ABSTRACT

WordPress is the world's most popular Content Management System (CMS) for creating and managing websites or blogs. With the popularity of this CMS, WordPress has also become a target for hackers to find security holes and launch exploits that certainly have an impact on WordPress users. This research aims to design a security control priority on WordPress from the exploits tested, especially those related to the network. The exploits that are carried out are exploitation of XML-RPC with Brute Force, DDoS, Packet Sniffing, Packet Data Manipulation, and Session Hijacking with the main target of exploitation is WordPress. The results of the exploitation will be analyzed using the threat approach to data security consisting of Disclosure, Alteration, and Denial and based on the OWASP Top Ten issued by OWASP. Then, each exploit will be evaluated for the severity of its vulnerability based on the category obtained from the CVSS score and recommend a security mechanism. The result of this research is a security control design based on OWASP standards for mitigation priorities against vulnerabilities exploited by threats in the WordPress CMS with the first priority order being Packet Sniffing exploits that fall into the Cryptographic Failures category with a severity level of High, the threat type is Disclosure, and the security mechanisms applied can be in the form of using SSL/TLS certificates on WordPress servers, Force HTTPS, and HTTP Strict Transport Security (HSTS). Meanwhile, the last place is filled by DDoS exploits covered by the Security Logging and Monitoring Failures category with a severity level of High, the threat type is Denial, and the security mechanisms that can be applied are the use of Web Application Firewall (WAF) and installing security plugins in WordPress. Future research can be in the form of adding variations in the type of exploitation or further analysis of the resources used during the exploitation process.

Keywords: Control Design, Exploitation, WordPress, Network