Abstrak

Website merupakan sekumpulan halaman pada suatu *domain* di internet yang dibuat dengan tujuan tertentu dan saling berhubungan serta dapat diakses secara luas melalui halaman depan (*home page*) menggunakan sebuah *browser* menggunakan URL *website*. SIM (*Security Information Management*) merupakan sistem yang digunakan sebagai pemantauan suatu sistem lainnya, yang dimana pemantauan tersebut difungsikan untuk melihat sebuah kegiatan yang bersifat keamanan. semakin maraknya penggunaan internet dikalangan masyarakat luas, semakin bertambahnya peluang kejahatan siber. seperti halnya kebocoran data yang berisikan informasi dari suatu *website* oleh oknum tak bertanggung jawab yang dapat merugikan banyak pihak. *Penetration testing* adalah salah satu cara untuk mensimulasikan metode yang mungkin akan digunakan oleh penyerang untuk menghindari atau menerobos mekanisme keamanan dan mendapatkan akses secara ilegal ke dalam suatu sistem. OWASP adalah singkatan dari *Open Web Application Security Project*, sebuah komunitas *online* yang memproduksi artikel, metodologi, dokumentasi, alat, dan teknologi di bidang keamanan aplikasi web. OWASP *TOP* 10 atau yang biasa disebut OWASP 10 adalah sebuah daftar yang dirilis oleh komunitas OWASP yang berisikan 10 daftar teratas kerentanan/celah keamanan yang dapat mengancam keamanan suatu website/aplikasi web. penelitian ini bertujuan untuk mengetahui apakah Sistem Informasi Manajemen (SIM) xxx telah menerapkan standar keamanan dan apakah terdapat celah keamanan. Setelah melakukan uji penetrasi menggunakan metode OWASP TOP 10 terhadap *website* xxx memiliki 4 celah keamanan yang perlu untuk diperbaiki demi keamanan *website* xxx kedepannya. Adapun celah keamanan yang ditemukan adalah *Broken Authentication, Sensitive Data Exposure, dan Security Misconfiguration*. Adapun celah lain yang ditemukan namun tidak termasuk dalam TOP 10 keamanan OWASP yaitu *Clickjacking*. metode OWASP TOP 10 efektif dijadikan sebagai standard keamanan untuk melakukan uji penetrasi terhadap suatu *website.* Hal itu disebabkannnya dengan *standard* keamanan yang dimiliki OWASP lengkap dan *detail* dilihat dari celah konfigurasi halaman *website* maupun konfigurasi *server*. banyak hasil temuan yang mengacu pada 10 *standard* keamanan OWASP tersebut

Kata kunci : Website,SIM(Sistem Informasi Manajemen), Penetration Testing, OWASP, OWASP TOP 10

Abstract

A website is a collection of pages on a domain on the internet that are created with a specific purpose and are interconnected and can be accessed widely through the home page using a browser using a website URL. SIM (Security Information Management) is a system that is used as a monitoring system for other systems, where the monitoring function is to see a security activity. The more widespread use of the internet among the wider community, the more opportunities for cybercrime to increase. such as data leakage containing information from a website by irresponsible persons which can harm many parties. Penetration testing is one way to simulate methods that an attacker might use to circumvent or break through security mechanisms and gain illegal access to a system. OWASP stands for Open Web Application Security Project, an online community that produces articles, methodologies, documentation, tools, and technologies in the field of web application security. OWASP TOP 10 or commonly called OWASP 10 is a list released by the OWASP community which contains the top 10 list of security vulnerabilities/vulnerabilities that can threaten the security of a website/web application. This study aims to determine whether the XXX Management Information System (SIM) has implemented security standards and whether there are security holes. After conducting a penetration test using the OWASP TOP 10 method on the xxx website, there are 4 security holes that need to be fixed for the security of the xxx website in the future. The security holes found were Broken Authentication, Sensitive Data Exposure, and Security Misconfiguration. Another vulnerability found but not included in the TOP 10 OWASP security is Clickjacking. The OWASP TOP 10 method is effective as a security standard for conducting penetration tests on a website. This is because OWASP's security standards are complete and detailed in terms of web page configuration gaps and server configurations. many findings refer to the 10 OWASP security standards

Keywords: Website, SIM (Management Information System), Penetration Testing, OWASP, OWASP TOP 10