Jurnal Teknologi Dan Sistem Informasi Bisnis Vol. 8 No. 2 April 2026 Hal.153-158
http://jurnal.unidha.ac.id/index.php/jteksis

E-ISSN : **2655-8238**
P-ISSN : **2964-2132**

Implementasi Sistem Deteksi *Defacement* Otomatis pada *Website* Pemerintah Menggunakan N8N

Faisal Anwar[a], Apriade Voutama[b]
[a]Sistem Informasi, Fakultas Ilmu Komputer, Universitas Singaperbangsa Karawang, ffaisalanwar52@gmail.com
[b]Sistem Informasi, Fakultas Ilmu Komputer, Universitas Singaperbangsa Karawang, apriade.voutama@staff.unsika.ac.id

Submitted: 16-03-2026 Reviewed: 20-03-2026 Accepted: 15-04-2026
https://doi.org/10.47233/jteksis.v8i1.2578

Abstract
Advances in information technology have encouraged the use of websites as a means of public services in various sectors. One sector that utilizes websites to support its services is the government sector. However, in its implementation, this system faces cybersecurity challenges, namely defacement attacks, which involve unauthorized changes to the appearance or content of a website that are often detected too late and can erode public trust. This research aims to develop a system capable of detecting indications of defacement attacks automatically and more quickly. The method applied in this research is a system experiment approach, which utilizes the n8n workflow automation platform, operated on a scheduled basis via schedule triggers. This system is tasked with monitoring website domains by applying analytical techniques based on keyword matching to page content that is potentially subject to change. The monitoring data is then processed using a function node to match specific keywords, such as "judol," "bokep," "gacor," and "slot," which frequently appear in defacement cases. Once keywords are detected, the system then sends a warning message to the administrator via Discord. The results show that the system is capable of automatically detecting keyword occurrences and sending a warning message via Discord webhook to the administrator when a change in website content is identified. This system also helps speed up the verification process by providing direct links to related pages so that handling can be done more quickly and effectively.
Keywords: *Website Defacement, Cyber Security, System Automation, Website Monitoring, n8n Workflow*

Abstrak
Kemajuan teknologi informasi mendorong penggunaan *website* sebagai sarana layanan publik di berbagai sektor. Salah satunya sektor yang menggunakan *website* dalam menunjang pelayanannya adalah sektor pemerintahan. Namun dalam penerapannya sistem ini menghadapi tantangan terkait keamanan siber yaitu serangan *defacement*, yakni perubahan tampilan atau konten *website* secara tidak sah yang seringkali terlambat diketahui dan dapat mengurangi kepercayaan masyarakat. Penelitian ini bertujuan untuk mengembangkan sistem yang mampu mendeteksi indikasi serangan *defacement* secara otomatis dan lebih cepat.. Metode yang diterapkan dalam penelitian ini adalah pendekatan eksperimen sistem, yang memanfaatkan *platform* otomasi *workflow* n8n yang dioperasikan secara terjadwal melalui *schedule trigger*. Sistem ini bertugas untuk memantau domain *website* dengan menerapkan teknik analisis yang berbasis pencocokan kata kunci pada konten halaman yang berpotensi mengalami perubahan. Data hasil pemantauan selanjutnya diolah menggunakan *function node* untuk melakukan pencocokan kata kunci tertentu, seperti “judol”, “bokep”, “gacor”, dan “slot”, yang sering muncul dalam kasus *defacement*. Setelah kata kunci terdeteksi, sistem kemudian mengirim pesan peringatan kepada *administrator* melalui discord. Hasil penelitian menunjukkan bahwa sistem mampu mendeteksi kemunculan kata kunci secara otomatis serta mengirimkan pesan peringatan melalui webhook Discord kepada *administrator* ketika teridentifikasi adanya perubahan konten pada *website*. Sistem ini juga membantu mempercepat proses verifikasi melalui penyediaan tautan langsung ke halaman terkait sehingga penanganan dapat dilakukan lebih cepat dan efektif.
Keywords*: Defacement Website*, Keamanan Siber, Otomatisasi Sistem, Monitoring *Website*, n8n *Workflow*

