BAB 1
PENDAHULUAN

1.1 Latar Belakang

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 [1].

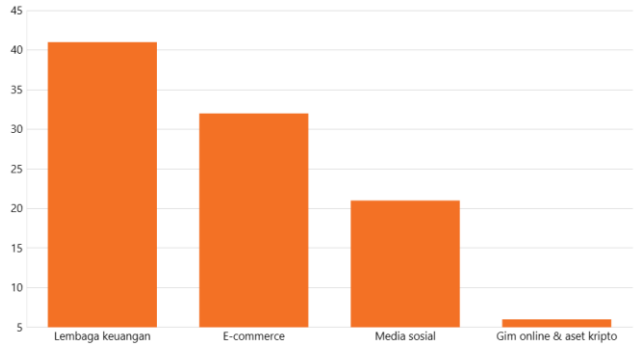
Website dapat diartikan sebagai sekumpulan halaman yang menyajikan berbagai jenis informasi, termasuk teks, gambar, animasi, suara, video, atau kombinasi dari semuanya, baik yang bersifat statis maupun dinamis. Halaman-halaman ini terhubung satu sama lain melalui jaringan, membentuk struktur yang saling 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 pemahaman pengguna [2].

Phishing merupakan strategi penipuan yang memanfaatkan metode rekayasa sosial untuk menyesatkan korban dengan berpura-pura sebagai lembaga atau individu terpercaya. Teknik ini sering kali melibatkan pengiriman *email* atau pesan yang tampak sah, dengan tujuan untuk memperdaya penerima agar memberikan informasi sensitif atau melakukan aksi yang menguntungkan pelaku [3].

Serangan *phishing* dapat berakibat fatal bagi baik individu maupun lembaga, menyebabkan masalah seperti pencurian identitas, pelanggaran privasi dengan kebocoran informasi yang bersifat rahasia, dan kerugian ekonomi yang signifikan. Dampak dari serangan ini tidak hanya terbatas pada kerugian materi, tetapi juga dapat menimbulkan kerusakan reputasi yang berkelanjutan dan mengganggu kestabilan di ruang siber [4].

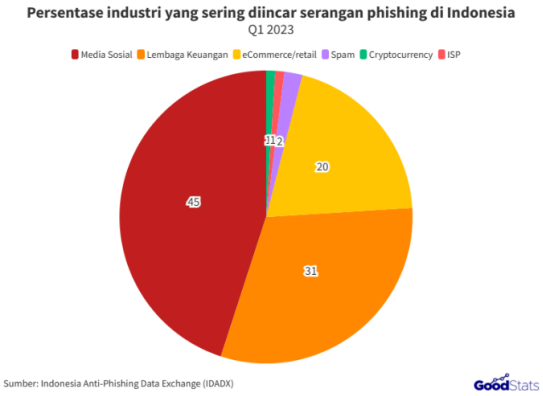
Untuk menghindari *phishing*, langkah-langkah pencegahan dapat diambil dengan memasang filter *email* yang efektif dalam membedakan antara *email* yang sah dan yang mencurigakan. Selain itu, penggunaan perangkat lunak anti-*phishing* merupakan cara tambahan yang efisien untuk memblokir upaya *phishing*. Hal Ini

termasuk penggunaan indikator keamanan di *browser*, seperti protokol HTTPS yang terverifikasi dengan sertifikat SSL, agar dapat memastikan keamanan situs *web* [5].



Gambar 1.1 Statistik Sebaran Serangan Phishing di RI Berdasarkan Sektor (Kuartal II-2022) [6]

Berdasarkan laporan Direktorat Tindak Pidana Siber Bareskrim Polri yang dipublikasikan di databoks.katadata.co.id, terjadi sekitar 5.579 serangan *phishing* di Indonesia pada kuartal II-2022. Jumlah ini mengalami peningkatan sekitar 41,52% dari bulan sebelumnya, di mana pada kuartal I-2022, terdapat 3.942 serangan. Lembaga keuangan menjadi target utama serangan *phishing* dengan persentase mencapai 41%. Selain itu, *e-commerce* juga menjadi sasaran dengan 32% serangan, media sosial sebanyak 21% serangan, dan Gim online dan aset kripto sebanyak 6% serangan.



