Alat OSINT Berbasis *Web* untuk Deteksi URL *Phishing* Menggunakan Integrasi API

A Web-Based OSINT System for Detecting Phishing URLs via API Integration

Alfian Syahli*[1], Rezki Kurniati[2], Nurmi Hidayasari[3]
[1,2,3]Jurusan Teknik Informatika, Politeknik Negeri Bengkalis
E-mail: [1]alfiansyahli435@gmail.com, [2]rezki@polbeng.ac.id, [3]nurmihidayasari@polbeng.ac.id*
**Corresponding author*
Received 18 July 2025; Revised 6 August 2025; Accepted 12 August 2025

Abstrak-*Phishing* merupakan teknik kejahatan siber yang memanfaatkan rekayasa sosial untuk mencuri data sensitif, seperti kredensial *login* dan informasi keuangan. Kesulitan dalam mendeteksi URL *phishing* yang sering kali tersamarkan menjadi permasalahan utama. Penelitian ini menawarkan solusi berupa alat *Open Source Intelligence* (OSINT) berbasis *web* yang dibangun menggunakan *framework Laravel* dan bahasa pemrograman PHP. Alat ini mengintegrasikan tiga API, *VirusTotal*, *WhoisXML*, dan *ip-api*—untuk memverifikasi keamanan URL secara otomatis. Dengan menggunakan metodologi *waterfall* untuk pengembangan dan siklus hidup OSINT untuk operasional, sistem ini mampu melakukan analisis mendalam terhadap URL yang diinput pengguna. Hasil pengujian kuantitatif terhadap 80 URL menunjukkan tingkat akurasi deteksi sebesar 98,75%, dengan hanya satu kasus *false positive*. Luaran dari penelitian ini adalah sebuah alat OSINT yang tidak hanya mampu mendeteksi URL *phishing* secara akurat, tetapi juga menyediakan laporan analisis mendetail, informasi domain, serta fitur edukasi berupa panduan dan kuis interaktif untuk meningkatkan kesadaran pengguna terhadap ancaman siber.

Kata Kunci : *Phishing, Open Source Intelligence, Application Programming Interface*, *Website* Deteksi URL *Phishing*, *Framework Laravel*

Abstract-*Phishing is a cybercrime technique that utilizes social engineering to steal sensitive data, such as login credentials and financial information. The primary challenge lies in the difficulty of detecting convincingly disguised phishing URLs. This research offers a solution in the form of a web-based Open Source Intelligence (OSINT) tool built with the Laravel framework and PHP programming language. The tool integrates three APIs—VirusTotal, WhoisXML, and ip-api—to automatically verify URL security. Employing a waterfall methodology for development and the OSINT lifecycle for its operational core, the system performs in-depth analysis on user-submitted URLs. Quantitative testing on a dataset of 80 URLs demonstrated a detection accuracy rate of 98.75%, with only a single false positive case. The output of this research is a web-based OSINT tool that not only accurately detects phishing URLs but also provides detailed analysis reports, domain intelligence, and educational features, including a phishing guide and an interactive quiz, to enhance user awareness of cyber threats.*

Keywords **:** *Phishing, Open Source Intelligence, Application Programming Interface, Phishing URL Detection Website, Laravel Framework*

1. PENDAHULUAN

Website dapat diartikan sebagai sekumpulan halaman yang menyajikan berbagai jenis informasi, termasuk teks, gambar, animasi, suara, video, atau kombinasi dari semuanya, baik yang bersifat statis maupun dinamis. Halaman-halaman ini terhubung satu sama lain melalui jaringan, membentuk struktur yang saling terkait. Inilah yang menjadikan *website* sebagai media informasi yang paling tepat, cepat, dan akurat, karena setiap informasi yang ditampilkan di halaman-halamannya dapat disampaikan dengan jelas dan saling melengkapi, sehingga memudahkan

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i3.13769

pemahaman pengguna [1]. *Phishing* merupakan strategi penipuan siber yang memanfaatkan rekayasa sosial untuk mengelabui korban agar menyerahkan informasi sensitif dengan menyamar sebagai entitas terpercaya [2]. Serangan *phishing* dapat dilakukan melalui alamat *email*, port terbuka, dan peramban *web* yang tidak aman [3]. Serangan ini dapat mengakibatkan dampak fatal seperti pencurian identitas, pelanggaran privasi, dan kerugian finansial yang signifikan, serta merusak reputasi dan mengganggu kestabilan di ruang siber [4].

Untuk menghadapi ancaman yang dinamis ini, penelitian ini mengusulkan pendekatan yang didasarkan pada kerangka kerja *Open Source Intelligence* (OSINT). *Open Source Intelligence* (OSINT) merupakan intelijen yang berasal dari berbagai sumber terbuka dan publik seperti media massa, internet, dan basis data publik, yang dikumpulkan dan diolah untuk disampaikan secara cepat kepada pihak yang membutuhkan guna memenuhi kebutuhan intelijen yang spesifik [5]. Dengan memanfaatkan OSINT, dimungkinkan untuk membangun alat pertahanan yang proaktif dengan mengagregasi informasi dari berbagai sumber data keamanan yang tersedia untuk umum.

Tinjauan terhadap sejumlah penelitian terkait menunjukkan bahwa upaya untuk mendeteksi dan memerangi serangan *phishing* telah menghasilkan beragam metode dan pendekatan. Sebagai contoh, pendekatan berbasis *machine learning* menjadi fokus utama banyak peneliti, dengan perbandingan berbagai algoritma klasifikasi untuk menemukan model yang paling optimal. Penelitian yang dilakukan oleh Mahmud dan Wirawan, membandingkan algoritma *Decision Tree*, *Random* Forest, dan *K-Nearest Neighbors* (KNN), di mana hasilnya menunjukkan Random *Forest* memiliki performa terbaik dengan akurasi 83,4% [6]. Keunggulan *Random Forest* juga ditegaskan dalam penelitian Windarni, dkk, yang setelah menerapkan seleksi fitur *Pearson Correlation*, menemukan bahwa Random *Forest* mencapai akurasi tertinggi sebesar 96,3% [7]. Studi lain oleh Muhammad Fahri (2025) yang berfokus pada Random *Forest* juga memperoleh hasil yang sangat efektif dengan akurasi mencapai 98,20% [8].

Penelitian Muhammad Rahul juga berkontribusi dalam eksplorasi ini dengan mengembangkan aplikasi deteksi *phishing* berbasis *web* menggunakan Algoritma *Decision Tree*. Hasil penelitiannya menunjukkan bahwa penggunaan algoritma tersebut secara signifikan meningkatkan akurasi deteksi *phishing*, mampu mengatasi kekurangan akurasi pada alat yang sudah ada [9]. Serupa dengan itu, Ryan Putra Ramadhan dan Teti Desyani menerapkan Algoritma J48 untuk identifikasi situs *phishing*. Hasilnya menunjukkan bahwa algoritma J48 mampu meningkatkan akurasi dan keandalan deteksi, meskipun membutuhkan data yang berkualitas dan bervariasi untuk mencapai hasil yang optimal [10].

