SKRIPSI

IMPLEMENTASI NUCKLEI VULNERABILITY SCANNER UNTUK MENDETEKSI KERENTANAN KEAMANAN PADA PLATFORM BERBASIS WEB (SECURE SYSTEM)

IMPLEMENTATION OF NUCKLEI VULNERABILITY SCANNER TO DETECT SECURITY VULNERABILITIES ON WEB-BASED PLATFORMS (SECURE SYSTEMS)

AHMAD AGUNG RIZALDI

D02 18 555

PROGRAM STUDI INFORMATIKA

FKULTAS TEKNIK

UNIVERSITAS SULAWESI BARAT

MAJENE

2024

BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan website adalah satu hal penting dalam perancangan sebuah website. Namun masih sering dijumpai pengembang website yang kurang teliti dalam meningkatkan keamanan website mereka. Seharusnya para pengembang website harus menerapkan keamanan website yang baik di awal perancangan website mereka, karena mungkin suatu saat website yang telah mereka bangun akan menjadi sasaran pengerusakan oleh peretas. Selain itu pengembang website juga harus sering mengikuti tren serangan terbaru agar mereka dapat mempertahankan dan memperbaiki website mereka dari hal- hal yang tidak diinginkan.(Gultom & Harahap, 2015)

Dalam sebuah website memerlukan tingkat keamanan yang tinggi untuk mencegah kebocoran, manipulasi, penghapusan, perubahan, pencurian data dan berpindahnya hak pengelolahan yang diakibatkan oleh pihak-pihak yang tidak bertanggung jawab. Di era perkembangan teknologi yang pesat, sebuah website memiliki banyak celah yang membuatnya rentan terhadap serangan.(Elu, 2017).

Bentuk serangan paling umum yang terjadi pada sebuah aplikasi web yaitu, *Malware*, *Penetration Testing*, *SQL Injection* dan sebagainya. Penyebab semua kerentanan yang teridentifikasi dalam aplikasi web, masalahnya disebabkan oleh input yang tidak diperiksa yang diakui sebagai yang paling umum. Berdasarkan data terbaru tahun 2022 dari WPScan, jumlah kerentanan baru yang ditemukan telah meningkat dalam beberapa tahun terakhir. Pada tahun 2021, lebih dari 5600 kerentanan baru telah ditemukan. Kemudian ada tambahan lebih dari 78 kerentanan baru telah ditemukan pada tahun 2022. (Sains, 2022)

Seiring dengan kemajuan teknologi, terdapat perubahan konstan dalam ekosistem keamanan informasi. *Nuclei Vulnerability Scanner* merupakan alat pemindaian keamanan yang mendapat popularitas dalam deteksi kerentanan pada

aplikasi web dan infrastruktur.Pada sebuah artikel yang berjudul (*The Ultimate Giudeto Finding Bugs With Nuclei*) yang dikembangkan oleh *Project Discovery*, *Nuclei* memanfaatkan templat-templat yang dapat disesuaikan untuk mengidentifikasi potensikerentanan keamanan.

Penelitian ini akan membahas dan menganalisis efektivitas *Nuclei Vulnerability Scanner* dalam mendeteksi kerentanan pada aplikasi web. Melalui pendekatan eksperimental dan analisis mendalam, penelitian ini diharapkan dapat memberikan wawasan baru yang dapat meningkatkan pemahaman kita tentang kinerja *Nuclei* dan potensinya dalam meningkatkan keamanan aplikasi web.

1.2 Rumusan Masalah

1.2.1 Bagaimana kinerja *Nuclei Vulnerability Scanner* dalam mendeteksi kerentanan keamanan pada aplikasi web?

1.2.2 Apakah *Nuclei* dapat memberikan hasil yang akurat dan relevan dalam pemindaiankerentanan pada aplikasi web?

1.3 Tujuan Dan Manfaat Penelitian

1.3.1 Tujuan Penelitian :

a. Menerapkan *Nuclei Vulnerability Scanner* dalam mendeteksi kerentanan pada aplikasi web.
b. Mengevaluasi *Nuclei* dalam konteks pemindaian keamanan pada aplikasi web.