PENDAHULUAN

Kemajuan teknologi informasi dan internet telah mendorong perubahan digital di berbagai bidang, termasuk dalam pelaksanaan layanan pemerintahan yang menggunakan sistem elektronik atau e-government. *Website* pemerintah memiliki peran yang sangat penting sebagai saluran untuk menyampaikan informasi publik, memberikan layanan administrasi, serta sebagai wadah komunikasi antara pemerintah dan masyarakat. Penggunaan *website* dalam pelayanan publik dapat meningkatkan transparansi, efisiensi layanan, serta kemudahan akses informasi bagi masyarakat secara umum. Meskipun begitu, meningkatnya penggunaan sistem berbasis web juga disertai dengan meningkatnya ancaman keamanan siber terhadap *website* yang menjadi salah satu tantangan utama dalam pengelolaan layanan digital pemerintah[1][2].

Salah satu jenis serangan siber yang sering terjadi pada *website* adalah web *defacement*. Serangan ini dilakukan dengan cara mengubah tampilan halaman *website* secara ilegal oleh pihak yang tidak bertanggung jawab. Perubahan tersebut

Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 5 No. 1 Januari 2023 Hal. 36-41
http://jurnal.unidha.ac.id/index.php/jteksis
E-ISSN :**2655-8238**
P-ISSN : **2964-2132**

bisa berupa penggantian desain halaman utama, penambahan pesan tertentu, atau penambahan konten yang tidak sesuai. Dalam sejumlah kasus, serangan *defacement* juga digunakan untuk menyisipkan konten yang melanggar hukum seperti promosi perjudian *online*, pornografi, atau konten lain yang tidak sesuai dengan tujuan resmi *website* suatu institusi. Serangan ini tidak hanya memengaruhi tampilan *website*, tetapi juga dapat merusak citra organisasi yang menjadi sasaran serangan[3].

Website pemerintah menjadi salah satu sasaran yang mudah diserang melalui *defacement* karena memiliki tingkat keterlihatan yang tinggi di internet dan menyimpan berbagai informasi publik yang penting. Beberapa penelitian menunjukkan bahwa sejumlah *website* dapat mengalami perubahan isi akibat serangan *defacement* yang dilakukan oleh individu yang tidak bertanggung jawab. Keadaan ini menunjukkan bahwa keamanan *website* adalah faktor penting yang perlu diperhatikan dalam pengelolaan layanan digital yang berbasis web[4].

Beragam penelitian sebelumnya telah menciptakan cara untuk mengidentifikasi serangan *defacement* pada *website*. Salah satu metode yang umum digunakan adalah file integrity monitoring, yaitu suatu cara yang mengawasi perubahan pada file sistem untuk mengidentifikasi modifikasi yang tidak sah pada *website*. Metode ini dapat dengan cepat mengenali perubahan pada file, sehingga *administrator* sistem dapat segera menyadari jika terdapat aktivitas yang mencurigakan pada server *website*[5]. Selain itu, peningkatan keamanan sistem melalui tes keamanan seperti penetration testing dapat membantu menemukan kelemahan sistem serta meningkatkan perlindungan terhadap berbagai jenis serangan siber[6].

Selain teknik *file integrity monitoring*, penelitian lain juga menggunakan analisis log sistem serta metode deteksi anomali untuk mengenali aktivitas yang dapat menjadi tanda adanya serangan terhadap sistem *website*. Pendekatan ini memungkinkan sistem untuk menganalisis aktivitasnya dengan lebih mendalam, sehingga proses identifikasi ancaman keamanan dapat dilakukan dengan lebih efisien[7][8].

