ABSTRACT

The development of the Internet in information technology is growing rapidly along with the growth of its users. Similarly, the crime rate in information technology is dangerous for both individual users and organizations. Based on data from the Directorate of Cyber Crime (Dittipidsiber) of the Criminal Investigation Unit of the Indonesian National Police, the Police received 2,259 reports of cybercrime cases from January to September 2020. It was recorded that reports on the spread of provocative content were the most widely reported, with 1,048 cases. In addition, the public also reports other cyber crimes such as online fraud, pornography, illegal access, data manipulation, data/identity theft, and so on. The XYZ website itself has experienced hacking attempts by several spam accounts which have an impact on both users and the XYZ website, besides that the XYZ website itself has repeated incidents of 1 to 2 cases in a span of 1 to 2 months. To anticipate these threats, a Vulnerability Assessment is carried out to identify, measure, and prioritize system vulnerabilities. In this case, we use the VAPT framework and Nessus tools to carry out a vulnerability assessment and analyze the vulnerabilities found on the PT. XYZ. Based on the results of the vulnerability assessment test on the XYZ website, there are 9 vulnerabilities found on the PT XYZ website, these vulnerabilities are 6 vulnerabilities that have a medium category, and 3 vulnerabilities that have a low category. In the medium category, there are 2 clickjacking vulnerabilities and 4 missing HSTS vulnerabilities, then in the low category there are 3 vulnerabilities in the form of Web Server Allows Password Auto-Completion where the password field will be filled automatically if previously logged in.

Keywords: Vulnerability Assessment, Cyber Crime, Nessus, VAPT Framework