Hack Track Bug Bounty Program

[1]R.M. Saritha,[2]Harish D,[3]Satheesh Kumar S,[4] Naveen S,[5]Usha D, [6]T. Kumanan

[1]Assistant Professor,[5,6]Professor

[2,3,4]IV Year B. Tech CSE Students

[1,2,3,4,5,6]Dept of Computer Science and Engineering,

[1,2,3,4,5,6]DR MGR Educational and Research Institute, Tamil Nadu, India

sarathisathish541@gmail.com, usha.cse@drmgrdu.ac.in

Abstract

Hacktrack is a bug bounty program. Users of the platform have the opportunity to properly report and get incentives for finding and revealing software defects and vulnerabilities. Hacktrack is a tool that lets people hone their bug bounty skills in a secure setting by identifying and reporting vulnerabilities. It shows the degrees of vulnerability severity and ranks them as low, medium, high, or critical so that problems may be prioritized and dealt with. We examine the economics of bug bounty schemes, examining the expenses and gains incurred by program administrators and the hackers who contribute to vulnerability discoveries. We discover that employing two more software engineers would now be more expensive on average than running a bug bounty program for a year.

Keywords: Bug Bounty Programs, Vulnerability Disclosure, Software Security.

Introduction

In a time of digital nnovation and connection, software system and application security is more important than ever. However, the speed at which technology is developing frequently outpaces our capacity to safeguard these systems against flaws that may be used by malevolent actors. Here's where HackTrack shines as a cybersecurity leader, enabling enterprises and ethical hackers to work together to fortify the digital space. Offering incentives to security researchers who are not affiliated with a company also known as "hackers" for discovering and disclosing flaws in software is a strategy that is becoming more and more common for doing so [1]. Self-driving vehicles, government systems, and electronic voting are just a few of the fields where this strategy is now being adopted [2],[4].

For instance, the Swiss government started a scheme where hackers could get paid e132,000 to discover weaknesses in a voting system. Hackers who found undetected methods of altering votes might receive rewards of up to e44,000 [2]. Another example is the "Hack the Pentagon" pilot initiative, which was started by the US Department of Defense (DoD) in April 2016 with the intention of evaluating the advantages of allowing hackers to identify vulnerabilities. 138 vulnerabilities were discovered and reported in less than six hours [5]. The DoD unveiled a new vulnerability disclosure policy as a result of the program's success, giving hackers access to other domains [3], [6]. Additionally, it has been suggested that US government agencies take involved in efforts to find vulnerabilities in open-source software [7]. In this case, a bug bounty platform usually facilitates the formal information sharing. Since 2013 [8], there have been an increasing number of new bug bounty programs available on platforms like HackerOne, with 50 new organizations establishing programs in 2018.

System Overview

As a proactive cybersecurity measure, companies can use bug bounty programs to encourage security experts, ethical hackers, and the general public to find and disclose vulnerabilities in their websites, apps, or software. By working together, we can leverage the cybersecurity community's aggregate experience to find and fix such vulnerabilities before malevolent actors can take advantage of them. Organizations usually establish guidelines, parameters, and a compensation plan to encourage people to disclose vulnerabilities in a responsible manner. By quickly resolving flaws that are found, this program not only improves security but also cultivates a good rapport between the company and the cybersecurity community. Bug bounty programs' open and collaborative structure highlights a dedication to strong cybersecurity procedures and ongoing development, which eventually strengthens digital environments against possible attacks.

Related Works

The vulnerability reward schemes for Firefox and Chrome offered by Mozilla and Google were examined by Finifter et al. [9]. Three years' worth of vulnerability reports (2010–2013) were examined to determine the compensation, level of severity, and frequency of reports. When the two applications are compared, it is evident that Google has addressed three times as many security flaws as Mozilla. Finifter et al. attribute this to the program's wider incentive structure and higher participation rate of white hat hackers (in comparison to the Google program) [9].For Google and Mozilla, the daily operating costs are $485 and $658, respectively; the total annual costs come to $177,025 ($485 × 365 days) and $240,170 ($658 × 365 days). Given that the current average salary of a software engineer is $65,133, this is about equivalent to the salary of three or four more software engineers. The authors contend that operating bug reward programs makes more financial sense than recruiting more researchers. The authors suggest further work that incorporates economic models to identify stages in a program's functioning, which serves as part of the inspiration for this contribution.

