PENTEST VS BUG BOUNTY

by Esteban Echandia*

*Pentester in Open-Sec, certified as eMAPT, and eJPT, he has experience on infrastructure tests and mobile applications. (https://www.linkedin.com/in/estebanechandia/)

In today 's digital era, information and data security is more important than ever. Companies of all sizes and fields face security threatness even more sophisticated than before, as you could have seen on previous publications we made and on the fresh & daily news. These all means that the safety of your systems, networks and applications, must be an absolute priority. Therefore, two techniques that we can use in order to identify vulnerabilities on systems and applications are: **Pentesting** and **Bug Bounty.**

The main objective of the pentesting is to identify the vulnerabilities and weaknesses of a system, network or application through a controlled attack simulation, in order to evaluate the effectiveness of the existing security measures and recommend improvements.

The pentesters, who are security experts, are used to work in a structured and methodological way (in Open-Sec we have a Framework that can be found on our GitHub), providing one detailed inform of the identified vulnerabilities. When we hire a pentesting service, we also acquire one complete evaluation of the system and we have the guarantee that they were tested against various attacks, the pentesters are also trained to look beyond the common vulnerabilities and search for more complex ones. In addition to identifying vulnerabilities, one experienced team of pentesters will also provide some practical recommendations to solve the detected problems, which can help to improve the security of the company in a more effective way.

On the other hand, the main goal of a bug bounty program is to reward the external security investigators (or *Bug Hunters*) for identifying vulnerabilities in the company 's systems. Unlike pentesters, the bug bounty investigators are not limited by a specific range and they can search for vulnerabilities in any part of the system that is in disposition of the program. Oftentimes, the bug bounty programs have wider focus and it is less structured than the pentesting, so there is no guarantee that the system has been tested.

If a bug bounty program is launched without previously performing a thorough security evaluation, we can receive a big quantity of vulnerability reports that could have been solved in a previous stage of the system development life cycle (SDLC in short). Instead of discovering these vulnerabilities before the system implementation, the bug bounty program will find them in the production stage, where the application is already exposed to an external malicious attacker.

At the same time, the reports generated from a bug bounty program results in a significant charge for the security team of the company. These reports can include a wide variety of vulnerabilities that many times require a detailed evaluation done by security experts to determine their impact and how to solve them.

Another disadvantage of trusting on a bug bounty program without realizing a pentesting before, is that the security investigators may not provide practical recommendations to correct the identified problems. On the other side, one pentesting report usually includes detailed recommendations to solve the scoped vulnerabilities, making the correction process easier and results in a more secure system.

It is always recommended to realize one pentest before launching any application or a new functionality to a bug bounty program. This will allow a complete evaluation of the security of the system, enabling the correction of problems before these are reported by the external

investigators. This will not only help to reduce the cost and workload associated with a bug bounty program, but also ensure that the system will be more secure and reliable for users and customers.

In conclusion, pentesting and bug bounty are two security techniques that complement each other utilized to identify vulnerabilities on systems and applications, but the bug bounty will not replace the pentesting when we talk about a whole complete security evaluation of a system. While bug bounty programs can help to identify vulnerabilities in a production stage, they do not guarantee that the evaluation has been done in a complete way in every aspect of the system.

Therefore, it is highly recommended to realize one pentesting before launching any system or application to a bug bounty program. This will ensure that all the important vulnerabilities have been identified and fixed beforehand.