JIKO (Jurnal Informatika dan Komputer) Akreditasi KEMENRISTEKDIKTI, No.105/E/KPT/2022
Vol. 5, No. 2, Agustus 2022, hlm. 150-155 p-ISSN: 2614-8897
DOI: 10.33387/jiko e-ISSN: 2656-1948

# *PERANCANGAN WEB DEFACEMENT MONITORING* DENGAN MENGGUNAKAN METODE KOMPARASI NILAI HASH1

**Nurina I Septiani[1], Agung Sediyono[2], Abdul Rochman[3]**

[1,2,3]Program Studi Teknik Informatika Fakultas Teknologi Industri Universitas Trisakti
Email: [1]nurina064001800511@std.trisakti.ac.id, [2]agung.sediyono@trisakti.ac.id, [3]abdul.rochman@trisakti.ac.id

**Abstrak**

(Naskah masuk: 31 Juli 2022, diterima untuk diterbitkan: 07 Agustus 2022)

Laman *website* merupakan sarana penyampaian informasi penting bagi suatu organisasi, termasuk instansi Pemerintah. Lebih dari itu, laman *website* juga memiliki peran yang signifikan dalam mempresentasikan citra organisasi. Berdasarkan hal tersebut, *website* perlu dijaga keutuhannya dari segala usaha perubahan informasi karena dapat berdampak kepada citra organisasi yang pada akhirnya dapat menurunkan kepercayaan publik terhadap organisasi tersebut. Salah satu yang sering terjadi adalah *Web Defacement*. Saat ini, pemantauan terhadap keterjadian *Web Defacement* di Organisasi XYZ dalam Kementerian ABC masih dilakukan secara manual dan pendeteksian perubahan tampilan dari halaman *website* tidak diketahui secara cepat. Supaya kerusakan informasi dapat diperbaiki dalam waktu singkat, diperlukan *Web Defacement Monitoring (WDM).* Penelitian ini mengusulkan pembuatan aplikasi WDM dengan menggunakan metoda Komparasi Nilai Hash SHA1. Aplikasi ini dapat mendeteksi adanya perubahan tampilan visual pada konten *text* dalam halaman *website*. Sebagai tindakan perlindungan atas serangan keamanan informasi dari *web defacement*, perlu dilakukan pemantauan tampilan dari halaman *website* pada sistem aplikasi. Hasil percobaan menunjukan aplikasi ini mampu mendeteksi sekecil apapun perubahan *text* yang ada pada laman *website*.

**Kata kunci**: *Web Defacement, Keamanan Informasi, Hash SHA1*

# *DESIGN OF WEB DEFACEMENT MONITORING USING THE SHA1 HASH VALUE COMPARISON METHOD*

***Abstract***

*Webpages are important pages to delivering information that is used by an organization, including government agencies. More than that, website pages also have a significant role in presenting the image of the organization. Therefore, it is important to keep the information integrity in every page because it can have an impact to the organization's image and then it can lead to the decrease of public trust to the organization. Till now, hacker tries to hack information integrity on website namely web defacement. Currently, monitoring of the occurrence of Web Defacement in the XYZ Organization within the Ministry of ABC is still done manually and the detection of changes in the appearance of the website page is not known quickly. To cop this issue, we need to design Web Defacement Monitoring (WDM). This research proposes WDM using the SHA1 Hash Value Comparison method. This website application that can detect changes in the visual appearance of text content on web pages. As a protection measure for information security attacks from web defacement, it is necessary to monitor the appearance of web pages on the application system. Experiment result show that this application performs to detect any changing text in webpage even only one character.*

**Keywords**: *Web Defacement, Information Security, Hash SHA1*

## 1. PENDAHULUAN

Penggunaan teknologi informasi oleh organisasi pemerintahan sekarang menjadi hal yang sangat penting, salah satunya dengan penggunaan *website* [1]. Penyampaian informasi untuk masyarakat bisa dimulai dari penyediaan *website* dimana hal tersebut juga sebagai langkah awal implementasi *e-Government* [11]. Lebih dari itu, *website* bukan hanya sebagai media penyampaian informasi, namun saat ini juga digunakan sebagai media untuk peningkatan citra organisasi pemerintah [2][3].