Background And Motivation

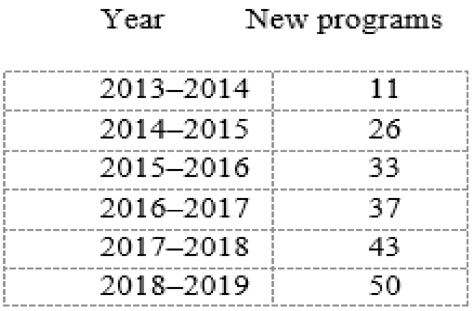
1. Background

The goal of vulnerability management is to enhance system security by locating, fixing, and reducing software vulnerabilities [12]. The operation of bug bounty programs (CMVM3.4) is recognized as a mature activity that satisfies the demand for vulnerability management in the most recent edition of the Building Security in Maturity Model (BSIMM9) [13]. In order to support security teams throughout the release and maintenance stages, bug reward programs are being included into frameworks for the secure software development lifecycle (SDLC) [14].

Numerous big companies run their own bug bounty and vulnerability rewards programs, such as Google, Facebook, and Microsoft [15] [17]. To promote their initiatives, many smaller organizations opt to use bug bounty sites like HackerOne, BugCrowd, and Cobalt [18] [20]. For organizations looking to manage a bug bounty program, HackerOne provides a variety of services that may be used for free or at a cost.

Organizations may promote their software to hackers through free hosting, with just a 5% fee added to any reward payments. Platforms have the advantage of making programs more visible, which enables many security researchers to look for vulnerabilities [21]. The platform is monetized through live assistance and fully managed programs, which enable organizations with no prior expertise to profit from running bug bounty programs.

Table 1. New programs from hackerone



Year	New programs
2013–2014	11
2014–2015	26
2015–2016	33
2016–2017	37
2017–2018	43
2018–2019	50

In order to reduce the amount of vulnerabilities, Raymond contended that increasing the number of people looking for vulnerabilities is advantageous: "Given enough eyeballs, all bugs are shallow" [22]. Independent security researchers with permission from an organization to find security flaws in networks, software, or hardware are known as "white hat hackers" [23].

2. Motivation

The quantity of applications available on HackerOne has nearly quadrupled from 82 to 212 since the 2015 research by Zhao et al. [18]. Up from 501 in the years 2010 to 2013, 2289 more rewarded reports have been made public on the Chromium bug tracker in the past two years [9]. There is great incentive to confirm the theories put out in the first two studies given this considerable increase in data that is available to the public. You may get six years of disclosure data for the oldest apps on HackerOne. It is possible to carry out a temporal analysis to look at the severity and frequency of reports over time. This makes it possible to evaluate and contrast the long-term effects of running a bug bounty program with the effects of recruiting more security researchers.

Existing System Architecture

Programs that reward bug bounty give companies a proactive, crowdsourced method of finding and fixing software flaws. Bug bounty programs offer a crucial line of defense against possible cyber threats by encouraging the responsible disclosure of vulnerabilities in exchange for monetary rewards. These initiatives encourage responsible disclosure, ongoing testing, and cooperation between companies and bug hunters, all of which contribute to increased security for digital assets, systems, and software**.**

