ABSTRACT

The development of information technology has become a necessity in improving the efficiency of an organization's performance, especially security, which is a key aspect that needs to be considered in the development of the XYZ website as the main gateway for prospective new students to register and access information related to new student activities such as test schedules, registration, filling out personal data forms, selection schedules, and other activities. With the increasing number of applicants accessing the website, the potential for security vulnerabilities also rises. XYZ has received reports that the XYZ website remains vulnerable to phishing attacks. This poses a serious threat that could undermine users' trust in the credibility of XYZ University. As the number of prospective students applying continues to grow, system security must be given special attention as a preventive measure against potential vulnerabilities. In this study, penetration testing was conducted using the Information System Security Assessment Framework (ISSAF) approach. The results of the penetration testing found that the XYZ website had a Local File Inclusion security vulnerability through path traversal, as well as 16 vulnerabilities with 4 medium, 8 low, and 4 informational levels. The priority for remediation will focus on the Local File Inclusion vulnerability, with the implementation of a whitelist, restricting access to directories such as /etc, ssh/, and home, and deploying a WAF like Apache ModSecurity. This aims to maintain public trust in XYZ University and protect the website from future attacks.

Keywords: *Information System Security, Penetration Testing, Website, ISSAF*