Chapter 7
Data Leakage and Privacy Concerns in Public Bug Bounty Platforms

Muhammad Hamad
Institute of Space Technology, Islamabad, Pakistan

Altaf Hussain
Institute of Space Technology, Islamabad, Pakistan

Majida Khan Tareen
Institute of Space Technology, Islamabad, Pakistan

ABSTRACT

For long-term relationships, the websites of various businesses store the PII and PHI of customers, which are mainly targeted by hackers. Cyber breaches mainly result in lack of customer trust and downfall of the business reputation. As a result, the customers become reluctant to share PII and PHI with online businesses until provided with the protection of sensitive data. The online resources of a business need to be in compliance with GDPR and PCI DSS. Companies undergo penetration testing of the infrastructure; for this, paid white hat hackers are hired under a legal contract. The companies also adopt RVDP program, where the Bug Bounty Platforms is one of the variants of RVDP. Security researchers are rewarded with an amount of bounty in the form of money or name in the hall of fame at official website for bugs' identification. Ideally, the security researcher would perform cyber security assessment. The vulnerabilities would be reported to intended stakeholders and the remediation measures with great deal of care so that PII and PHI won't be exploited by anyone.

DOI: 10.4018/978-1-6684-6914-9.ch007

INTRODUCTION

The computer is one of history's biggest inventions and has a huge impact on our lives. Computers are found to be excellent at performing computing tasks at a speed unmatchable by human beings. These computing devices made their way to each and every sector and reduced the human workload. After the advent of the Internet, the world became a global village and introduced the sense of being connected among people no matter in which geographical regions they live in. So broadly speaking, computers are a set of electronic circuits, along with software which defines how this hardware will operate and for communicating with other devices of same nature, it has an additional component for network establishment.

This paradigm shift opened new channels of collaboration and coexistence. The people from far apart regions became friends using social networking sites, researchers started working together on problems of mutual interest, and businessmen started trading on e-commerce sites.

So, for every other internet-connected task, a specific kind of software was required and then was created by IT Personnel. In the software requirement engineering process, both functional and nonfunctional requirements are discussed by stakeholders. The functional requirements are the core features of software for which it is about to get designed. Functional requirements clearly mention what kind of inputs the software should be capable of receiving, what processing it should perform on input data and what resultant output is required to be displayed. In contrast to this, non-functional requirements are mostly quality related things like user-experience, scalability, compatibility and security.

Like any other assets, this software is owned by some specific people e.g., Amazon multinational e-commerce company is owned by Jeffrey Preston Bezos and Facebook, a famous social media platform is owned by Mark Elliot Zuckerberg. According to a recent survey, there are 2.93 billion active Facebook users per month. Facebook has a huge database of private data associated with these 2.93 billion people. On the same lines Amazon, PayPal or any other Fintech company plays with lot of financial data of normal users. People now a days are very concerned about how the owner of respective software would manage, store, transmit and secure their critical/sensitive data. So, in the recent past, this concern of people has shifted security from non-functional requirement to functional requirement.

But there is a very peculiar difference between functional requirements (FR) and non-functional requirements (NFR), which is, that the explanation of FR is explicit and once the software is developed it is easy for client to assess if the objectives were truly met. In case of NFR, the extent to which certain requirements are fulfilled varies from person to person and there are no absolute criteria of quantification e.g., if the quality assessment of application is to be performed by multiple different persons at same time and their test case is to grade the usability of application, it seems definite that their grades won't match. The point here is to establish an idea that although security or cyber security switched from NFR to FR, still there is nothing like ultimate security and if someone has access to unlimited space and time every system ought to be breakable. So for better security assessment let's dissect the concept of information and cyber security and its 3 pillars.

Information Security Vs Cyber Security

Information security and cybersecurity are related but distinct concepts. Information security refers to the practice of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. It focuses on safeguarding the confidentiality, integrity, and availability of information, whether in digital or non-digital form. Cybersecurity, on the other hand, is