1.3.2 Manfaat Penelitian:

a. Bagi Peneliti dan Akademisi :

- Menambah literatur terkait dengan penerapan *Nuclei vulnerability Scanner* untuk mendeteksi kerentanan keamanan pada aplikasi web.
- Menyediakan dasar untuk penelitian lebih lanjut dalam pengembangan alat pemindaian keamanan.

b. Bagi Pengembang Aplikasi Web:

- Memberikan pemahaman yang lebih baik tentang cara menjaga keamanan aplikasi web.
- Menyediakan panduan praktis untuk memilih dan menggunakan alat pemindaian yang sesuai.

1.4 Batasan Masalah

1.4.1 Penelitian fokus pada Penerapan *Nuclei Vulnerability Scanner* untuk mendeteksi kerentanan keamanan terhadap aplikasi web.

1.4.2 Analisis keamanan yang dilakukan hanya berfokus pada kerentanan yang dapat di deteksi oleh *Nuclei*, dan aspek keamanan lainnya mungkin tidak tercakup sepenuhnya.

1.4.3 Batasan waktu dan sumber daya mungkin mempengaruhi tingkat penerapan *Nuclei*pada aplikasi web.

Dengan merinci rumusan masalah, tujuan, manfaat, dan batasan masalah seperti di atas, penelitian ini diharapkan dapat memberikan kontribusi yang signifikan dalam pemahaman dan pengembangan alat pemindaian keamanan, khususnya dalam konteks aplikasi web.

BAB II
TINJAUAN PUSTAKA

2.1 Pengertian Website

Website adalah layanan penyajian informasi yang menggunakan konsep tautan (hyperlink) untuk memudahkan pengguna internet dalam mencari informasi. Situs webadalah kumpulan halaman web yang saling berhubungan di mana file-file tersebut saling terkait dan dapat dilampirkan file gambar, video atau file statis dan dinamis lainnya. Informasi atau file yang terdapat pada website disimpan pada web server dan biasanya ditulis dalam format HTML atau *hypertext markup language*. *Hyperlink* adalah referensi dalam dokumen *hypertext* ke dokumen lain, yang dapat berupa grafikatau teks di dalam dokumen, dan biasanya digaris bawahi atau ditandai dengan warna biru. Sebuah web biasanya terdiri dari halaman atau halaman yang ditempatkan di server web, dapat diakses melalui internet atau jaringan area lokal, yang merupakan file teks yang berisi tag dalam format HTML(Elu, 2017)

2.2 Pengertian Aplikasi Web

Keamanan sebuah aplikasi berbasis web dapat dinilai dengan cara melakukan percobaan penetrasi atau penerobosan terhadap aplikasi web dimaksud, baik secara manual atau otomatis menggunakan alat bantu seperti perangkat lunak scanning.(Sains,2022)

2.3 Pengertian Vulnerability

Menurut (Kamilah & Hendri Hendrawan, 2019) pada analisis keamanan jaringan yang menggunakan *Nmap* dan *Nessus*. *Vulnerability* merupakan suatu kelemahan dimana sebuah sistem rentan terhadap serangan. Hampir sebagian serangan yang ada saat ini merupakan hasil dari pendayagunaan terhadap port-port yang terbuka. pendayagunaan kerentanan merupakan metode umum lain penyusupan.

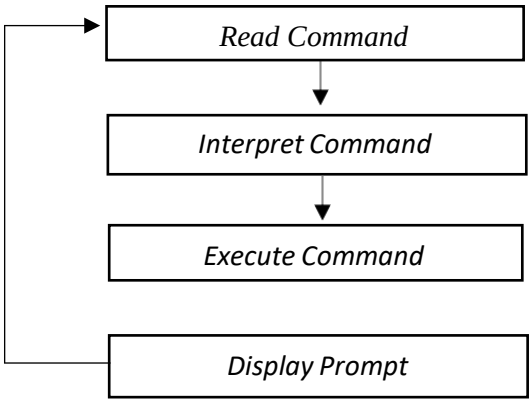
2.4 Keamanan Website

Keamanan website adalah satu hal penting dalam perancangan sebuah website. Tujuan jangka panjangnya yaitu menghasilkan model penanganan yang baik dari setiap celah keamanan pada website berdasarkan tingkat kerentanan sebuah website. Sedangkan tujuan khususnya menganalisis beberapa celah keamanan yang terdapat pada website dan tingkat kerentanan setiap website. Beberapa masalah pada celah keamanan seperti : *cross-site scripting, information leakage, authentication and authorization, Session management, SQL injection, CSRF* dan lain – lain.(Gultom & Harahap, 2015)

