CHAPTER I INTRODUCTION

I.1 Background

Technological developments have occurred throughout the world rapidly, all countries are competing for the technological advancement of their own countries and as a competitive arena with other countries. As time goes by, technology has developed to become more sophisticated. It can help in every aspect of daily life, both in industry and household activities. Technological development has a lot of benefits there is for transportation, communication, education, etc.

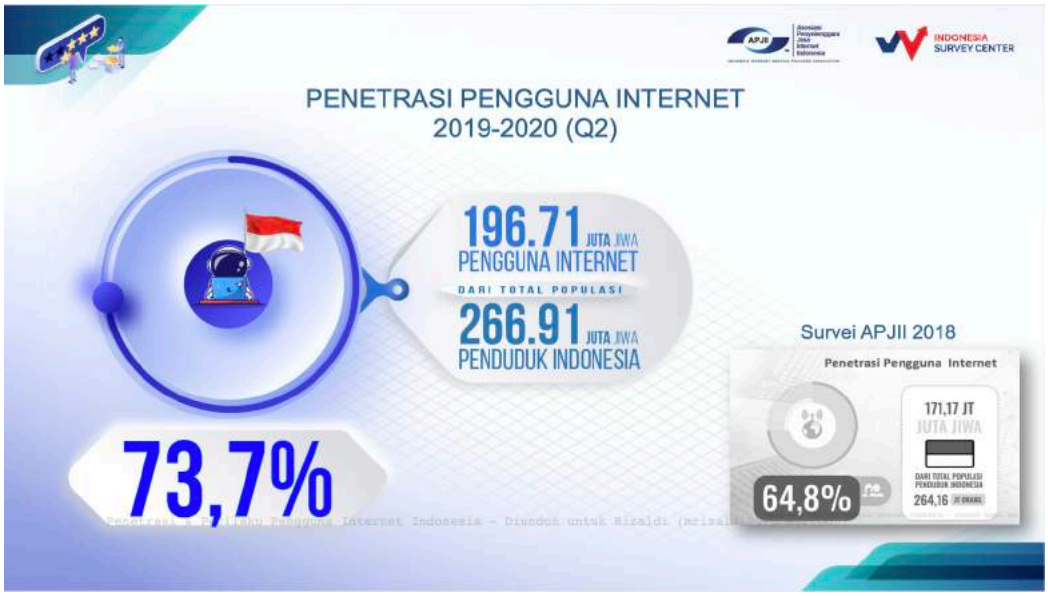

Figure I.1. Number of Users Internet in Indonesia (APJII, 2020)

Based on the survey conduct by *Asosiasi Penyelenggara Jasa Internet Indonesia* (APJII). The user internet in Indonesia is 196.71 million people from the total population of 266.91 million people or 73.7 % of people in Indonesia using the Internet. The number of users of the Internet in Indonesia is increased year by year. In 2018 the number of users of the internet in Indonesia is 64.8 % or 171.17 million and in 2019-2020 the number of users is increased to be 73.7 % or 196.71 million people. (APJII, 2020).

Besides the rapid development of internet users in Indonesia, there is a party that abuses the moment. They try to find the vulnerabilities of applications and exploit them. The example of the vulnerabilities that can be utilized by the hacker is SQL

Injection, Cross-Site Scripting (XSS), Security miss-configuration, etc (OWASP, 2017). To prevent the application from attackers, the application needs to implement hardening. Hardening is a technique that has a function to reduce the risk that causes by vulnerabilities. While eliminating the vulnerabilities the attackers or malicious software will have fewer opportunities to attack the application.

XYZ web application is a website that integrates the lab assistant recruitment process. The purpose of this website is to collect files from prospective assistants and then determine whether or not the participants who take part will pass the recruitment. Unfortunately, this website is not implementing hardening yet.

One way to strengthen an application is to do a system test where the results of this system test can be seen whether the website has any vulnerabilities. So that it can be minimized by closing the vulnerabilities that have been founded.

In this research, hardening was carried out based on the OWASP Web Security Testing Guide (WSTG). Open Web Application Security Project or known as OWASP is a free and open community focused on improving the security of the application (OWASP, 2014). This research was conducted in 5 stages, namely problem statement, planning, simulation, analysis, and the final stage. This research was conducted using the application contained in Kali Linux.

I.2 Problem Statement

Based on the background of the problems previously described, we can get the formulation of the problem in this research are:

1. What is the vulnerability in XYZ web applications?
2. How to strengthen the XYZ web application so that irresponsible parties do not easily hack it?

I.3 Research Objectives

Based on the problem statement above, we get the objectives of this research are:

1. What are the vulnerabilities in the application.
2. The recommendation is that can close the vulnerabilities in the application.

I.4 Research Scopes

1. The operating system that is used to analyze the vulnerabilities is Kali Linux.
2. Do not attempt to penetrate the firewall of the hosting server.
3. The server used is a hosting server.
4. Use 3 technique information gathering, data validation testing, and client side testing.

I.5 Research Benefits

The benefit that can be obtained in this research are :

1. For Institution

   From the result of research that has been conducted, the Institution will get benefits from a secure web application.
2. For User

   The benefit obtains by the user is the creation of a sense of security from data theft.
3. For Researcher

   This research can add insight to the researcher, and the researcher can implement the knowledge obtained and learned from lectures.