ABSTRACT

SECURITY ANALYSIS OF XYZ BOARDING SCHOOL FOUNDATION WEBSITE USING OWASP WEB SECURITY TESTING GUIDE

By
M. Ato' ulloh
21102165

With the rapid development of digital technology, websites have become one of the main platforms for information management, including for educational institutions such as the XYZ Pondok Foundation. Although it offers many conveniences, the use of this technology also poses growing cybersecurity threats. Website security is of utmost importance, as the site stores sensitive information such as personal data, educational data, and financial information of students. Threats such as Cross-Site Scripting (XSS), SQL Injection, Brute Force, Clickjacking, and Distributed Denial of Service (DDoS) attacks can compromise the integrity and confidentiality of such data. This study aims to analyze the information system security of the website owned by the XYZ Boarding School Foundation. The method used in this study is Penetration Testing based on the OWASP Web Security Testing Guide to detect and evaluate potential vulnerabilities. The testing was conducted using various security testing tools, such as OWASP ZAP, SQLMap, WPScan, Burp Suite, and LOIC to simulate several types of attacks, including Cross-Site Scripting (XSS), Clickjacking, SQL Injection, Brute Force, and Distributed Denial of Service (DDoS). The results of the study showed that the website was vulnerable to several types of attacks, such as Clickjacking and DDoS, with successful Clickjacking and DDoS attacks. However, the website was not successfully exploited in Reflected XSS, SQL Injection, and Brute Force attacks. The vulnerabilities were found in suboptimal server configurations, such as the absence of X-Frame-Options settings to protect against Clickjacking and the website's inability to handle DDoS attacks. Recommendations for addressing the vulnerabilities include adding X-Frame-Options to HTTP responses, implementing Content Security Policy (CSP), using a Web Application Firewall (WAF) to protect against DDoS attacks, and regularly updating WordPress themes and plugins to address vulnerabilities in the themes used. The partner of the Pondok XYZ Foundation has evaluated the research findings and accepted the recommendations for improvement. They are committed to adding the X-Frame-Options header and considering the implementation of Content Security Policy (CSP). To address the DDoS threat, the partner is implementing a Web Application Firewall (WAF), but for now has implemented traffic filtering on the router. The partner also plans to update WordPress themes and plugins and schedule regular system maintenance to prevent vulnerabilities.

Keywords: Website Security, OWASP, Penetration Testing, Boarding School