Walaupun begitu, kegiatan pemantauan keamanan *website* di berbagai organisasi masih dilakukan secara manual, sehingga deteksi perubahan pada *website* sering kali terlambat. Situasi ini dapat mengakibatkan *website* berada dalam keadaan terdeface untuk periode waktu yang cukup lama sebelum diambil langkah pemulihan. Oleh karena itu, diperlukan suatu sistem pemantauan yang dapat berfungsi secara otomatis untuk mengawasi perubahan yang terjadi pada *website* secara terus-menerus.

Sejalan dengan kemajuan teknologi otomasi sistem, berbagai platform otomatisasi *workflow* kini mulai digunakan untuk menghubungkan berbagai layanan digital secara otomatis. Salah satu platform yang dapat dimanfaatkan adalah n8n, yaitu perangkat lunak otomasi *workflow* yang bersifat *open-source*, yang memungkinkan pengguna untuk menghubungkan berbagai aplikasi, layanan, atau API dalam suatu *workflow* otomatis yang berbasis node. Dengan metode ini, tahapan pengumpulan data, pengolahan informasi, dan pengiriman pemberitahuan dapat dilakukan secara otomatis dalam satu sistem yang terintegrasi[9][10][11][12].

Berdasarkan permasalahan tersebut, kajian ini memiliki tujuan untuk menerapkan sistem deteksi *defacement* secara otomatis pada *website* pemerintah dengan memanfaatkan teknologi n8n. Penguatan sistem keamanan pada aplikasi berbasis web merupakan hal yang sangat penting untuk mencegah berbagai jenis serangan, seperti peretasan, penyalahgunaan akses, dan gangguan layanan pada server web[13]. Sistem yang dirancang diharapkan dapat secara otomatis mengawasi perubahan pada *website* dan memberikan pemberitahuan kepada *administrator* jika terdeteksi tanda-tanda serangan *defacement*. Oleh karena itu, penelitian ini diharapkan dapat memberikan bantuan dalam pengembangan sistem pemantauan keamanan *website* pemerintah serta mendukung perbaikan pengelolaan dan penilaian sistem informasi berbasis web di dalam organisasi[14].

METODE PENELITIAN

Penelitian ini menerapkan metode eksperimen sistem untuk menciptakan mekanisme otomatis yang mendeteksi *defacement* pada situs web dengan memanfaatkan platform otomatisasi *workflow*. Sistem ini dibuat dengan n8n sebagai pengatur *workflow* otomatis dan dioperasikan dalam lingkungan kontainer menggunakan Docker. Teknologi Docker sangat populer karena dapat menawarkan lingkungan sistem yang seragam dan mudah untuk direplikasi di berbagai infrastruktur komputasi[15][16]. Di samping itu, metode otomatisasi alur kerja memungkinkan penggabungan berbagai layanan dalam satu proses otomatis, sehingga pemantauan sistem dapat dilakukan dengan lebih efektif[9].

Penelitian ini dilakukan melalui empat langkah utama, yaitu identifikasi masalah, analisis kebutuhan, perancangan sistem, serta implementasi sistem. Proses tahapan penelitian tersebut dapat dilihat pada gambar 1 yang berisi diagram alur metode penelitian.

Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 5 No. 1 Januari 2023 Hal. 36-41
http://jurnal.unidha.ac.id/index.php/jteksis

E-ISSN :**2655-8238**
P-ISSN : **2964-2132**

Gambar 1. Tahapan Penelitian

2.1 Identifikasi Masalah

Langkah awal dalam penelitian ini adalah mengidentifikasi isu-isu keamanan pada *website*, terutama yang berkaitan dengan serangan web *defacement*. Serangan ini dapat mengakibatkan perubahan tampilan situs web tanpa izin dan penyertaan konten yang tidak layak seperti iklan perjudian *online* atau informasi ilegal lainnya. Oleh karena itu, diperlukan suatu sistem pemantauan yang dapat secara otomatis mendeteksi perubahan konten di *website*, sehingga *administrator* sistem dapat segera mengetahui jika terdapat tanda-tanda serangan[1][3].

