Jurnal Publikasi Ilmu Komputer dan Multimedia

E-ISSN: 2808-8999
P-ISSN: 2808-9375

Penerapan Analisis Komparatif Efektivitas *OWASP ZAP* dan *Nikto* dalam Mendeteksi Celah Keamanan *Web Server*

Robit Maula [1*], Fahmi Fachri[2]

[1] Teknik Informatika, Universitas Ma'arif Nahdlatul Ulama Kebumen; email : maularobit95@gmail.com
[2] Teknik Informatika, Universitas Ma'arif Nahdlatul Ulama Kebumen; email : fahmifachriumnu@gmail.com

Abstract:

The integration of web-based information systems in the business sector, such as the planetkomputer.my.id website, is crucial for providing efficient services, yet it remains highly vulnerable to exploitation threats and data integrity manipulation. A real problem discovered in this research object is data inconsistency caused by abnormal price changes in the shop's product price list. This study aims to identify the exact location of these security flaws—whether originating from application code or server misconfigurations—while comparing the effectiveness of security scanning tools in detecting vulnerabilities. The proposed method is a qualitative-descriptive applied security assessment using a Black-Box Testing approach with two security scanners, namely OWASP Zed Attack Proxy (ZAP) and Nikto, executed through the stages of Reconnaissance, Vulnerability Scanning, and Data Analysis. The results indicate that both tools successfully identified several security vulnerabilities with Medium to Low risk levels. The core synthesis reveals complementary detection characteristics; OWASP ZAP proved thorough in detecting web application logic and session weaknesses, such as the absence of Anti-CSRF tokens and the HttpOnly flag on cookies, whereas Nikto was more sensitive in identifying misconfigurations at the web server architecture level and network technical information leaks. In conclusion, combining these two assessment tools is highly effective in providing a comprehensive security evaluation to formulate neat and systematic mitigation recommendations for the shop's IT infrastructure management.

Keywords: *Web Application Security; Vulnerability Assessment; OWASP ZAP; Nikto Web Scanner; planetkomputer.my.id*

Abstrak:

Integrasi sistem informasi berbasis web pada sektor bisnis seperti website planetkomputer.my.id sangat penting untuk menyediakan layanan yang efisien, namun di sisi lain memiliki kerentanan tinggi terhadap ancaman eksploitasi dan manipulasi integritas data. Masalah nyata ditemukan pada objek penelitian ini berupa ketidakkonsistenan data akibat adanya perubahan harga yang tidak wajar pada daftar harga (price list) produk toko. Penelitian ini bertujuan untuk mengidentifikasi letak celah keamanan tersebut—apakah bersumber dari kode aplikasi atau miskonfigurasi server—sekaligus membandingkan efektivitas perangkat pemindai dalam mendeteksi kerentanan. Metode yang diusulkan adalah pengujian keamanan terapan kualitatif-deskriptif dengan pendekatan Black-Box Testing menggunakan dua security scanners, yaitu OWASP Zed Attack Proxy (ZAP) dan Nikto, yang dieksekusi melalui tahapan Reconnaissance, Vulnerability Scanning, hingga Data Analysis. Hasil penelitian menunjukkan bahwa kedua tools berhasil mengidentifikasi sejumlah celah keamanan dengan tingkat risiko Medium hingga Low. Sintesis utama menunjukkan karakteristik deteksi yang saling melengkapi; OWASP ZAP terbukti mendalam dalam mendeteksi kelemahan level logika aplikasi web dan sesi seperti absennya token Anti-CSRF dan status HttpOnly flag pada cookie, sedangkan Nikto lebih sensitif dalam mengidentifikasi miskonfigurasi pada level arsitektur web server dan kebocoran informasi teknis jaringan. Kesimpulannya, penggabungan kedua alat uji ini sangat efektif dalam memberikan evaluasi keamanan

Diterima: tanggal
Direvisi: tanggal
Diterima: tanggal
Diterbitkan: tanggal
Versi sekarang: tanggal

menyeluruh guna merumuskan rekomendasi mitigasi dan perbaikan sistem secara rapi dan sistematis bagi pengelola infrastruktur IT toko.

Kata kunci: Keamanan Aplikasi Web; Vulnerability Assessment; OWASP ZAP; Nikto Web Scanner; planetkomputer.my.id

1. Pendahuluan

Perkembangan teknologi informasi yang sangat pesat telah mengubah paradigma interaksi manusia di berbagai sektor, mulai dari ekonomi, pendidikan, hingga pemerintahan. Integrasi sistem informasi berbasis web kini menjadi pilar utama dalam menyediakan layanan yang efisien, cepat, dan dapat diakses dari mana saja tanpa batasan waktu. Namun, ketergantungan yang tinggi terhadap aplikasi web ini secara otomatis meningkatkan risiko keamanan data yang tersimpan di dalamnya. Setiap inovasi teknologi baru seringkali dibarengi dengan munculnya teknik serangan siber yang semakin kompleks dan sulit dideteksi oleh sistem keamanan konvensional.

Keamanan aplikasi web bukan lagi sekadar pilihan tambahan, melainkan sebuah kebutuhan fundamental bagi setiap organisasi yang beroperasidi ruang digital. Ancaman siber seperti pencurian data identitas, perusakan tampilan situs (deface), hingga kebocoran data rahasia perusahaan terus menghantui para pengelola infrastruktur IT. Kerugian yang ditimbulkan tidak hanya bersifat finansial, tetapi juga mencakup hilangnya reputasi dan kepercayaan publik terhadap instansi atau unit usaha tersebut. Oleh karena itu, pengelola sistem harus proaktif dalam mengidentifikasi titik lemah sebelum dieksploitasi oleh pihak yang tidak bertanggung jawab.