Studi komparatif yang lebih luas dilakukan oleh Fauzan, dkk yang menguji *Naïve Bayes*, *Random Forest*, dan *Decision Tree*, di mana *Random Forest* kembali menjadi yang terbaik dengan akurasi 97,2% [11]. Sementara itu, Indriani, dkk mengeksplorasi algoritma yang lebih kompleks dan menemukan bahwa *Gradient Boosting* memberikan hasil terbaik dengan akurasi sempurna 100% dan waktu komputasi tercepat [12]. Algoritma lain juga dieksplorasi, seperti dalam penelitian "Aplikasi Pendeteksi Situs *Phising* Berbasis *Website* Menggunakan Metode *Naïve Bayes*", yang berhasil mengembangkan aplikasi dengan hasil memuaskan, mencapai akurasi 98% pada data *training* dan 96% pada data *testing* [13]. Ada pula penelitian "Aplikasi Pendeteksi *Website Phishing* Menggunakan *Machine Learning*" yang menggunakan algoritma *Support Vector Machine* (SVM). Hasil dari penelitian tersebut menunjukkan bahwa penggunaan SVM mampu mencapai akurasi deteksi terbaik sebesar 85.71% [14].

Tantangan dataset yang tidak seimbang juga menjadi perhatian. Nugraha, dkk, menerapkan metode *ensemble* dan menemukan bahwa pada dataset *binary class*, *Random Forest* menjadi yang terbaik (akurasi 96,4%), sedangkan pada dataset *multiclass*, metode *Stacking* lebih unggul (akurasi 88,8%) [15]. Pendekatan *deep learning* juga diterapkan oleh Handoyo dan Putra, menggunakan *Long Short-Term Memory* (LSTM), yang hasilnya menunjukkan kinerja baik pada kelas mayoritas namun menurun pada kelas minoritas seperti *phishing* (*recall* 55%), menyoroti pentingnya penanganan data yang tidak seimbang [16]. Selanjutnya, penelitian "Aplikasi Deteksi

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i3.13769

Phising Berbasis *Android*" dirancang untuk melindungi pengguna perangkat seluler dari SMS *phishing*. Hasilnya menunjukkan bahwa aplikasi tersebut dapat digunakan dengan akurasi yang baik, namun masih memerlukan penelitian lebih lanjut untuk meningkatkan performa deteksinya [17].

Di sisi lain, pendekatan yang berbasis *Open Source Intelligence* (OSINT) menawarkan perspektif yang berbeda. Penelitian "*OSINT-based Email Analyzer for Phishing Detection*" mengembangkan sebuah alat analisis *email*. Hasilnya adalah sebuah alat yang dapat membantu mengidentifikasi *email* berpotensi berbahaya dengan tingkat akurasi yang memadai, berkontribusi pada pencegahan proaktif [18]. Menariknya, OSINT tidak hanya digunakan untuk bertahan. Penelitian "*Phishing Attacks Facilitated by Open-Source Intelligence*" membuktikan bahwa alat-alat OSINT dapat digunakan untuk mengumpulkan informasi dan menciptakan serangan *phishing* yang sangat kredibel dan efektif. Hal ini diperkuat oleh studi "*A Toolkit for Security Awareness Training against Targeted Phishing*", di mana OSINT digunakan untuk membuat *email* simulasi yang disesuaikan untuk pelatihan keamanan. Hasilnya, *toolkit* tersebut mampu meningkatkan kredibilitas *email phishing* simulasi, sehingga pelatihan menjadi lebih efektif [19].

Meskipun penelitian-penelitian tersebut memberikan kontribusi berharga dalam deteksi *phishing* menggunakan *machine learning* atau penerapan OSINT untuk tujuan spesifik seperti analisis *email* dan pelatihan, terdapat celah penelitian (*research gap*) yang jelas: kurangnya sebuah alat terpadu berbasis *web* yang dapat diakses publik yang tidak hanya bergantung pada satu jenis analisis, melainkan secara aktif mensintesis beberapa aliran intelijen yang berbeda secara *real-time*. Banyak metode yang ada berfokus pada analisis fitur URL statis atau data historis, yang mungkin kurang efektif terhadap serangan *zero-day* yang polanya belum dikenali.

Kebaruan (*novelty*) utama dari penelitian ini adalah mengisi celah tersebut dengan mengimplementasikan kerangka kerja OSINT secara praktis melalui sintesis tiga API yang saling melengkapi: *VirusTotal* untuk reputasi ancaman, *WhoisXML* untuk intelijen historis domain, dan *ip-api* untuk intelijen geolokasi jaringan. Kontribusi utamanya bukan pada penciptaan algoritma baru, melainkan pada integrasi dan penyajian data intelijen multi-sumber ini ke dalam sebuah alat berbasis *web* yang mudah digunakan. Pendekatan ini mengubah proses deteksi dari sekadar klasifikasi biner (aman/berbahaya) menjadi penyediaan laporan intelijen kontekstual yang mendalam, serta memberdayakan pengguna melalui fitur edukasi tambahan dalam bentuk kuis dan informasi terkait phishing untuk meningkatkan kesadaran keamanan siber.

Penelitian ini mengisi celah tersebut dengan mengusulkan sebuah inovasi berupa alat berbasis *web* yang dibangun menggunakan *framework Laravel*, yang mengadopsi arsitektur MVC (*Model-View-Controller*). *Laravel*, sebagai kerangka kerja PHP berlisensi MIT, meningkatkan kualitas *software* dengan mengurangi biaya pengembangan dan perawatan serta meningkatkan pengalaman pengguna melalui sintaks yang mudah dipahami dan efisien [20]. Selain itu, *Laravel* juga meningkatkan keamanan aplikasi dengan melindungi dari serangan siber seperti *SQL Injection*, *cross-site request forgery*, dan *data tempering* [21]. Sedangkan PHP sebagai bahasa pemrograman *server-side open-source*, memungkinkan pengguna untuk mengubah dan mengembangkan aplikasi atau sistem sesuai kebutuhan mereka [9]. Kontribusi utama dari penelitian ini bukanlah pada penggunaan teknologi *web* tersebut, melainkan pada sintesis tiga aliran intelijen yang berbeda melalui integrasi API, *VirusTotal* yang merupakan layanan pemindaian file dan aplikasi yang menggunakan sekitar 60 pemindai antivirus untuk melabeli konten berbahaya berdasarkan *hash* yang diunggah pengguna [22]. *WhoisXML* menyediakan akses ke 15,6 miliar catatan historis *WHOIS*, yang digunakan untuk meneliti asal-usul *Non-Existent Domains* (*NXDomains*), terutama yang berasal dari domain kedaluwarsa [23]. Terakhir, *ip-api* adalah layanan geolokasi yang terintegrasi dalam sistem *IWAEAIT* untuk melacak lokasi geografis (negara, kota) pengirim email *phishing* melalui alamat IP-nya, yang diekstrak dari *header email* [24]. Dengan integrasi API, aplikasi dapat otomatis memeriksa keamanan URL yang dimasukkan pengguna. Jika sebuah URL terdeteksi berbahaya, sistem akan langsung

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i3.13769

memberikan peringatan. API berfungsi sebagai jembatan yang memungkinkan aplikasi berkomunikasi dengan layanan lain tanpa perlu tahu detail teknis implementasinya [25].

