INTISARI

Studi ini melaksanakan analisis keamanan terhadap situs web *Computer-Based Test (CBT)* di SMK Darussalam Karangpucung dengan menerapkan metode *penetration testing* berbasis *Information System Security Assessment Framework (ISSAF).* Studi ini bertujuan untuk mengevaluasi tingkat kerentanan sistem CBT dalam mengelola data ujian, informasi peserta didik, serta hasil ujian yang bersifat sensitif. Analisis dilakukan dengan mengidentifikasi potensi celah keamanan, termasuk absennya implementasi *header* keamanan yang esensial, penggunaan pustaka *JavaScript* yang telah usang, serta eksposur file tersembunyi yang tidak terlindungi. Pengujian juga mencakup evaluasi risiko serangan *Cross-Site Scripting (XSS), Distributed Denial of Service (DDoS),* dan *clickjacking* guna menilai ketahanan sistem terhadap ancaman siber.

Hasil analisis menunjukkan bahwa sistem masih memiliki beberapa kelemahan yang berpotensi dieksploitasi, antara lain kurangnya mekanisme perlindungan terhadap serangan *clickjacking* serta penggunaan pustaka *JavaScript* yang rentan terhadap eksploitasi. Kendati demikian, sistem terbukti memiliki ketahanan terhadap serangan DDoS serta menerapkan perlindungan yang cukup efektif terhadap serangan XSS melalui kebijakan keamanan konten. Penggunaan alat uji seperti *ZAP, Nmap*, dan *WhatWeb* memungkinkan identifikasi kelemahan sistem secara menyeluruh guna mendukung proses evaluasi keamanan yang lebih komprehensif.

Sebagai tindak lanjut, kajian ini merekomendasikan penerapan *Content Security Policy (CSP),* pengamanan terhadap file sensitif, pembaruan pustaka *JavaScript* yang memiliki potensi risiko keamanan, serta penguatan perlindungan terhadap serangan *clickjacking*. Temuan dalam studi ini diharapkan dapat berkontribusi dalam peningkatan keamanan situs web pendidikan serta meningkatkan kesadaran akan pentingnya keamanan siber di lingkungan akademik.
.

Kata kunci: *Penetration Testing, ISSAF, Cross-Site Scripting, Distributed Denial of Service,* keamanan *website*.

ABSTRACT

This study conducts a security analysis of the Computer-Based Test (CBT) website at SMK Darussalam Karangpucung by applying the penetration testing method based on the Information System Security Assessment Framework (ISSAF). This study aims to evaluate the vulnerabilities of the CBT system in managing exam data, student information, and sensitive test results. The analysis identifies potential security weaknesses, including the absence of essential security headers, the use of outdated JavaScript libraries, and the exposure of unprotected hidden files. The testing also includes an evaluation of the risks of Cross-Site Scripting (XSS), Distributed Denial of Service (DDoS), and clickjacking attacks to assess the system's resilience against cyber threats.

The analysis results indicate that the system still has several vulnerabilities that could be exploited, such as the lack of protection against clickjacking attacks and the use of JavaScript libraries that are susceptible to exploitation. Nevertheless, the system has demonstrated resilience against DDoS attacks and has implemented effective protection against XSS attacks through content security policies. The use of testing tools such as ZAP, Nmap, and WhatWeb facilitates a comprehensive identification of system weaknesses, supporting a more thorough security evaluation process.

As a follow-up, this study recommends the implementation of a Content Security Policy (CSP), protection of sensitive files, updating vulnerable JavaScript libraries, and strengthening protection against clickjacking attacks. The findings of this study are expected to contribute to enhancing the security of educational websites and raising awareness of cybersecurity in academic environments.

Keywords: Penetration Testing, ISSAF, Cross-Site Scripting, Distributed Denial of Service, website security.