DEVOTION
Journal of Research and Community Service
Volume 4, Number 8, August 2023
e-ISSN: 2797-6068 and p-ISSN: 2777-0915

BUG BOUNTY HUNTING: A CASE STUDY OF SUCCESSFUL VULNERABILITY DISCOVERY AND DISCLOSURE

Isma Elan Maulani[1], Riska Anggraeni[2]
Universitas Muhammadiyah Cirebon, Indonesia[1]
SMK SBS Kuningan, Indonesia[2]
Email: ismaelanmaulani068@gmail.com, riiskaan662@gmail.com

KEYWORDS
bug bounty hunting; vulnerability device software; security researcher; security company; effectiveness; benefits; challenges

ABSTRACT
This research is a case study on bug bounty hunting as a successful approach to finding and uncovering vulnerabilities in software. The purpose of this study is to understand the effectiveness of bug bounty hunting and its benefits in improving company security. Qualitative research methods were used by analyzing data from bug bounty programs that were successful in finding significant vulnerabilities. The results showed that bug bounty hunting proved to be effective in capturing various types of vulnerabilities, including web application vulnerabilities, network protocol vulnerabilities, hardware security vulnerabilities, and mobile app vulnerabilities. Security researchers play a critical role in the success of the bug bounty hunt, with their expertise in bug hunting and deep understanding of the technology. The benefits of bug bounty hunting include increased software security, cost efficiency, and increased company reputation for security and credibility. However, challenges such as finding hidden vulnerabilities and coordinating with enterprises need to be overcome. Recommendations include strengthening collaboration between enterprises and security researchers, establishing effective communication channels, and proactively responding to vulnerability reports.

INTRODUCTION

In the digital era that continues growing, security device soft be one aspect critical in ensure integrity, confidentiality, and availability system. Attack to device soft can consequence loss financially significant, sensitive data leaks, and damaging reputation A organization. For overcome challenge these, companies and organizations has adopt various strategies for strengthen security device soft them (Subashini & Kavitha, 2011).

One approach that has become popular in industry technology is the program's bug bounty (Breidenbach et al., 2018). The program's bug bounty makes it possible company For involve community expert security independent, which is known as a security researcher, in effort For find vulnerability security in device soft them(Votipka et al., 2018). In this framework program , security researchers are invited For in a manner active look for vulnerability, reporting findings they to company, and accept imbalance form prize money or confession on contribution them.

Study This aim For do study deep about effectiveness of bug bounty hunting in find and reveal findings successful vulnerability (Maillart et al., 2017). Through Study focused cases, we will analyze the processes, techniques, and results achieved by participating security researchers in certain bug bounty programs. In context this , case Study will focuses on bug bounty programs that have show success in find and overcome vulnerability significant security.

First of all, it's important For understand why bug bounty hunting became so important and popular. In environment device increasingly soft complex, company often face challenge in find and fix existing vulnerabilities (Mu et al., 2018). In a number of case, vulnerability Possible No detected during the internal development process or inspection security routine.

With involve a changing and experienced community of security researchers, the company can widespread effort they in find possible vulnerabilities missed before.

The bug bounty program also provides incentive for security researchers to participate in look for vulnerability. With give present or confession to those who succeed find vulnerability, this program get up motivation and interest in look for weakness security . this help create ecosystem where the experts security own incentive For contribute in increase security device soft in a manner whole.

Besides In addition , the bug bounty program also provides benefit for company or the organization that launched it. In a number of case, costs incurred For remote bug bounty program more efficient than rent team internal security or face consequence attacks that don't detected (Carlin, 2015). In Lots case, the company that launched the bug bounty program has succeed find vulnerability as critical as possible No will detected without participation community security external.

However, even though the bounty program has bugs potency big, there a number necessary challenge overcome (LaToza & Van Der Hoek, 2015). one challenge main is coordination between companies and security researchers. Company must develop clear and efficient processes For accept report vulnerability, validate findings, and deliver award to inventors (Chang et al., 2016). Besides that's a problem laws and policies are also necessary noticed in arrange response to report vulnerability.

