**Title: Hunt Bugs, Earn Bucks, Save the World**

**Author:** Sartaj Jamal Chowdhury

A bug bounty is a reward given off to an extremely tech-savvy person or a security research group who helps detect and mitigate a bug or a set of shortcomings in a cyber product or service of a company. Most certainly, the bug bounty hunter has to perform a set of aggressive operations on the technology to succeed. Hence, it is imperative that the users or the said company is not harmed as a result of such bold measures. Therefore to ensure safety, there are a set of rules and scopes set by the organization which the bug hunter has to abide.

A scope is a domain defined by the owner of the software. Meta can be an example, with all their miscellaneous applications, websites and services (Such as, Facebook, Instagram, etc.). Not all of these components owned by Meta fall within the scope where a bug hunter is allowed to poke around. However, a lot of them are, and that creates a sweet opportunity for hackers to legally and ethically test their mysterious mastery out. On the other side, if the curious minds do end up entrapping any malicious bug or threat, that sure is a giant win for the company and may even save them a big fortune someday.



**What is a bug bounty program and who is a bug bounty hunter?**

In the ever so evolving world of technology, the various ways malicious hackers exploit cyber systems (often technically termed as attack vectors or threat landscapes) are also drastically developing. As a result, at times it is difficult for even the biggest tech based enterprises to stay ahead of the cyber criminals out there all by themselves. Henceforth, these organisations may decide to delegate their information security tasks by initiating an open-source approach. A call for support from white-hat hackers all around the globe, to help strengthen the security aspects of a tech firm, is known as a bug bounty program or incentivised vulnerability disclosure.

Due to it’s open source nature a bug bounty hunter can be anyone who is learning the science or art of ethical hacking. To be more specific it can be anyone of us, who is curious enough to try. Companies do not mind who you are, as long as you are above a certain age you are good to go hunting. However, in order to make a significant contribution one has to be equipped with some specific skillset, tools and experience.

**Is it a popular practice in Bangladesh?**

A lot of bug bounty hunters, according to a recent data analysis by Bugcrowd (one of the largest bug bounty and vulnerability disclosure platforms on the internet) are from India, USA, Pakistan, Bangladesh, and Indonesia. It is also a great opportunity for bug hunters from developing countries to collect more and more bounties and get their pockets heavy while contributing in the growth of their nation’s economy.

Even though Bangladesh being a rising home for a plethora of tech giants, the number of these companies who have a bug bounty program are very scarce. Two notable tech societies are iPay and Pathao, who have official bug bounty programs.

**Lastly, how does it work? Where to get started?**

We must learn to walk before we run. Ergo, getting familiar with the fundamentals of cybersecurity methodologies, related tools and regular practice through participation in “Catch The Flag”, “Hack The Box”, etc. can be a good start. Next step is to learn about a company’s bug bounty scope. Then picking up a certain product from that perimeter depends on an individual’s interest and skillset. If the bug hunters are able to make any decent discovery, they will have to prepare a bug bounty report and submit it to the company who will analyze it and respond after a certain time. Lastly, if the company concludes that the vulnerability or bug discovered is worth a reward, according to their policies, they will lead the bug hunter through the payment procedures.

**Let’s put an end to cyber crimes, shall we?**

Tech societies across the world are more increasingly trying to foster a community of companies and individuals who consider security as their foremost concern. This can ensure that the ever more increasing users of technology can feel safer in the cyber environment and also the companies can grow bigger, better, faster and stronger. Moreover, it is also a great opportunity for IT security practitioners to acquire real world experience and even make a living while being self-employed. Needless to say even students can indulge into this exciting adventure as a side-quest. Such incentivised programs may also attract malicious hackers into a brighter path, since it comes with the same kind of thrill, but also provides with handsome reward, dignity and the opportunity to make the virtual world a better place.