ABSTRACT

The number of global data leaks in the third quarter of 2022 reached 72.45 million accounts, with Indonesia ranking third. One of the main causes is weak website security, including government sites. The X District Court website is the object of research to identify vulnerabilities and improve its security using the Penetration Testing Execution Standard (PTES) method. This topic is important because many government sites are prone to cyber attacks, such as Distributed Denial of Service (DDoS) and Clickjacking. The current condition shows that although some sites have been protected by firewalls, many other vulnerabilities such as unregulated security headers or CMS themes are vulnerable to exploitation. The solution implemented includes six stages of PTES: data collection, threat modeling, vulnerability analysis, exploitation, post-exploitation, and reporting. Research was conducted using tools such as OWASP ZAP, WPScan, and SQL Map. The main results show that only the Clickjacking attack was successfully exploited, while the other four attacks XSS, SQL Injection, Brute Force, and DDoS have not managed to exploit the website due to firewall protection. The contribution of this research is to know the security system of the website and provide recommendations for improvements, such as adding X-Frame-Options headers and Traffic Filtering methods, to improve the security of government websites.

Keywords: System security, Penetration Testing, PTES, Website