A Systematic Study of Hunting Bugs

Shrey Sethi
FCA,
Manav Rachna International University,
Faridabad, Haryana, India
E-mail: shreysethi55@gmail.com

Sachin Sharma
FCA,
Manav Rachna International University,
Faridabad, Haryana, India
E-mail: sachin.fca@mriu.edu.in

Abstract: *Bug Bounty Program are designed to encourage security researcher, cyber security professionals or hackers to exploit Vulnerability in software or in web applications. Bug Bounty also helps developers to fix Vulnerabilities for which individual get rewarded on the basis of type of bug reported.*

Bug bounty program plays an important role in increasing the security of websites, web applications and softwares.

Keywords*: Bug Bounty, Vulnerability,Security, Exploits, Web Application, Crowdsourcing.*

I. INTRODUCTION

Now a day's Companies are fighting with each other when it comes to cybersecurity. In spite of everything of how powerful this will affect to their security; Big companies are always have been targeted by the thousands of malicious hackers worldwide. But the bug bounty program provides the platform to all the security researchers to compete among them self.

Bug Bounty Program also helps the companies to enhance their security as it is tested by different security professionals at the time of bug bounty program or hacker bounty program.

The Bug Bounty hunters are helpful hackers who expose and help to fix security vulnerabilities in some of the big and large software or web applications that uses the internet. These programs grant the permission to hackers or developer to locate and fix security bugs before the normal user is familiar with them. Bug bounty programs have been enforced by very big giant companies like Google, Adobe, Yahoo, Twitter and Uber. The reward is based on individuals for finding a what type security flaw is and how it will affect the users. Reward may offer a cash rewards, acknowledgement or any subscription to their product. Bug reports prerequisite suitable and proper information about the bug so that is comes in their bug bounty program will be able to recreate the vulnerability. Various IT companies offers these types of motivates or encourages incentives to improve and get more communication from end users or from clients. In this paper, we focus on proper and systematic study how bug hunters hunt bug in Bug Bounty Program [10]. Some of the related study are as follow:

Finifter [1] et al performed an empirical study to better understand two well-known vulnerability rewards programs, which software vendors use to encourage communityparticipation in finding and responsibly disclosing software vulnerabilities. Both programs appeareconomically efficient, comparing favourably to thecost of hiring full-time security researchers.

Laszka [2] et al developed an economic framework and investigate the strengths and weaknesses of existing canonical approaches for effectively incentivizing higher validation efforts by white hats. They also introduce a novel approach, which may improve efficiency by enabling different white hats to exert validation effort at their individually optimal levels.

Maillart[3] et al recognized that bug bounty programs create tensions, for organizations running them on the one hand, and for security researchers on the other hand. At the level of one bug bounty program, security researchers face Problems The probability of finding additional bugs decays fast, and thus can hardly be matched with a sufficient increase of monetary rewards. Their results inform on the technical and economic mechanisms underlying the dynamics of bug bounty program contributions, and may in turn help improve the mechanism design of bug bounty programs that get increasingly adopted by cybersecurity savvy organizations.

II. THE EVALUATIONOF BUG BOUNTY

Bug Bounty Programs are becoming more popular nowadays because it helps in enhancing the security of particular website or web application

However, it becomes popular approach of discovering security bugs on the internet. Google, Yahoo and Uber are the examples of the companies nowadays running Bug Bounty programs.

But how did it all begin?

In 1995 - Netscape launches first bug bounty after that in 2002 - I Defense - Middleman for bug bounties, 2004 - Mozilla Firefox Bug bounty so this list goes on and on. This figure represents the bug bounty program timeline. [6]

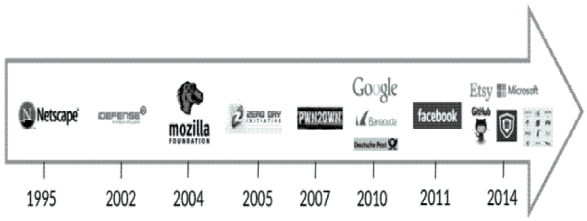

Fig.1: Evaluationof Bug Bounty Programs [4]

III. BUG BOUNTY PROGRAMS

Bug Bounties is also known as responsible disclose programmers are setup by the big companies to encourage people to report serious security flaw found on their web application or in software. This is the perfect way to review web application about their security. Bug bounty program is a deal provided by many websites by which a person can earn recognition and knowledgeable for reporting security bugs, those who exploits and find vulnerabilities. Bug bounty is an honor given for discovering and reporting a security flaw in a singular product. [9]

IV. MOST COMMON VULNERABILITIES FOUND IN WEB APPLICATIONS

- SQL Injection (Sqli)
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Components with Known Vulnerabilities (E.g. Heartbleed and Shellshock)
- Invalidated Redirects and Forwards [7]

V. WHY BUG BOUNTY HUNTER HUNTING BUGS?

- Bug Bounty Hunting Values Resume.
- Increase in the possibility of getting job in the Industry.
- Glory and Fame.
- Increase in the Knowledge.
- New releases are ready for test and also measure the skills of yours.
- Learn well- described test method's or Mechanisms.
- Use this as a new challenge to solve Problems.[12]

VI. MYTHS AND REALITY

Due to lack of available knowledge about how actual people find security related bugs in real-world systems which force to create myths about this industry.