Pada keamanan sistem informasi, *threat* (ancaman keamanan informasi) merupakan keadaan dimana kerentanan yang dimiliki oleh suatu sistem memungkinkan dieksploitasi atau dimanfaatkan oleh

pihak yang tidak bertanggung jawab untuk melakukan serangan keamanan informasi. Ancaman yang mengeksploitasi kerentanan tersebut dapat menyebabkan hilangnya kerahasiaan, keutuhan, dan ketersediaan dari aset bisnis. Ancaman selalu ada sehingga tidak bisa dihilangkan namun bisa dikendalikan [4]. Indonesia sendiri termasuk negara terbesar dalam hal *threat exposure rate* [15].

Menurut UU ITE No 11 tahun 2008, "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik"[5]. Dalam UU ITE tersebut dikatakan melakukan manipulasi, manipulasi disini adalah merubah halaman *website* atau sejenisnya menjadi tidak sesuai akan mendapatkan sanksi hukum. Aksi peretasan yang biasa terjadi pada *website* adalah *web defacement*. *Web Defacement* merupakan serangan pada satu halaman *web* atau situs *web* dengan melakukan perubahan tampilan visual pada konten yang tidak sah. Serangan ini dilakukan secara sebagian atau diganti sepenuhnya dengan merubah konten halaman *web*, mengganti halaman *web* sepenuhnya ataupun menghapus halaman *web* [6].

*Web defacement* bisa menyerang *website* swasta maupun organisasi pemerintah. Pada organisasi swasta, sistem informasi penjualan *online* berbasis web pada batik Widi Nugraha Ngawi [9] bisa terkena *web defacement* yang dapat menyebabkan informasi harga yang ditampilkan berubah dan menyebabkan kerugian bagi pengelola yang pada akhirnya berdampak pada kepercayaan pelanggan. Pada organisasi pemerintah, *web defacement* termasuk ke dalam *security incident yang* dilaporkan, ditangani, dan dipublikasikan secara berkala oleh Id-SIIRTI/CC [10].

Organisasi XYZ yang mengelola keamanan aset informasi Data Center (DC) Kementerian ABC harus melindungi kerahasiaan, keutuhan, dan ketersediaan aset informasi. Sebagai tindakan perlindungan atas serangan keamanan informasi pada sistem aplikasi dari *web defacement*, Organisasi XYZ secara berkala melakukan pemantauan tampilan dari halaman *website* pada sistem aplikasi. Saat ini, pemantauan tampilan dari suatu *website* pada sistem aplikasi masih dilakukan secara manual dan pendeteksian perubahan tampilan dari halaman *website* tidak diketahui secara cepat. Hal tersebut dapat menyebabkan terekspos nya kejadian tersebut oleh media nasional sehingga berdampak pada menurunnya reputasi Kementerian ABC. Berdasarkan data 3 tahun terakhir, kejadian *web defacement* yang mengeksploitasi *web* Kementerian ABC dan terekspos oleh media nasional mengalami peningkatan.

Dalam mengatasi permasalahan tersebut, penulis mengajukan aplikasi *Web Defacement Monitoring* yang dapat mendeteksi perubahan tampilan halaman *web* dan mengirimkan notifikasi hasil pendeteksiannya. Pengiriman notifikasi berguna untuk mempercepat penanganan kejadian *web defacement*.