Gambar 1.2 Persentase Industri yang Sering Diincar Serangan Phishing di Indonesia Periode Januari-Maret 2023 [7]

Selain itu, berdasarkan grafik dari Indonesia Anti-Phishing Data Exchange (IDADX) yang dipublikasikan di goodstats.id, selama kuartal pertama tahun 2023,

sektor yang paling sering menjadi target serangan phishing di Indonesia adalah media sosial dengan persentase 45%. Sektor lain yang juga menjadi sasaran utama adalah lembaga keuangan (31%), eCommerce/retail (20%), dan sektor lainnya seperti spam, cryptocurrency, dan ISP dengan persentase yang lebih kecil. Data ini menyoroti pentingnya meningkatkan kesadaran dan perlindungan terhadap ancaman phishing, terutama di sektor-sektor yang paling rentan.

Fenomena ini menunjukkan adanya peningkatan kasus serangan phishing yang perlu diwaspadai, khususnya yang menargetkan lembaga keuangan. Data menunjukkan bahwa sektor keuangan menyumbang 31% dari total serangan phishing pada kuartal pertama tahun 2023. Oleh karena itu, memperkuat keamanan siber di sektor ini menjadi sangat penting untuk melindungi informasi keuangan dan data pribadi yang sensitif. Upaya yang perlu dilakukan meliputi meningkatkan kesadaran di kalangan karyawan dan nasabah, serta memperkuat infrastruktur keamanan agar dapat mendeteksi dan menangani ancaman phishing dengan lebih baik.

Penelitian ini akan merancang alat OSINT berbasis *web* untuk deteksi URL *phishing* 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 [8]. PHP, sebagai bahasa pemrograman *server-side open-source*, memungkinkan pengguna untuk mengubah dan mengembangkan aplikasi atau sistem sesuai kebutuhan mereka [9].

Dalam rancang bangun alat OSINT deteksi url *phishing* peneliti menggunakan metode *waterfall*. Metode *Waterfall* adalah sebuah pendekatan dalam pengembangan sistem di mana setiap fase dilaksanakan secara berurutan. Dalam implementasi metode ini, setiap langkah harus diselesaikan sepenuhnya sebelum melanjutkan ke tahap berikutnya, dimulai dari tahap pertama hingga yang terakhir [10].

Dalam merancang alat deteksi url *phishing* berbasis *web*, salah satu komponen penting adalah kemampuan untuk memverifikasi keamanan URL secara efektif.

Penggunaan API *VirusTotal, WhoisXML* dan *ip-api* dapat menjadi solusi optimal dalam hal ini. *VirusTotal* adalah platform yang menyediakan layanan pemindaian untuk aplikasi dan file dengan menggunakan sekitar 60 pemindai antivirus. Pengguna dapat mengunggah hash dari aplikasi, dan *VirusTotal* akan mengembalikan label yang diberikan oleh masing-masing pemindai, serta informasi mengenai konten [11]. *WhoisXML* merupakan sumber yang menyediakan informasi historis *WHOIS* yang penting untuk penelitian tentang *NXDomains*. Peneliti menggunakan basis data *WhoisXML* yang mencakup 15.6 miliar catatan *WHOIS* historis untuk mengidentifikasi dan menganalisis asal-usul *NXDomains*, khususnya yang disebabkan oleh nama domain yang kedaluwarsa [12]. *ip-api* digunakan dalam sistem IWAEAIT (*Integrated Web-based Approach for Email Analysis Investigation Tool*) sebagai layanan geolokasi untuk melacak asal *email phishing* melalui alamat IP pengirim. Layanan ini terintegrasi melalui API untuk mengekstrak informasi lokasi geografis (seperti negara, kota, dan koordinat) dari header *email*, membantu identifikasi sumber serangan *phishing* tanpa memerlukan keahlian teknis khusus [13]. Dengan integrasi API ini, aplikasi diharapkan dapat secara otomatis memeriksa URL yang diinput oleh pengguna, memberikan informasi jika URL tersebut teridentifikasi sebagai berbahaya.

