Secure Startup is to propose a system, that can test a website for vulnerabilities, while educating students on cyber security, through crowdsourcing. The basic idea is to understand, if such a system can help students learn necessary cyber skills and also have testers, who can successfully run tests, generating quality results. This report also presents an analysis on the engagement of twitter bots in crowdsourcing testers.

### 5.1. RESPONSE RATE:

Secure Startup uses twitter bots to crowdsource the testers. The basic task of the bot is to attract as many crowdworkers as possible and gain their responses to achieve faster quality results. To achieve its goal, the bot has to appear as a genuine twitter user, and not a spam account. Hence, the bot tweets content related to cyber security, is always active, retweets interesting content, and tries to maintain maximum followers. Table 5.1 and 5.2 presents the bot's account details, which summarizes its activity and engagement on twitter.

| <b>BOT</b>            | <b>No. of tweets</b> | <b>No. of users following</b> | <b>No. of followers</b> | <b>No. of Likes</b> | <b>No. of Retweets</b> |
|-----------------------|----------------------|-------------------------------|-------------------------|---------------------|------------------------|
| <b>SECURE STARTUP</b> | 158                  | 246                           | 112                     | 3                   | 93                     |

Table 5.1: Twitter Bot's Account Details

| <b>BOT</b>            | <b>No. of Times Bot's Content was Retweeted</b> | <b>No. of Likes received</b> | <b>No. of User Mentions</b> |
|-----------------------|---|------------------------------|-----------------------------|
| <b>SECURE STARTUP</b> | 871   | 674                          | 28                          |

Table 5.2: Analytics on Twitter Bot's Content

The values presented in the above tables, depicts that the twitter bot was highly active on twitter, which can help build trust and gain maximum responses. To crowdsource testers, the bot sent tweets to the experts and students, stored in its excel spreadsheet, to participate in a crowdtesting platform, that helps Startups secure the website. These tweets resulted in gaining only 2 responses. The next strategy applied by the bot, was to include one line description of the

system, which would help users understand the system and eventually the bot could gain maximum responses. The bot received 9 responses by experts, asking for additional details about the system. The bot managed to gain responses from experts but, this strategy proved unsuccessful to gain student responses because, students did not understand the idea behind Secure Startups due to the lack of explanation and were not motivated enough with any incentives. Moreover, twitter imposes a character limit of 140 characters on each tweet, which hinders the bot from providing a detailed explanation on this system. Hence, the third strategy applied by the bot, is to attach a word document, with every tweet that explains the system, the incentives that can be earned, and the role that each tester has to play. This strategy proved to be successful as the bot managed to gain higher number of responses compared to the other strategies. This strategy made the users aware of the system’s goal, responsibilities, motivating factors and incentives, which motivated them in participating in this system. A summary of the responses obtained is represented in Figure 5.1.

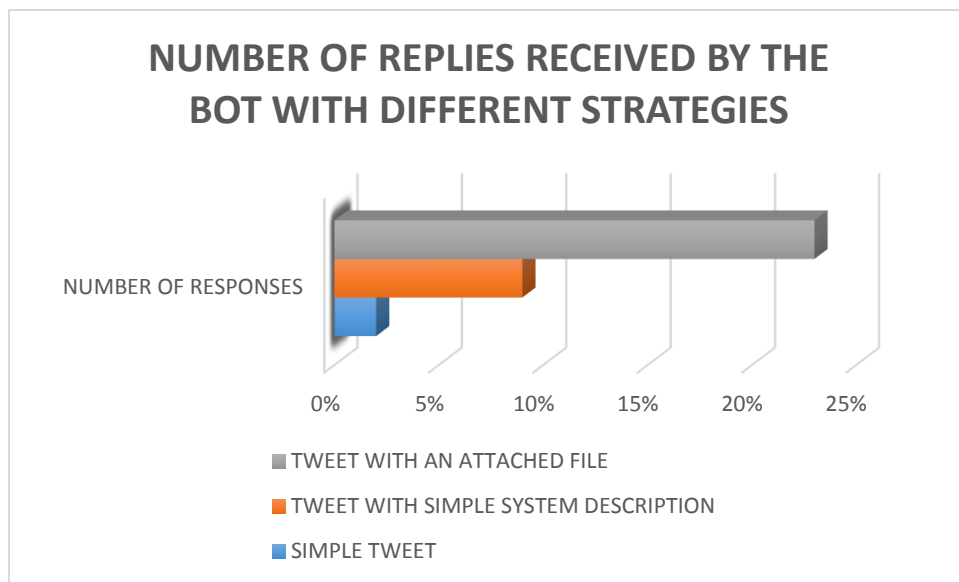


Figure 5.1: Reply Rate Graph

It is also important to analyze response rate generated from different categories of testers, that the bot interacts with. This helps in developing an effective bot, that can interact with every group of tester, in as humanly manner as possible. The response rate of each category is presented in Figure 5.2.