## 2. METODE PENELITIAN

Metode penelitian yang digunakan adalah Metode *Prototyping* [7][13], dengan tahapan sebagai berikut:

1. *Requirements Analysis*
   Pada tahap ini, dilakukan beberapa hal yaitu:
   a. Penggalian informasi kebutuhan *user*, yang dapat dituangkan dalam Aplikasi *Web Defacement Monitoring*
   b. Pengumpulan data dukung yang dibutuhkan dalam membangun Aplikasi *Web Defacement Monitoring*
   c. Melakukan pemetaaan antara kebutuhan dan data dukung yang telah didapatkan, kemudian melakukan analisis dari data tersebut.
2. *Design and Planning*
   Pada tahap ini, dilakukan beberapa hal yaitu:
   a. Membuat *design* atau rancangan aplikasi. Perancangan aplikasi yang digambarkan dalam bentuk *Use Case Diagram, Class Diagram* dan *Activity Diagram.*
   b. Identifikasi komponen / ruang lingkup dalam aplikasi *Web Defacement Monitoring*.
   c. Melakukan perancangan *user interface*.
3. *Code*
   Dalam tahap ini mulai dilakukan pembangunan Aplikasi *Web Defacement Monitoring*, dengan melakukan pengkodean atau menuangkan rancangan aplikasi yang telah dibuat sebelumnya ke dalam bentuk aplikasi dengan menggunakan bahasa pemrograman *python*.

   Pada pendeteksian perubahan tampilan halaman *web*, penelitian ini menggunakan metode algoritma SHA1 *hashing* [8][14]. Dalam prosesnya, data daftar URL master dari *database* terlebih dahulu diambil kemudian langkah selanjutnya yang dilakukan, yaitu *crawling* data. *Crawling* data merupakan metode untuk mengumpulkan data informasi yang diinginkan dalam suatu *website* [12]. Pada penelitian ini, *crawling* digunakan untuk mengambil data halaman *website* terkini. Setelah proses tersebut berhasil, hasil *crawling* url yang berupa teks dihapus semua karakter *whitespace* sehingga menyambung menjadi 1 teks panjang tanpa jeda (*string*). Kemudian string tersebut dipotong tanpa jeda sesuai dengan panjang yang diinginkan dan disimpan dalam bentuk *list* (*chunk*). Setiap *chunk* potongan *string* dienkripsi menggunakan SHA1. Selanjutnya *hash* awal dengan *hash* terkini dibandingkan untuk mendapatkan hasil komparasi.

   Dalam rangka memenuhi hal tersebut, diperlukan pembangunan aplikasi yang dapat

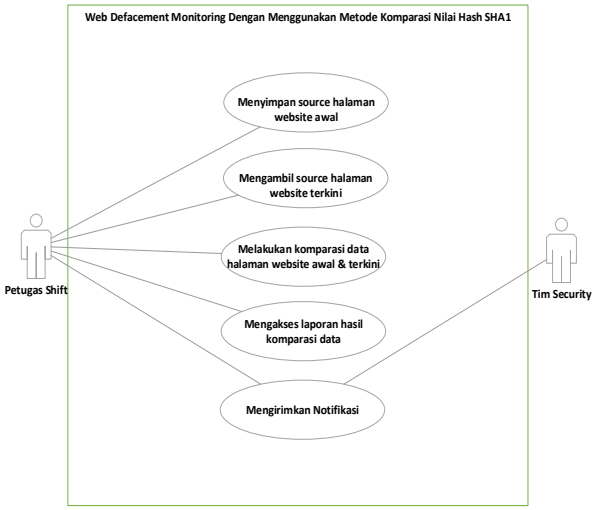
mengirimkan anomali hasil pendeteksian *web defacement* ke pengguna aplikasi. Fitur ini diperlukan oleh petugas keamanan informasi di Organisasi XYZ dalam mendeteksi adanya insiden *web defacement* agar dapat ditangani sesegera mungkin. Dengan demikian, *output* dalam penelitian ini adalah aplikasi *Web Defacement Monitoring* berdasarkan metode algoritma SHA1 *hashing* beserta hasil pengujian terhadap keakurasian perubahan data pada beberapa halaman web di sistem TIK yang memiliki tingkat kritikalitas tinggi atau sangat tinggi di Kementerian ABC.