Berdasarkan penelitian terdahulu yang dilakukan oleh Muhammad Rahul pada tahun 2023, dengan judul "Pengembangan Aplikasi Deteksi Phising Berbasis Web Menggunakan Algoritma Decision Tree". Tujuan penelitian ini adalah untuk membuat aplikasi berbasis *web* yang menggunakan algoritma *Decision Tree* untuk menemukan tautan *phishing*. Analisis, desain, pengkodean, dan pengujian adalah semua komponen model pengembangan *Waterfall* yang digunakan. Untuk proses *backend* tertentu, *Python* digunakan, tetapi *PHP* dan *Laravel* digunakan untuk membangun aplikasi ini. Salah satu fitur utama aplikasi adalah otentikasi pengguna yang aman dan alat deteksi *phishing*, yang mengidentifikasi ancaman *phishing* melalui analisis URL. Hasil penelitian menunjukkan bahwa penggunaan algoritma *Decision Tree* secara signifikan meningkatkan akurasi deteksi *phishing*. Aplikasi ini telah diuji secara menyeluruh untuk memastikan akurasi dan keandalan. Singkatnya, aplikasi ini memberikan perlindungan yang lebih andal dan mudah

digunakan untuk melindungi pengguna dari *phishing* karena berhasil mengatasi kekurangan akurasi pada alat deteksi *phishing* yang ada [9].

Berdasarkan penelitian sebelumnya yang dilakukan oleh Ryan Putra Ramadhan dan Teti Desyani, "Implementasi Algoritma J48 untuk Identifikasi Website Phising" pada tahun 2023. Tujuan dari penelitian ini adalah untuk menerapkan algoritma J48 untuk menemukan situs *web phishing*. Analisis, desain, pengkodean, dan pengujian adalah langkah-langkah *waterfall* dalam pengembangan sistem yang digunakan. Implementasi algoritma J48 melibatkan analisis *link* domain dari situs *web* yang akan diidentifikasi. Proses ini meningkatkan deteksi situs *phishing*. Hasil penelitian menunjukkan bahwa algoritma J48 mampu meningkatkan akurasi dan keandalan dalam mendeteksi situs *phishing*, meskipun masih diperlukan data yang berkualitas dan bervariasi serta kombinasi dengan algoritma lain untuk mencapai hasil yang optimal [14].

1.2 Permasalahan

Phishing merupakan salah satu teknik kejahatan *cyber* yang paling sering terjadi dan memiliki dampak luas, terutama di sektor keuangan yang menjadi target utama. Pelaku kejahatan menggunakan *email* dan media sosial sebagai sarana untuk menyebarkan tautan atau lampiran berbahaya, yang ketika diakses oleh korban dapat mengakibatkan pencurian data pribadi dan informasi keuangan yang sensitif. Masalah ini diperburuk oleh kemampuan pelaku untuk menyamarkan URL *phishing* mereka sehingga tampak meyakinkan, sering kali dengan memanfaatkan informasi dari sumber terbuka atau melalui teknik rekayasa sosial.

Oleh karena itu, sangat penting untuk mengambil tindakan preventif dalam mendeteksi dan menghalangi serangan *phishing*, terutama yang sering kali muncul melalui *email* dan *platform* media sosial. Langkah-langkah ini termasuk edukasi yang dapat diandalkan mengenai cara mengidentifikasi URL *phishing*, seperti dengan memeriksa identitas pengirim *email* dengan hati-hati, menghindari menekan tautan yang mencurigakan, dan tidak membuka lampiran dari sumber yang tidak terpercaya.

Urgensi dari penelitian ini terletak pada meningkatnya frekuensi dan kecanggihan serangan *phishing*, yang mengakibatkan kerugian finansial dan pencurian identitas dalam skala besar, khususnya di sektor keuangan. Data dari laporan keamanan siber menunjukkan bahwa serangan *phishing* terus meningkat setiap tahun, dengan metode yang semakin sulit dideteksi oleh orang awam. Tanpa adanya alat yang dapat diandalkan dalam mendeteksi dan menganalisis URL *phishing*, individu dan organisasi, terutama di sektor keuangan, tetap berada dalam risiko tinggi terhadap serangan ini.

