ABSTRACT

The internet is one of the needs that will never be separated from people's lives today. The internet has become a medium used by people to communicate, search for data or information, channel creativity, support economic and business activities, and much more. When people access the internet, one of the elements of the internet that will always be accessed is a website. Any information provided on the internet from any source will have its own website which the owner has created to display the required information or data. The XYZ Health Foundation is no exception, which has a website so that it can easily provide information and data that can be known by the general public. With the high use of internet access and websites, security threats to the integrity and confidentiality of information and resources on websites are a big problem. Vulnerability and security testing can prevent cyber incidents from occurring on related websites. The tests carried out in this study used the black box testing method and the NIST SP 800 - 115 standard. Vulnerability analysis was carried out using several tools such as Zenmap, OWASP ZAP, and Burp Suite. From the vulnerability analysis, it was found that on the XYZ Health Foundation website there are 12 vulnerabilities consisting of 4 vulnerabilities with a medium risk level, 6 vulnerabilities with a low risk level, and 2 vulnerabilities with a risk informational level. At the stage of testing the vulnerability with Burp Clickbandit, it produces information about the potential for a ClickJacking attack. After testing and analysis, recommendations are made that can be used as a reference to make the XYZ Health Foundation website safer.

Keywords: *website, vulnerability analysis, security*, NIST SP 800 – 115.