2. METODE PENELITIAN

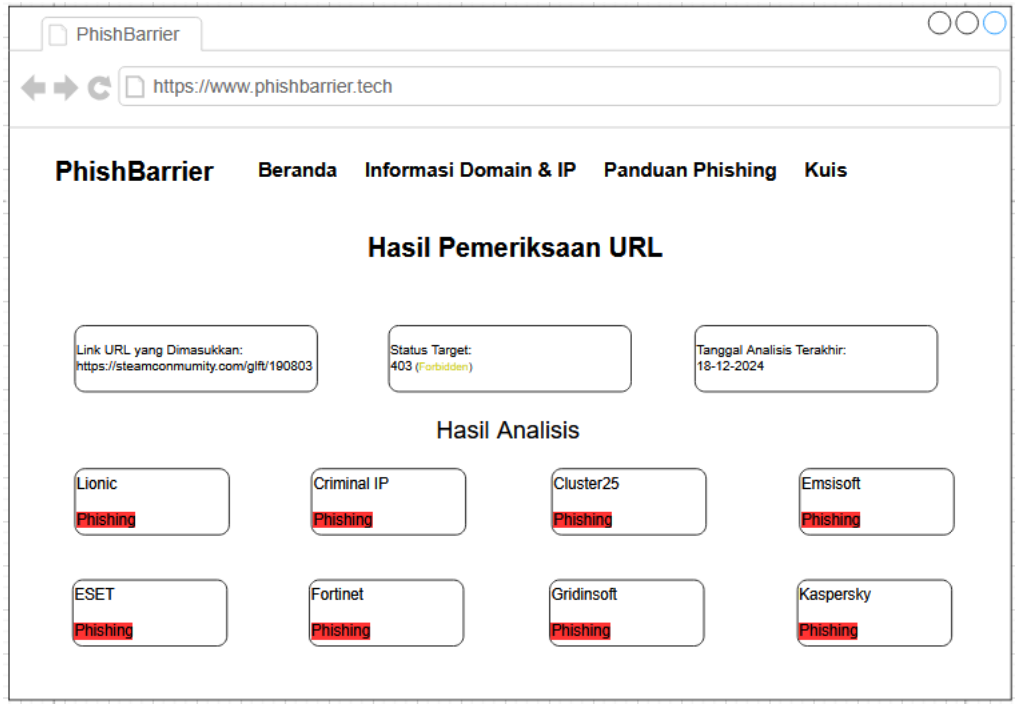
Pendekatan pengembangan sistem secara keseluruhan menggunakan metodologi *waterfall*. Metode *Waterfall* adalah sebuah pendekatan dalam pengembangan sistem di mana setiap fase dilaksanakan secara berurutan [26]. Model ini dipilih karena sifat proyek yang memiliki tujuan dan ruang lingkup yang jelas, mengintegrasikan serangkaian API yang telah ditentukan ke dalam sebuah aplikasi *web*. Pendekatan sekuensial dari *waterfall* yang dimulai dari tahap awal pengembangan sistem hingga melalui seluruh proses analisis, desain, pengkodean, pengujian, dan pemeliharaan memastikan bahwa setiap tahap diselesaikan dengan matang sebelum melanjutkan ke tahap berikutnya [27].

Sementara model *waterfall* berfungsi sebagai kerangka kerja manajemen proyek, operasional inti dari alat ini yang dirancang berdasarkan siklus hidup OSINT. Didalam OSINT terdapat 4 tahapan, yaitu *collection*, *processing*, *exploitation*, dan *production* [5]. Implementasi siklus ini dalam alat adalah sebagai berikut:

1. *Collection* (Pengumpulan Data): Tahap ini dimulai ketika pengguna memasukkan sebuah URL yang dicurigai ke dalam antarmuka web. Pada tahap ini, sistem mengumpulkan data primer (URL target) dari pengguna. Untuk keperluan pengujian dan validasi sistem, data URL juga dikumpulkan dari sumber publik yang menyediakan daftar URL *phishing* aktif, seperti *OpenPhish*, untuk memastikan sistem diuji terhadap ancaman dunia nyata yang relevan.
2. *Processing* (Pemrosesan Data): Setelah URL diterima, sistem melakukan pemrosesan awal. Data mentah (URL) diubah menjadi format yang dapat digunakan oleh layanan eksternal. URL yang dimasukkan akan dinormalisasi untuk memastikan formatnya sesuai standar yang dibutuhkan oleh setiap API, lalu di-*encode* menggunakan Base64 sesuai spesifikasi API *VirusTotal* untuk proses identifikasi yang aman.
3. *Exploitation* (Eksploitasi dan Analisis): Ini adalah inti dari mesin analitik alat. Sistem secara simultan membuat tiga permintaan API ke layanan eksternal untuk mengekstrak intelijen yang dapat ditindaklanjuti. Masing-masing API memiliki peran spesifik:
    - API *VirusTotal*: Digunakan untuk analisis reputasi ancaman. "*VirusTotal* adalah platform yang menyediakan layanan pemindaian untuk aplikasi dan file dengan menggunakan sekitar 60 pemindai antivirus" [22]. Sistem mem-*parsing* respons API untuk mendapatkan skor konsensus dari puluhan vendor keamanan, mengidentifikasi apakah URL tersebut telah ditandai sebagai berbahaya, *phishing*, atau *malware*.
    - API *WhoisXML*: Digunakan untuk intelijen domain. "*WhoisXML* merupakan sumber yang menyediakan informasi historis *WHOIS*" [23]. Sistem mengekstrak data kunci seperti tanggal pendaftaran dan kedaluwarsa domain, informasi registrar, dan data kontak. Informasi ini sangat penting untuk mengidentifikasi domain yang baru dibuat, yang merupakan indikator umum dari aktivitas *phishing*.
    - API *ip-api*: Digunakan untuk intelijen jaringan dan geolokasi. "*ip-api* digunakan dalam sistem IWAEAIT sebagai layanan geolokasi untuk melacak asal *email phishing* melalui alamat IP pengirim" [24]. Sistem mengambil alamat IP server, nama penyedia layanan internet (ISP), dan lokasi geografis server. Data ini memberikan konteks tentang infrastruktur yang menopang situs *web* tersebut.
4. *Production* (Produksi): Pada tahap akhir, intelijen yang telah dianalisis dari ketiga sumber tersebut disintesis dan disajikan kepada pengguna dalam format laporan yang terpadu dan mudah dipahami. Laporan ini mencakup ringkasan status keamanan, hasil analisis dari setiap

