ABSTRACT

As information technology grows rapidly, it can provide positive things in the dissemination of information. The website is one of the results of the development of information technology as a medium for conveying information. XYZ as an education transformation partner has a website that contains sensitive data such as bootcamp class package purchase data, but penetration testing has never been carried out to improve the security of its system. This study uses the OWASP Top – 10 2021 framework with the black box testing method to conduct penetration testing on the XYZ website. Testing is conducted to identify potential security vulnerabilities that may be exploited by irresponsible parties. The test results found several significant vulnerabilities such as problems with user agent fuzzer, improper input validation, information disclosure, vulnerabilities related to security headers, plugins and themes that need to be updated, brute force and user enumeration risks, and insufficient logging. Recommendations for improvement include the implementation of input validation, proper security headers, anti-CSRF mechanisms, improvements to cookie configurations, plugin and theme updates, implementation of rate limiting and CAPTCHA, and improved logging and monitoring systems.

Keywords— ***Kali Linux, Cybercrime, Penetration Testing, Website***