INTISARI

Perkembangan internet dan layanan online yang pesat meningkatkan risiko keamanan data, terutama pada sistem informasi berbasis website. STT Wiworotomo Purwokerto sebagai institusi pendidikan bergantung pada website untuk penyebaran informasi akademik dan administratif. Namun, insiden peretasan pada 20 Agustus 2024 mengungkap adanya celah keamanan yang perlu segera diatasi. Penelitian ini melakukan pengujian penetrasi pada lima subdomain dinamis website STT Wiworotomo Purwokerto menggunakan Information System Security Assessment Framework (ISSAF) guna mengidentifikasi kerentanan. Hasil pengujian menemukan beberapa kerentanan, seperti Content Security Policy (CSP) Header Not Set, Strict-Transport-Security Header Not Set, Authentication Request Identified, dan Vulnerable JS Library, dengan satu kerentanan tingkat tinggi pada subdomain perpustakaan. Simulasi serangan Cross-Site Scripting (XSS), SQL Injection, Brute-force Attack, dan Remote Code Execution (RCE) tidak berhasil memperoleh akses root atau hak istimewa, tetapi menunjukkan adanya potensi eksploitasi. Selain itu, DNSSEC belum dikonfigurasikan, sehingga meningkatkan risiko manipulasi DNS. Berdasarkan hasil penelitian, diperlukan peningkatan keamanan melalui implementasi DNSSEC, pembaruan pustaka JavaScript, konfigurasi header keamanan, serta mitigasi terhadap serangan brute-force. Penelitian selanjutnya disarankan untuk mengoptimalkan eksploitasi dan post-exploitation dalam metode ISSAF, mengombinasikannya dengan framework lain seperti OWASP Testing Guide, serta mengeksplorasi teknik serangan lanjutan seperti fuzzing dan chained exploitation. Studi lebih lanjut juga perlu mengkaji bypass keamanan terhadap sistem yang telah menerapkan mitigasi. Penelitian ini dapat menjadi referensi dalam meningkatkan keamanan sistem informasi website STT Wiworotomo Purwokerto serta mencegah insiden serupa di masa mendatang.

Kata kunci: Keamanan website, Pengujian penetrasi, ISSAF, Kerentanan sistem, STT Wiworotomo Purwokerto.

ABSTRACT

The rapid development of the internet and online services has increased data security risks, especially in web-based information systems. STT Wiworotomo Purwokerto, as an educational institution, relies on its website for academic and administrative information dissemination. However, a hacking incident on August 20, 2024, revealed security vulnerabilities that need immediate mitigation. This study conducted penetration testing on five dynamic subdomains of the STT Wiworotomo Purwokerto website using the Information System Security Assessment Framework (ISSAF) to identify vulnerabilities. The results detected several vulnerabilities, including Content Security Policy (CSP) Header Not Set, Strict-Transport-Security Header Not Set, Authentication Request Identified, and Vulnerable JS Library, with one high-level vulnerability found in the library subdomain. Attack simulations, including Cross-Site Scripting (XSS), SQL Injection, Brute-force Attack, and Remote Code Execution (RCE), failed to gain root access or privileged rights but indicated potential exploitation risks. Additionally, DNSSEC has not been configured, increasing the risk of DNS manipulation. Based on the findings, security enhancements are needed through the implementation of DNSSEC, JavaScript library updates, security header configuration, and brute-force attack mitigation. Future research is recommended to optimize exploitation and post-exploitation techniques in ISSAF, integrate it with other security frameworks such as the OWASP Testing Guide, and explore advanced attack techniques such as fuzzing and chained exploitation. Further studies should also examine security bypass methods for systems with existing mitigations. This study should serve as a reference for improving the security of the STT Wiworotomo Purwokerto website and preventing similar incidents in the future.

Keywords: Website security, Penetration testing, ISSAF, System vulnerabilities, STT Wiworotomo Purwokerto.