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i3.13769

vendor keamanan, serta detail informasi domain dan IP. Tahap ini mengubah data teknis yang kompleks menjadi output yang dapat langsung digunakan oleh pengguna untuk mengambil keputusan.



Gambar 1 Contoh Halaman Laporan URL yang Telah Terdeteksi

Dengan memadukan metodologi *waterfall* untuk pengembangan dan siklus hidup OSINT untuk operasional, penelitian ini tidak hanya membangun sebuah situs *web*, tetapi juga mengimplementasikan alur kerja pengumpulan dan analisis intelijen yang sistematis dan dapat dipertanggungjawabkan secara akademis.

3. HASIL DAN PEMBAHASAN

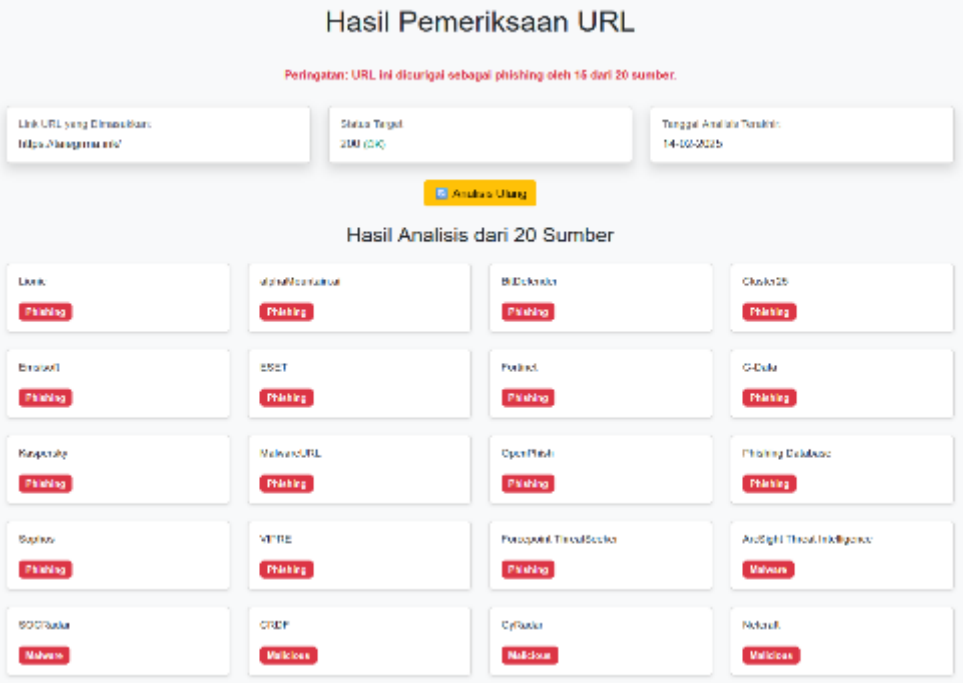
3.1 Analisis Kasus Deteksi

Analisis kualitatif terhadap kasus-kasus spesifik memberikan bukti nyata tentang cara kerja sistem dan nilai dari setiap aliran data intelijen.

1. Kasus 1: Deteksi URL Phishing Aktif (https://taiegrma.ink/)
    - Proses analisis untuk URL ini secara langsung merepresentasikan keseluruhan siklus hidup OSINT. Tahap *Collection* dimulai saat URL *https://taiegrma.ink/* yang dicurigai dianalisis. Setelah melalui tahap *Processing* di latar belakang (normalisasi dan *encoding*), sistem masuk ke tahap inti, yaitu *Exploitation*. Pada tahap ini, API *VirusTotal* digunakan untuk analisis reputasi ancaman, di mana hasilnya menunjukkan bahwa 15 dari 20 vendor keamanan menandai URL ini sebagai *phishing*.
    - Di sinilah arsitektur OSINT menunjukkan kekuatannya. Analisis tidak berhenti pada vonis awal. Tahap *Exploitation* dilanjutkan dengan pengumpulan intelijen pendukung dari API *WhoisXML* dan *ip-api*. Informasi bahwa domain *taiegrma.ink* mungkin baru saja didaftarkan (seperti yang biasa ditemukan pada situs sekali pakai) dan di-*hosting* di lokasi yang tidak wajar akan memberikan

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i3.13769

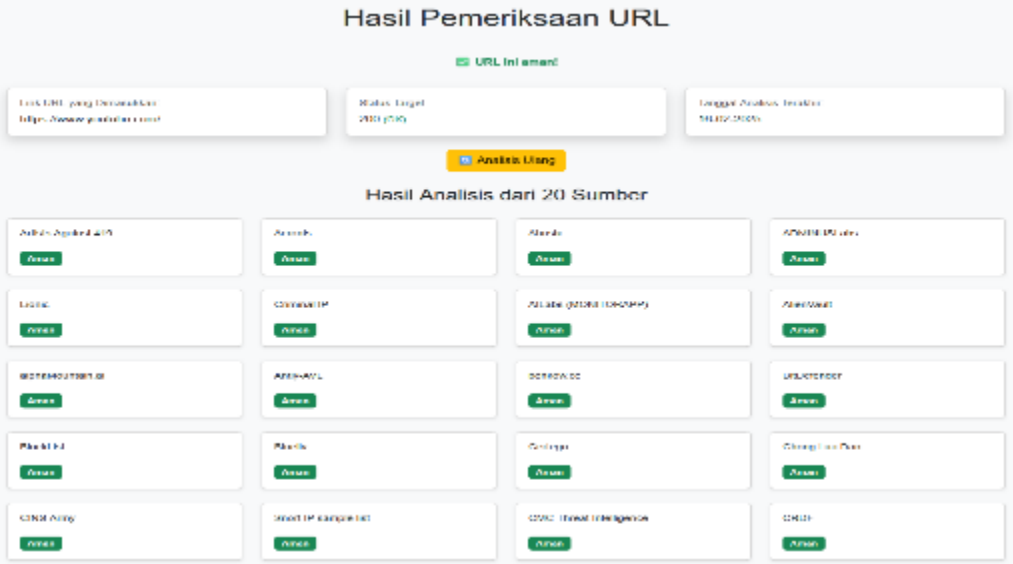
konteks krusial. Tahap terakhir, *Production*, adalah saat semua intelijen ini disintesis dan disajikan kepada pengguna dalam satu laporan terpadu seperti yang terlihat pada Gambar 2. Kombinasi dari reputasi ancaman, imaturitas domain, dan infrastruktur yang mencurigakan menghasilkan produk intelijen yang jauh lebih meyakinkan daripada label *phishing* tunggal.