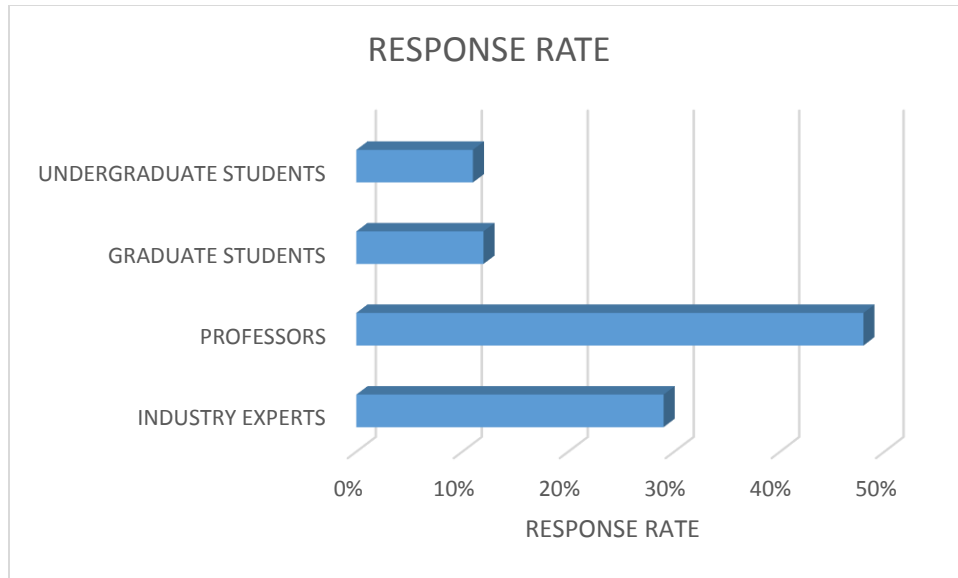


Figure 5.2: Graph Representing the Response Rate Generated by each Category of Tester

## 5.2. SYSTEM HYPOTHESIS RESULTS:

To analyze the system hypothesis, a crowd of 70 testers, hired from social media platform, were asked to Sign up for the crowdtesting platform, Secure Startup. They were then asked to fill in their profile on the web application. Secure Startup had a setup of 6 test tasks, and 2 trainings. The tasks were selected from the OWASP training guide, [58] to test a website called as, [www.zaful.com](http://www.zaful.com). The given trainings were simple games, created for basic cyber security education. The group of testers were comprised of, students majoring in computer related fields, experts working in the industry, and university professors researching and interested in the field of cyber security. The next sub sections present the results obtained after analyzing the system metrics.

### 5.2.1. LEARNING RATE:

To analyze the learning rate of the students, it is important to understand:

- a) if the students complete the trainings,
- b) if the students feel that, the cyber security concepts practiced by them, in the form of tasks will be helpful in their career development.

c) if the students, enjoy learning theoretical concepts, if they are explained as a task description for every task.

Figure 5.3 represents the number of testers who completed the trainings. Training 1 is completed by 76% of the testers, while training 2 is completed by 97% of the testers. Although training 2 is completed by a higher number of testers when compared to training 1, the overall number of testers who completed both the trainings is relatively high.

To analyze if the students, understand the cyber skills and find this learning approach helpful, Secure Startups asks the students to complete a feedback form, and answering questions related to their learning capabilities after using this system. The results obtained after analyzing the feedback form, are represented in Figure 5.4 and Figure 5.5

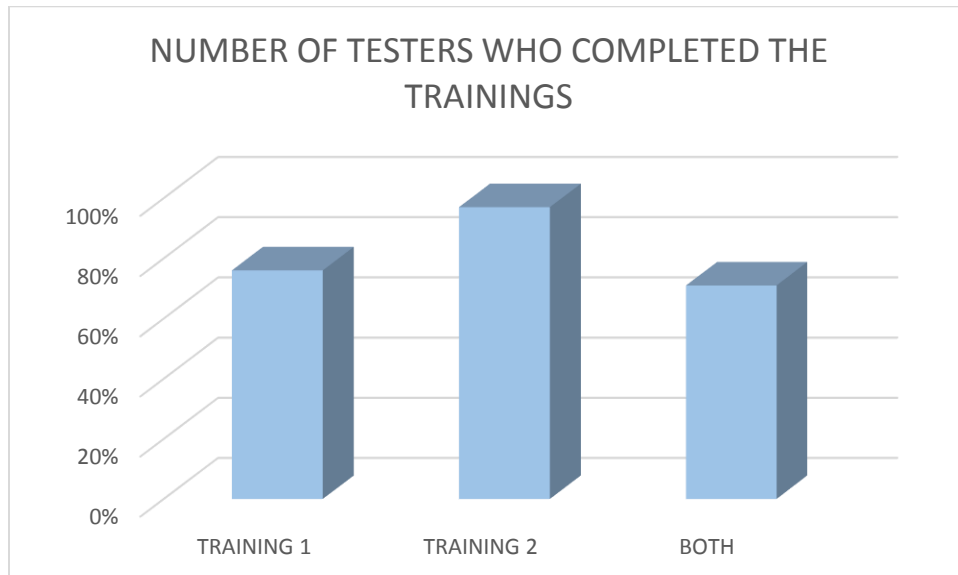


Figure 5.3: Graph Representing the Number of Testers Who Completed the Given Trainings

Figure 5.4 presents students feedback for the question, “Do you think, learning these skills will help you in your career?” 72.8% of the testers, feel that learning cyber skills, through Secure Startup will help students learn the necessary, real-world cyber skills for their career.

Figure 5.5 presents, the results of the feedback, for the question, “How useful is the cyber security information given in each task?” This information is used to analyze if the testers can learn the theory behind each task when it is included as a task description, which explains the concept of the task, its importance and how to test a small part of the website.

