ABSTRACT

CLOUDFRI HARDENING WITH SECURITY HARDENING METHOD ON SAP.CLOUDFRI.ID WEBSITE

By

MUHAMMAD RIFKI OKTOVA

NIM: 1202174074

Hardening is an attempt to reduce security risks by eliminating potential attacks and strengthening the attack surface of the system. This study aims to identify vulnerabilities that exist on the sap.cloudfri.id website which is then carried out with a hardening procedure to minimize threats to the website. By using the security hardening method, vulnerability scanning and exploit testing is also carried out.Tests are carried out to find vulnerabilities found on the sap.cloudfri.id website as research objects and take advantage of the analysis results from vulnerability scanning to exploit objects. The vulnerability scanning tools used include Nmap, Nessus, Vega, and Nikto which produce analysis results for exploits to be carried out which aim to confirm that the website has a vulnerability described by the scanning tools. This exploit also refers to the OWASP Top 10 about the most critical security risks for a website that has become the standard for website development. To perform the exploitation in this research, tools are used, namely Metasploit Framework, SQLMap, and BurpSuite. The results of the analysis of the results of the vulnerability and the results of website exploitation can receive attacks in the form of Session Hijacking, Man-in-the-Middle, and DoS attacks.

Keywords— Hardening, Vulnerability Scanning, Exploit