Gambar 2 Hasil Pemeriksaan *Website Taiegrma*

2. Kasus 2: Verifikasi URL yang Sah. Untuk memvalidasi bahwa sistem tidak terlalu agresif, URL yang sah dan populer seperti *https://www.youtube.com/* yang diuji pada tanggal 16 Februari 2025. Kasus ini menunjukkan bagaimana arsitektur OSINT sangat efektif dalam mengurangi *false positive* dan membangun kepercayaan pengguna. Pada pengujian ini (Gambar 3), tahap *Exploitation* melalui API *VirusTotal* menghasilkan kesimpulan "Aman" dari semua sumber analisis yang ada. Tahap *Production* kemudian menyajikan hasil ini secara jelas dan dapat dipercaya. Dengan menunjukkan konsensus dari berbagai vendor keamanan bahwa situs tersebut bersih, alat ini secara efektif mengonfirmasi legitimasi URL dan membuktikan kemampuannya untuk tidak salah menandai situs yang aman sebagai ancaman.

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i3.13769



Gambar 3 Hasil Pemeriksaan *Website Youtube*

3. Kasus 3: Kasus ini menyoroti bagaimana arsitektur OSINT mengubah alat ini dari sekadar "detektor" menjadi "instrumen intelijen". Seperti yang terlihat pada Gambar 4, pengujian pada domain *polbeng.ac.id* tidak berfokus pada deteksi ancaman, melainkan pada kemampuan tahap *Exploitation* untuk mengumpulkan data kontekstual yang kaya. Melalui API *WhoisXML* dan *ip-api*, alat ini berhasil mengekstrak dan menampilkan informasi penting seperti Registrar (PT Jetcoms Netindo), Tanggal Kedaluwarsa (31-10-2025), Alamat IP (103.163.138.107), dan ISP (PT. Beon Intermedia). Tahap *Production* kemudian menyajikan data ini dalam sebuah laporan yang terstruktur. Bagi seorang analis keamanan atau pengguna tingkat lanjut, informasi ini sangat berharga untuk melakukan investigasi lebih dalam atau sekadar untuk memverifikasi detail teknis sebuah domain.

Hasil Pemeriksaan Informasi Domain dan IP	
Domain	polbeng.ac.id
Registrar	PT Jetcoms Netindo
Expires Date	2025-10-31 23.59.59 UTC
Whois Server	whois.pandi.or.id
IP Address	103.163.138.107
Country	Indonesia
Region	East Java
City	Prapen
Latitude	-7.32785
Longitude	112.738
ISP	PT. Beon Intermedia
Organization	PT Byakta Digital Ekosistem
Timezone	Asia/Jakarta

Gambar 4 Hasil Pemeriksaan Informasi Domain *Website* Polbeng

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i3.13769

3.2 Kinerja dan Akurasi Sistem

Evaluasi kuantitatif terhadap efektivitas sistem dilakukan melalui serangkaian pengujian menggunakan dataset yang terdiri dari 80 URL, yang mencakup URL *phishing* yang diketahui dan URL yang sah. Hasil utama dari pengujian ini menunjukkan bahwa alat yang dikembangkan mampu mencapai tingkat akurasi deteksi keseluruhan sebesar 98,75%. Tingkat akurasi yang tinggi ini menunjukkan bahwa pendekatan integrasi multi-API sangat efektif dalam membedakan antara situs yang berbahaya dan yang aman. Untuk memberikan gambaran yang lebih rinci tentang kinerja sistem, hasil pengujian disajikan dalam bentuk tabel yang mengilustrasikan kemampuan sistem dalam mengklasifikasikan URL dengan benar dan menyoroti jenis kesalahan yang terjadi.

Tabel 1 Hasil Pengujian Akurasi Deteksi

Kategori URL	**Jumlah URL**
Phishing (Terdeteksi dengan benar)	40
Aman (Terdeteksi Sebagai *Phishing*)	1
Aman (Terdeteksi dengan benar)	39
Total	**80**

Akurasi = Jumlah Deteksi Benar ÷ Total URL diuji ×100
= 79 ÷ 80 ×100
= 98,75 %

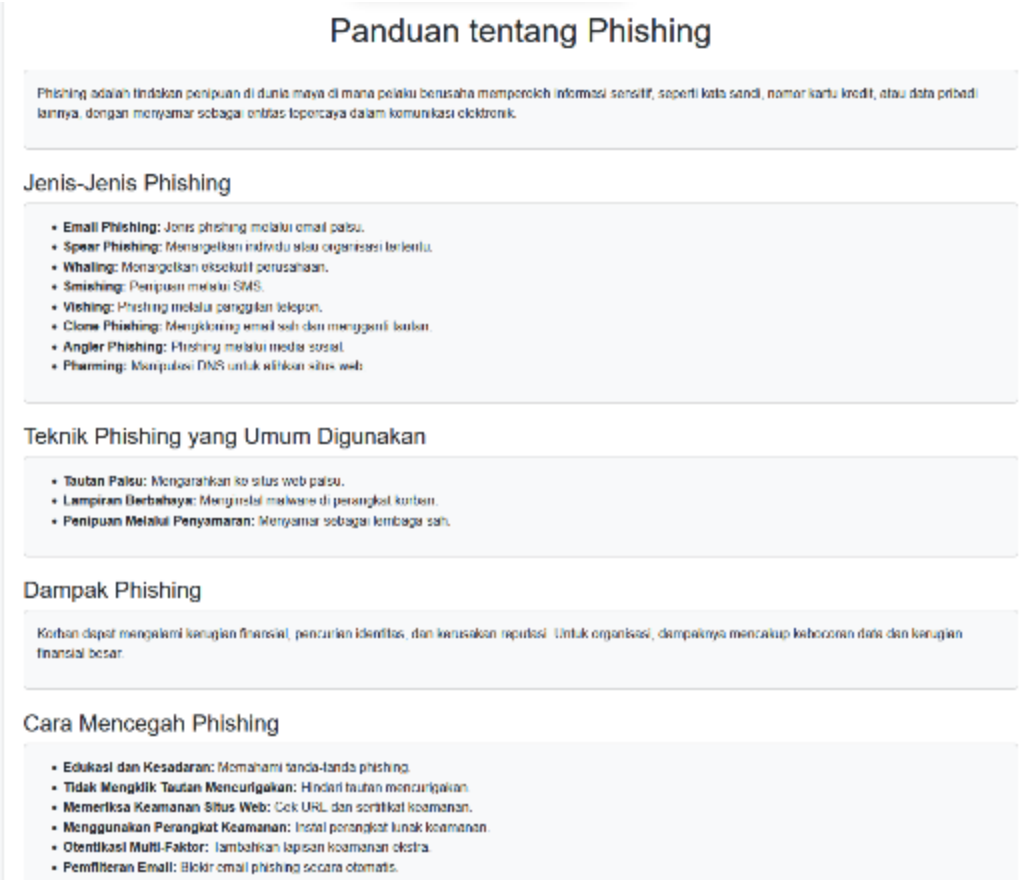
Hasil pengujian menunjukkan akurasi deteksi sistem yang sangat tinggi, mencapai 98,75%. Dari total 80 URL yang diuji, sistem berhasil mengidentifikasi 79 URL dengan benar, yang terdiri dari 40 URL *phishing* dan 39 URL aman. Terdapat hanya satu kesalahan deteksi, di mana satu URL aman keliru teridentifikasi sebagai *phishing* (*False Positive*). Tingkat akurasi ini diperoleh dengan membagi total deteksi yang benar (79) dengan jumlah keseluruhan URL yang diuji (80).