MYTH: Only very brave, brilliant and people can find security flaws. Bug Hunters are the extraordinary persons in the information security world.

REALITY: You don't need have to be a brilliant to find a security flaws. The most crucial bug hunting element are the skills and to put prior experiences into practice and an eagerness to work for deep and lengthy hours, usually with no conclusion. To find bugs you have to quick and use some methodically, this helps to have huge security knowledge.

MYTH: Bug Hunting always an illegal and there is a destructive motivation behind the hunting for security bugs. Bug hunters are crackers and black hatted trying to find ways into our personal information and in networks.

REALITY: Security bugs are generally accidental, and the people who hunt bugs have mixed motivations. For example, looking for bugs in a web application is a great way for the users to assess the product's security flaws before buying it, or for testers to analyzers to

find weaknesses which are neglected in the development process. There are also individual bug bounty hunters who seek for fame or a delightful job.

MYTH: The person that finds a security flaws knows everything about the product and he also know how to exploit it.

REALITY: In general tester knows how exploit bug but this is not necessary that he knows everything about the product, security bugs are highlighted by the people who has the understanding exploiting the bugs. And he also knows why a bug exists, and how to fix it perfectly. This requires enough additional effort that does not undoubtedly relate to the bug-finding process.[8]

VII. ROLE OF BUG BOUNTY PROGRAMS

Bug bounty program plays a crucial role in providing the extra income to people as well as companies sure about the security related issues. There are numerous varieties of programs build by Big companies like. Facebook, Microsoft, Uber and Hacker One Which payouts made for vulnerabilities found in their products. Open source software like Perl, PHP, and Python also pays if someone find security flaws. A vulnerability in the GNU Bash Unix shell and the reward of $20,000 is given to Stéphane Chazelas for finding vulnerability, a Unix/ Linux and telecom professional detected the Shellshock vulnerability in September 2014. Google also started this program in 2010 rewarded the qualifying bugs between $100 to $20,000 based on the severity of the bug. And it's not just tech companies who are eagerly to start bug bounty program but there are a lot of companies like United Airlines also started bug bounty program and also gives an outstanding payout of a million air miles for a high priority bug. In India, well-funded startups have also started their bug bounty programs by giving a token or some reward. Indian Startups like Zomato has received till now over 55 reports on HackerOne. Ola's bounty program rewards a minimum of Rs.1000 for bugs discovered, but Ola doesn't comment on the maximum payout is. [11]

VIII. METHODOLOGY

In Fig 2 there is briefly discuss the steps involved in the process of Bug Bounty Hunting.

Fig. 2. Process of Bug Bounty Hunting

A. SELECTING THE TARGET

The first step in the process of Bug Bounty Hunting is Selecting the target in which we will evaluate and select our target. After selecting the target next step is to gather as much information as we can about our target because if we have a maximum information about our target we will come to know the parameters in which we have to work so it will give us better results which will directly motivate us so let's take an Example. of https://www.google.com First thing while hinting a bug is to what we are targeting like selecting sub-domains or different domains and different acquisitions and also check that their bug bounty program is valid on their acquisitions. After this check, what reward or bounty the company is giving. In image, there is a detailed information about google bug bounty program what google is offering for different bugs and also from its sensitivity.

Reward amounts

Rewards for qualifying bugs range from $100 to $20,000. The following table outlines the usual rewards chosen for the most common classes of bugs:

	accounts.google.com	Other highly sensitive services [1]	Normal Google applications	Non-integrated acquisitions and other lower priority sites [2]
Remote code execution	$20,000	$20,000	$20,000	$1,337 - $5,000
SQL injection or equivalent	$10,000	$10,000	$10,000	$1,337 - $5,000
Significant authentication bypass or information leak	$10,000	$7,500	$5,000	$500
Typical XSS	$7,500	$5,000	$3,133.7	$100
XSRF, XSSI and other common web flaws	$500 - $7,500	$500 - $5,000	$500 - $3,133.7	$100

[1] This category includes products such as Google Search (*https://www.google.com*), Google Wallet (*https://wallet.google.com*), Google Mail (*https://mail.google.com*), Google Code Hosting (*code.google.com*), Chrome Web Store (*https://chrome.google.com*), Google App Engine (*https://appengine.google.com*), Google Admin (*https://admin.google.com*), Google Developers Console (*https://console.developers.google.com*), and Google Play (*https://play.google.com*).