2.5 Sistem operasi Linux

Pada penelitian (Eka Pratama & Wiradarma, 2018) yang berjudul *implementasi katoolin sebagai penetrasi tools kali linux pada linux ubuntu 16.04 (studi kasus: reverse engineering file .apk),* sistem operasi linux dikenal dengan sifat *open-source,* yang artinya setiap orang dapat menggunakannya dengan bebas mengembangkan Linux dengan kode sumber yang tersedia. Buah dari pengembangan Linux Dikenal sebagai distribusiLinux. Ada banyak jenis distribusi Linux, menurut Kegunaannya masing-masing, salah satunya adalah Kali Linux. Kali Linux adalah distribusi Linux Dirancang khusus untuk menembus keamanan sistem komputer. Kali Linux menggunakan berbagai Berbagai alat (tools) untuk menjalankan fungsinya. Contoh dari tools sistem operasi linux yang akan digunakan pada penelitian ini yaitu *command prompt* atau *shell*. *Shell Linux* adalah alat berbasis teks untuk berinteraksi dengan komputer. *Shell Linux* juga biasa disebut sebagai *xterm*, *console*, terminal, perintah *shell*, atau kerang.

Shell adalah antarmuka antara pengguna dan sistem. *Shell*, juga sering disebut interpreter, menjalankan sebuah loop yaitu, menerima perintah, menafsirkan perintah, mengeksekusi perintah, dan menunggu perintah input berikutnya. Ini adalah grafik siklus *Interpreter* sederhana yang berjalan di *shell* unix atau GNU/Linux. dapat dilihat pada gambar 2.1 (Azikin, 2004-2007).



Gambar 2.1 *Iinterpreter Loop* (Azikin,2004-2007)

2.6 Penelitian Terkait

Penelitian terkait bertujuan sebagai pendukung untuk melakukan penelitian yang digunakan sebagai referensi penulis. Adapun penelitian terkait dengan Analisis Keamanan Web Menggunakan *Nucklei Vulnerability Scanner* diantarannya dapat dilihat pada tabel 2.1

Tabel 2.1 Penelitian Terkait

No	Nama Peneliti	Judul Penelitian	Tujuan Penelitian	Hasil Penelitian & Kesimpulan	Persamaan	Perbedaan
1	Afif Zirwan (2022)	Pengujian dan Analisis Keamanan Website Menggunakan Acunetix Vulnerability Scanner	Penelitian ini bertujuan untuk melakukan pengujian dan analisa sejauh mana keamanan website ITP dan memberikan Saran pemecahan masalah dari hasil analisa. Pengujian dilakukan dengan menggunaka n tools Acunetix Vulnerability Scanner.	Hasil yang diperoleh adalah website ITP sudah mendapatkan peringkat 1 atau low threat level yang dimana ini sudah dikategoringan aman berdasarkan Acunetix WVS karena pada level 1 vulnerability yang ditemukan hanya bersifat informasional saja	Menganalisa vulnerability atau celah keamanan yang ada pada website dan memberikan solusi terhadap masalah yang ditemukan, dengan tujuan laporan dari hasil penelitian ini dapat menjadi acuan bagi pengembang atau administrator sistem untuk melakukan perbaikan dengan pengembangan sistem.	Perbedaan penelitian ini adalah menganalisis vulnerability yang terdapat pada website menggunakan tools tools Acunetix web vulnerability scanner.
2	Muhammad	Analisa	Untuk	Hasil penelitian ini	Metode	Penelitian ini