Fenomena nyata mengenai kerentanan integritas data dapat diamati pada website ***planetkomputer.my.id*** di mana ditemukan adanya perubahan harga yang tidak wajar pada daftar harga (price list) produk. Ketidakkonsistenan data ini mengindikasikan adanya celah keamanan yang memungkinkan pihak luar atau skrip berbahaya melakukan manipulasi informasi tanpa otorisasi yang sah. Kejadian ini menjadi bukti kuat bahwa sistem informasi yang digunakan untuk aktivitas bisnis sangat rentan terhadap serangan yang menargetkan integritas data transaksi. Jika hal ini dibiarkan tanpa adanya audit keamanan yang rutin, maka kepercayaan pelanggan terhadap akurasi informasi di website tersebut dapat menurun drastis.

Kasus pada ***planetkomputer.my.id*** tersebut memberikan gambaran bahwa serangan siber tidak selalu bertujuan untuk melumpuhkan sistem secara total, melainkan bisa berupa modifikasi data secara halus. Manipulasi pada harga produk merupakan ancaman serius bagi stabilitas ekonomi sebuah unit usaha karena dapat menyebabkan kerugian finansial secara langsung bagi pemilik toko. Oleh karena itu, sangat penting untuk mengetahui apakah kerentanan tersebut bersumber dari celah pada kode aplikasi web atau adanya kelemahan konfigurasi pada sisi server. Di sinilah peran perangkat pemindai otomatis dibutuhkan untuk memetakan titik masuk mana saja yang paling berisiko dieksploitasi oleh peretas.

Saat ini, terdapat berbagai macam perangkat lunak pemindai keamanan (security scanners) yang tersedia, baik yang bersifat komersial maupun sumber terbuka (open source). Dua perangkat lunak yang paling sering digunakan oleh praktisi keamanan siber di seluruh dunia adalah *OWASP* Zed Attack Proxy (*ZAP*) dan *Nikto*. Meskipun keduanya memiliki tujuan yang sama, yaitu menemukan celah keamanan, namun keduanya memiliki filosofi dan mekanisme kerja yang sangat berbeda. Perbedaan ini mencakup cara pemindaian, kelengkapan basis data kerentanan, hingga format laporan akhir yang dihasilkan sebagai bahan evaluasi bagi tim pengembang.

OWASP ZAP dikenal sebagai alat yang sangat komprehensif karena dilengkapi dengan antarmuka grafis (GUI) yang memudahkan pengguna dalam melakukan pemindaian dinamis. Perangkat ini mampu bertindak sebagai intercepting proxy yang memungkinkan penguji untuk memanipulasi permintaan (request) dari browser ke server secara langsung. Selain itu, *OWASP ZAP* didukung oleh komunitas global yang besar, sehingga basis data kerentanannya selalu diperbarui mengikuti standar keamanan terbaru. Fitur pemindaian aktif dan pasif yang dimilikinya menjadikannya alat favorit untuk pengujian penetrasi pada aplikasi web yang memiliki alur logika yang kompleks.

Di sisi lain, *Nikto* merupakan alat pemindai berbasis baris perintah (CLI) yang telah menjadi standar industri selama bertahun-tahun karena efisiensi dan kecepatannya. Berbeda dengan *ZAP*, *Nikto* lebih fokus pada pemindaian konfigurasi server web, pendeteksian file sensitif yang bocor, serta pengecekan perangkat lunak server yang sudah kedaluwarsa. Alat ini sangat ringan dan dapat diintegrasikan dengan mudah ke dalam skrip otomatisasi keamanan karena tidak membutuhkan sumber daya perangkat keras yang besar. Keunggulan utama *Nikto* terletak pada kemampuannya mendeteksi lebih dari 6700 item berbahaya dan file- file instalasi standar yang seringkali menjadi pintu masuk peretasan.

Berdasarkan fenomena perubahan harga pada planetkomputer.my.id dan perbedaan karakteristik kedua alat tersebut, maka diperlukan penelitian lebih lanjut mengenai efektivitas keduanya. Penelitian ini bertujuan untuk membandingkan akurasi dan kemampuan deteksi antara *OWASP ZAP* dan *Nikto* dalam menemukan kerentanan yang ada pada objek penelitian. Hasil dari penelitian ini diharapkan dapat menjadi panduan bagi administrator website dalam memilih security tools yang paling optimal untuk mengamankan aset digitalnya. Oleh karena itu, penelitian ini diajukan dengan judul "Analisis Komparatif Efektivitas *OWASP* Zed Attack Proxy (*ZAP*) dan *Nikto* dalam Mendeteksi Celah Keamanan pada Web Server planetkomputer.my.id ".

2. Tinjauan Literatur

2.1. Landasan Teori

2.1.1 Keamanan Aplikasi

Keamanan aplikasi web adalah cabang dari keamanan informasi yang berfokus secara khusus pada keamanan situs web, aplikasi web, dan layanan web. Secara prinsip, keamanan web bertujuan untuk melindungi aset digital dari serangan yang mengeksploitasi kerentanan dalam kode aplikasi atau konfigurasi server. Fokus utamanya adalah menjaga tiga pilar utama keamanan informasi, yaitu kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) data.

2.1.2 Vulnerability Assessment (Penilaian Kerentanan)

Vulnerability Assessment adalah proses sistematis untuk mengidentifikasi, mengukur, dan mengklasifikasikan kerentanan keamanan dalam suatu sistem komputer, jaringan, atau infrastruktur komunikasi. Dalam konteks aplikasi web, proses ini melibatkan penggunaan alat pemindai otomatis dan manual untuk menemukan celah yang bisa dieksploitasi oleh penyerang. Hasil dari penilaian ini biasanya berupa daftar kerentanan yang disusun berdasarkan tingkat risiko (Tinggi, Sedang, Rendah).

2.1.3 OWASP Zed Attack Proxy (ZAP)

OWASP ZAP adalah alat pengujian penetrasi terintegrasi yang bersifat open- source untuk menemukan kerentanan pada aplikasi web. ZAP dirancang untuk digunakan oleh orang-orang dengan berbagai latar belakang keamanan, mulai dari pengembang hingga penguji penetrasi profesional. Fitur unggulannya meliputi intercepting proxy, automated scanner, serta kemampuan untuk melakukan spidering (menjelajahi struktur website secara otomatis).