[2] Note that acquisitions qualify for a reward only after the initial six-month blackout period has elapsed.

Fig. 3: Sample image of Google Bug Bounty Hunting. [5]

B. Finding and Exploitingthe Bugs

- This process involves different Steps.
- Preparation.

- Foot printing.
- Enumeration & Fingerprinting.
- Identification of Vulnerabilities.
- Attack - Exploit the Vulnerabilities.

C. Preparation

- Identification of Targets - Company Websites, Mail Servers, Computer, Network etc.
- Specifics on Denial of Service Tests, Social Engineering, etc.
- Prior Knowledge of the systems.

D. Foot Printing

- Administrative Contacts.
- IP Range.
- DNS Servers.
- Collecting as much Information about the Target.
- Problems revealed by Administrators.

E. Enumeration & Fingerprinting

- Specific targets determined.
- Identification of Services / Open Ports.
- Operating System Enumeration.

F. Identification of Vulnerabilities

- Vulnerabilities.
- Insecure Configuration.
- Weak passwords.
- Unpatched vulnerabilities in services, Operating systems, applications.

I. Attack - Exploit the Vulnerabilities

- Obtain as much information from the Target Asset.
- Gaining Normal Access.
- Escalation of privileges.

J. Reporting

- Follow Proper Methodology of reporting a bug Exploited Conditions & Vulnerabilities that could not be Exploited.
- Proof for Exploits.
- Practical Security Solutions.

IX. CONCLUSION

In this paper, you have studied proper and systematic way how bug hunters hunt bug in Bug Bounty Program. If someone wants to participate in bug bounty program, follow these steps which we have written in this paper and follow simple steps to achieve your goal. Bug Bounties program performance very good for big companies to crosscheck their security. Overall objective of bug bounty program is to cut the costs and to identify defect and alsorepairs Bugs. These programs also help to maintenance software and cost effective. When new functions have been released you can found vulnerability. it also helps us to know the new ones and different Methods to find and exploit vulnerabilities. These programs help to increase your knowledge. Bug bounty programs are very favorable to Big companies because they boost hackers to report security vulnerabilities before they're exploited by the bad guys. Small organizations are started benefit from these programs. Companies such as Bugcrowd, Hackerone, Bugwolf, Hatforce ,CrowdSecurify are set up and running bug bounty programs on side of customers, they are accepting bug submitting and validating them, as well as Doing the payouts when needed. Enterprise-sponsored bug bounties to grow in reputation.

REFERENCES

[1] http://devd.me/papers/vrp-paper.pdf

[2] http://aronlaszka.com/papers/laszka2016banishing.pdf

[3] https://arxiv.org/pdf/1608.03445.pdf

[4] https://cobalt.io/blog/the-history-of-bug-bounty-programs/

[5] https://www.google.co.in/about/appsecurity/reward-program/

[6] https://blog.cobalt.io/the-history-of-bug-bounty-programs-50def4dcaab3#.2m4wefkop

[7] https://www.owasp.org/index.php/Top_10_2013-Top_10

[8] http://whatis.techtarget.com/definition/bug-bounty-program

[9] https://en.wikipedia.org/wiki/Bug_bounty_program

[10] https://www.tripwire.com/state-of-security/vulnerability-management/11-essential-bug-bounty-programs-of-2015/

[11] https://www.quora.com/How-does-one-become-a-bug-bounty-hunter

[12] AUSTIN, A., AND WILLIAMS, L. One technique is not enough: A comparison of vulnerability discovery techniques. In Empirical Software Engineering and Measurement (ESEM), 2011 International Symposium on (2011), IEEE, pp. 97-106.

[13] CATAL, C., AND DIRI, B. A systematic review of software fault prediction studies. Expert Systems with Applications 36, 4 (2009), 7346-7354.

[14] EDMUNDSON, A., HOLTKAMP, B., RIVERA, E., FINIFTER, M.,METTLER, A., AND WAGNER, D. An Empirical Study on the Effectiveness of Security Code Review. In Proceedings of the International Symposium on Engineering Secure Software and Systems (March 2013).

[15] SCHOLTE, T., BALZAROTTI, D.,AND KIRDA, E.Quovadis a study of the evolution of input validation vulnerabilities in web applications. Financial Cryptography and Data Security (2012),284-298

❒