

**ANALISIS KERENTANAN WEB SERVER UNIVERSITAS MUHAMMADIYAH YOGYAKARTA
MENGUNAKAN SHODAN.IO**



Disusun oleh :

Rifqi Ichsan An Nibras

20200140066

**PROGRAM STUDI TEKNOLOGI INFORMASI FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH YOGYAKARTA**

2024

HALAMAN PERNYATAAN

Saya yang bertanda tangan dibawah ini:

Nama : Rifqi Ichsan An Nibras
NIM : 20200140066
Program Studi : Teknologi Informasi
Fakultas : Teknik
Universitas : Universitas Muhammadiyah Yogyakarta
Jenis Karya : Skripsi
Judul Karya : Analisis Keamanan Web Server Universitas Muhammadiyah Yogyakarta Menggunakan Shodan.io

Menyatakan dengan benar dan tanpa paksaan bahwa:

1. Skripsi ini merupakan skripsi asli hasil karya saya sendiri dengan arahan dan bimbingan dari dosen pembimbing.
2. Karya ini tidak memuat hasil karya orang lain kecuali acuan dan kutipan yang telah disebutkan sumbernya.
3. Karya ini belum pernah diajukan untuk memperoleh gelar akademik (sarjana, magister, dan doctor) di Universitas Muhammadiyah Yogyakarta atau institusi lainnya.

Yogyakarta, Agustus 2024

Penulis



Rifqi Ichsan An Nibras

KATA PENGANTAR

Assalamualaikum Wr. Wb.

Segala puji dan syukur penulis panjatkan kehadirat Allah SWT atas berkat dan, rahmat dan karunianya penulis dapat menyelesaikan skripsi dengan judul **Analisis Keamanan Web Server Universitas Muhammadiyah Yogyakarta Menggunakan Shodan.io**. Penyusunan skripsi ini merupakan salah satu syarat yang harus dipenuhi untuk mencapai gelar sarjana pada strata 1 (S1) Prodi Teknologi Informasi Universitas Muhammadiyah Yogyakarta.

Dalam penyelesaian penelitian dan penulisan skripsi ini, penulis banyak memperoleh bantuan baik pengajaran, bimbingan dan arahan dari berbagai pihak baik secara langsung maupun tidak langsung. Untuk itu penulis menyampaikan penghargaan dan terima kasih yang tak terhingga kepada:

1. Ucapan syukur yang sangat banyak tanpa batas kehadirat Allah SWT, yang senantiasa memberikan kelancaran dan kemudahan selama penulis melakukan penelitian ini.
2. Kedua orang tua yang senantiasa memfasilitasi dan mendoakan penulis tiada henti sehingga penulis bisa menyelesaikan studi S-1 pada tahap akhir dari perkuliahan ini.
3. Bapak Ir. Eko Prasetyo, M.Eng., Ph.D. selaku dosen pembimbing I yang selalu membimbing penulis dari awal dengan penuh kesabaran sehingga penulis bisa menyelesaikan penelitian ini.
4. Bapak Cahya Damarjati, S.T., M.Eng., Ph.D. selaku dosen pembimbing II yang selalu membimbing penulis dari awal dengan penuh kesabaran sehingga penulis bisa menyelesaikan penelitian ini.
5. Vinca Aprilian selaku pasangan penulis yang senantiasa memberikan dukungan dan motivasi tanpa henti. Salah satu faktor penting bagi penulis sehingga bisa menyelesaikan studi S-1 ini.

6. Teman-teman kontrakan penulis, Syariah, dan DLBforTech, yang selalu membantu penulis dalam banyak hal serta memberikan warna baru dalam setiap fase perjalanan penulis selama studi S-1.

Penulis memohon maaf apabila dalam penulisan ini terdapat kesalahan dalam pemilihan kata dan susunan penulisan, serta penulis pun menyadari bahwa skripsi ini belum sempurna. Oleh karena itu, segala saran dan masukan yang membangun guna penyempurnaan skripsi ini sangat penulis harapkan. Semoga skripsi ini bermanfaat khususnya bagi penulis, umumnya bagi semua pihak

Wassalamualaikum Wr. Wb.

Yogyakarta, Agustus 2024

Penulis



Rifqi Ichsan An Nibras

DAFTAR ISI

HALAMAN PENGESAHAN I.....	i
Go to page 2 PENGESAHAN II.....	ii
HALAMAN PERNYATAAN.....	iii
KATA PENGANTAR	iv
DAFTAR ISI.....	vi
DAFTAR GAMBAR.....	viii
DAFTAR SINGKATAN	ix
INTISARI	x
ABSTRACT	xi
BAB I.....	1
PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Tugas Akhir	3
1.5 Manfaat Tugas Akhir	4
1.6 Sistematika Penulisan	4
BAB II.....	6
TINJAUAN PUSTAKA.....	6
2.1 Keamanan Jaringan	6
2.2 Web Server	7
2.3 Shodan.io	8
2.4 Common Vulnerabilities and Exposures (CVE)	9
2.5 Internet	11
2.6 Passive Reconnaissance	13
2.7 Serangan Siber	15
BAB III.....	18

METODE TUGAS AKHIR	18
3.1 Metode Penelitian	18
BAB IV.....	24
HASIL DAN PEMBAHASAN	24
4.1 Pendahuluan	24
4.2 Hasil Pengumpulan Data Menggunakan Shodan.io	24
4.3 Analisis Data dan Identifikasi Kerentanan	26
4.4 Solusi untuk Memperbaiki dan Menutup Celah Keamanan	35
4.5 Analisis Perbandingan Kerentanan Web Server	42
BAB V	46
KESIMPULAN DAN SARAN	46
5.1 Kesimpulan	46
5.2 Saran	47
DAFTAR PUSTAKA	49
LAMPIRAN	52

DAFTAR GAMBAR

Gambar 3. 1 Alur Penelitian	18
Gambar 3. 2 Shodan.io Main Page	19
Gambar 3. 3 Pencarian menggunakan ASN	20
Gambar 3. 4 Pencarian menggunakan IP Address.....	21
Gambar 4. 1 Kerentanan pada Web Server MMRS UMY	44
Gambar 4. 2 Kerentanan pada Web Server Sign-in Page	45

DAFTAR SINGKATAN

C

CVE *Common Vulnerabilities and Exposures* adalah sistem referensi standar untuk mengidentifikasi dan mendokumentasikan kerentanan keamanan dalam perangkat lunak atau sistem. Setiap CVE memiliki kode unik yang digunakan untuk melacak dan mengelola informasi tentang kelemahan yang dapat dieksploitasi oleh peretas

H

HTTP

Hypertext Transfer Protocol adalah protokol komunikasi yang digunakan untuk mengirim dan menerima data di *web*. Protokol ini memungkinkan pengiriman informasi seperti teks, gambar, video, dan file lainnya antara *server* dan klien (misalnya, *browser*). HTTP berfungsi sebagai dasar komunikasi web, di mana klien mengirimkan permintaan (*request*) ke *server*, dan *server* merespons dengan data yang diminta.

W

Web Server

Perangkat lunak atau perangkat keras yang berfungsi untuk menerima, memproses, dan mengirimkan permintaan halaman *web* dari klien melalui *protocol* HTTP atau HTTPS.