	fathurozzi (2021)	keamanan website menggunakan metode Footprinting dan Vulnerability Scanning pada website kampus	menganalisis seberapa banyak celah bagi peretas celah bagi peretas yang terdapat dalam website kampus.	telah menemukan informasi terkait website target (website lembaga pendidikan di indonesia) dan beberapa peringatan kerentanan setelah dilakukan pengujian pemindaian kerentanan dengan tingkat resiko tinggi hingga rendah sehingga peneliti merekomendasikan perbaikan kerentanan untuk menimalkan lubang.	penelitian yang digunakan dalam penelitian ini adalah metode Ethical Hacking yang menitikberatkan pada teknik vulnerability Scanning dengan hanya menguji serangan pasif.	tidak menggunakan Nuclei Vulnerability.
3	Gregorius Hendita Artha Kusuma (2022)	Implementasi Owasp Zap Untuk Pengujian Keamanan Sistem Informasi Akademik	Tujuan dari penelitian ini adalah untuk mengidentifikasi kerentanan yang terdapat pada website Sistem Informasi Akademik Universitas serta melakukan	Analisis kerentanan website dengan teknik OWASP ZAP dengan bantuan beberapa tools keamanan mampu mengetahui tingkat keamanan suatu website berdasarkan hasil scan dan pengujian yang telah dilakukan dimana hampir setiap	Mengidentifikasi kerentanan website,pengujian serta analisi lebih mendalam untuk mengetahui kondisi kerentanan pada sebuah website.	Metode penelitian yang digunakan sebagai parameter keamanan website adalah OWASP Top-10 202.

			pengujian dan analisis untuk mengetahui kondisi kerentanan website Sistem Informasi Akademik Universitas dengan menggunakan OpenWeb Application Security Project (OWASP).	kategori pengujian mampu menemukan kerentananmeskipun ada beberapakategori yang tidak memiliki kerentanan.		
4	Arief Budiman,Saiful Ahdan,Muham madAziz (2021)	Analisis celah keamanan aplikasiweb e-learning universitas ABC dengan *vulnerability Assesment*	bertujuan untuk mendeteksi kerentanan, mendeskripsik an kerentanan, menilai kerentanan berdasarkan Common Vulnerability Scoring System, dan memberikan	Aplikasi Web E-Learning di UniversitasABC dikatakan rentan, karena mempunyai dampak serius yang mempengaruhi Kerahasiaan, Integritas,dan Ketersediaan aplikasi web E-Learning melalui	Sama-sama menganalisis celah keamanan suatu web dengan menerapkan *vulnerability Assesment* untuk mendeteksi dan melaporkan kerentanan.	Perbedaannya tools yang digunakan toolswhois, dig, nslookup, NMAP. Dengan 6 tahapan *VAPT Life Cycle.*

			solusi.	kerentanan yang dimilikinya. Oleh karena itu, Universitas ABC harus segera melakukan perbaikan dan evaluasi terhadap keamanan Aplikasi Web E-Learning agar risiko kerentanan padaAplikasi Web E-Learning dapat dikurangi.		

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Adapun kesimpulan yang dapat diperoleh yakni sebagai berikut :

1. *Nuclei* dapat mempercepat proses pengujian keamanan dengan otomatisasi pemindaian dan analisis kerentanan.
2. *Nuclei* dapat digunakan untuk melakukan pemindaian pada baerbagai jenis target termasuk situs web, aplikasi web, dan infrastruktur jaringan.
3. *Nuclei* memungkinkan pengguna untuk membuat dan mengedit template sendiri sesuai dengan kebutuhan spesifik pengguna.
4. *Nuclei* menyediakan laporan yang terperinci tentang kerentanan yang ditemukan, termasuk tingkat keparahan, deskripsi kerentanan dan langkah-langkah remediasi yang direkomendasikan.

Dengan demikian kesimpulan utama dalam penggunaan *Nuclei* adalah bahwa *Nuclei* merupakan alat yang kuat dalam mendeteksi kerentanan keamanan sistem dan aplikasi dengan cara yang cepat, efisien, dan dapat disesuaikan.