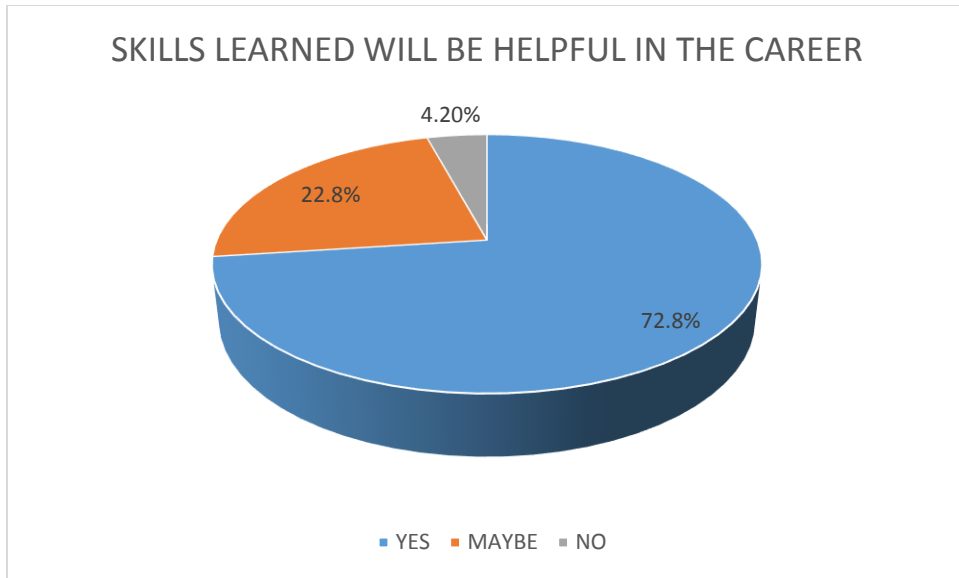


Figure 5.4: Graph Representing the Use of Secure Startup in Career Development

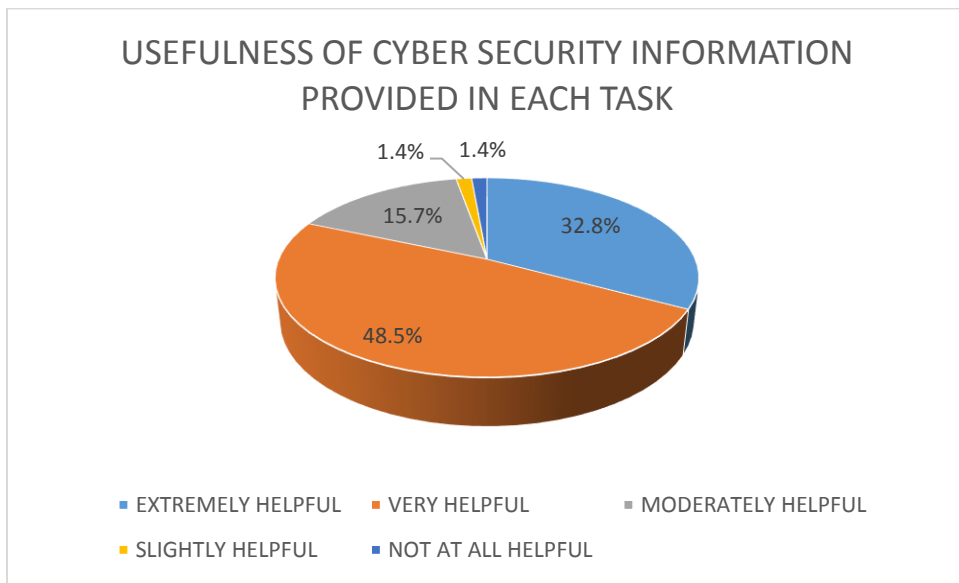


Figure 5.5: Graph Representing Students Feedback on the Task Description

### 5.2.2. TASK COMPLETION RATE:

In this section, we calculate the number of tasks completed by each user. The results obtained from these calculations help in analyzing the usability of the system.