2.1.4 Nikto Web Scanner

Nikto adalah pemindai server web sumber terbuka (GPL) yang melakukan pengujian komprehensif terhadap server web untuk beberapa item, termasuk lebih dari 6700 file/program yang berpotensi berbahaya. Nikto fokus pada pendeteksian item konfigurasi server yang tidak aman, pengecekan versi server yang kedaluwarsa, dan identifikasi masalah pada header HTTP. Alat ini beroperasi melalui command-line interface (CLI), menjadikannya sangat ringan dan cepat.

2.1.5 Severity Level (Tingkat Bahaya)

Severity level adalah skala penilaian yang digunakan untuk menentukan seberapa serius dampak dari suatu kerentanan keamanan jika berhasil dieksploitasi. Biasanya, skala ini dibagi menjadi empat kategori:

a. Critical/High: Risiko besar yang membutuhkan perbaikan segera (misal: kebocoran basis data).
b. Medium: Risiko menengah yang dapat mengganggu fungsi tertentu.
c. Low: Risiko aaaakecil yang sulit dieksploitasi.
d. Informational: Temuan yang bersifat informasi mengenai sistem tanpa risiko keamanan langsung.

2.2 Kajian yang Relevan

2.2.1 Penulis: Aris dkk. (2023)

Judul : Analisis Keamanan Website Instansi Pemerintah Menggunakan Metode OWASP Top 10 dan Penetration Testing.

Metode : Vulnerability Assessment menggunakan OWASP ZAP dengan pendekatan Black-Box.

Hasil : Ditemukan celah kritis berupa SQL Injection dan Sensitive Data Exposure pada 3 dari 5 website yang diuji.

Perbedaan : Penelitian Aris dkk. berfokus pada website profil instansi pemerintah yang bersifat statis, sedangkan penelitian ini berfokus pada website bisnis planetkomputer.my.id yang memiliki fungsi transaksi dan manajemen harga dinamis.

2.2.2 Penulis: Pratama & Wijaya (2022)

Judul : Uji Komparasi Tools Vulnerability Scanner Nikto dan Nessus pada Web Server Berbasis Linux.

Metode : Eksperimen pemindaian pada server Apache dan Nginx.

Hasil : Nikto lebih unggul dalam mendeteksi outdated server software, sedangkan Nessus lebih detail dalam pelaporan manajemen risiko.

Perbedaan : Penelitian tersebut membandingkan Nikto dengan alat komersial (Nessus) untuk performa server, sedangkan penelitian ini membandingkan Nikto dengan OWASP ZAP untuk mendeteksi celah pada level aplikasi web (price list).

2.2.3 Penulis: Gunawan & Setiawan (2022)

Judul : Analisis Kerentanan Website Menggunakan Nikto Web Scanner Berdasarkan Versi Web Server.

Metode : Observasi terhadap berbagai versi OpenSSL dan Apache.

Hasil : Nikto berhasil mengidentifikasi celah Heartbleed dan Poodle pada server yang belum diperbarui (patched).

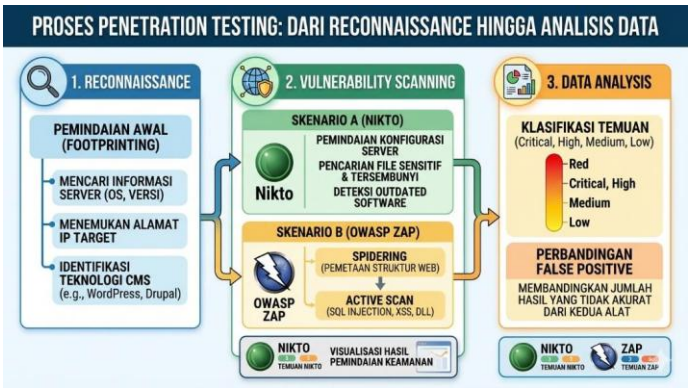
Perbedaan : Gunawan hanya menggunakan satu alat (Nikto) untuk pengecekan versi server, sedangkan penelitian ini melakukan komparasi dua alat untuk menemukan kerentanan logika aplikasi.

3. Metode

Jenis penelitian ini termasuk dalam penelitian terapan (applied research) karena hasil penelitian diharapkan dapat langsung dimanfaatkan oleh pihak Planet Komputer dalam meningkatkan keamanan sistem informasi yang dimiliki. Pendekatan yang digunakan adalah kualitatif-deskriptif, karena penelitian ini tidak hanya berfokus pada hasil numerik, tetapi juga menggambarkan proses penerapan, hasil identifikasi kerentanan, serta rekomendasi mitigasi yang dihasilkan. Melalui pendekatan ini, peneliti dapat menjelaskan secara rinci fenomena yang terjadi di lingkungan sistem web server yang diteliti.

3.1. Metode dan Lokasi Penelitian

Dalam konteks penelitian ini, metodologi berfungsi sebagai panduan dalam identifikasi kerentanan pada *web server planet komputer Kebumen* guna mengidentifikasi kerentanan serta menentukan langkah mitigasi yang tepat. Pengujian dilakukan dengan pendekatan Black-Box Testing, dimana penguji tidak mengetahui kode program internal website. Metodologi yang digunakan mengacu pada fase Information Gathering hingga Analysis. Berikut gambar tahapan metodologi pengujian.



Gambar 1. Proses Pengujian

Gambar diatas menjelaskan alur metodologi pengujian, yaitu:

1. Reconnaissance (Information Gathering): Melakukan footprinting untuk mengetahui informasi server, alamat IP, dan teknologi CMS yang digunakan oleh target.
2. Vulnerability Scanning:
   Skenario A (Nikto): Melakukan pemindaian terhadap konfigurasi server, file sensitif, dan outdated software.
   Skenario B (OWASP ZAP): Melakukan spidering untuk memetakan struktur web, kemudian menjalankan Active Scan untuk mencari celah seperti SQL Injection dan XSS.
3. Data Analysis: Data dari kedua alat diklasifikasikan berdasarkan tingkat bahaya (Critical, High, Medium, Low) dan dibandingkan jumlah False Positive-nya