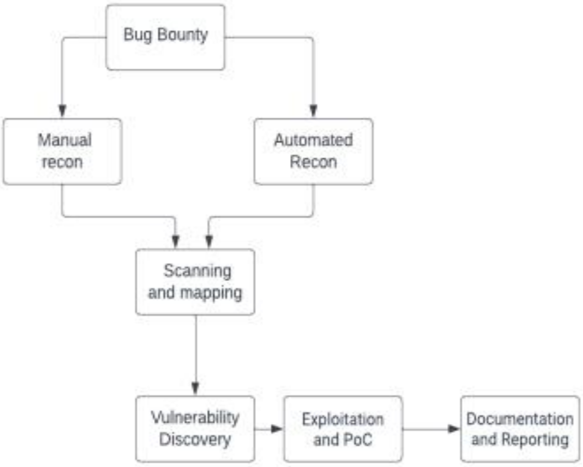


Fig.1: Existing Architecture Diagram

Proposed System Architecture

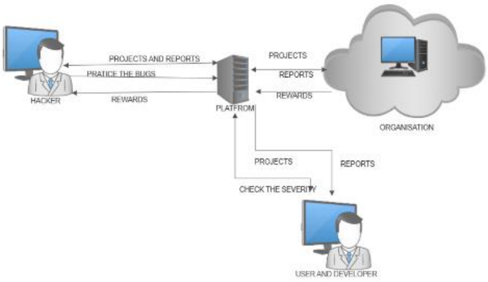


Fig.2 Proposed Architecture Diagram

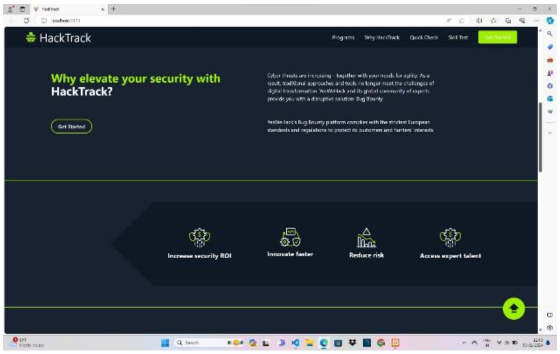
A vulnerability is indicated when it is mentioned, meaning that it was found or recognized when utilizing one of the website's tools or services. To find possible security risks or vulnerabilities inside a target system or network, this may entail executing tests, performing scans, or evaluating the data produced by the platform. Security experts, ethical hackers, and companies frequently utilize these technologies to find flaws in their networks and systems. A person or automated system has submitted a file or URL to Hack track in order to scan it for possible dangers, such as malware, viruses, or malicious activity. This is shown when the file or URL is suggested in Hack track. The platform then uses its collection of security technologies to scan the supplied item and generates a report outlining the analysis's findings. Hack track is frequently employed in bug bounty schemes to denote weaknesses or problems that have been found and reported by security researchers or ethical hackers via the Hack track network. When a vulnerability is reported on Hack track, it indicates that a hacker has filed a report describing the problem, which is now being reviewed and verified by the company managing the bug bounty program.

1. User Management Module

One essential element of a bug bounty program that helps to simplify and protect communication between the company managing the scheme and the researchers or ethical hackers taking part in it is the User Management Module. This module covers the methodical arrangement, validation, and correspondence with participants in vulnerability discovery and disclosure.

The module is in charge of controlling access levels and participant permissions. Organizations may designate different levels of access to distinct program assets based on the experience and performance history of ethical hackers. This guarantees that users will only communicate with the systems and apps that are specifically mentioned in the scope of the bug bounty program.

Lastly, the mechanism for rewards and recognition is managed by the User Management Module. When vulnerabilities are successfully found and reported, the module makes sure that the participants receive the right kind of incentive, which might be in the form of cash, recognition, or public recognition.



Why elevate your security with HackTrack?

Get Started

Cyber threats are increasing – together with your needs for agility. As a result, traditional approaches and tools no longer meet the challenges of digital transformation. YesWeHack and its global community of experts provide you with a disruptive solution: Bug Bounty.

YesWeHack's Bug Bounty platform complies with the strictest European standards and regulations to protect its customers and hunters' interests.