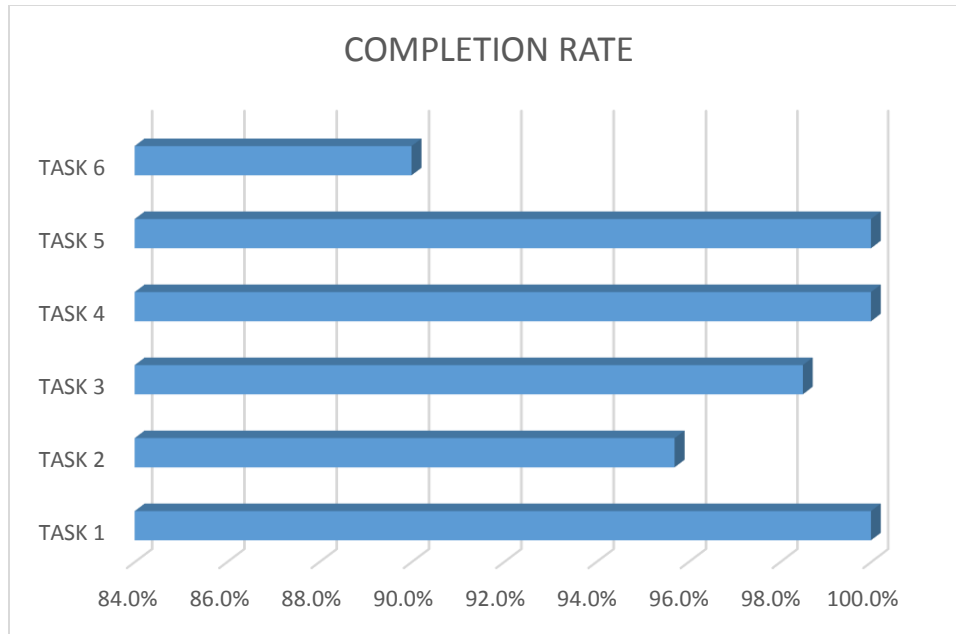


Figure 5.6: Task Completion Rate Graph

Figure 5.6 represents a graph, showing the task completion rate, of each task. It simply represents the number of testers, who have completed a particular task. But, the completion rate, is not a sufficient metric to analyze the task completion rate of the entire system, based on the given sample data, as it will not necessarily remain fixed for the entire system. Hence, we also have to evaluate the confidence intervals, to understand the feasible scope of the completion rate of this entire system, which determines the actual completion rate of this system. The calculations used to derive the actual completion rate are based on the Adjusted-Wald binomial confidence interval [63]. Table 5.3 presents the actual completion rate values along with the completion rate values of the given sample data. From the values depicted in this table, we can say that, if the observed completion rate for task 1 is 100%, then we can be 95% confident the actual completion rate of task 1 will be greater than 96%, which means that 96% of the testers of this entire system, will complete task 1. Similar statements can be generated for the remaining tasks. Finally, the average completion rate of this system is computed to be 96%.

| TASK                   | TASK 1 | TASK 2 | TASK 3 | TASK 4 | TASK 5 | TASK 6 |
|------------------------|--------|--------|--------|--------|--------|--------|
| COMPLETION RATE        | 100%   | 95.7%  | 98.5%  | 100%   | 100%   | 90%    |
| CONFIDENCE LEVEL       | 95%    | 95%    | 95%    | 95%    | 95%    | 95%    |
| ACTUAL COMPLETION RATE | 96%    | 88%    | 92%    | 96%    | 96%    | 80%    |

Table 5.3: Task Completion Rate Values based on Adjusted Value Binomial Confidence Interval

**5.2.3. TASK EFFECTIVENESS RATE:**

Completion rate, generates values to analyze, number of tasks completed by the testers and task effectiveness rate is a metric to evaluate the performance and accuracy of every tester, for each task. It is important to evaluate each testers performance, to understand the effectiveness of the system. The results obtained after calculating the task effectiveness are represented in a graph, in the Figure 5.7.

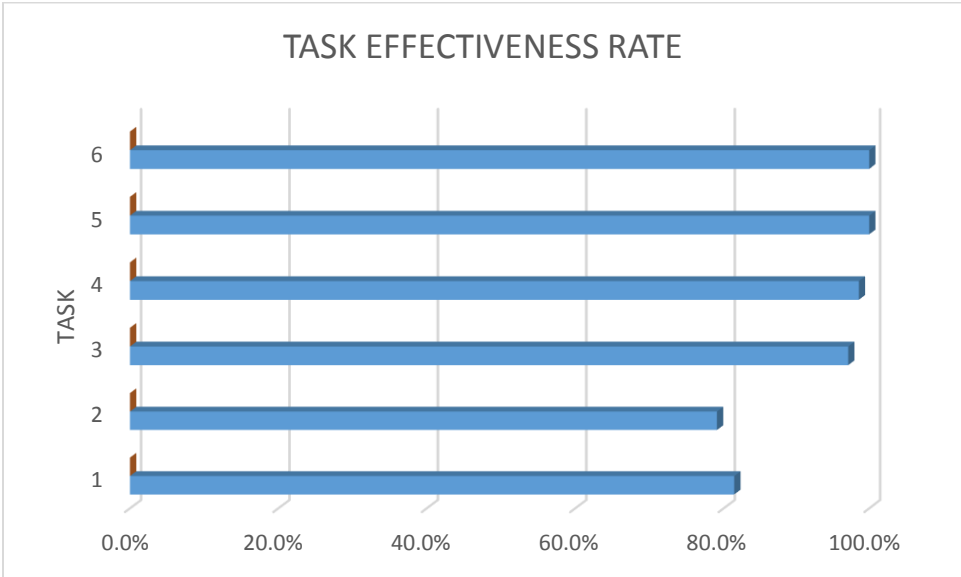


Figure 5.7: Task Effectiveness Rate Graph



### 5.2.4. NUMBER OF FALSE NEGATIVES:

It is important for any software testing system to not generate false negatives. To evaluate the number of false negatives generated by Secure Startup, we calculated the number of users, who were not able to perform a task successfully, or the users who generated wrong results. The false negative values for each task is represented in Figure 5.8.