3.2 Sumber Data

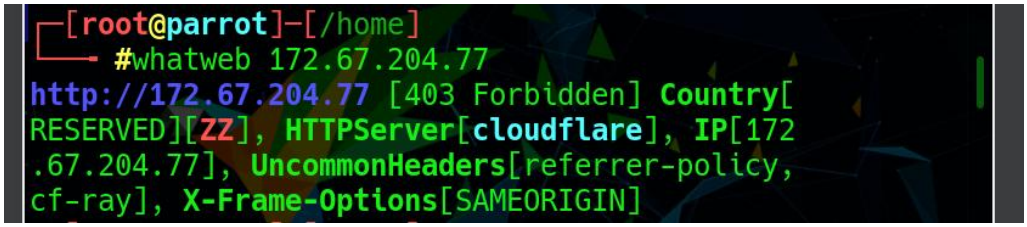
Sumber data dalam penelitian ini dibagi menjadi dua kategori utama:

1. Data Primer:
   Hasil Pemindaian (Scanning): Data mentah berupa log dan laporan temuan kerentanan yang dihasilkan langsung dari running tools OWASP ZAP dan Nikto terhadap target planetkomputer.my.id .
   Observasi Langsung: Data mengenai arsitektur website, teknologi web server, dan fitur-fitur dinamis yang ada pada objek penelitian.
2. Data Sekunder:
   Studi Literatur: Referensi dari jurnal penelitian terdahulu, buku teks mengenai Cybersecurity, dan dokumentasi resmi dari OWASP serta Nikto.
   Basis Data Kerentanan: Referensi dari CVE (Common Vulnerabilities and Exposures) untuk memvalidasi temuan celah keamanan yang dideteksi oleh alat.

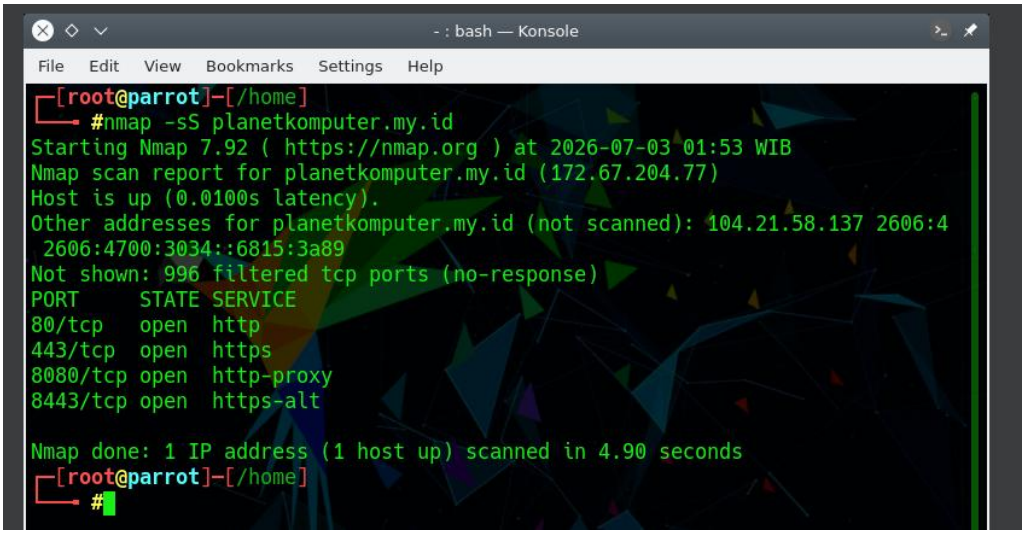
4. Hasil dan Pembahasan

Hasil dan Pembahasan akan menguraikan seluruh rangkaian proses *penetration testing* secara sistematis berdasarkan tiga tahapan utama yang telah dilaksanakan. Pembahasan diawali dengan tahap ***Reconnaissance*** untuk melakukan pemindaian awal berupa pencarian informasi *server, alamat IP*, hingga identifikasi teknologi *CMS* target. Selanjutnya, proses memasuki tahap ***Vulnerability Scanning*** yang mengeksplorasi dua skenario pengujian menggunakan alat pemindai *Nikto dan OWASP ZAP*. Alur pembahasan kemudian diakhiri dengan tahap *Data Analysis* guna mengklasifikasikan tingkat bahaya temuan serta melakukan perbandingan *false positive* dari kedua alat tersebut.

4.1 . Reconnaissance



Gambar 2. Proses Pemindaian *WhatWeb "planetkomputer.my.id"*



Gambar 3. Proses Pemindaian *Nmap "planetkomputer.my.id"*

Gambar 2 adalah hasil Pemindaian *WhatWeb*. Pengujian menggunakan alat *WhatWeb* terhadap alamat IP target 172.67.204.77 yaitu *planetkomputer.my.id* berhasil mengidentifikasi komponen teknologi yang digunakan pada situs web tersebut. Hasil pemindaian menunjukkan respons status kode 403 Forbidden yang menandakan adanya pembatasan akses langsung ke alamat IP tersebut. Selain itu, ditemukan bahwa target menggunakan layanan ***HTTPServer Cloudflare*** yang berfungsi sebagai reverse proxy sekaligus pelindung keamanan situs. Pemindaian ini juga mendeteksi beberapa informasi penting lainnya seperti UncommonHeaders (referrer-policy, cf-ray) serta implementasi keamanan X-Frame-Options berstatus SAMEORIGIN.

