ABSTRACT

Determining vulnerabilities and determining risk level in Docker tha has vulnerabilities will be a discussion. To obtain vulnerability data and also identify exploits from attackers, a vulnerability scanner is used, namely Aquasec and for exploitation a simulation is carried out in carrying out the exploitation. Aquasec detecred a vulnerability in Docker assets. Data from Aquasec is ananlyzed to obtain risk results which are closely related to vulnerability and exploitation. The results of the analysis between vulnerabilities and exploits, produce risks that are categorized in attacks according to the STRIDE framework. The results that have been given, provide risk with Medium level vulnerabilities and often occur in exploitative vulnerabilities. The amount of risk obtained is 32.5 against vulnerabilities in Docker. The risk is an attack in the form of information disclosure. This requires dealing with the risks that often occur during the exploitation of various walkthroughs. It would be better if the research on Docker was broader by looking at various aspects of Docker.

*Keywords**:** Docker, STRIDE, Vulnerability, Risk, Aquasec*