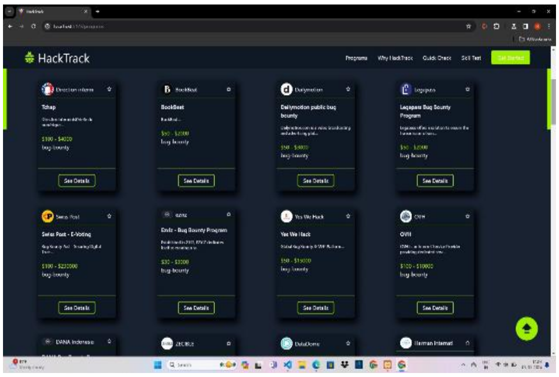
Fig.3 User Management Module

2. Bug Bounty Program

Within an entire bug bounty program, the "Bug Bounty Program Module" is a crucial component that coordinates the many phases of vulnerability discovery, reporting, and fixation. A well-defined collection of elements that work together to simplify the bug bounty procedure are usually included in this module.

Because a bug bounty program is dynamic, the module's "Continuous Improvement Mechanism" makes sure that improvements are made continuously. The efficacy, flexibility, and resilience of the program against new cybersecurity threats are enhanced by frequent evaluations, feedback loops, and component changes.

To summarize, the Bug Bounty Program Module functions as the central operational hub of the bug bounty program, coordinating the other components to provide a flexible, cooperative, and efficient structure for detecting and resolving security flaws.



Tchap
$100 - $4000
bug-bounty
See Details

BookBeat
$50 - $2000
bug bounty
See Details

Dailymotion public bug bounty
$50 - $5000
bug-bounty
See Details

Lepapeo Bug Bounty Program
$50 - $2000
bug-bounty
See Details

Swiss Post - E-Voting
$100 - $230000
bug-bounty
See Details

Eviiz - Bug Bounty Program
$30 - $3000
bug-bounty
See Details

Yes We Hack
$50 - $15000
bug bounty
See Details

OVH
$100 - $10000
bug-bounty
See Details

Fig.4 Bug Bounty Program Module

3. Skill Test Module

A Bug Bounty Program's skill test module is a tactical element designed to evaluate the knowledge and skills of participating security researchers and ethical hackers. This module acts as a first check to make sure that people or groups have the necessary abilities and understanding to recognize and report security issues. It usually consists of a series of simulated tasks that participants must complete to show off their expertise in various cybersecurity domains. These tasks are meant to resemble real-world events. These difficulties might include encryption, network vulnerabilities, web application security, and more. In addition to helping firms assess participant proficiency, the Skill Test Module enables ethical hackers to become acquainted with the unique systems and technologies used by the organization.

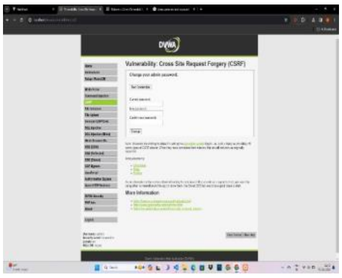
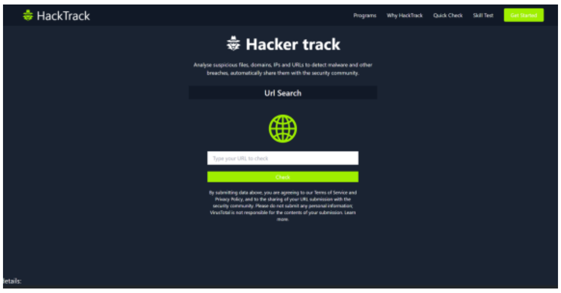


Fig.5 Skill Test Module

4. User Testing Module

When it comes to guaranteeing the security and usability of an application or system from the standpoint of the end user, the User Testing Module in a bug bounty program is essential. This part entails hiring security experts or ethical hackers to evaluate the platform's overall usability, user interface, and user experience. Testers concentrate on finding weaknesses in areas like authentication, permission, input validation, and user data security that might directly affect the end user. The bug bounty program defines the scope of the User Testing Module, indicating the areas in which ethical hackers should focus their efforts. This could entail determining user session vulnerabilities, analyzing the security of handling personal information, and gauging the efficacy of password rules.