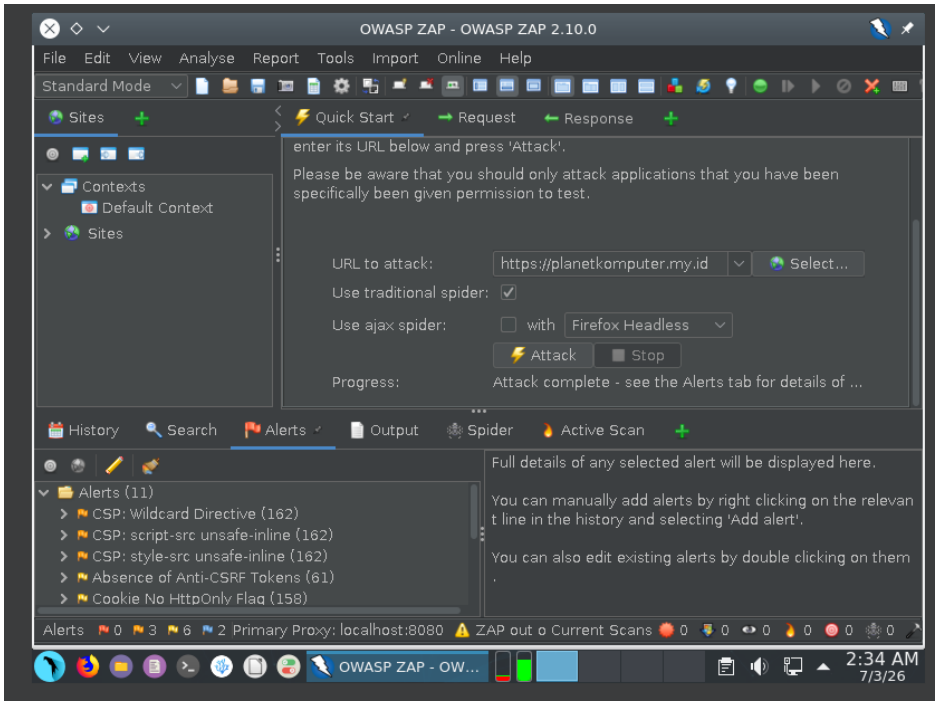
Artinya, situs web target tidak bisa diakses sembarangan secara langsung melalui alamat IP-nya (muncul pesan 403 Forbidden atau akses ditolak). Selain itu, situs ini tidak langsung terhubung ke server asli, melainkan dilindungi di balik layanan Cloudflare (sebuah sistem keamanan dan akselerasi web). Di dalamnya juga sudah terpasang pengaman tambahan (X-Frame-Options) untuk mencegah serangan siber yang mencoba memanipulasi tampilan situs.

Gambar 3 adalah Hasil Pemindaian Nmap dengan perintah nmap *-sS planetkomputer.my.id* berhasil mendeteksi informasi host beserta port yang terbuka menggunakan metode SYN Stealth Scan. Sistem mengidentifikasi bahwa domain tersebut aktif pada IP 172.67.204.77 dengan waktu latensi yang sangat cepat, yaitu sekitar 0.0100 detik. Dari total port yang dipindai, sebanyak 996 port TCP berada dalam status filtered karena tidak memberikan respons akibat proteksi keamanan. Sementara itu, terdapat 4 port utama yang berstatus open (terbuka), yaitu port 80/tcp (http), 443/tcp (https), 8080/tcp (http-proxy), dan port 8443/tcp (https-alt).

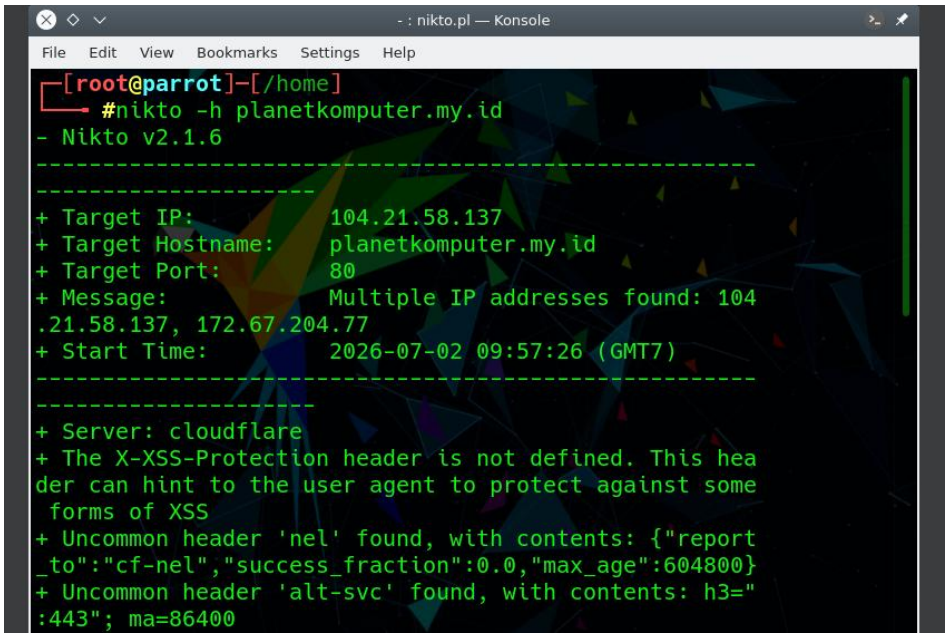
Artinya, sistem mendeteksi bahwa domain target dalam kondisi aktif dan berjalan sangat cepat. Dari ribuan "pintu masuk" (port) yang ada di server tersebut, sistem keamanan target berhasil menyembunyikan atau menyaring (filtered) 996 port agar tidak bisa diintip. Namun, ada 4 pintu utama yang terbuka (open), yaitu jalur untuk lalu lintas web biasa (Port 80 & 8080) serta jalur aman yang terenkripsi (Port 443 & 8443). Pintu-pintu terbuka inilah yang biasanya

menjadi jalur masuk utama bagi pengguna, sekaligus menjadi celah yang akan diuji lebih lanjut oleh seorang penetration tester.

4.2 Vulnerability Scanning



Gambar 4. Proses Pemindaian *OWASP ZAP "planetkomputer.my.id"*



Gambar 5. Proses Pemindaian *Nikto "planetkomputer.my.id"*

Gambar 4 adalah Hasil Pemindaian OWASP ZAP. Proses pemindaian menggunakan OWASP ZAP terhadap target https://planetkomputer.my.id menggunakan fitur Traditional Spider telah selesai dilaksanakan sepenuhnya (Attack complete). Berdasarkan ringkasan pada tab Alerts, sistem mendeteksi total 11 peringatan celah keamanan yang dikelompokkan berdasarkan bendera tingkat risiko. Temuan tersebut didominasi oleh masalah konfigurasi pada Content Security Policy (CSP) seperti aturan Wildcard Directive, serta penggunaan

unsafe-inline pada elemen script dan style. Selain itu, ditemukan pula celah risiko berupa hilangnya token anti-CSRF (Absence of Anti-CSRF Tokens) serta ketiadaan parameter HttpOnly pada konfigurasi cookie target.

