ABSTRACT

CLOSING SECURITY VOCATIONS USING THE HARDENING METHOD

(CASE STUDY: CLOUDFRI)

BY:

MUHAMMAD FARIZQI SETIAWAN

1202170314

Security Hardening is a method aimed at increasing the security of a system so that a system is not easily exploited or attacked by irresponsible parties. This study aims to identify vulnerabilities that exist in the tap2go.cloudfri website-based application as well as analyze and perform hardening procedures on the website. This study uses the Security Hardening method as a research guide. When using the security hardening method, vulnerability scanning and penetration testing are also carried out. The results of this study are analysis of vulnerability scanning and penetration testing. The vulnerabilities found were vulnerability to DDoS attacks, unencrypted communications, non-installation of Anti-ClickJacking and outdated use of SSL/TLS. Penetration testing carried out is a simulation of DDos, Drupalgeddon, Interception and SQL Injection 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 web server to minimize security holes in the tap2go.cloudfri website-based application.

Keywords: *Security Hardening, vulnerability, Penetration Testing.*