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the sharing of your URL submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

Fig.6 User Testing Module

5. Security Module

One of the most important parts of a bug bounty program's security module is its ability to protect the program from potential vulnerabilities and maintain the integrity of the entire cybersecurity project. This lesson covers a broad strategy for risk response and mitigation. The module also has extensive authentication procedures and access restrictions to limit and confirm user access to the critical portions of the bug bounty program. Organizations may keep their programs safe from unwanted access and preserve their integrity by putting strict user authentication procedures in place.

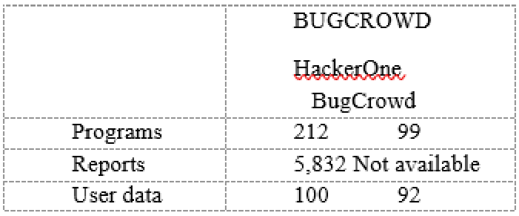
Developing trust in the bug bounty program is largely dependent on the security module. Organizations that prioritize platform security create a secure and dependable environment in which ethical hackers may conduct vulnerability identification. This dedication to security not only raises the program's legitimacy but also helps the organization's cybersecurity procedures to be improved over time.

System Data

The abundance of publicly accessible data on HackerOne and BugCrowd's platforms led to their selection. Every program data that was accessible in the directory was gathered for HackerOne. The program debut date, the quantity of reports resolved, the minimum bounty, and the average bounty were the data for each program. The most recent reports that have been filed are detailed in the Hacktivity section. Every record includes the time of submission and the username of the hacker who filed the report. Occasionally, additional details are shown, such as the vulnerability's description, severity rating, and prize amount. All of the entries in this section were gathered.

Additionally, program data was gathered from BugCrowd, however it was not as comprehensive as the HackerOne directory. The number of vulnerabilities found and the average compensation were gathered for every software. For every hacker, BugCrowd offers comprehensive user performance statistics. This information was gathered for users who were inducted into a program's Hall of Fame with the most points.

Table 2. Summary of information



	BUGCROWD HackerOne BugCrowd
Programs	212 99
Reports	5,832 Not available
User data	100 92

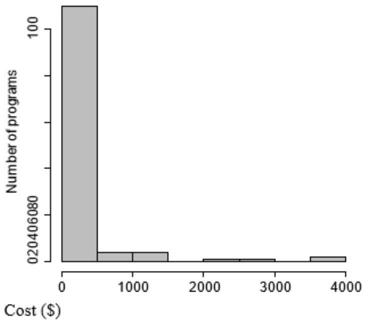


Fig.7 Histogram of Bug Bounty Program

Results And Discussions

Hack Track gives ethical hackers a place to submit vulnerabilities to companies, enabling vulnerability disclosure efforts and bug bounty programs. Security experts may use Hack Track online Application as a training tool to learn finding and taking advantage of vulnerabilities in online apps. In order to help security experts and companies find and fix security flaws, Hack Track provides a range of tools and resources for vulnerability assessment and penetration testing. It provides thorough information about the security status of files and URLs by combining many antivirus engines and analytic technologies, helping users to spot possible threats.

Conclusion

Hack track encourages cooperation between enterprises and ethical hackers, improving security via incentive bug reporting and responsible disclosure. Hack track gives security experts a practical way to hone their expertise and discover common online application flaws. Hack Track provides helpful information to help identify and mitigate security threats through penetration testing and vulnerability assessments.

It is a useful tool that users may use to evaluate the security of files and URLs, assisting in the early detection and mitigation of such risks. Together, these platforms enable people and organizations to recognize and efficiently fix security weaknesses, resulting in a more secure digital environment. We are going to totally automate work by implementing a user test module in the future.