Important For note that the bounty program bug is not solution single For all problem security device soft . this program should used as mutual components complete with practice security device existing software there , incl inspection security routine , testing penetration , and robbery code. Bug bounty program available become an important pillar in security strategy company, however must managed with thoughtful and integrated with approach comprehensive security.

In study this, we will choose A Study representative case bug bounty program that has succeed in find and overcome vulnerability significant security. we will analyze the process, successes, and contributions made by participating security researchers in the programme . With understand contributing factors to the success of the bug bounty program, we hope can identify practice best and lesson valuable For implemented by other companies that want launched a similar program (Lam, 2014).

Through study this, we hope can give more understanding Good about effectiveness of bug bounty hunting in find and reveal findings successful vulnerability. Research results This can give outlook valuable for considering organization implementing a bug bounty program, as well can become base For enhancement security device soft in a manner thoroughly in the future (Moser & Korstjens, 2018). Moreover, The purpose of this study is to understand the effectiveness of bug bounty hunting and its benefits in improving company security.

RESEARCH METHOD

Study This will use approach study involving qualitative Study case as method main For collect and analyze data (Moser & Korstjens, 2018). Method study qualitative suitable For exploration complex and contextual phenomena, such as effectiveness of bug bounty hunting in find and reveal findings vulnerability (Maillart et al., 2017). Through approach this, we will get deep understanding about the processes, experiences, and perspectives of the security researchers involved in the bug bounty program that became focus Study case.

following is steps to be followed in method study qualitative this:

1) Election Studies Case

In study this, will chosen One Study case from the bug bounty program that has succeed in find and reveal findings significant vulnerability. Election Study case This will based on

criteria like reputation company, scale bug bounty program, success in find vulnerabilities, and availability of relevant data (Walshe & Simpson, 2020).

2) Collection :
   a. Deep Interview:
      Security researchers who have participate in the selected bug bounty program will interviewed in a manner deep (Alomar et al., 2020) . interview will involve question related experience they in bug bounty hunting, techniques used , difficult challenges, as well as disclosure and collaboration processes with company, interview will recorded and transcribed will used For analysis next.
   b. Analysis Documents:
      Documents related to bug bounty programs such as policies, guidelines, reports vulnerability, and communication between companies and security researchers will collect and analyze. Documents This will give more understanding deep about program structure, procedure disguise, and policy award.
3) Analysis:
   a. Coding and Categorization:
      Collected data from interviews and documents will encoded and ignored For identify themes general, problems that arise, as well successful practices and strategies on a bug bounty hunt.
   b. Analysis thematic:
      Through analysis thematic, will searching for emerging patterns, trends, and findings from data. this will help in understand factors that contributed to the success of the bug bounty program, the obstacles encountered, as well as the experiences and perspectives of the security researchers involved.
   c. Triangulation:
      Data from interview will confirmed and strengthened with use data from analysis document. This will give explanation and validity more more about the findings research.
4) Interpretation and Conclusion:
   Based on data analysis, findings will interpreted and presented in a manner deep. Study This will identify practice best, successful strategy, as well challenges faced on a bug bounty hunt. Conclusion will taken For understand factors keys that contribute to the success of the bug bounty program and its implicit in increase security device soft.

   Through method study qualitative this is expected can obtain deep insight about security researcher experience in bug bounty hunting, as well factors that play a role in success of the bug bounty program. Study this too can give recommendation practical for other companies that want similar launch program For increase effectiveness disclosure and disclosure vulnerability in a manner success.

RESULTS AND DISCUSSION

RESULTS

Studies case about successful bug bounty hunting This disclose a number of results important related with disclosure and disclosure vulnerability (Ruohonen & Allodi, 2018). following is results of study

Identification Significant Vulnerabilities

1) Selected bug bounty program succeed in find significant vulnerabilities in the device soft or the system being tested vulnerabilities. This own potency road Serious to security associated companies and users.