Artinya, sistem mendeteksi adanya kelemahan dalam pengaturan keamanan internal situs web. Masalah pada CSP (Content Security Policy) berarti situs kurang ketat dalam mengatur kode luar mana saja yang boleh berjalan, sehingga rentan disisipi kode palsu. Hilangnya Token Anti-CSRF berarti penyerang berpotensi memanipulasi tindakan pengguna (seperti klik jebakan), sementara ketiadaan parameter HttpOnly pada cookie membuat data sesi login pengguna berisiko dicuri oleh skrip jahat.

Gambar 5 adalah Hasil Pemindaian Nikto. Pengujian kerentanan menggunakan alat Nikto v2.1.6 dijalankan melalui perintah nikto -h planetkomputer.my.id dengan menargetkan port default 80. Dari hasil pemindaian awal, alat ini berhasil mengonfirmasi bahwa target berada di balik server Cloudflare dan mendeteksi adanya penggunaan beberapa alamat IP publik yang berbeda. Informasi keamanan penting yang berhasil diidentifikasi adalah tidak ditemukannya konfigurasi proteksi serangan Cross-Site Scripting pada header (The X-XSS-Protection header is not defined). Di samping ketiadaan pengaman XSS tersebut, Nikto juga berhasil mengekstrak beberapa konten dari informasi uncommon header yang aktif, yaitu header 'nel' dan 'alt-svc'.

Artinya, server target dikonfirmasi menggunakan pelindung Cloudflare dan memiliki lebih dari satu alamat IP. Namun, dari sisi konfigurasi, server ini dinyatakan tidak memiliki pelindung XSS (X-XSS-Protection tidak diatur), yang berarti server tidak memerintahkan peramban (browser) pengguna untuk memblokir jika ada serangan siber jenis Cross-Site Scripting. Sementara penemuan header 'nel' dan 'alt-svc' adalah informasi tambahan yang menunjukkan bagaimana server tersebut mengatur laporan eror jaringan dan pengalihan jalur alternatif.

4.3 Data Analysis

Pada tahapan ini, dilakukan analisis dan klasifikasi terhadap seluruh temuan kerentanan (*alerts*) yang berhasil dideteksi oleh OWASP ZAP dan Nikto pada web server planetkomputer.my.id. Proses klasifikasi ini merujuk pada standar tingkat keparahan risiko risiko keamanan (*Severity Level*) yang dibagi menjadi *High*, *Medium*, *Low*, dan *Informational/Informasi*. Selain melakukan klasifikasi, tahapan ini juga menganalisis efektivitas serta perbandingan hasil dari kedua alat uji untuk melihat kesamaan (*overlap*) maupun perbedaan indikasi celah keamanan yang ditemukan. Tabel di bawah ini merangkum seluruh hasil temuan beserta klasifikasi tingkat risiko dari kedua *tools*:

Tabel 1. Klasifikasi dan Komparasi Temuan Kerentanan

No	Nama Kerentanan / Temuan Keamanan	Tools yang Mendeteksi	Klasifikasi Risiko (Severity)	Potensi Dampak / Arti Temuan
1	**Absence of Anti-CSRF Tokens**	OWASP ZAP	**Medium**	Kerentanan di mana aplikasi web tidak memvalidasi token unik saat pengguna melakukan aksi sensitif, sehingga penyerang dapat memicu transaksi ilegal atas nama korban (*Cross-Site Request Forgery*).
2	**The X-XSS-Protection Header is not Defined**	Nikto	**Low**	Server tidak mengirimkan instruksi kepada *browser* untuk mengaktifkan filter penyaringan bawaan terhadap serangan pemalsuan skrip lintas situs (*Cross-Site Scripting*).
3	**Cookie No HttpOnly Flag**	OWASP ZAP	**Low**	*Cookie* sesi login tidak dikunci dengan parameter *HttpOnly*, yang berarti data sesi tersebut rentan dicuri apabila

				penyerang berhasil mengeksekusi skrip jahat (*XSS*) di sisi klien.
4	**CSP: Wildcard Directive**	OWASP ZAP	**Low**	Kebijakan keamanan konten (*Content Security Policy*) menggunakan tanda bintang/wildcard (*), sehingga memberikan izin yang terlalu longgar bagi server untuk memuat aset dari sumber mana saja.
5	**CSP: script-src unsafe-inline**	OWASP ZAP	**Low**	Konfigurasi CSP yang memperbolehkan penulisan kode JavaScript langsung di dalam elemen HTML (*inline*), yang secara tidak langsung melemahkan pertahanan terhadap serangan injeksi skrip.
6	**CSP: style-src unsafe-inline**	OWASP ZAP	**Low**	Konfigurasi CSP yang memperbolehkan manipulasi gaya tampilan secara langsung (*inline CSS*), meningkatkan risiko gangguan visual atau eksploitasi elemen desain.
7	**Uncommon Header 'nel' Found**	Nikto	**Informational**	Penemuan informasi *header Network Error Logging* yang memberikan rincian teknis tentang bagaimana server melaporkan kegagalan jaringan kepada pihak luar.
8	**Uncommon Header 'alt-svc' Found**	Nikto	**Informational**	Penemuan informasi mengenai ketersediaan protokol jaringan alternatif (seperti HTTP/3) yang didukung oleh server.
9	**Uncommon Headers ('referrer-policy', 'cf-ray')**	OWASP ZAP / WhatWeb	**Informational**	*Header* yang mengidentifikasi kebijakan rujukan (*referrer*) serta penanda pelacakan jaringan internal dari infrastruktur Cloudflare.