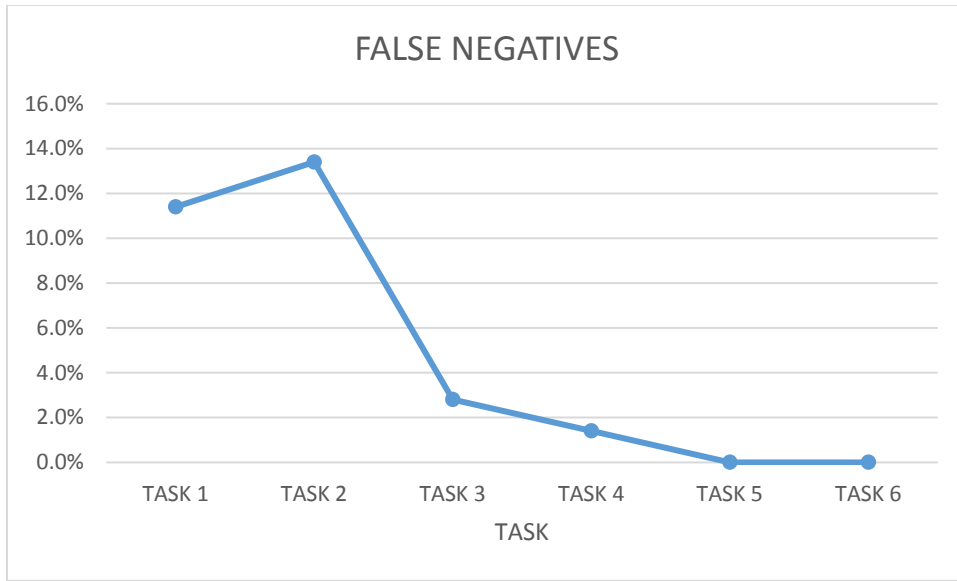


Figure 5.8: Graph Representing the False Negative Rate

## 6. DISCUSSION:

The results obtained in Section 5, are used to analyze the effectiveness of this platform, as a crowdtesting and learning medium. We analyzed different metrics to evaluate the learning rate, usability, accuracy, and performance of this system. Also, secure startups, deploys twitter bots, to hire testers, so it is important to understand the categories of people, that the bot is interacting with, for it to be effective. Hence, we started analyzing the overall replies received by the bot and the response rate of different categories of testers. It was observed that the response rate, generated through strategy 3 (23%), was the highest when compared to other strategies. Although this response rate is higher than the other strategies, it is not sufficient in building a crowdtesting platform. It was observed that the lower reply rate of Strategy 3 is due to the non-availability of monetary incentives. Usually crowdtesting platforms, offer higher cash rewards, and cash payments to its testers, which results in gaining greater number of testers for their platforms. But, we are trying to investigate, non-monetary approaches to build a testing and learning platform, particularly for startups who have constrained assets. The results obtained from strategy 3, are not completely discouraging, as they suggest that, if this strategy is applied on different social media platforms, reaching out to as many users as possible, there is a high probability of crowdsourcing more number of testers, who will be sufficient to build a crowdtesting platform. We also evaluated the response rate of each tester category. It was observed that the bot received higher number of responses from the experts (77%). This is due to the fact that, experts value cyber security skills, and understand its importance in today's world. On the other hand, students are unaware of the industry level security problems, and are already busy with their educational level homework and tests, which restricts them from participating in such systems. When we further analyzed the testers response rate, we found that, 48% of university professors responded to the bot, when compared to the industry professionals (29%). This was because the bot reached out to more number of professors. The overall results suggest that the twitter bot can be a helpful tool in automating the hiring process as it is capable of hiring a decent number of testers, if used effectively on different social media platforms.

Secure Startup provides students with a practical experience on the real-world cyber skills. To evaluate this system's capability as a learning platform, we generate the learning rate of students. Based on the feedback, it can be noted that the students find Secure Startup as a helpful

learning medium that can help them enhance their cyber security knowledge by practically performing the security tests. 72.8% of the students consider that these cyber skills are strongly going to help them in their career and the hands-on experience of industry level security testing will expose them to real-world cyber threats. To comprehend a student's learning rate, it is also important to evaluate his performance. Every task is associated with a theoretical description which explains the importance of the task in security testing, the procedure of conducting the test and sometimes an appropriate example for a better understanding of the topic. If a student comprehends this material well, he can then execute the task correctly. So, a student's performance also determines his learning rate. It is observed that the average rate of successful task completion is 92.7% which demonstrates this platform's ability to act as a strong learning medium. Secure Startup presents a new learning approach, where students are educated through micro tasks, and the results provide a positive insight on the learning capabilities of students.

To capture the usability, accuracy and performance of Secure Startup as a crowdtesting platform, we evaluate the task completion rate, the task effectiveness rate, and false negative rate. The task completion rate generates a binary value which helps in understanding if a task is completed or not. It gives a measurement of the success scenario of the system, which then must be constantly maintained by the testers. Every system should aim for a higher completion rate, where maximum number of testers complete all the given tasks. From the results generated, we can be 95% confident that the average completion rate of this system will at least be 96%. This means that 96% percent of the testers, will complete all the given tasks, leaving no task unattended. Thus, a startup website will be checked thoroughly, as all the given tasks will be completed by the system's testers.

Measuring the usability of the system is an important metric, but, it is also necessary to evaluate the accuracy of each task undertaken by a tester. If a tester completes all the tasks, but only generates false negative results, then the completion rate can no longer be a valid measurement to analyze the success scenario of this system. Hence, we also measure the task effectiveness or the performance of each tester. It was observed that task effectiveness rate for the last four tasks, were approximately 100%, while Task 1 and Task 2 have a low performance rate of 81% and 79% respectively. Testers did not comprehend the instructions listed on Task 1 and Task 2, which led to low task efficiency rate. As the testers progressed through the tasks and started

receiving feedback on their work, they got a better understanding on the working of the system and the use of instructions under each task, and then were able to perform better. Hence, we understand that there is a need to incorporate a system tutorial, that explains the working of the platform and the vulnerability detection process, which is based on the task description and task instructions. This helps in preparing the testers, to deal with the process of detecting vulnerabilities effectively. However, the overall task effectiveness rate of this system is high enough to guarantee a strong testing scenario that will help startups detect maximum number of vulnerabilities and also offer solutions to remediate them.