2.2 Analisis Kebutuhan

Tahap ini bertujuan untuk mengkaji kebutuhan sistem yang diperlukan dalam pengembangan sistem deteksi *defacement* secara otomatis. Analisis dilakukan berdasarkan permasalahan yang teridentifikasi pada proses pemantauan situs web yang masih berjalan dengan cara manual. Analisis kebutuhan sistem disajikan dalam Tabel 1.

Tabel 1. Analisis Kebutuhan

Tabel Analisis Kebutuhan		
Masalah	**Dampak**	**Kebutuhan**
Monitoring situs masih dilakukan secara manual	Waktu pengecekan lebih lama, potensi human error tinggi	*Workflow* otomatis yang berjalan berkala tanpa campur tangan operator
Belum ada sistem yang mendeteksi kata kunci berbahaya seperti "judol", "bokep"	*Defacement* bisa terlambat diketahui	Sistem perlu memiliki fitur pencocokan kata kunci pada konten HTML
Tidak ada notifikasi cepat ketika terjadi perubahan konten	Penanganan insiden terlambat	Integrasi dengan Discord Webhook untuk alert real-time
Workflow sulit dikembangkan jika dibuat manual atau berbasis *script*	Skalabilitas rendah	Sistem harus modular menggunakan node pada n8n agar mudah diperluas
Akses situs perlu dilakukan berkala tanpa pengawasan	Tingkat keamanan tidak stabil	Menetapkan interval *schedule trigger* sebagai pemicu *workflow*

2.3 Perancangan Sistem

Pada tahap perancangan sistem, dirancang mekanisme untuk mendeteksi *defacement* dengan menggunakan otomatisasi *workflow* berbasis n8n. Sistem ini dirancang dalam bentuk *workflow* yang terdiri dari beberapa node utama yang saling terkait. Pendekatan alur kerja visual pada platform otomatisasi memungkinkan integrasi berbagai layanan dilakukan secara terpisah dan dapat dengan mudah disesuaikan[12].

Alur kerja yang dikembangkan dalam penelitian ini terdiri dari tiga komponen utama, yaitu:

A. *Schedule trigger*

Node ini berfungsi sebagai pemicu otomatis yang menjalankan proses pemantauan situs web secara rutin berdasarkan interval waktu yang telah ditentukan. Interval waktu ini dapat diatur berdasarkan hitungan detik, menit, jam, hari, minggu, hingga bulan.

B. Function / Node JavaScript

Node ini berfungsi untuk membaca isi halaman situs web yang sedang dipantau dan melakukan perbandingan dengan data sebelumnya untuk menemukan perubahan konten yang mungkin menunjukkan tanda-tanda serangan *defacement*.

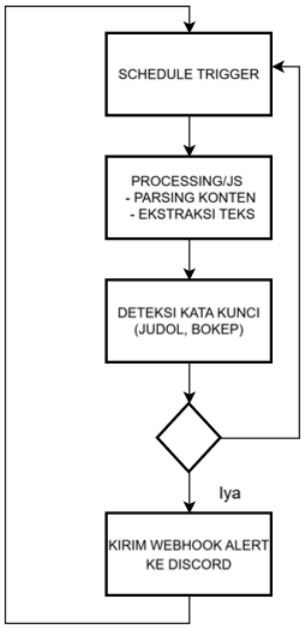
C. Webhook Discord

Node ini berfungsi sebagai titik akhir untuk notifikasi yang akan mengirimkan pesan secara otomatis kepada *administrator* sistem apabila terdeteksi adanya perubahan konten pada situs web. Discord dipilih sebagai media notifikasi karena menyediakan mekanisme webhook yang mudah diintegrasikan dengan berbagai layanan otomatisasi tanpa memerlukan konfigurasi yang kompleks. Selain itu, pesan yang dikirim melalui Discord dapat diterima secara real-time pada perangkat pengguna, sehingga *administrator* dapat segera mengetahui adanya indikasi perubahan konten yang mencurigakan dan melakukan tindakan penanganan lebih cepat.