5.2 Saran

Berdasarkan penelitian yang telah dilakukan, maka saran yang dapat diberikan oleh penulis ialah Melihat hasil dari penelitian ini membuktikan bahwa *Nuclei Vulnerability Scanner* dapat mempermudah pengguna maupun pengembang dalam mendeteksi tingkat kerentanan keamanan yang terdapat dalam situs web, aplikasi web, dan infrastruktur jaringan, serta memberikan informasi tentang langkah-langkah dalam remediasi kerentanan.

DAFTAR PUSTAKA

Abdul Fattah Hasibuan, Tommy dan Divi Handoko (2023). Analisis Keretanan Website Dengan Aplikasi Owasp Zap Website Train Analysis With Owasp Zap App

Azikin, Askari. *Debian GNU/Linux 2nd Edition*. http://debianindonesia.org, 2004- 2007.

Darojat, Esti Zakia, Eko Sediyono dan Irwan Sembiring. "Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner." *Jurnal Sistem Informasi Bisnis* (2022): 36-44.

Eka Pratama, I. P. A., & Wiradarma, A. A. B. A. (2018). Implementasi Katoolin Sebagai Penetrasi Tools Kali Linux Pada Linux Ubuntu 16.04 (Studi Kasus: Reverse Engineering File .Apk). *Jurnal RESISTOR (Rekayasa Sistem Komputer)*, *1*(2), 86–93. https://doi.org/10.31598/jurnalresistor.v1i2.278

Elu, A. M. (2017). Rancang Bangun Aplikasi Pendeteksian Vulnerability Structured Query Language (Sql) Injection Untuk Keamanan Website. *Respati*, *8*(22), 111–124. https://doi.org/10.35842/jtir.v8i22.53

Fatkhurozzi, M. (2021). Analisa Keamanan Website Menggunakan Metode Footprinting Dan Vulnerability Scanning Pada Website Kampus. *Prosiding Seminar Nasional Informatika Bela Negara*, *2*, 144–148. https://doi.org/10.33005/santika.v2i0.74

Gauravgandal. *Nuclei-Fast and Customizable Vulnerability Scanner*. 28 July 2021. https://www.geeksforgeeks.org/nuclei-fast-and-cutomizable-vulnerability-scanner/. 31 October 2023.

Gultom, L. M., & Harahap, M. (2015). *Analisis Celah Keamanan Website Instansi*. *02*,1–7.

Kamilah, I., & Hendri Hendrawan, A. (2019). Analisis Keamanan Vulnerability pada Server Absensi Kehadiran Laboratorium di Program Studi Teknik Informatika.*Prosiding Semnastek*, *16*(0), 1–9.

https://jurnal.umj.ac.id/index.php/semnastek/article/view/5233

Kristanto, Albertus Ari, Yulius Harjoseputro dan Joseph Eric Samodra. "Implementasi Golang dan New Simple Queue pada Sistem Sandbox Pihak Ketiga Berbasis REST API." *JURNAL RESTI (Rekayasa Sistem dan Teknologi Informasi)* (2021): 745 - 750. ISSN Media Elektronik: 2580-0760 .

Munjal, M. N. (2013). Ethical Hacking: an Impact on Society. *Cyber Times International Journal of Technology & Management*, *7*(1).

Molavi Arman (2020). Metode Pertahanan Web Server Terhadap Distributed Slow HTTP DoS Attack

Sains, J. I. (2022). *ANALISIS KEAMANAN APLIKASI WEB MENGGUNAKAN ZAP Yuswandi*. *6*(4), 39–42.

The Ultimate Giude to Finding Bugs With Nuclei. 12 October 2022. https://blog.projectdiscovery.io/ultimate-nuclei-giude/. 31 October 2023.

Zidane, Muamar. "Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naïve Bayes." *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer* (2022): 172-180 . e-ISSN: 2548-964X

The OWASP Top Ten 2024

https://jakarta.telkomuniversity.ac.id/web-defacement-definisi-contoh-cara-kerja-serta-penanganan-serangan-peretas/