False negative results have a negative impact on the system's output. Hence, every security testing system should have a 0% false negative rate. Upon, evaluation we discovered that the false negative rate, of task 4 and task 5 were 0%, but similar results were not obtained for the remaining tasks. Task 1 and Task 2 had a relatively higher rate of 11.5% and 13.4% respectively. But, the advantage of crowdtesting is that that an incorrect result generated by a small group testers, can be overruled by the majority testers. Though we have a false negative rate of 13.2% for Task 2, the number of results generated correctly by the testers is 86.6%, and this result will finally be considered for the report generation. Hence, another advantage of this platform is that it helps in isolating false negatives.

The overall results of this system are highly influenced by the approach of microtasks. As the testing process was broken down into microtasks, the testers could easily understand the concepts, which helped them in generating greater number of valid results. Microtasks also helped in boosting the learning rate of students, which resulted in attaining a positive feedback on the learning value of this system. The final results have been positive in pursuing the system's value which lays in enhancing the security of a startup website and providing a new approach for practical cyber security education.

## **7. LIMITATIONS:**

Secure Startup can be used as an effective platform for crowdtesting and remediating vulnerabilities. However, it faces several limitations on the scope of testing. One of the factors that contributes to the limited scope of this system is the social media platform used for hiring testers. Secure Startup only uses Twitter to crowdsource testers from different backgrounds and expertise. It is important to explore the capabilities of other platforms like LinkedIn and Facebook for gathering potential crowd testers. Hence, integrating Secure Startup with other social media platforms remains a topic for future work

Creating microtasks enforces overhead on the system administrator. The administrator has to be constantly active and create new tasks for each new vulnerability that is detected, in order to swiftly resolve them. Nonetheless, microtasks have been successful in gaining maximum task completion rate which contributes to high usability and accuracy of this system. Due to microtasking, testers now have to spend less time on each task, which gives them an opportunity to complete more number of tasks.

OWASP Testing Guide, provides a long checklist of tasks to be performed while testing [58] The insights of this report are limited, as this system is tested against only 6 set of tasks to analyze the tester's performance and the usability of this system. Therefore, it is difficult to generalize these results throughout the system, which has about a hundred microtasks for detecting vulnerabilities. However, the results presented in this report are enthusiastically positive about a future in crowdtesting, that can also be implemented as learning medium.

Another factor limiting the scope of this system, is the entry of malicious testers. Secure Startups crawls every twitter user's data effectively, to ensure that the bot contacts only genuine users. Moreover, every tester must sign a non-disclosure form, that prevents a tester from participating in any kind of malicious activities. But, these steps, do not completely protect Secure Startup against fake users who disguise themselves to be knowledgeable security experts.

## **8. CONCLUSION AND FUTURE WORK:**

This report presents Secure Startup - a novel system, that aims to provide startups with a platform to protect their websites in a cost-effective manner, while educating students about the real-world cyber skills. The basic idea, is to understand, if such a system can help students learn the necessary cyber skills while, running successful tests and generating quality results for the startups. This report illustrates the design, working and the metrics used to assess Secure Startup as a successful learning and testing platform and it also discusses the working of twitter bots to hire reliable testers. We found that the trainings and expert feedback, helped students better understand the testing concepts, and this lead to an increase in their task performance. We also observed that the overall task effectiveness rate of this system is high enough to guarantee a strong testing scenario that will help startups detect maximum number of vulnerabilities and also offer solutions to remediate them. Crowdstesting framework, which involves the use of microtasks, helped in isolating the false negative values generated by this system.

Secure Startup, has been developed with an intention to help startups remain secure as they are the group of organization who are the most vulnerable to cyber threats and attacks. Hence, expanding the scope of the system to provide security to other types of software systems and organizations will remain a topic for future work. Although the crowdstesting approach used in this system is reliable, one can never depend on a single technique to ensure that every vulnerable point present in the website has been addressed. Hence, it important to emphasize security in the source code of the website, along with acclimating different testing approaches and not relying on one single approach to declare a website as a secure place.

Open issues that should be included in future work incorporate designing a reputation system for Secure Startup, that help in filtering out malicious users easily. Future work could also implement online bots on different social media platforms to hire more number of testers and study the interactions between bots and humans on a wider range to increase the effectiveness of the bot. Conducting an in-depth study to evaluate the usability of the system by analyzing the system performance on larger set of microtasks is definitely, an area worth exploration.

## 9. BIBLIOGRAPHY:

- [1] J. Fonseca, M. Vieira and H. Madeira. Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks. Presented at 13th Pacific Rim International Symposium on Dependable Computing (PRDC 2007). 2007 . DOI: 10.1109/PRDC.2007.55.
- [2] T. Hoßfeld, C. Keimel, M. Hirth, B. Gardlo, J. Habigt, K. Diepold, P. Tran-Gia. CrowdTesting: A novel methodology for subjective user studies and QoE evaluation. *University of Würzburg, Tech.Rep 4862013*.
- [3] (9 April 2017). *Crowdsourcing*. Available: <https://en.wikipedia.org/wiki/Crowdsourcing>.
- [4] D. C. Rowe, B. M. Lunt and J. J. Ekstrom. The role of cyber-security in information technology education. *Proceedings of the 2011 Conference on Information Technology Education 2011*. . DOI: 10.1145/2047594.2047628.
- [5] G. B. White and D. J. DiCenso. Information sharing needs for national security. Presented at Proceedings of the 38th Annual Hawaii International Conference on System Sciences. 2005, . DOI: 10.1109/HICSS.2005.320.
- [6] R. Sandhu, R. Krishnan and G. B. White. Towards secure information sharing models for community cyber security. Presented at 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing(CollaborateCom 2010). 2010.DOI: 10.4108/icst.collaboratecom.2010.3.
- [7] R. Singel. Cyberwar hype intended to destroy the open internet. *Threat Level* [<https://www.wired.com/2010/03/cyber-war-hype/>]. 2010.
- [8] *Cyber Security Theatre Vs. Real Thing*. Available: <https://www.forbes.com/sites/waynecrews/2011/03/16/cybersecurity-theater-vs-the-real-thing/#3ce933a432bc>.
- [9] *Intel Security Research Report*. Available: <https://www.vansonbourne.com/client-research/16021601TC?A=WebApp&CCID=31197&Page=22&Items=15;>.
- [10] P. W. Singer and A. Friedman. *Cybersecurity: What Everyone Needs to Know 2014*.
- [11] K. Trimmer, C. Schou and K. Parker. Enforcing early implementation of information assurance precepts throughout the design phase. *Journal of Informatics Education Research 9(1)*, pp. 95-120. 2007.
- [12] C. E. Irvine and S. Chin. Integrating security into the curriculum. *Computer 31(12)*, pp. 25-30. 1998.
- [13] M. Hentea, H. S. Dhillon and M. Dhillon. Towards changes in information security education. *Journal of Information Technology Education 5(2006)*, pp. 221-233. 2006.