4. *Tests*
   Dalam tahap ini, dilakukan *testing performance* Aplikasi *Web Defacement Monitoring* yang telah selesai dibangun.
5. *Release*
   Dalam tahap ini, dilakukan *release* Aplikasi *Web Defacement Monitoring* dengan cara melakukan *hosting* aplikasi tersebut ke *server local* atau *development*. Pada tahap ini, harus dipastikan bahwa integrasi antara fitur yang sudah dan akan dilakukan *release* untuk dapat berjalan dengan baik ketika proses *release* selesai dilakukan.

## 3. HASIL DAN PEMBAHASAN

1. *Use Case Diagram*

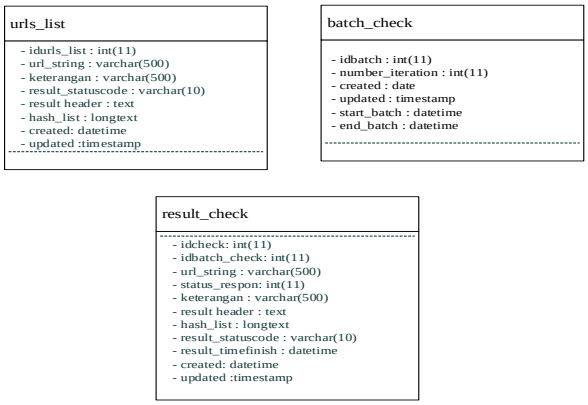
Pada perancangan aplikasi *Use Case Diagram* terdapat 2 aktor dan 5 use case. Perancangan *Use Case Diagram* dapat dilihat pada Gambar 2.




Gambar 2. *Use Case Diagram Aplikasi Web Defacement Monitoring*

2. *Class Diagram*

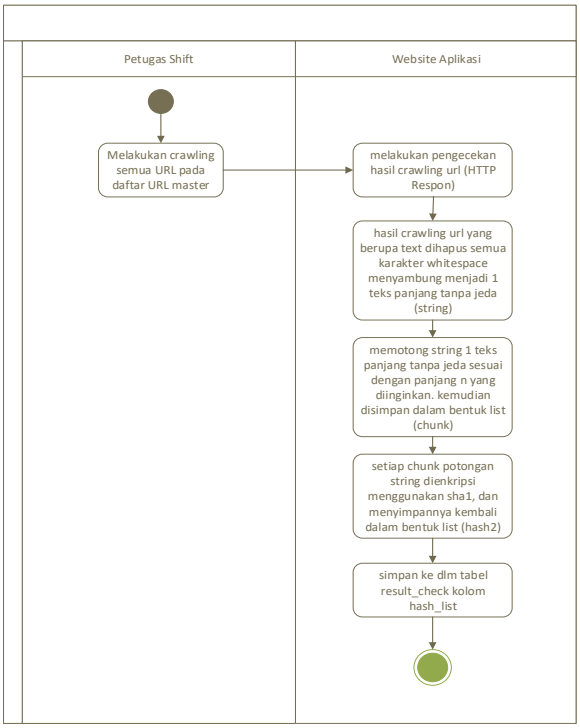
Pada perancangan *Class Diagram* terdapat 3 tabel, yaitu urls_list untuk menyimpan data url yang akan dilakukan pengecekan dengan metode *hash*, batch_check untuk menyimpan data history url yang dilakukan pengecekan, dan result_check untuk menyimpan data hasil pengecekan akhir. Perancangan *Class Diagram* dapat dilihat pada Gambar 3.