Dalam konteks ini, perancangan alat OSINT berbasis *web* yang dikembangkan menggunakan *Framework Laravel* dan Bahasa Pemrograman PHP menjadi penting untuk proaktif mengidentifikasi dan mencegah serangan *phishing*. OSINT digunakan untuk mengumpulkan dan mengolah informasi dari sumber-sumber terbuka dan publik, seperti media massa, internet, dan basis data publik, guna memenuhi kebutuhan intelijen yang spesifik dan disampaikan secara cepat kepada pihak yang membutuhkan. Dalam konteks penelitian ini, OSINT digunakan sebagai tahapan dalam mendeteksi URL *phishing* dengan mengintegrasikan API *VirusTotal, WhoisXML,* dan *ip-api*, yang mencakup URL situs-situs berbahaya dan berpotensi sebagai *phishing*. Oleh karena itu, alat ini akan membantu pengguna, terutama di lembaga keuangan, dalam mendeteksi URL *phishing* dengan menyediakan analisis mendetail tentang tautan yang mencurigakan, serta memberikan rekomendasi tindakan yang perlu diambil.

Sebagai tambahan, peneliti juga merencanakan untuk membuat halaman/menu khusus dalam alat ini yang akan berisi pembahasan tentang *phishing* dan soal-soal terkait. Halaman ini akan menyediakan informasi edukatif mengenai *phishing*, panduan untuk mendeteksi serangan, serta kuis untuk meningkatkan pemahaman pengguna. Dengan adanya halaman ini, diharapkan pengguna dapat lebih siap menghadapi ancaman *phishing* dan melindungi diri mereka dengan lebih efektif.

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut:

a. Penelitian hanya fokus pada deteksi URL *phishing* menggunakan API *VirusTotal*, *WhoisXML*, dan *ip-api*. Tidak ada pengembangan atau implementasi algoritma *machine learning* dalam proses deteksi.
b. Penelitian tidak mencakup pengembangan fitur otomatisasi seperti pemblokiran URL secara langsung di *browser* atau perangkat pengguna.
c. Deteksi URL *phishing* hanya bergantung pada API *VirusTotal*, *WhoisXML*, dan *ip-api* untuk memperoleh data dan hasil analisis.
d. Sistem hanya dikembangkan menggunakan *framework Laravel* dan bahasa pemrograman PHP, dengan antarmuka berbasis *web*.

1.4 Tujuan

Berdasarkan permasalahan yang ada, tujuan dari penelitian ini adalah merancang dan membangun alat OSINT berbasis *web* yang andal untuk mendeteksi URL *phishing* dan memeriksa informasi suatu domain. Selain itu, alat ini juga akan memberikan informasi kepada pengguna dengan menyajikan informasi tentang *phishing* dan menyediakan latihan interaktif berupa soal-soal terkait *phishing*.

1.5 Manfaat

Manfaat dari penelitian "Penerapan API dalam Alat OSINT untuk Mendeteksi URL *Phishing* Berbasis *Web*" antara lain:

a. Membantu masyarakat maupun organisasi dalam mendeteksi URL phishing, sehingga dapat mencegah pencurian data pribadi.
b. Mengurangi risiko pencurian data pribadi melalui *email* dan media sosial.
c. Memberikan informasi kepada pengguna tentang bagaimana mengidentifikasi dan menghindari phishing.
d. Membantu orang yang menekuni bidang keamanan siber dengan menyediakan alat tambahan untuk memperkuat upaya mereka dalam mendeteksi dan mencegah serangan phishing.

1.6 Sistematika Penulisan

Sistematika pembahasan dalam skripsi yang meliputi:

1. Bab 1 Pendahuluan

   Bab ini menjelaskan latar belakang, permasalahan, tujuan, manfaat, dan batasan masalah yang akan dibahas dalam skripsi.

2. Bab 2 Kajian Pustaka

   Bab ini berisi teori-teori dan penelitian terdahulu yang relevan dengan topik penelitian, untuk memberikan dasar pemahaman terkait masalah yang diteliti.

3. Bab 3 Deskripsi Sistem

   Bab ini menjelaskan perancangan sistem, mulai dari analisis kebutuhan, desain, hingga komponen-komponen yang digunakan dalam sistem.

4. Bab 4 Eksperimen dan Analisis

   Pada bab ini dijelaskan tentang eksperimen yang dilakukan untuk menguji sistem, serta hasil dan analisis yang diperoleh dari eksperimen.

5. Bab 5 Penutup

   Bab ini berisi kesimpulan dari penelitian yang telah dilakukan, serta saran untuk pengembangan lebih lanjut.