- [14] M. Dark, R. Epstein, L. Morales, T. Counterline, Q. Yuan, M. Ali, M. Rose, N. Harter. A framework for information security ethics education. Presented at 10th Colloquium for Information Systems Security Education-University of Maryland. 2006, .
- [15] G. White and G. Nordstrom. Security across the curriculum: Using computer security to teach computer science principles. Presented at Proceedings of the 19th National Information Systems Security Conference. 1996, .
- [16] G. Engel and E. Roberts. Computing curricula 2001 computer science. *IEEE-CS, ACM.Final Report* 2001.
- [17] B. D. Cone, C. E. Irvine, M. F. Thompson, T. D. Nguyen. A video game for cyber security training and awareness. *Comput. Secur.* 26(1), pp. 63-72. 2007.
- [18] M. T. Huber and P. Hutchings. Integrative learning: Mapping the terrain. the academy in transition. *Association of American Colleges and Universities* 2004.
- [19] L. ben Othmane, V. Bhuse and L. T. Lilien. Incorporating lab experience into computer security courses. Presented at Computer and Information Technology (WCCIT), 2013 World Congress On. 2013, .
- [20] L. Chen and C. Lin. Combining theory with practice in information security education. Presented at Proceedings of the 11th Colloquium for Information Systems Security Education. 2007, .
- [21] J. Boleng and D. Schweitzer. A hands-on approach to information operations education and training. Presented at Proceedings of the 14th Colloquium for Information Systems Security Education. 2010, .
- [22] *Security Testing*. Available: [https://en.wikipedia.org/wiki/Security\\_testing](https://en.wikipedia.org/wiki/Security_testing).
- [23] M. E. Khan. Different forms of software testing techniques for finding errors. *International Journal of Computer Science Issues* 7(3), pp. 11-16, 2010.
- [24] Y. Huang S. Huang, T. Lin, C. Tsai. Web application security assessment by fault injection and behavior monitoring. Presented at Proceedings of the 12th International Conference on World Wide Web. 2003, .
- [25] *The importance of Web Application Security Testing*. Available: <http://www.it-labs.com/the-importance-of-web-application-security-testing/>.
- [26] P. A. P. Salas, P. Krishnan and K. J. Ross. Model-based security vulnerability testing. Presented at Software Engineering Conference, 2007. ASWEC 2007. 18th Australian. 2007.
- [27] D. Scott and R. Sharp. Abstracting application-level web security. Presented at Proceedings of the 11th International Conference on World Wide Web. 2002.



- [28] B. Potter and G. McGraw. Software security testing. *IEEE Security & Privacy* 2(5), pp. 81-85. 2004.
- [29] G. McGraw. Automated code review tools for security. *Computer* 41(12), 2008.
- [30] H. Uwano, M. Nakamura, A. Monden, K. Matsumoto. Analyzing individual performance of source code review using reviewers' eye movement. Presented at Proceedings of the 2006 Symposium on Eye Tracking Research & Applications. 2006.
- [31] B. W. Boehm. *Software Engineering Economics* 1981197.
- [32] K. Hamasaki, R. G. Kula, N. Yoshida, A. E. Cruz, K. Fujiwara, H. Iida, Who does what during a code review? datasets of oss peer review repositories. Presented at Proceedings of the 10th Working Conference on Mining Software Repositories. 2013.
- [33] J. Heffley and P. Meunier. Can source code auditing software identify common vulnerabilities and be used to evaluate software security? Presented at System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference On. 2004.
- [34] B. Blanchet. NWG1: static analysis-summary (MPII). *NWG1: Static Analysis-Summary (MPII)*.
- [35] J. Remillard. Source code review systems. *IEEE Software* 22(1), pp. 74-77. 2005.
- [36] A. Edmundson, B. Holtkamp, E. Rivera, M. Finifter, A. Mettler, D. Wagner;. An empirical study on the effectiveness of security code review. Presented at International Symposium on Engineering Secure Software and Systems. 2013.
- [37] G. McGraw. *Software Security: Building Security In* 20061.
- [38] N. Antunes and M. Vieira. Evaluating and improving penetration testing in web services. Presented at Software Reliability Engineering (ISSRE), 2012 IEEE 23rd International Symposium On. 2012.
- [39] A. G. Bacudio, X. Yuan, B. B. Chu, M. Jones. An overview of penetration testing. *International Journal of Network Security & its Applications* 3(6), pp. 19. 2011.
- [40] J. Nilsson and V. Virta. Vulnerability scanners. *Royal Institute of Technology, Stockholm* 2006.
- [41] H. Holm T. Sommestad, J. Almroth, M. Persson. A quantitative evaluation of vulnerability scanning. *Information Management & Computer Security* 19(4), pp. 231-247. 2011.
- [42] N. Khoury, P. Zavarisky, D. Lindskog, R. Ruhl. Testing and assessing web vulnerability scanners for persistent SQL injection attacks. Presented at Proceedings of the First International Workshop on Security and Privacy Preserving in E-Societies. 2011.