3.3 Fitur Panduan Tentang *Phishing* dan Kuis Interaktif

Selain fungsi deteksi inti, alat ini dirancang dengan komponen edukasi yang kuat untuk meningkatkan kesadaran pengguna, yang terdiri dari Halaman Panduan tentang *Phishing* dan Kuis Interaktif.

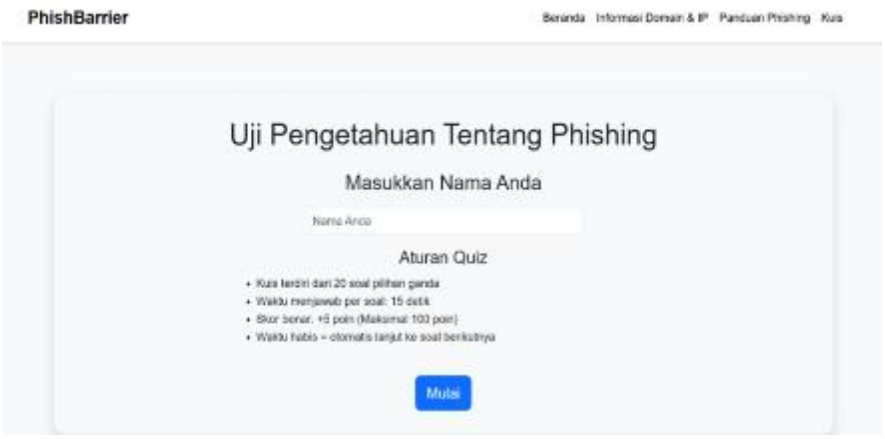
4. Panduan Tentang *Phishing*: Halaman ini berfungsi sebagai pusat pengetahuan yang komprehensif. Halaman ini menyajikan informasi terstruktur mengenai berbagai aspek *phishing*, termasuk definisi, "Jenis-Jenis *Phishing*", "Teknik *Phishing* yang Umum Digunakan", "Dampak *Phishing*", dan panduan praktis tentang "Cara Mencegah *Phishing*". Dengan menyajikan konten yang jelas, fitur ini bertujuan untuk membekali pengguna dengan pengetahuan yang diperlukan untuk mengidentifikasi dan menghindari ancaman secara mandiri.

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i3.13769



Gambar 5 Halaman Panduan Tentang *Phishing*

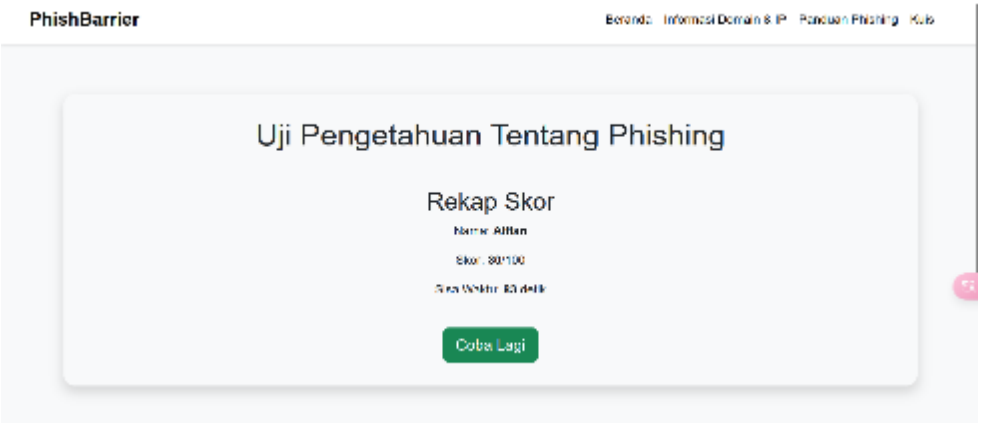
5. Kuis Interaktif: Untuk memperkuat pembelajaran, alat ini menyertakan fitur kuis interaktif. Pengguna memulai dengan memasukkan nama, kemudian dihadapkan pada 20 soal pilihan ganda dengan batas waktu 15 detik per soal. Setiap jawaban yang benar memberikan 5 poin. Setelah kuis selesai, halaman rekapitulasi menampilkan skor akhir, nama pengguna, dan sisa waktu, serta opsi untuk mencoba lagi. Fitur kuis ini tidak hanya menguji pemahaman pengguna tentang materi dalam panduan tetapi juga menciptakan pengalaman belajar yang menarik dan memotivasi.



Gambar 6 Halaman Utama Kuis

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i3.13769

Gambar 7 Soal Pada Menu Kuis



Gambar 8 Halaman Hasil Kuis

3.4 Analisis Kesadaran dan Kebutuhan Pengguna berdasarkan Survei

Survei ini dilakukan untuk memahami kesadaran dan kebutuhan pengguna terkait ancaman *phishing* serta pentingnya alat deteksi URL *phishing* dalam menjaga keamanan online. Responden memberikan jawaban terkait pengalaman mereka terhadap *phishing* dan pandangan mereka terhadap alat pendeteksi URL *phishing*.