Model alur kerja visual ini mendukung peneliti dalam memahami pergerakan data dari satu node ke node lainnya serta memfasilitasi proses evaluasi ketika alur kerja tidak berjalan seperti yang diharapkan.

Di bawah ini merupakan penjelasan tentang cara kerja sistem yang digambarkan melalui diagram alur.

Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 5 No. 1 Januari 2023 Hal. 36-41
http://jurnal.unidha.ac.id/index.php/jteksis
E-ISSN :2655-8238
P-ISSN : 2964-2132



Gambar 2. Diagram Alur Sistem

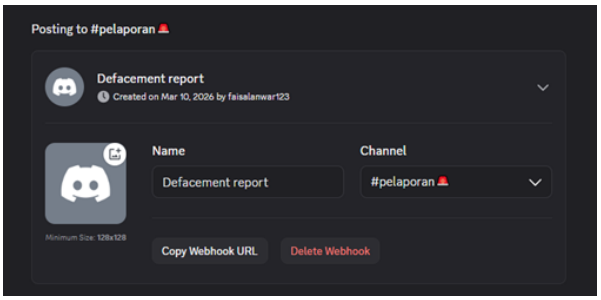
2.4 Implementasi Sistem

Proses pelaksanaan dilakukan dengan meng-install dan menjalankan platform n8n melalui Docker di lingkungan pengujian lokal (localhost). Penggunaan lingkungan localhost bertujuan untuk menguji sistem yang sedang dikembangkan sebelum diterapkan di lingkungan yang lebih luas. Pendekatan ini banyak diterapkan dalam pengembangan perangkat lunak untuk memastikan bahwa sistem berfungsi dengan baik dan mengurangi kesalahan konfigurasi selama proses implementasi[17].

Pada tahap ini, konfigurasi alur kerja atau *workflow* di n8n dilakukan sesuai dengan desain sistem yang telah disusun. Sistem tersebut kemudian terhubung dengan situs web yang akan diawasi dengan node function yang sudah diatur. Penelitian ini diujikan ke salah satu domain milik pemerintah, yaitu domain bekasikab.go.id. Situs web tersebut digunakan sebagai objek pengujian untuk mengamati kemampuan sistem dalam mendeteksi perubahan isi halaman situs yang mungkin menunjukkan tanda-tanda serangan *defacement*.

Gambar 3.Alur Kerja Sistem

Alur kerja n8n ini dibuat untuk secara otomatis memantau kata kunci di domain yang ditargetkan. Node *Schedule trigger* diatur untuk melakukan pemindaian setiap 30 menit. Selanjutnya, Fungsi Node memanfaatkan skrip JavaScript untuk menyaring kata kunci tertentu dan menyiapkan template untuk pesan darurat. Kata kunci difokuskan pada kata-kata yang tidak pantas yang sering dimasukkan oleh pihak-pihak yang tidak bertanggung jawab, seperti “judol”, “gacor”, “bokep” dan “slot”. Selanjutnya, function yang menemukan kata kunci tersebut akan mengirim pesan melalui Node Webhook ke saluran Discord yang telah ditentukan sebelumnya.



Gambar 4. Webhook Discord

HASIL DAN PEMBAHASAN

3.1 Pengujian Sistem

Pengujian sistem dilakukan dengan mengatur sistem pemantauan untuk mendeteksi munculnya kata kunci tertentu yang sering muncul pada kasus *defacement*, yaitu “judol”, “bokep”, “gacor”, dan “slot”. Sistem ini beroperasi dengan pemantauan yang dilakukan setiap 30 menit melalui *schedule trigger* dalam alur kerja n8n. Penentuan waktu ini dimaksudkan untuk menguji apakah sistem dapat berfungsi dengan stabil pada awal penerapannya dan dapat mendeteksi perubahan konten dalam waktu yang cukup singkat.