- [43] *CrowdTesting*. Available: <https://www.infosys.com/IT-services/validation-solutions/features-opinions/Documents/gamification-crowdsourced-testing.pdf>;
- [44] S. Zogaj, U. Bretschneider and J. M. Leimeister. Managing crowdsourced software testing: A case study based insight on the challenges of a crowdsourcing intermediary. *Journal of Business Economics* 84(3), pp. 375-405. 2014.
- [45] A. L. Zanatta, L. S. Machado, G. B. Pereira, R. Prikladnicki, E. Carmel. Software crowdsourcing platforms. *IEEE Software* 33(6), pp. 112-116. 2016.
- [46] (21 February 2017). *Web Design*. Available: [https://en.wikipedia.org/wiki/Web\\_design](https://en.wikipedia.org/wiki/Web_design).
- [47] S. Guide. Red Hat Enterprise Linux 3. 2003.
- [48] M. Yan, H. Sun and X. Liu. iTest: Testing software with mobile crowdsourcing. Presented at Proceedings of the 1st International Workshop on Crowd-Based Software Development Methods and Technologies. 2014, .
- [49] *A How-To Guide to Crowdtesting*. Available: [https://www.testbirds.com/fileadmin/Whitepaper-Studies/Testbirds\\_Whitepaper\\_How-to-Crowdtesting\\_EN.pdf](https://www.testbirds.com/fileadmin/Whitepaper-Studies/Testbirds_Whitepaper_How-to-Crowdtesting_EN.pdf).
- [50] R. K. Mok, W. Li and R. K. Chang. A user behavior based cheat detection mechanism for crowdtesting. Presented at ACM SIGCOMM Computer Communication Review. 2014.
- [51] *Crowdtesting: A win:win for organizations and customers*. Available: [http://www.infosysblogs.com/testing-services/2016/08/crowd\\_testing\\_a\\_win-win\\_for\\_or.html](http://www.infosysblogs.com/testing-services/2016/08/crowd_testing_a_win-win_for_or.html);
- [52] (2015). *Crowdtesting-What is it?*. Available: <https://mycrowd.com/blog/crowdtesting/>.
- [53] E. Ferrara, O. Varol, C. Davis, F. Menczer, and A. Flammini. 2016. The rise of social bots. *Commun. ACM* 59, 7 (June 2016), 96-104. DOI: <https://doi.org/10.1145/2818717>
- [54] S. Savage, A. Monroy-Hernandez and T. Höllerer. Botivist: Calling volunteers to action using online bots. Presented at Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing. 2016.
- [55] L. M. Aiello, M. Deplano, R. Schifanella, G. Ruffo. People are strange when you're a stranger: Impact and influence of bots on social networks. *arXiv Preprint arXiv:1407.8134* 2014.
- [56] (2016). *Can Social Media be used in an Effective way in Crowdsourcing?*. Available: <http://socialnomics.net/2016/09/08/can-social-media-be-used-in-an-effective-way-in-crowdsourcing/>.

- [57] (2014). *Enterprise Crowdtesting*. Available: [https://www.passbrains.com/fileadmin/user\\_upload/user\\_upload/Media/Articles\\_on\\_miscellaneous\\_sources/testingexperience-25\\_03\\_14-enterprise-crowdtesting.pdf](https://www.passbrains.com/fileadmin/user_upload/user_upload/Media/Articles_on_miscellaneous_sources/testingexperience-25_03_14-enterprise-crowdtesting.pdf).
- [58] M. Meucci, E. Keary and D. Cuthbert. Owasp testing guide v3. *OWASP Foundation* 162008.
- [59] C. Sarasua, E. Simperl and N. Noy. Crowdmap: Crowdsourcing ontology alignment with microtasks. *The Semantic Web–ISWC 2012* pp. 525-541. 2012.
- [60] J. M. Leimeister, M. Huber, U. Bretschneider, H. Krcmar. Leveraging crowdsourcing: Activation-supporting components for IT-based ideas competition. *J. Manage. Inf. Syst.* 26(1), pp. 197-224. 2009.
- [61] A. Ståhlbröst, C. M. Angelopoulos, O. Evangelatos, S. Krco, S. Nikoletseas, T. Raptis, S. Ziegler. Understanding modes of crowdsourcing and related crowd motivators. Presented at ISPIIM Conference Proceedings. 2015.
- [62] T. D. LaToza, W. B. Towne, C. M. Adriano, A. Van Der Hoek. Microtask programming: Building software with a crowd. Presented at Proceedings of the 27th Annual ACM Symposium on User Interface Software and Technology. 2014.
- [63] A. Agresti and B. A. Coull. Approximate is better than “exact” for interval estimation of binomial proportions. *The American Statistician* 52(2), pp. 119-126. 1998.

