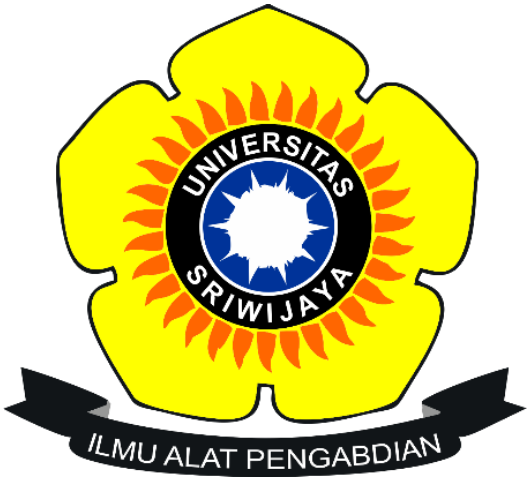
MANAJEMEN KEAMANAN INFORMASI

LAPORAN ANALISIS PADA WEBSITE JOOX.COM DAN SURABAYA.GO.ID



OLEH

Nama	**:**	**Narwastu Kartika Dewi**
NIM	**:**	**09031181520001**
Kelas	**:**	**SI Regular 6A**

Dosen Pembimbing : Deris Stiawan, M.T., Ph.D.

JURUSAN SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

- **JOOX.COM**

Joox (berasal dari kata “jukebox”) merupakan layanan musik streaming legal melalui internet dengan sentuhan personal yang diluncurkan oleh Tencent Holdings Ltd asal Shenzen, Tiongkok, yang merupakan perusahaan di balik instant messaging WeChat. Tersedia dalam bentuk mobile app (Android dan iOS) dan situs web, para pengguna dapat mendengarkan lebih dari dua juta lagu dan playlist pilihan lokal dan internasional secara gratis, serta mengunduhnya untuk didengarkan secara offline.

Data-data yang yang ada didapatkan dari website Whois, netcraft, dan aplikasi nmap. Serta untuk mencari vurnerability dicari pada website cvedetails.

Analisis Scanning pada website joox.com dapat dilihat pada table berikut :

	**Data Collection**	**Site**	http://joox.com
		Domain	joox.com
		Registrar	MarkMonitor Inc.
		Registration Date	2001-03-08
		Expiration Date	2019-09-05
		Updated Date	2017-08-05
		Organization	Shenzhen Tencent Computer Systems CO.,Ltd, Tencent Building Kejizhongyi Avenue Hi-tech Park, Nanshan District, Shenzhen, 518057, China
		Top Level Domain	Commercial entities (.com)
		Hosting country	
		DNS Admin	hostmaster@joox.com
		IP address	203.205.142.141
		OS	
		Web Server	
		Port	53/tcp open domain MikroTik RouterOS named or OpenDNS Updater
	Vulnerability	**CVE-2017-8338**	Kerentanan di MikroTik Versi 6.38.5 memungkinkan penyerang jarak jauh yang tidak berkepentingan untuk

			membuang semua CPU yang ada melalui paket UDP yang membanjir pada port 500 (digunakan untuk L2TP over IPsec), mencegah router yang terkena menerima koneksi baru; semua perangkat akan diputuskan dari router dan semua log dihapus secara otomatis.
		CVE-2016-0746	Gunakan-setelah bebas kerentanan dalam resolver di nginx sebelum 1.8.1 dan 1.9.x sebelum 1.9.10 memungkinkan penyerang jarak jauh menyebabkan penolakan layanan (crash proses pekerja) atau mungkin memiliki dampak lain yang tidak ditentukan melalui respons DNS yang dibuat terkait dengan Pemrosesan respons CNAME
		CVE-2016-1247	Paket nginx sebelum 1.6.2-5 + deb8u3 pada Debian jessie, paket nginx sebelum 1.4.6-1ubuntu3.6 di Ubuntu 14.04 LTS, sebelum 1.10.0-0ubuntu0.16.04.3 di Ubuntu 16.04 LTS, dan sebelum 1.10. 1-0ubuntu1.1 di Ubuntu 16.10, dan ebuild nginx sebelum 1.10.2-r3 di Gentoo memungkinkan pengguna lokal mengakses akun pengguna server web untuk mendapatkan hak istimewa root melalui serangan symlink pada log kesalahan.
		CVE-2018-5703	Fungsi tcp_v6_syn_recv_sock di net / ipv6 / tcp_ipv6.c di kernel Linux melalui

			4.14.11 memungkinkan penyerang untuk menyebabkan penolakan layanan (lemparan di luar batas penulisan) atau mungkin memiliki dampak lain yang tidak ditentukan melalui vektor yang melibatkan TLS.

Tabel Analisis Scanning Pada Website joox.com

- **Surabaya.go.id**

Website Surabaya.go.id merupakan website yang dikelola oleh pemerintahan kota Surabaya yang bertujuan memberikan informasi yang terkait dengan pemerintahan kota Surabaya sehingga dapat memudahkan pelayanan bagi masyarakat kota Surabaya.

Data-data yang yang ada didapatkan dari website Whois, netcraft, dan aplikasi nmap. Serta untuk mencari vurnerability dicari pada website cvedetails.

Analisis Scanning pada website Surabaya.go.id dapat dilihat pada table berikut :

PEMERINTAH KOTA SURABAYA	Data Collection	**Site**	http://www.surabaya.go.id
		Domain	surabaya.go.id
		Registrar	unknown
		Registration Date	10-May-2000
		Expiration Date	31-Jan-2019
		Updated Date	21-Jan-2018
		Organization	PT Telkom, Ketintang, Surabaya, Jawa Timur, 60231, ID
		Top Level Domain	Indonesia (.go.id)
		Hosting country	
		DNS Admin	udienz@rad.net.id
		IP address	203.205.142.141
		OS	
		Web Server	NGINX versi 1.6.2

		Port	80/tcp open http nginx 1.6.2
			113/tcp closed ident
	Vulnerability	**CVE-2016-1247**	Paket nginx sebelum 1.6.2-5 + deb8u3 pada Debian jessie, paket nginx sebelum 1.4.6-1ubuntu3.6 di Ubuntu 14.04 LTS, sebelum 1.10.0-0ubuntu0.16.04.3 di Ubuntu 16.04 LTS, dan sebelum 1.10. 1-0ubuntu1.1 di Ubuntu 16.10, dan ebuild nginx sebelum 1.10.2-r3 di Gentoo memungkinkan pengguna lokal mengakses akun pengguna server web untuk mendapatkan hak istimewa root melalui serangan symlink pada log kesalahan.
		CVE-2018-5703	Fungsi tcp_v6_syn_recv_sock di net / ipv6 / tcp_ipv6.c di kernel Linux melalui 4.14.11 memungkinkan penyerang untuk menyebabkan penolakan layanan (lemparan di luar batas penulisan) atau mungkin memiliki dampak lain yang tidak ditentukan melalui vektor yang melibatkan TLS.
		CVE-2017-18017	Fungsi tcpmss_mangle_packet di net / netfilter / xt_TCPMSS.c di kernel Linux sebelum 4.11, dan 4.9.x sebelum 4.9.36, memungkinkan penyerang jarak jauh menyebabkan penolakan layanan (penggunaan setelah bebas dan korupsi memori) atau mungkin tidak ditentukan Dampak lainnya dengan memanfaatkan kehadiran

			xt_TCPMSS dalam tindakan iptables.

Tabel Scanning Pada Website Surabaya.go.id