2) Findings vulnerability covers various type gap security, like vulnerabilities in web applications, weaknesses protocol network, loophole device security hardware, and vulnerabilities in mobile applications. this show the effectiveness of the bug bounty program in catch weaknesses are diverse and complex .

Bug Bounty Program Success

1) Participation of Security Researchers: Participating security researchers in this bug bounty program play role important in success. Skill they in hunting insects, knowledge about relevant technology, and capabilities For identify vulnerability in a manner effective is factor key in find significant vulnerability.
2) Collaboration with Company: Good collaboration between security researchers and companies is factor important in The Success of the Bug Bounty Program. Open communication, responsive, and close cooperation between second for party possible invention effective vulnerability and appropriate disclosure time.

Profit from Bug Bounty Hunting

1) Enhancement Security: Successful bug bounty hunting program possible company For identify and fix vulnerability the previous one No known, this in a manner significant increase level security device software and systems used by the company.
2) Efficiency Cost: Within period long , bug bounty program can become more efficient in a manner financial compared to with recruit team internal security or depend on service company security external, this program utilise expertise and skills from number of participating security researchers without must give wages full or contract period long.
3) Enhancement Reputation : A capable successful bug bounty program find and overcome vulnerability with fast and precise can increase reputation company in matter safety and reliability. This can get up trust customers and users to product or service company.

Challenge in Bug Bounty Hunting

1) destruction in find Vulnerability: The process of hunting insects frequently need intensive effort and in - depth knowledge about the technology involved. security researchers face challenge in identify and exploit hidden vulnerabilities or complex.
2) Response and Coordination with the Company: Some security researchers face challenge in get proper response from company related report vulnerability. Slow coordination or not enough responsive can hinder resolution and completion vulnerability.
3) Study This give deep understanding about bug bounty hunting and giving proof real about success in find and reveal significant vulnerability. Research results This can give insights and recommendations for other companies that want launch a bug bounty program for increase security device soft them and protect user them.

DISCUSSION

Study This focus on bug bounty hunting as effective method in find and reveal vulnerability device soft (Wijayasekara et al., 2012). Through Study case about success in disclosure and disclosure vulnerability, various relevant aspects language.

Bug Bounty Hunt Effectiveness

Study This show that bug bounty hunting has been proven effective in find significant vulnerabilities in the device soft. Selected bug bounty program succeed find various type vulnerability, start from gap security on web applications up to device vulnerabilities hard . Success This show that bug bounty hunting can be complete method testing security traditional and up level security device soft in a manner whole.

Security Researcher Role

Security researchers play role central in success of the bug bounty program. Skill they In hunting insects, deep understanding about technology involved , and dedication they in find

vulnerability become factor key in reach positive results. Study This underline importance build good cooperation between companies and security researchers for reach optimal results .

Benefits of Bug Bounty Hunting

The bug bounty hunting program provides significant benefits for company . In period long, this program can envy costs that will issued For recruit team internal security or use service company security external. Besides it, through bug bounty hunting, company can increase security device soft them and fix previous vulnerability No detected, so minimize risk attacks and violations security.

Challenge in Bug Bounty Hunting

Study it also identifies a number of challenges faced on a bug bounty hunt. Challenge the covers difficulty in find hidden vulnerabilities or complex, as well effective coordination between security researchers and companies in overcome report vulnerability. Respond challenge This with the right way can fix bug bounty hunting process and ensure success in find vulnerability (Zhao et al., 2017).

Through discussion this, research This give deep insight about bug bounty hunting and its success in find and reveal vulnerability (Breidenbach et al., 2018). Discussion this is also underlined importance close cooperation between companies and security researchers, as well benefits that can obtained by the company through implementation program bug bounty.