Gambar 3. *Class Diagram Aplikasi Web Defacement Monitoring*

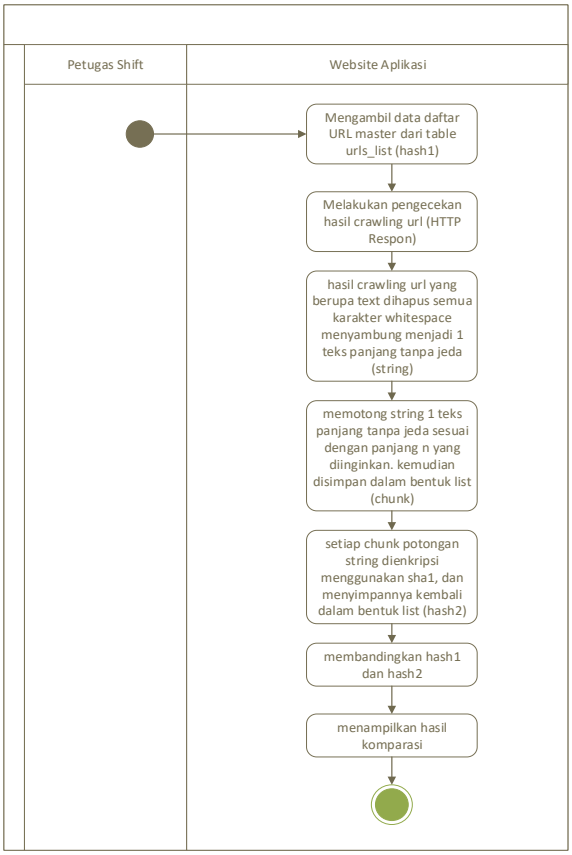
3. *Activity Diagram*

Pada perancangan *Activity Diagram* terdapat 3 aktivitas yang didefinisikan, yaitu aktivitas saat melakukan *crawl master*, cek *deface*, dan mengirim hasil komparasi ke aplikasi telegram. Pada Gambar 4 dapat terlihat aktivitas awal yang terjadi di dalam aplikasi mulai dari *crawling* url master, proses *hash*, hingga simpan hasil *hash* master.



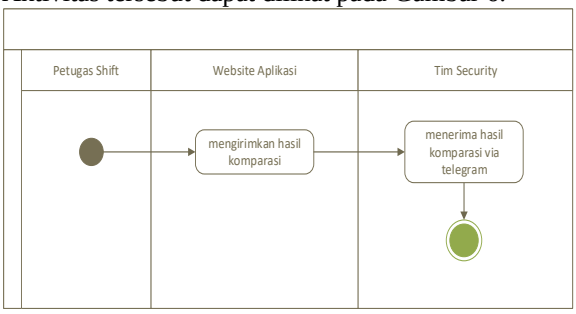

Gambar 4. *Activity Diagram* saat *Crawl Master*

Setelah hasil *hash* master disimpan, hasil *hash* master tersebut dijadikan acuan awal untuk kemudian dikomparasikan dengan hasil *hash* berikutnya. Pada Gambar 5 dapat terlihat proses komparasi, mulai dari mengambil hasil *hash* master, *crawling* url terkini, proses *hash* terkini, komparasi hasil *hash* master dengan *hash* terkini, hingga menampilkan hasil komparasi.




Gambar 5. *Activity Diagram* saat melakukan cek *deface*

Pada aktivitas terakhir, hasil komparasi antara *hash* master dan *hash* kedua dikirimkan dari Petugas *Shift* ke Tim *Security* melalui aplikasi Telegram. Aktivitas tersebut dapat dilihat pada Gambar 6.

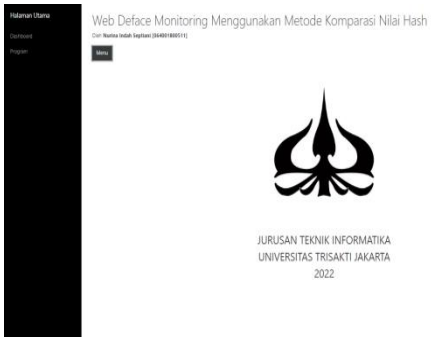



Gambar 6. *Activity Diagram* saat mengirim telegram

4. Penjelasan mengenai *Web Defacement Monitoring* Dengan Menggunakan Metode Komparasi Nilai Hash SHA1

4.1. Halaman Utama

Pada halaman utama, *user* akan diberikan 2 pilihan menu, yang pertama yaitu adalah *Dashboard* dan yang kedua adalah Program.