Survei dilakukan dengan mengumpulkan data dari 40 responden yang menjawab pertanyaan terkait pengalaman mereka dengan *phishing*, tingkat kekhawatiran, dan ketertarikan terhadap alat deteksi URL *phishing*. Data dikumpulkan dalam bentuk skala *Likert* dengan pilihan mulai dari "Sangat Setuju" hingga "Sangat Tidak Setuju". Adapun hasil survei yang dilakukan di *google form* menunjukkan:

Tabel 2 Hasil Survei Pada *Google Form*

No	Soal	SS (%)	S (%)	N (%)	TS (%)	STS (%)
1	Saya pernah menerima *email*, pesan atau link yang mencurigakan yang meminta informasi pribadi.	5 (12.50%)	16 (40.00%)	2 (5.00%)	9 (22.50%)	8 (20.00%)
2	Saya pernah menjadi korban	6 (15.00%)	13 (32.50%)	6 (15.00%)	6 (15.00%)	9 (22.50%)

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i3.13769

	atau hampir menjadi korban *phishing* (penipuan *online*).					
3	Saya merasa khawatir terhadap ancaman *phishing* (penipuan *online*) saat menggunakan internet.	25 (62.50%)	11 (27.50%)	2 (5.00%)	1 (2.50%)	1 (2.50%)
4	Saya selalu memeriksa keamanan URL/link sebelum mengkliknya.	24 (60.00%)	12 (30.00%)	4 (10.00%)	0 (0.00%)	0 (0.00%)
5	*Website* yang bisa mendeteksi URL/*link phishing* (penipuan *online*) sangat diperlukan.	28 (70.00%)	11 (27.50%)	1 (2.50%)	0 (0.00%)	0 (0.00%)
6	Saya akan lebih percaya diri membuka URL/link jika ada alat yang dapat memverifikasi keamanannya.	26 (65.00%)	13 (32.50%)	1 (2.50%)	0 (0.00%)	0 (0.00%)
7	Saya merasa fitur analisis informasi domain dan IP (seperti alamat IP, negara dan kota) akan meningkatkan kepercayaan saya terhadap alat deteksi *phishing*.	18 (45.00%)	20 (50.00%)	1 (2.50%)	0 (0.00%)	1 (2.50%)
8	Saya yakin alat ini dapat membantu dalam mencegah *phishing* (penipuan *online*)	20 (50.00%)	18 (45.00%)	2 (5.00%)	0 (0.00%)	0 (0.00%)
9	Saya tertarik dengan fitur panduan tentang *phishing* (penipuan *online*) yang tersedia dalam alat ini.	23 (57.50%)	14 (35.00%)	2 (5.00%)	1 (2.50%)	0 (0.00%)
10	Saya tertarik dengan adanya kuis interaktif untuk menguji pengetahuan saya tentang *phishing* (penipuan *online*) dalam alat ini.	23 (57.50%)	13 (32.50%)	3 (7.50%)	1 (2.50%)	0 (0.00%)

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i3.13769

Hasil survei mengungkapkan tingginya kesadaran responden terhadap ancaman *phishing*. Sebanyak 52,5% (gabungan Sangat Setuju dan Setuju) pernah menerima pesan mencurigakan, dan 47,5% mengaku pernah atau hampir menjadi korban *phishing*. Kekhawatiran terhadap ancaman ini tercermin dari 90% responden yang merasa khawatir saat menggunakan internet, serta 90% yang rutin memeriksa keamanan URL sebelum mengklik. Mayoritas responden (97,5%) juga menegaskan pentingnya alat pendeteksi *phishing*.

Kepercayaan terhadap alat pencegahan *phishing* pun tinggi: 97,5% menyatakan akan lebih percaya diri membuka tautan dengan alat verifikasi, dan 95% yakin alat tersebut dapat mencegah serangan. Dukungan juga terlihat pada fitur analisis domain/IP (95%) serta minat terhadap edukasi, seperti panduan (92,5%) dan kuis interaktif (90%).

Meski demikian, sekitar 20-22,5% (gabungan Tidak Setuju dan Sangat Tidak Setuju) masih kurang waspada, menunjukkan perlunya sosialisasi lebih lanjut. Kategori Netral sengaja tidak dimasukkan dalam analisis karena tidak merepresentasikan sikap tegas/baik mendukung maupun menolak, sehingga fokus tetap pada respons yang jelas. Secara keseluruhan, temuan ini menekankan pentingnya kombinasi alat deteksi canggih, edukasi proaktif, dan kampanye kesadaran untuk mengatasi risiko *phishing*.

4. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian, sebuah alat *Open Source Intelligence* (OSINT) berbasis *web* telah berhasil dirancang menggunakan API *VirusTotal*, *WhoisXML*, dan *ip-api* untuk mendeteksi URL *phishing* dengan tingkat akurasi mencapai 98,75%. Alat ini tidak hanya efektif dalam deteksi, tetapi juga meningkatkan kesadaran pengguna melalui informasi tambahan dan kuis. Untuk pengembangan lebih lanjut, disarankan agar dilakukan penambahan fitur analisis konten *web*, kolaborasi dengan lembaga keamanan siber, serta pengujian dan pembaruan sistem secara berkala, guna memastikan alat tetap optimal dan aman dalam menghadapi ancaman yang terus berkembang.

DAFTAR PUSTAKA

[1] W. Andriyan, S. Septiawan, and A. Aulya, "PERANCANGAN WEBSITE SEBAGAI MEDIA INFORMASI DAN PENINGKATAN CITRA PADA SMK DEWI SARTIKA TANGERANG," *Jurnal Teknologi Terpadu*, vol. 6, pp. 79–88, 2020, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JTT

[2] A. Muftiadi, T. P. M. Agustina, and M. Evi, "Studi kasus keamanan jaringan komputer: analisis ancaman phising terhadap layanan online banking," *Jurnal Ilmiah Teknik*, vol. 1, pp. 60–65, 2022.

[3] U. Maryam, "Phishing Attacks Facilitated by Open-Source Intelligence," *Journal of Computer and Information Engineering*, vol. 17, no. 10, pp. 587–590, 2023.

[4] R. Syah, "STRATEGI KEPOLISIAN DALAM PENCEGAHAN KEJAHATAN PHISING MELALUI MEDIA SOSIAL DI RUANG SIBER," *Jurnal Impresi Indonesia*, vol. 2, no. 9, pp. 864–870, Sep. 2023, doi: 10.58344/jii.v2i9.3594.

[5] M. F. Safitra and L. Abdurrahman, "Open-up International Market Opportunities: Using the OSINT Crawling and Analyzing Method," *SEIKO : Journal of Management & Business*, vol. 6, no. 1, pp. 923–931, 2023, doi: 10.37531/sejaman.vxix.346.