CONCLUSION

This review bug bounty hunting as successful approach in find and reveal device vulnerabilities soft. Through Study case about bug bounty program success , conclusion who can taken. Proven bug bounty hunting program effective in find significant vulnerability. Through participation of expert security researchers, the program capable identify possible vulnerabilities No detected through method testing security traditional. Diversity The vulnerabilities found also show effectiveness approach This in catch various type gap security.

Security researcher plays role crucial in insect bounty hunting success. Skill they in insect hunting, understanding profound technology , and dedication they in find vulnerability become factor important in reach successful result. Good cooperation between companies and security researchers are key in create conducive environment For disclosure and disclosure vulnerability.

The implementation of the bug bounty program provides significant benefits for company. Besides increase security device easy , this program also can envy usual costs issued For recruit team internal security or use service company security external . Success in find vulnerability also contributes to reputation company in matter safety and reliability .

Bug bounty hunting is also facing a number of challenge , incl difficulty in find hidden vulnerabilities and coordination effective between security researchers and companies . For overcome challenge this company can strengthen cooperation with security researchers, providing channel good communication, and respond report vulnerability in a manner proactive. Overall, bug bounty hunting has proven as effective method in find and reveal device vulnerabilities soft . In context security continuous cyber developing , the bug bounty implementation program can be an efficient strategy for company For increase security and protect user them. Important for company For get up strong partnership with security researchers and ensure process disclosure responsive and effective vulnerabilities. With because of this, a bug bounty hunt is possible become element important in effort protect enterprise systems and data from potential attack harm.

REFERENCES

Alomar, N., Wijesekera, P., Qiu, E., & Egelman, S. (2020). " You've got your nice list of bugs,

now what?" vulnerability discovery and management processes in the wild. *Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security*, 319–339.

Breidenbach, L., Daian, P., Tramèr, F., & Juels, A. (2018). Enter the hydra: Towards principled bug bounties and exploit-resistant smart contracts. *27th {USENIX} Security Symposium ({USENIX} Security 18)*, 1335–1352.

Carlin, J. P. (2015). Detect, disrupt, deter: A whole-of-government approach to national security cyber threats. *Harv. Nat'l Sec. J.*, *7*, 391.

Chang, V., Kuo, Y.-H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. *Future Generation Computer Systems*, *57*, 24–41.

Lam, J. (2014). *Enterprise risk management: from incentives to controls*. John Wiley & Sons.

LaToza, T. D., & Van Der Hoek, A. (2015). Crowdsourcing in software engineering: Models, motivations, and challenges. *IEEE Software*, *33*(1), 74–80.

Maillart, T., Zhao, M., Grossklags, J., & Chuang, J. (2017). Given enough eyeballs, all bugs are shallow? Revisiting Eric Raymond with bug bounty programs. *Journal of Cybersecurity*, *3*(2), 81–90.

Moser, A., & Korstjens, I. (2018). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *European Journal of General Practice*, *24*(1), 9–18.

Mu, D., Cuevas, A., Yang, L., Hu, H., Xing, X., Mao, B., & Wang, G. (2018). Understanding the reproducibility of crowd-reported security vulnerabilities. *27th {USENIX} Security Symposium ({USENIX} Security 18)*, 919–936.

Ruohonen, J., & Allodi, L. (2018). A bug bounty perspective on the disclosure of web vulnerabilities. *ArXiv Preprint ArXiv:1805.09850*.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1–11.

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

Walshe, T., & Simpson, A. (2020). An empirical study of bug bounty programs. *2020 IEEE 2nd International Workshop on Intelligent Bug Fixing (IBF)*, 35–44.

Wijayasekara, D., Manic, M., Wright, J. L., & McQueen, M. (2012). Mining bug databases for unidentified software vulnerabilities. *2012 5th International Conference on Human System Interactions*, 89–96.

Zhao, M., Laszka, A., & Grossklags, J. (2017). Devising effective policies for bug-bounty platforms and security vulnerability discovery. *Journal of Information Policy*, *7*, 372–418.