PENGUJIAN CELAH KEAMANAN WEBSITE MENGGUNAKAN TEKNIK PENETRATION TESTING DAN METODE OWASP(OPEN WEB APPLICATION SECURITY PROJECT) TOP 10 PADA WEBSITE SISTEM INFORMASI MANAJEMEN (SIM) xxx

SKRIPSI

YUM THURFAH AFIFA ROSALIAH

1710511046

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2021

ENGUJIAN CELAH KEAMANAN WEBSITE MENGGUNAKAN TEKNIK PENETRATION TESTING DAN METODE OWASP(OPEN WEB APPLICATION SECURITY PROJECT) TOP 10 PADA WEBSITE SISTEM INFORMASI MANAJEMEN (SIM) xxx

SKRIPSI

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana Komputer

YUM THURFAH AFIFA ROSALIAH

1710511046

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2021

PERNYATAAN ORISINALITAS

Tugas Akhir ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Yum Thurfah Afifa Rosaliah

NIM : 1710511046

Tanggal : 25 Juli 2021

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 25 Juli 2021

Yang Menyatakan

(Yum Thurfah Afifa Rosaliah)

PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMISI

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, Saya yang bertanda tangan dibawah ini:

Nama : Yum Thurfah Afifa Rosaliah

NIM : 1710511046

Fakultas : Ilmu Komputer

Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah Saya yang berjudul:

Pengujian celah keamanan website menggunakan teknik penetration testing dan metode OWASP(Open Web Application Security Project) TOP 10 Pada Website SIM xxx

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Tugas Akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 25 Juli 2021

Yang Menyatakan

(Yum Thurfah Afifa Rosaliah)

LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Skripsi berikut:

Nama	:	Yum Thurfah Afifa Rosaliah
NIM	:	1710511046
Program Studi	:	Informatika
Judul Tugas Akhir	:	Pengujian celah keamanan website menggunakan teknik penetration testing dan metode OWASP(Open Web Application Security Project) TOP 10 Pada Website SIM xxx

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi S1 Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Henki Bayu Seta, S.Kom, MTI.
Penguji I

Bambang Tri Wahyono, S.Kom, M.Si.
Penguji II

REVISI_2021

1 Jayanta, S.Kom., M.Si.
Dosen Pembimbing I

Bayu Hananto, S.Kom., M.Kom.
Dosen Pembimbing II

Dr. Ermatita, M. Kom.
Dekan

Yuni Widiastiwi, S.Kom, M.Si.
Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Ujian : 08 Juli 2021

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

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas segala Nikmat-Nya, sehingga Skripsi ini berhasil diselesaikan. Penulis ingin mengucapkan terima kasih kepada:

1. Mama(Rusdiati), Papa(Ali Hanapia), dan kakak penulis(Susanti Rosaliah, Maya Rosaliah, Deltiana Rosaliah yang selalu mendoakan, memberikan dorongan dan nasihat agar dapat menyelesaikan skripsi ini.
2. Bapak Jayanta, S.Kom., M.Si & Bapak Bayu Hananto, S.Kom., M.Kom selaku dosen pembimbing I & pembimbing II Skripsi yang membantu memberikan saran dan masukkan untuk menyelesaikan skripsi ini
3. Bang Rico Andreas yang banyak membantu dan memberi masukkan yang sangat bermanfaat dalam proses penyelesaian penelitian ini.
4. Andhika Wisnu, Syifa Sabrina, Yohanne Marintan sebagai teman topik skripsi seperjuangan yang saling memberi support, masukkan, dan dukungan.
5. Teman-teman Roomchat AmongUs & Tilitibis, dan TI-B(uyung) yang memberikan warna dan canda tawa semasa perkuliahan.
6. Ibu, Bapak Dosen Informatika UPN Veteran Jakarta atas segala pembelajaran dan ilmu-ilmu yang bermanfaat semasa perkuliahan.
7. Teman-teman Informatika 2017 yang selalu mendukung semasa perkuliahan.
8. Senior Informatika 2015 dan 2016 yang banyak memberikan masukkan semasa perkuliahan mapupun skripsi.
9. Sahabat sahabat penulis semasa sekolah (Tiara, helisda, via, keket, cher, mia, allen, ivan, aldian, anisa, aziz, fikran) dan yang lainnya yang tidak disebutkan yang selalu ada sampai saat ini dalam memberikan semangat dan selamat atas semua proses dan pencapaian selama ini

Jakarta, 25 Juni 2021

Penulis

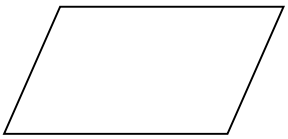
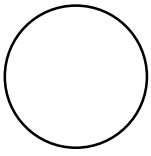
Daftar Isi

Daftar Tabel

Daftar Gambar

Daftar Simbol

Simbol	Nama Simbol	Keterangan
	Simbol Proses	Menggambarkan Proses

	Simbol Dokumen	Dokumen yang dibutuhkan dalam proses sistem
	Simbol arah data atau arus data	Sebagai petunjuk arah data dan arus data pada proses
	Simbol Terminator	Simbol untuk permulaan atau akhir dari suatu kegiatan
	Simbol Data	Simbol sebagai masukan atau keluaran data untuk suatu proses
	Simbol konektor	Simbol untuk sambungan pada halaman yang sama