[6] A. F. Mahmud and S. Wirawan, "Deteksi Phishing Website menggunakan Machine Learning Metode Klasifikasi," *Sistemasi: Jurnal Sistem Informasi* , vol. 13, no. 4, pp. 2540–9719, 2024, [Online]. Available: http://sistemasi.ftik.unisi.ac.id

[7] V. Aprelia Windarni, A. Ferdita Nugraha, S. Tri Atmaja Ramadhani, D. Anisa Istiqomah, F. Mahananing Puri, and A. Setiawan, "DETEKSI WEBSITE PHISHING

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i3.13769

MENGGUNAKAN TEKNIK FILTER PADA MODEL MACHINE LEARNING," *Information System Journal (INFOS)*, vol. 6, no. 1, 2023.

[8] M. Fahri, "Penerapan Algoritma Random Forest untuk Deteksi Phishing pada Website," *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 6, no. 2, pp. 186–194, Jun. 2025, doi: 10.62527/jitsi.6.2.472.

[9] M. Rahul, "PENGEMBANGAN APLIKASI DETEKSI PHISING BERBASIS WEB MENGGUNAKAN ALGORITMA DECISION TREE," 2023.

[10] R. P. Ramadhan and T. Desyani, "Implementasi Algoritma J48 Untuk Identifikasi Website Phising," *Jurnal Ilmu Komputer, Teknik dan Multimedia*, vol. 1, no. 2, pp. 46–54, Jun. 2023.

[11] R. Fauzan, A. V. Vitianingsih, D. Cahyono, A. L. Maukar, and Y. A. B. Suprio, "Penerapan Algoritma Klasifikasi pada Machine Learning untuk Deteksi Phishing," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 5, no. 2, pp. 531–540, Mar. 2025, doi: 10.57152/malcom.v5i2.1968.

[12] V. Indriani, H. Listiyono, and Saefurrahman, "DETEKSI PHISHING WEBSITE MENGGUNAKAN SUPPORT VECTOR MACHINE, GRADIENT BOOSTING, DAN NEURAL NETWORKS," *JATI (Jurnal Mahasiswa Teknik Informatika)* , vol. 9, no. 2, 2025.

[13] M. Zaidan Zufar, "APLIKASI PENDETEKSI SITUS PHISING BERBASIS WEBSITE MENGGUNAKAN METODE NAÏVE BAYES," 2023.

[14] D. Wahyudi, "APLIKASI PENDETEKSI WEBSITE PHISHING MENGGUNAKAN MACHINE LEARNING," 2020.

[15] A. Ferdita Nugraha, R. Faticha, A. Aziza, and Y. Pristyanto, "Penerapan metode Stacking dan Random Forest untuk Meningkatkan Kinerja Klasifikasi pada Proses Deteksi Web Phishing," *Jurnal Infomedia: Teknik Informatika, Multimedia & Jaringan*, vol. 7, no. 1, 2022.

[16] T. F. Handoyo and M. P. K. Putra, "Optimasi Bobot Kelas LSTM untuk Deteksi URL Phishing pada Dataset Tidak Berimbang," *Jurnal Informatika: Jurnal Pengembangan IT*, vol. 10, no. 1, pp. 20–36, Jan. 2025, doi: 10.30591/jpit.v10i1.8128.

[17] Rangga Gelar Guntara, "Aplikasi Deteksi Phising Berbasis Android Menggunakan Metode Pengembangan Perangkat Lunak DSRM," *Jurnal Minfo Polgan*, vol. 12, no. 1, pp. 303–310, Mar. 2023, doi: 10.33395/jmp.v12i1.12379.

[18] F. Pavanello, S. Virtanen, J. Isoaho, M. Giaimo, and S. Cagol, "OSINT-based Email Analyzer for Phishing Detection," University of Turku, 2023.

[19] S. Pirocca, L. Allodi, and N. Zannone, "A Toolkit for Security Awareness Training against Targeted Phishing," in *Information Systems Security*, 2020. [Online]. Available: https://securityaffairs.co/wordpress/83630/

[20] R. Renaldo Prasena and H. Sama, "STUDI KOMPARASI PENGEMBANGAN WEBSITE DENGAN FRAMEWORK CODEIGNITER DAN LARAVEL," *Conference on Business, Social Sciences and Innovation Technology*, vol. 1, pp. 613–621, 2020, [Online]. Available: http://journal.uib.ac.id/index.php/cbssit

[21] B. T. Mahardika, "Perancangan Sistem Informasi Perpusatakaan Berbasis Web dengan Laravel," *Jurnal Sains & Teknologi*, vol. 13, no. 2, pp. 104–112, Sep. 2023.

[22] A. Salem, S. Banescu, and A. Pretschner, "Maat: Automatically Analyzing VirusTotal for Accurate Labeling and Effective Malware Detection," *ACM Transactions on Privacy and Security*, vol. 24, no. 4, pp. 1–38, 2020, doi: 10.1145/3465361.

[23] G. Liu *et al.*, "Dial 'N' for NXDomain: The Scale, Origin, and Security Implications of DNS Queries to Non-Existent Domains," in *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, Association for Computing Machinery, Oct. 2023, pp. 198–212. doi: 10.1145/3618257.3624805.

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i3.13769

[24] F. Bari and S. H. A. Rahman, "An Integrated Web-Based Approach for Email Analysis Investigation Tool," in *Proceedings of the 2024 9th International Conference on Cloud Computing and Internet of Things*, New York, NY, USA: ACM, Nov. 2024, pp. 92–100. doi: 10.1145/3704304.3704317.

[25] H. Setiawan and M. N. Ghiffari, "Sistem Informasi Covid-19 Berbasis Mobile Dengan Framework Flutter dan Application Programming Interface (API)," *Jurnal Teknologi Informasi dan Komunikasi (TIKomSiN)*, vol. 10, no. 2, pp. 35–41, Nov. 2022, doi: 10.30646/tikomsin.v10i2.640.

[26] B. Fachri and R. Wahyu Surbakti, "PERANCANGAN SISTEM DAN DESAIN UNDANGAN DIGITAL MENGGUNAKAN METODE WATERFALL BERBASIS WEBSITE (STUDI KASUS: ASCO JAYA)," *Journal of Science and Social Research*, vol. 4, no. 3, pp. 263–267, 2021, [Online]. Available: http://jurnal.goretanpena.com/index.php/JSSR

[27] R. Gustina and H. Leidiyana, "SISTEM INFORMASI PENGGAJIAN KARYAWAN BERBASIS WEB MENGGUNAKAN FRAMEWORK LARAVEL," *Jurnal Sistem Informasi*, vol. 7, no. 1, pp. 34–40, Mar. 2020.

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI :10.62411/tc.v24i3.13769