Analisis Komparatif Efektivitas Temuan:

Karakteristik Deteksi: OWASP ZAP terbukti lebih efektif dan mendalam dalam mendeteksi kelemahan di level logika aplikasi web dan sesi (seperti Anti-CSRF dan status HttpOnly flag pada cookie). Sebaliknya, Nikto lebih sensitif dalam mengidentifikasi miskonfigurasi pada level header web server dan informasi mentah server (Uncommon Headers).

Korelasi Temuan (Overlap): Kedua tools secara tidak langsung mendeteksi area kelemahan yang sama pada proteksi Cross-Site Scripting (XSS). OWASP ZAP menemukannya lewat celah kelonggaran konfigurasi CSP (unsafe-inline), sementara Nikto menemukannya lewat ketiadaan *header X-XSS-Protection*. Hal ini menunjukkan bahwa kedua alat saling melengkapi dalam mengonfirmasi bahwa web server target memang memiliki proteksi minimal terhadap ancaman manipulasi skrip.

Langkah mitigasi

Berikut adalah format tabel mitigasi dan rekomendasi perbaikan untuk keamanan web server *planetkomputer.my.id* agar penulisan di dalam Bab 4 skripsi Anda terlihat lebih sistematis, rapi, dan mudah dievaluasi:

Tabel 2. Langkah Mitigasi untuk perbaikan Web Planet Komputer

No	Nama Kerentanan	Klasifikasi Risiko	Langkah Mitigasi / Solusi Teknis	Target Komponen

1	**Absence of Anti-CSRF Tokens**	**Medium**	Mengintegrasikan token kriptografi yang unik, acak, dan berbasis sesi (*nonce*) pada setiap komponen formulir (*form*) aplikasi web. Server harus memvalidasi token ini pada setiap permintaan *POST/PUT* untuk mencegah manipulasi transaksi pihak ketiga.	Aplikasi Web / *Source Code*
2	**Cookie No HttpOnly Flag**	**Low**	Memperbarui konfigurasi manajemen sesi di server dengan menambahkan atribut HttpOnly dan Secure pada *header* Set-Cookie. Hal ini memastikan *cookie* tidak dapat diintip oleh skrip JavaScript klien dan hanya dikirim via jalur HTTPS.	Konfigurasi Web Server / Sesi
3	**CSP: Wildcard Directive & Unsafe-Inline**	**Low**	Memperketat konfigurasi *Content Security Policy* (CSP) dengan menghapus tanda bintang (*) dan parameter unsafe-inline. Sumber skrip dan gaya harus didefinisikan secara eksplisit (hanya dari domain tepercaya) atau menggunakan mekanisme *nonce/hash*.	*Header* Respons Web Server

6. Kesimpulan

Berdasarkan hasil analisis komparatif, dapat disimpulkan bahwa pengujian keamanan pada web server planetkomputer.my.id berhasil mengidentifikasi sejumlah celah keamanan dengan tingkat risiko Medium hingga Low, seperti absennya token Anti-CSRF, ketiadaan flag HttpOnly pada cookie, serta kelemahan konfigurasi header CSP dan XSS. Dalam mendeteksi celah-celah tersebut, OWASP ZAP terbukti sangat efektif dan mendalam untuk memeriksa kelemahan pada logika aplikasi serta manajemen sesi pengguna. Di sisi lain, Nikto menunjukkan keunggulan dalam memindai miskonfigurasi arsitektur server, ketiadaan header proteksi, serta kebocoran informasi teknis pada level jaringan. Dengan demikian, penerapan kedua alat ini terbukti saling melengkapi dalam memberikan evaluasi keamanan yang menyeluruh guna merumuskan rekomendasi mitigasi yang tepat bagi target.

Ucapan Terima Kasih:

Ucapan terimakasih disampaikan kepada pihak Universitas Ma'arif Nahdlatul Ulama Kebumen atas dukungan serta fasilitas yang telah diberikan selama pelaksanaan penelitian ini. Penulis juga mengucapkan terimakasih yang sebesar-besarnya kepada dosen pembimbing, bapak Fahmi Fachri, S.M., M.Kom., atas bimbingan, arahan, serta masukan yang sangat membantu dalam penyusunan dan penyelesaian penelitian ini, selanjutnya untuk Planet Komputer terimakasih sudah di inzikan untuk riset pada website nya Semoga segala ilmu dan kebaikan yang diberikan mendapatkan balasan yang setimpal. Selain itu, penulis menyampaikan rasa terimakasih yang tulus kepada kedua orang tua atas dukungan, doa, serta motivasi yang tiada henti selama proses penyusunan jurnal ini. Dukungan tersebut menjadi kekuatan utama bagi penulis dalam menyelesaikan penelitian ini dengan baik. Penulis juga mengucapkan terimakasih kepada seluruh pihak yang telah membantu dan berkontribusi, baik secara langsung maupun tidak langsung, dalam proses penelitian ini sehingga dapat terselesaikan dengan baik.Sebagai penutup, penulis juga mengapresiasi diri sendiri atas usaha, ketekunan, dan komitmen dalam menyelesaikan penelitian ini hingga akhir. Semoga hasil yang dicapai dapat memberikan manfaat dan menjadi langkah awal untuk pengembangan penelitian selanjutnya

Referensi

[1] A. Rochman, R. R. Salam, dan S. A. M., "ANALISIS KEAMANAN WEBSITE DENGAN INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK (ISSAF) DAN OPEN WEB APPLICATION SECURITY PROJECT (OWASP) DI RUMAH SAKIT XYZ," *Pharmacognosy Magazine*, vol. 75, no. 17, hal. 399–405, 2021.

[2] M. Amirul, N. Tristanti, G. Pramuja, dan I. Fanani, "Analisis dan Pengujian Kerentanan Website Menggunakan OWASP ZAP," vol. 3, no. 1, hal. 36–50, 2024.

[3] S. Andriansyah dan Nurhasanah, "Analisis Keamanan Website SMP Negeri 2 Bagan Sinembah Dengan Framework ISSAF (Studi Kasus : SMP Negeri 2 Bagan Sinembah) Elpi. Konsep Desain Menentukan Hull Type, Material, Dan Propulsi Unmanned Surface Vehicle (Usv) Untuk Patroli Di Wilayah Rokan Hiir Dengan Metode Desicion Tree, Lcm," hal. 478–486, 2020.

