ABSTRACT

CLOUDFRI HARDENING WITH SECURITY HARDENING METHOD ON *WEBSITE*-BASED APPLICATION TAP2GO.CLOUDFRI.ID

By

RIFQI ZAIN NAUFAL

1202170272

Hardening is a method to minimize security holes in the system, and this method can be done in various systems. With the rapid development of technology at this time, criminals can exploit security gaps in a system. This study aims to find out how high the level of security and security gaps are contained in the tap2go.cloudfri website-based application and then determine what recommendations should be made in hardening and minimizing security gaps with the security hardening method carried out to the remediate stage. In this study, simulations were carried out, namely vulnerability scanning and penetration testing with OWASP as a guide in selecting vulnerability scanning tools and in performing penetration testing. The results of this study are analysis of vulnerability scanning and penetration testing. The vulnerabilities identified were vulnerability to DoS attacks, unencrypted communications, and outdated use of SSL/TLS. Penetration testing carried out is a simulation of SQL injection, DoS, Session hijacking, and Interception attacks. The results of the penetration testing found that the system was safe from SQL injection attacks because there was already a firewall to withstand these attacks. On the other hand, for other types of attacks, the system was not secure and needed to be reconfigured on the webserver to minimize the security holes in the tap2go.cloudfri website-based application.

Keywords: Hardening, Vulnerability Scanning, Penetration testing, OWASP