References

[1] H. Fryer and E. Simperl, “Web science challenges in researching bug bounties,” in Proceedings of the 2017 ACM on Web Science Conference. ACM, 2017, pp. 273–277.

[2] Euro News. (2019, Feb) Euro News: Switzerland paying e-voting hackers. [Online]. Available: https://www.euronews.com/2019/02/13/ switzerland-offers-cash-to-hackers-who-can-crack-its-e-voting-system.

[3] Department of Defense. (2018, Oct) United States Department of Defense: Expanding hack the Pentagon. [Online]. Available: https://dod.defense.gov/News/NewsReleases/News-Release-View/Article/1671231/department-of-defense-expands-hack-the-pentagoncrowdsourced-digital-defense-pr/

[4] AI Trends. (2019, Feb) AI trends: Bug bounties and AI systems: The case of AI self-driving cars. [Online]. Available: https://www.aitrends.com/ai-insider/bug-bounties-and-ai-systems-thecase-of-ai-self-driving-cars/

[5] HackerOne. (2016, Jul) HackerOne: Hacking the pentagon.[Online].Available: https://www.hackerone.com/blog/hack-the-pentagon-results

[6] A. T. Chatfield and C. G. Reddick, “Cybersecurity innovation in government: A case study of US Pentagon’s vulnerability reward program,” in Proceedings of the 18th Annual International Conference on Digital Government Research. ACM, 2017, pp. 64–73.

[7] A. Schwartz, R. Knake, and Belfer Center for Science and International Affairs, Government’s Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process. Harvard Kennedy School, Belfer Center for Science and International Affairs, 2016.

[8] HackerOne. (2019, Jan) HackerOne: Bug bounty program directory. [Online].Available: https://hackerone.com/directory.

[9] M. Finifter, D. Akhawe, and D. Wagner, “An empirical study of vulnerability rewards programs,” in USENIX Security Symposium, 2013, pp. 273–288.

[10] Glassdoor. (2019, Jan) Glassdoor: Software engineer salaries in london. [Online].

[11] M. Blatter, S. Muehlemann, and S. Schenker, “The costs of hiring skilled workers,” European Economic Review, vol. 56, no. 1, pp. 20–35, 2012. [12] P. Foreman, Vulnerability management. Auerbach Publications, 2009.

[13] BSIMM. (2018, Oct) BSIMM9: Building security in maturity model version 9. [Online]. Available: https://www.bsimm.com/download/

[14] BugCrowd. (2018, Aug) BugCrowd: Integrating crowdsourced security with the SDLC. [Online]. Available: https://www.bugcrowd.com/blog/integrating-crowdsourced-securitywith-the-software-development-lifecycle/

[15] Google. (2019, Jan) Google: Vulnerability reward program. [Online]. Available: https://www.google.com/about/appsecurity/reward-program/index.html

[16] Facebook. (2018, Sep) Facebook: Whitehat program. [Online]. Available: https://www.facebook.com/whitehat

[17] Microsoft. (2018, Jul) Microsoft: Bug bounty programs. [Online]. Available: https://www.microsoft.com/en-us/msrc/bounty

[18] HackerOne. (2019, Jan) HackerOne: HackerOne bug bounty platform. [Online]. Available: https://www.hackerone.com/

[19] BugCrowd. (2019, Jan) BugCrowd: BugCrowd bug bounty platform. [Online]. Available: https://www.bugcrowd.com/

[20] Cobalt. (2019, Jan) Cobalt: Bug bounty platform. [Online]. Available: https://cobalt.io

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

[22] E. Raymond, “The cathedral and the bazaar,” Knowledge, Technology & Policy, vol. 12, no. 3, pp. 23–49, 1999.

[23] M. Rouse. (2007, Jun) Search Security: Whitehat hacker definition.