Proses pengawasan dilakukan pada domain bekasikab. go.id dengan memanfaatkan metode pencarian yang berdasarkan kata kunci di halaman web yang telah terindeks. Setiap siklus pengawasan akan meneliti apakah ada munculnya kata kunci yang telah ditentukan. Jika sistem mendeteksi adanya kemungkinan kemunculan kata kunci tersebut, maka alur kerja akan secara otomatis mengirimkan pemberitahuan kepada *administrator* melalui webhook Discord.

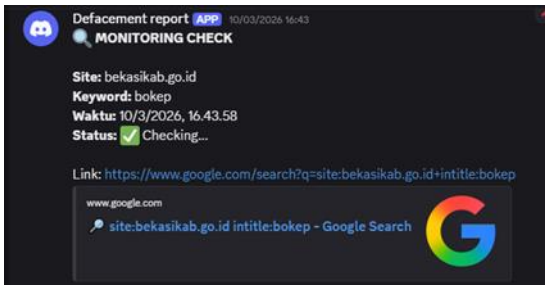
Berdasarkan hasil uji yang telah dilaksanakan, sistem dapat mengenali semua kata kunci yang telah ditetapkan sebelumnya. Selain itu, sistem juga berhasil secara otomatis mengirimkan pesan pemberitahuan yang mencakup informasi mengenai domain yang telah terdeteksi, kata kunci yang

Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 5 No. 1 Januari 2023 Hal. 36-41
http://jurnal.unidha.ac.id/index.php/jteksis

E-ISSN :**2655-8238**
P-ISSN : **2964-2132**

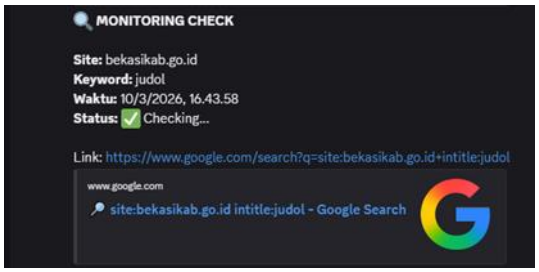
ditemukan, serta waktu pelaksanaan proses pemantauan.

Notifikasi yang diterima melalui Discord juga menyertakan link langsung menuju hasil pencarian yang terkait dengan domain yang sedang dipantau. Dengan adanya tautan ini, *administrator* dapat dengan mudah dan cepat mengakses laman yang menunjukkan perubahan isi tanpa harus melakukan pencarian secara manual.



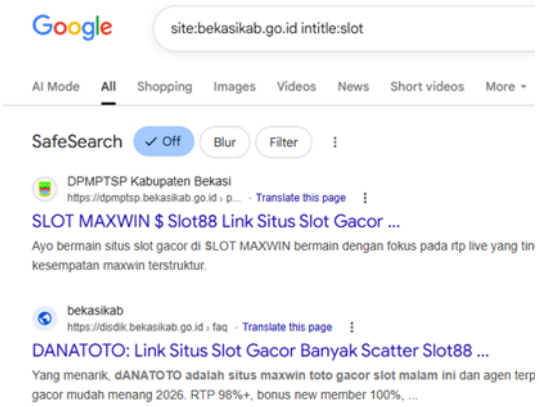
Gambar 5. Pesan dengan kata kunci bokep

Gambar 6. Pesan dengan kata kunci slot



Gambar 7. Pesan dengan kata kunci judol

Gambar 8. Pesan dengan kata kunci gacor



Gambar 9. Isi tautan pada pesan

Selanjutnya dilakukan pemantauan sistem untuk menguji apakah sistem benar-benar mengirim pesan sesuai dengan *schedule trigger* yang sudah diatur, yaitu setiap 30 menit. Hasil pemantauan tersebut kemudian disajikan kedalam tabel pengujian.