Gambar 7. Halaman Utama

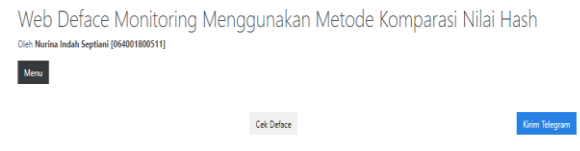
4.2 *Dashboard* dan Grafik

Tampilan berikut merupakan tampilan pada halaman *dashboard* yang menampilkan nilai dari komparasi *hash*. Nilai 0 yang berarti hasil pengecekan halaman *website* tidak sama dengan aslinya, dan nilai 100 yang berarti sama dengan aslinya.


Gambar 8. Halaman *Dashboard*

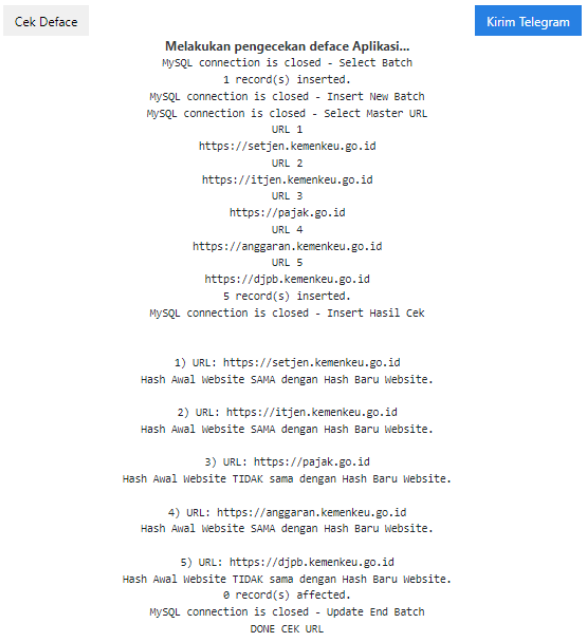
Apabila diklik pada setiap url *name* maka tampilan akan diarahkan ke halaman *detail* yang menampilkan grafik dari hasil pengecekan pada setiap *batch*. Grafik yang disajikan adalah diagram garis.

4.3 Halaman Program




Gambar 9. Halaman Program

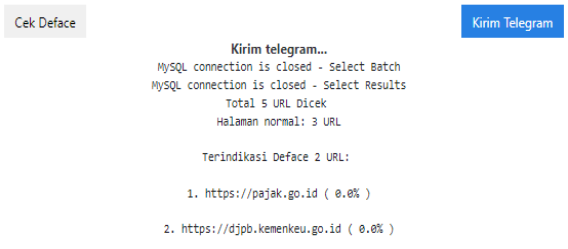
Halaman Program merupakan halaman yang memiliki 2 menu yaitu Cek *Deface* dan Kirim Telegram.




Gambar 10. Hasil Proses Cek *Deface*

Pada gambar di atas menunjukkan proses saat *user* menjalankan menu Cek *Deface*. Proses pertama kali yang dilakukan ialah mengambil data daftar URL *master* dari *database*, kemudian langkah selanjutnya yang dilakukan yaitu melakukan perulangan pengecekan hasil *crawlimg* url untuk mengambil data halaman *website* terkini. Setelah proses tersebut berhasil, hasil *crawling* url yang berupa *text* dihapus semua karakter *whitespace* menyambung menjadi 1 teks panjang tanpa jeda (*string*). Kemudian *string* tersebut dipotong tanpa jeda sesuai dengan panjang n yang diinginkan dan disimpan dalam bentuk *list* (*chunk*). Setiap *chunk* potongan *string* dienkripsi menggunakan SHA1. Selanjutnya *hash* awal dengan *hash* terkini dibandingkan untuk mendapatkan hasil komparasi.

4.4 Hasil Pengecekan pada Telegram




Gambar 11. Halaman Kirim Telegram

Pada halaman proses Kirim Telegram, hanya menunjukkan jumlah total URL di cek, jumlah halaman URL yang normal serta nama url yang terindikasi *deface*.

