ANALISA *VULNERABILLITY ASSESMENT* UNTUK MENGETAHUI KERENTANAN WEBSITE SMK NEGERI 2 KOTA TERNATE MENGGUNAKAN *FRAMEWORK* (OWASP) VERSI 4

Ali Rahmat Alkatiri[1], Saiful Do. Abdullah[2], Salkin Lutfi[3]

[123]Program Studi Informatika, Fakultas Teknik, Universitas Khairun
Email: [1]alialkatiri29@gmail.com, [2]saifulabdullah12@gmail.com, [3]salkin.lutfi@unkhair.ac.id

Abstrak

Pengujian sistem keamanan website adalah hal yang penting di era perkembangan yang melaju dengan pesat, Semakin berkembangnya sistem informasi juga di lihat dengan tingginya serangan keamanan, Data serangan Cyber menunjukan tingkat keamanan dalam negeri cukup rentan dengan jumlah total serangan mencapai 100 juta kasus, Vullnerabillity Assesment menjadi solusi Dengan Semakin Kompleksnya ancaman siber, Penelitian ini dilakukan dengan tujuan untuk peningkatan keamanan website, Berdasarkan Vullnerabillity Assesment menggunakan Framework OWASP Versi 4 dengan mengevaluasi potensi kerentanan sehinggah dapat mengambil langkah langkah pencegahan yang efektif. keamanan website menggunakan Framework OWASP Versi 4 dalam pengujian menggunakan document OWASP pada objek yang di uji serta kerentanan tersebut di kategorikan apakah masuk dalam top 10 OWASP, Dengan menggunakan Framework OWASP Versi 4 ini bisa mengidentifikasi dan mengevaluasi potensi dari kerentanan dan meningkatkan keamanan website dengan rekomendasi dari analisa kerentanan yang di temukan.Berdasarkan Pengujian pada website smkn2ternate.sch.id hasil dari pengujian adalah ditemukan (3) kerentanan yang masuk dalam top 10 OWASP yaitu Application Disclosure, Vulnerable Js Llibrary, X-Frame-Option Header Not Set dan tidak ditemukan kerentanan (2) yaitu Sql Injection dan XSS (Cross Site Scripting) hasil dari pengujian yaitu Website smkn2ternate.sch.id belum aman karena memiliki kerentanan yang masuk dalam Kategori top 10 OWASP 2023 yaitu Security Missconfiguration [A05] : 2023 Vulnerable and Outdated Components [A06] : 2023. temuan kerentanan yang berhasil di exploitasi menjadi faktor pengelolah website harus lebih memperhatikan kerentanan tersebut, dengan mengikuti rekomendasi perbaikan untuk mengatasi kerentanan tersebut.

Kata kunci : *Penetration Testing*, Analisa *Vullnerabillity Assesment*, OWASP TOP 10 2021, *Smk Negeri 2 Kota* Ternate

Abstract

Testing website security systems is important in an era of rapid development. The increasing development of information systems can also be seen by the high number of security attacks. Cyber attack data shows that the level of domestic security is quite vulnerable with the total number of attacks reaching 100 million cases. Vulnerability Assessment is solution: With increasingly complex cyber threats, this research was conducted with the aim of improving website security, based on a Vulnerability Assessment using the OWASP Version 4 Framework by evaluating potential vulnerabilities so that effective preventive measures can be taken. Website security uses the OWASP Version 4 Framework in testing using OWASP documents on the objects being tested and the vulnerabilities are categorized as to whether they are included in the OWASP top 10. By using the OWASP Version 4 Framework you can identify and evaluate potential vulnerabilities and improve website security with recommendations from analysis of the vulnerabilities found. Based on testing on the smkn2ternate.sch.id website, the results of the testing were that (3) vulnerabilities were found which were included in the top 10 of OWASP, namely Application Disclosure, Vulnerable Js Llibrary, X-Frame-Option Header Not Set and no vulnerabilities were found (2) namely Sql Injection and] : 2023. The discovery of vulnerabilities that have been successfully exploited is a factor for website managers to pay more attention to these vulnerabilities, by carrying out scanning vulnerability assessments and following recommendations for improvements to overcome these vulnerabilities.

Keywords: *Penetration Testing, Vulnerability Assessment Analysis, OWASP TOP 10 2021, SMK Negeri 2 Ternate City*