Tabel 2. Pengujian Sistem

Waktu Pengujian	Kata Kunci Terdeteksi	Domain	Notifikasi	Status
22:00	semua	bekasikab.go.id	Terkirim	Berhasil
22:30	semua	bekasikab.go.id	Terkirim	Berhasil
23:00	semua	bekasikab.go.id	Terkirim	Berhasil
23:30	semua	bekasikab.go.id	Terkirim	Berhasil

KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, dapat ditarik disimpulkan bahwa sistem yang dibuat untuk mengotomatiskan pendeteksian *defacement* pada situs web pemerintah dapat berfungsi dengan baik. Sistem yang dikembangkan dengan menggunakan alur kerja otomatis di platform n8n dapat melakukan pemeriksaan secara rutin terhadap domain yang telah ditentukan serta mengidentifikasi munculnya kata kunci yang mungkin menunjukkan adanya perubahan konten pada situs web. Hasil dari pengujian menunjukkan bahwa sistem berhasil mengenali kata kunci yang telah ditentukan, yaitu “judol”, “bokep”, “gacor”, dan “slot”, serta mampu secara otomatis mengirimkan notifikasi peringatan kepada *administrator* melalui Discord. Notifikasi tersebut juga menyertakan tautan menuju hasil pencarian yang relevan, sehingga *administrator* dapat dengan segera melakukan verifikasi terhadap halaman yang diduga telah mengalami perubahan.

Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 5 No. 1 Januari 2023 Hal. 36-41
http://jurnal.unidha.ac.id/index.php/jteksis

E-ISSN : **2655-8238**
P-ISSN : **2964-2132**

Walaupun sistem telah dapat melakukan fungsi pemantauan dan pemberitahuan dengan efektif, masih ada kemungkinan untuk melakukan perbaikan dalam penelitian di masa mendatang. Pengembangan dapat dilakukan dengan mengintegrasikan metode pemindaian langsung pada isi halaman *website*, sehingga proses deteksi tidak hanya bergantung pada pencarian kata kunci. Selain itu, sistem dapat diperluas dengan menambahkan integrasi notifikasi ke berbagai platform lain seperti email atau aplikasi pesan instan, sehingga informasi peringatan dapat diterima oleh *administrator* melalui beberapa saluran komunikasi. Melalui pengembangan ini, diharapkan sistem pemantauan keamanan situs web akan menjadi lebih tepat, cepat, dan mampu beradaptasi dengan berbagai jenis serangan *defacement*.

UCAPAN TERIMAKASIH

Rasa terima kasih penulis sampaikan kepada semua pihak yang telah membantu proses penelitian ini. Kepada Tuhan Yang Maha Esa, kepada kedua orang tua yang selalu menyertakan doa, kepada dosen mata kuliah Karya Tulis Ilmiah Program Studi Sistem Informasi UNISKA yang telah memberi arahan agar artikel ilmiah ini menjadi lebih baik dan kepada teman yang sudah memberikan saran dan dukungan agar penulis selalu semangat dalam menuntaskan artikel ilmiah ini.

DAFTAR PUSTAKA

[1] Y. Jumaryadi and J. Desmon, "Systematic Literature Review: Serangan Deface *Website* sebagai Bentuk Kejahatan Siber," *Just IT J. Sist. Informasi, Teknol. Inf. dan Komput.*, vol. 14, no. 2, pp. 106–112, 2023. https://doi.org/10.24853/justit.14.2.106-112

[2] F. E. Putri and F. Z. An Nibras, "Analysis of *Website* Vulnerability to *Defacement* Attacks," *J. Sist. Inf. dan Teknol. Inf.*, vol. 2, no. 1, pp. 152–156, 2025. https://doi.org/10.33197/justinfo.v2i1.1806

[3] P. Agustin and A. Wahyu, "Analisis Keamanan Situs .go.id Terhadap Serangan Web *Defacement* Judi *Online*," *In Search*, vol. 24, no. 1, 2025. https://doi.org/10.37278/insearch.v24i1.1125

[4] L. M. Zagi, G. P. Digdo, and W. Shalannanda, "Just Dork and Crawl: Measuring Illegal *Online* Gambling *Defacement* in Indonesian *Websites*," *arXiv Prepr.*, 2025. https://doi.org/10.48550/arXiv.2508.19368