[4] S. Andriyani, M. F. Sidiq, dan B. P. Zen, "Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework Issaf Pada Website SMK Al-Kautsar," *Journal Informatic and Information Technology*, hal. 1–13, 2023.

[5] U. N. Cendana, A. History, dan S. Chain, "Optimalisasi Transformasi Digital dalam Pengelolaan Supply Chain Perusahaan," vol. 4, hal. 186–192, 2025.

[6] F. Cobit dan P. Telkom, "AUDIT TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN," *Jurnal Software Engineering and Information System (SEIS)*, vol. 4, no. 2, 2024.

[7] N. D. Darno dan E. L. Tjiong, "Analisis Celah Keamanan Pada Website PDDIKTI Menggunakan Metode Penetration Testing Dan Framework ISSAF," vol. 12, no. 02, hal. 1–13, 2025.

[8] F. N. Dhanendra dan A. Sujarwo, "Strategi Keamanan pada Sistem Bank Air Kami v2 menggunakan Trias CIA," vol. 4, hal. 1048–1062, 2024.

[9] S. EkoPrasetyo dan N. Hassanah, "Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode Issaf," *Jurnal Ilmiah Informatika*, vol. 9, no. 02, hal. 82–86, 2021, doi: 10.33884/jif.v9i02.3758.

[10] F. Fachri, "Optimasi Keamanan Web Server Terhadap Serangan Brute-Force Menggunakan Penetration Testing," *Jurnal Teknologi Informasi Dan Ilmu Komputer*, vol. 10, no. 1, hal. 51–58, 2023, doi: 10.25126/jtiik.20231015872.

[11] "Framework Integrasi Digital Forensic Readiness dan Information Security Management System di lingkungan Pemerintahan," 2024.

[12] H. S. Harahap, A. A. Rahman, I. Suraswati, dan S. N. Neyman, "Memahami Cara Kerja Phishing menggunakan Tools pada Kali Linux," *Journal of Internet and Software Engineering*, vol. 1, no. 2, hal. 1–11, 2024.

[13] H. Herman, I. Riadi, Y. Kurniawan, dan I. A. Rafiq, "Analisis Keamanan Website Menggunakan Information System Security Asessment Framework (ISSAF)," *Jurnal Teknologi Informatika Dan Komputer*, vol. 9, no. 1, hal. 126–136, 2023, doi: 10.37012/jtik.v9i1.1439.

[14] M. O. Hoshmand dan S. Ratnawati, "Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity," vol. 5, no. 2, hal. 679–686, 2023.

[15] M. Issaf, "Analisis dan Rekomendasi Keamanan Website Kampus X," vol. 6, no. 1, hal. 830–843, 2025.

[16] M. F. Issaf dan M. Koprawi, "Analisis Keamanan Website Pada Instansi XYZ Melalui Penetration Testing," vol. 5, no. 1, hal. 547–555, 2025.

[17] M. Khairi, B. Rianto, dan M. Jalil, "Pengaruh teknologi dalam transformasi ekonomi dan bisnis di era digital 1," vol. 7, hal. 71–78, 2025.

[18] H. Nasution dan A. Abdul, "Analisis Performa Web server Apache dan Go Pada Protokol HTTP (Hypertext Transfer Protocol) Performance Analysis of Apache and Go Web servers on HTTP Protocol (Hypertext Transfer Protocol)," vol. 02, no. 2, 2024, doi: 10.26418/juara.v2i2.81914.

[19] S. A. Nugroho dan T. Rochmadi, "Analisis Keamanan Sistem Informasi Pusaka Magelang Menggunakan Open Web Application Security Project (OWASP) Dan Information Systems Security Assessment Framework (ISSAF) Security Analysis Of Magelang Pusaka Information System Using Open Web Application Security Project (OWASP) And Information Systems Security Assessment Framework (ISSAF)," vol. 7, no. 1, hal. 56–61, 2024.

[20] M. Amirul, Y. Safitri, dan S. Saputra, "Analisis Keamanan Sistem Informasi Akademik XYZ Menggunakan Information System Security Assessment Framework (ISSAF) Security Analysis of XYZ Academic Information System Using Information System Security Assessment Framework (ISSAF)," *Jurnal Pengembangan*, vol. 1, hal. 50–60, 2025.

[21] H. Sandhiyadini Rosari, M. Syaibani Al Hakim, E. Sibagariang, A. Rosadi Kardian, dan P. Siber dan Sandi Negara, "Analisis Kecepatan MySQL dan PostgreSQL pada Windows 11 dan Kali Linux 2022," *Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)*, vol. 8, hal. 213–222, 2023.

[22] E. P. Silmina, A. Firdonsyah, dan R. A. A. Amanda, "Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetration Test Dan Issaf," *Transmisi*, vol. 24, no. 3, hal. 83–91, 2022, doi: 10.14710/transmisi.24.3.83-91.

[23] Z. M. Subekti, K. Mukiman, M. Lutfi, S. Auliya, R. E. Putra, dan U. B. Saleh, "RANCANG BANGUN INFRASTRUKTUR WEB SERVER," vol. 2, no. 1, hal. 144–151, 2024.

[24] M. Tahir dan M. Risky, "Analisis Keamanan Website Dinas Pemerintahan Yogyakarta Dengan Metode PTES (Penetration Testing Execution Standard)," vol. 09, hal. 118–125, 2024.

[25] F. M. H. Tjiptabudi dan R. I. Ndaumanu, "Evaluasi Celah Keamanan Website Dana Pensiun X Melalui Penetration Testing Berdasarkan ISSAF Framework," *Jurnal Algoritma*, vol. 21, no. 2, hal. 9–17, 2024, doi: 10.33364/algoritma/v.21-2.1644.

[26] A. W. Wardhana dan H. B. Seta, "Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode ISSAF pada Website Universitas XYZ," *Informatik: Jurnal Ilmu Komputer*, vol. 17, no. 3, hal. 226, 2021, doi: 10.52958/iftk.v17i3.3653.