## 4. KESIMPULAN

Berdasarkan penelitian, didapatkan kesimpulan bahwa hasil perancangan aplikasi *Web Defacement Monitoring* dengan menggunakan metode komparasi nilai *hash* SHA1 dapat membantu pemantauan *Web Defacement.* Aplikasi *Web Defacement Monitoring* dapat membantu Petugas *Shift* di Organisasi XYZ dalam memantau ada atau tidaknya *Web Defacement* dengan lebih mudah, terotomasi, dan lebih cepat untuk mendapatkan hasilnya. Fitur untuk mengirimkan hasil komparasi secara otomatis melalui aplikasi Telegram juga sangat membantu dalam hal pelaporan. Tim *Security* Organisasi XYZ dapat turut memantau dan menganalisis berdasarkan hasil pemantauan yang dikirim melalui Telegram. Saran untuk perancangan dan pengembangan ke depannya adalah penambahan fitur *scheduler*. Hal ini untuk membantu Petugas *Shift* agar tidak melakukan klik tombol secara manual dan hasil komparasi dapat terkirim dengan durasi waktu yang lebih konsisten.

## 5. DAFTAR PUSTAKA

[1] S Ilham, M.N. Norma, G Anthonius. 2018. “Peranan Penggunaan Website Sebagai Media Informasi Dinas Pariwisata Kabupaten Halmahera Utara”

[2] Y. J. Aprianantа dan L. S. Wijaya, 2018. “Penggunaan Website dan Media Sosial dalam Membangun Citra Positif Perguruan Tinggi”., *Jurnal Komunikatif*, vol.7 no 2, pp. 187–209

[3] B. S. Dianingtyas dan N. S. Rejeki. 2014. “Pengaruh Kualitas Informasi Website Terhadap Citra Pemerintah Kabupaten Wonogiri”, *Universitas Atma Jaya, Yogyakarta*

[4] Yaksha., 2020. Overview of Cybersecurity Status in ASEAN and the EU: Sociedade Portuguesa de Inovacao (SPI)

[5] Undang-undang Republik Indonesia nomor 19 Tahun 2016 tentang Perubahan Atas Undang Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik

[6] R. K. Verma. 2015. “Implementation of Web Defacement Detection Technique”., *IJIET (International Journal of Innovations in Engineering and Technology*), vol 6 (1), pp.134-135

[7] R. S Pressman., 2020. Software Engineering: A Practitioner’s Approach

[8] Y. M. Rambonang. 2015. “Klien Autentikasi Menggunakan Algoritma SHA-1 Dengan Protokol Two Way Challenge-Response pada Transaksi Web-based”., Universitas Sanata Dharma, Yogyakarta

[9] N A Febriyanti dan M Y Arnol. 2020. “Perancangan Sistem Informasi Penjualan Online Berbasis Web pada Batik Widi Nugraha Ngawi”, *JIKO (Jurnal Informatika dan Komputer)*, vol.3(3), pp 153-158

[10] APCERT., 2018. APCERT Annual Report 2018
[11] F Masyhur, 2014. "Kinerja Website Resmi Pemerintah Provinsi di Indonesia Official Website Performance Local Government in Indonesia", *Jurnal Pekommas*, vol.17 (1), pp 9-14
[12] F A Suhamo dan L Listiyoko. 2018. "Aplikasi Berbasis Web dengan Metode Crawling sebagai Cara Pengumpulan Data untuk Mengambil Keputusan", *Seminar Nasional Rekayasa Teknologi Informasi*, pp. 105–109. ISBN:978-602-53437-0-4
[13] D Purnomo. 2017. "Model Prototyping Pada Pengembangan Sistem Informasi"., *JIMP - Jurnal Informatika Merdeka Pasuruan*, vol.2(2), pp. 54–61
[14] G E Setyawan, A Pinandito, F Pradana, 2015, "Performasi Kalkulasi Hash SHA-1 Pada Sistem Embedded Arduino", vol. 5(3), pp. 39-44, ISSN: 2087-0132
[15] J E W Prakasa. 2020. "Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi"., *Jurnal Ilmiah Teknologi Informasi Asia* , vol.14(2), pp. 75–84, ISSN: 2580-8397 (O); 0852-730X (P)