[5] C. Kurniawan and A. Triayudi, "File Integrity Monitoring as a Method for Detecting and Preventing Web *Defacement* Attacks," *J. Online Inform.*, vol. 9, no. 2, pp. 276–285, 2024. https://doi.org/10.15575/join.v9i2.1326

[6] N. Mamuriyah, S. E. Prasetyo, and A. O. Sijabat, "Rancangan Sistem Keamanan Jaringan dari Serangan DDoS Menggunakan Metode Pengujian Penetrasi," *J. Teknol. dan Sist. Inf. Bisnis*, vol. 6, no. 1, pp. 162–167, 2024. https://doi.org/10.47233/jteksis.v6i1.1124

[7] D. A. Artika, D. Rumahorbo, M. H. Al-Majid, and D. Kiswanto, "Implementasi Sistem Keamanan *Website* dengan Analisis Log dan Deteksi Aktivitas Anomali Menggunakan Isolation Forest," *J. Inform. dan Tek. Elektro Terap.*, vol. 13, no. 3S1, 2025. https://doi.org/10.23960/jitet.v13i3S1.8133

[8] B. Haryanto and D. W. Chandra, "Implementasi Wazuh Integritas File untuk Perlindungan Keamanan Berdasarkan Aktivitas Log di BTSI UKSW," *J. Indones. Manaj. Inform. dan Komun.*, vol. 5, no. 1, pp. 183–192, 2024. https://doi.org/10.35870/jimik.v5i1.447

[9] A. R. Amir and S. M. Atif, "Evaluating *Workflow* Automation Efficiency Using n8n," 2026. https://doi.org/10.48550/arXiv.2602.01311

[10] R. D. Ahmad H., E. A. Hadi, and E. Rusnandi, "Automation of Technical Documentation Validation *Workflow*s Based on GitHub Using n8n During Software Development Stages," *J. Multimed. Technol. Appl. Softw.*, vol. 2, no. 2, pp. 64–69, 2025. https://doi.org/10.71266/jmtas.v2i2.62

[11] A. Ramadhani, M. D. Yantoro, M. F. Akmal, M. Mahfud, and Fauzi, "Chatbot Otomatis dengan n8n dan AI untuk Analisis Data dan Pelaporan Hasil," *J. Ris. Tek. Komput.*, vol. 2, no. 2, pp. 18–23, 2025. https://doi.org/10.69714/x1p94182

[12] W. Pratama and F. A. Ahda, "Inovasi Agen AI dalam Sistem Pencatatan Struk Digital Otomatis Berbasis n8n," *J. FASILKOM*, vol. 15, no. 3, 2025. https://doi.org/10.37859/jf.v15i3.10366

[13] T. Mary and N. Febriyani, "Peningkatan keamanan sistem informasi berbasis Laravel 12 dengan rate limiting dan role-based access control (RBAC)," *J. Teknol. dan Sist. Inf. Bisnis*, vol. 7, no. 3, pp. 473–481, 2025. https://doi.org/10.47233/jteksis.v7i3.1976

[14] Y. Permatasari and R. F. Aji, "Evaluasi dan Rekomendasi Perbaikan Proses Pemenuhan Permintaan Layanan Teknologi Informasi: Studi Kasus PT Bank XYZ," *J. Teknol. dan Sist. Inf. Bisnis*, vol. 7, no. 1, 2025. https://doi.org/10.47233/jteksis.v7i1.1769

[15] D. Merkel, "Docker: Lightweight Linux Containers for Consistent Development and Deployment," *Linux J.*, no. 239, 2014. https://dl.acm.org/doi/10.5555/2600239.2600241

[16] C. Pahl, "Containerization and the PaaS Cloud," *IEEE Cloud Comput.*, vol. 2, no. 3, pp. 24–31, 2015. 10.1109/MCC.2015.51

[17] R. Pressman and B. Maxim, *Software Engineering: A Practitioner's Approach*, 9th ed. New York: McGraw-Hill Education, 2020. https://books.google.com/books?id=bL7QZHtWvaUC