e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI : http://dx.doi.org/10.30872/jim.v14i1.1431

Implementasi Metode Simple Additive Weighting Pada Penentuan Peringkat Kerentanan Website (Studi Kasus Website Universitas Negeri Aceh)

Mukhroji [1], Rizal Munadi [2], Syahrial [3]
[1] Magister Teknik Elektro, Fakultas Teknik, Universitas Syiah Kuala
[2,3]Wireless and Networking Research Group (Winner), Teknik Elektro, Fakultas Teknik, Universitas Syiah Kuala
Jalan Teungku Syech Abdurrauf No.7, Darussalam, Banda Aceh,23111, Indonesia.
E-Mail : roeji5990@gmail.com [1], rizal.munadi@unsyiah.ac.id [2], syahrial@unsyiah.ac.id [3].

ABSTRAK

Dewasa ini, penggunaan website sebagai media informasi merupakan suatu hal lazim yang dilakukan oleh berbagai institusi atau organisasi. Informasi yang disajikan sangat bervariatif, dari hanya informasi sederhana hingga informasi yang sensitif yang memerlukan penanganan keamanan yang baik. Terjadinya tindakan penyusupan atau penyalahgunaan terhadap suatu website dapat dilakukan oleh pihak tertentu dengan berbagai motif jika tindakan pengamanan tidak diimplementasikan. Akibatnya, kerentanan website dapat mengganggu informasi yang diakses oleh masyarakat. Oleh karena itu, dalam penelitian ini kerentanan website menjadi fokus yang dikaji dan pengujian kerentanan dilakukan dengan software Open Web Application Security Project (OWASP). Kemudian, hasil dari pengujian dengan OWASP akan diimplementasikan dengan menggunakan metode Simple Additive Weighting (SAW). Penerapan metode SAW ini akan menghasilkan pengurutan nilai kerentanan dari setiap website yang diuji dan dapat menjadi gambaran kualitas keamanan website Universitas Negeri di Provinsi Aceh. Berdasarkan hasil pengujian diperoleh tingkat kerentanan tertinggi terjadi pada universitas yang tidak menggunakan CMS sebagai aplikasi pada website yang dibangun.

Kata Kunci – kerentanan, website, OWASP, SAW, keamanan

1. PENDAHULUAN

Penyajian informasi berbasis online merupakan bagian dari keterbukaan informasi bagi pengguna dan dapat diakses dimana saja secara cepat. Dalam dunia akademik, informasi yang terkait dengan kegiatan suatu institusi pendidikan disaji melalui portal informasi dengan berbagai informasi. Beberapa contoh layanan seperti website yang memuat sistem informasi akademik pengisian KRS secara online, informasi hasil evaluasi penilaian mata kuliah, pendaftaran perkuliahan secara online merupakan peningkatan efektivitas dan efisiensi dibandingkan cara konvensional.

Akses yang dapat dilakukan dari mana saja seiring dengan meningkatnya ketersediaan layanan akses internet bagi masyarakat, baik dengan koneksi langsung dengan jaringan fisik (kabel) atau jaringan nirkabel (*wireless*). Disisi lain, kemudahan akses ini dapat disalahgunakan oleh pihak yang tidak berhak jika faktor keamanan kurang diperhatikan. Oleh karena itu, keamanan informasi didalam *website* merupakan hal yang sangat penting dan harus dipertimbangkan dalam pembangunan sistem informasi. Berbagai tindak kejahatan pada Teknologi Informasi dan Komunikasi (TIK), memungkinkan terjadinya penyusupan dan aksi kontra produktif dan mengganggu sistem informasi, pencurian data, menghapus bahkan mengganti data penting *website.*

Apabila ini terjadi pada *website* kampus maka akan mengacaukan sistem yang ada didalamnya, tentu sangat besar kerugian yang akan dialami.Dalam era digital saat ini, peran teknologi Internet dirasakan makin besar karena hampir semua kegiatan bisnis dalam organisasi dapat dilakukan melalui dunia maya. Melalui Internet, segala informasi yang diinginkan dengan mudah dan cepat dapat diperoleh. Keunggulan ini tentunya dimanfaatkan oleh perguruan tinggi dalam meningkatkan mutu pendidikan dan layanannya melalui media berbasis *website*. Lebih jauh lagi *website* bagi suatu universitas merupakan wajah universitas tersebut di dunia maya (Dermawan Baginda Napitupulu, 2016).

Untuk menjaga konsistensi layanan informasi berbasis *website*, maka faktor keamanan perlu menjadi perhatian. Fokus masalah keamanan ini menjadi obyek yang dikaji oleh organisasi dalam proyek *Open Web Application Security Project* (OWASP).Dalam upaya memberikan pengamanan bagi website, OWASP menerbitkan suatu metodeyang dapat digunakan untuk menemukan celah keamanan, sehingga dengan adanya standar keamanan yang bisa digunakan para *developer* akan memberikan keamanan pada *website* yang dibangun (Riska, Ahmad & Christiyo, 2013).

Penelitian terkait mengenai kerentanan *website* telah banyak dilakukan. Aplikasi teknik serangan yang digunakan untuk mendeteksi kerentanan juga berbeda-beda.Pada penelitian yang dilakukan terhadap *website* Instansi Pemerintah (Studi Kasus Aceh) dengan menggunakan aplikasi w3af telah dilakukan dan diperoleh hasil, sekitar 50% *website* yang mempunyai celah keamanan terhadap serangan *SQL Injection*(Rizal, Surya, Ernita & Elizar, 2013). Hasil didominasi oleh *website* yang menggunakan CMS dengan proporsi terbesar, sekitar 87,5% menggunakan CMS Joomla. Pada beberapa penelitian lain, ditemukan gangguan umumnya terjadi pada halaman yang dikelola oleh administrator. Oleh karena itu, halaman (*web page*) perlu ditingkatkan pengamanan dengan melakukan

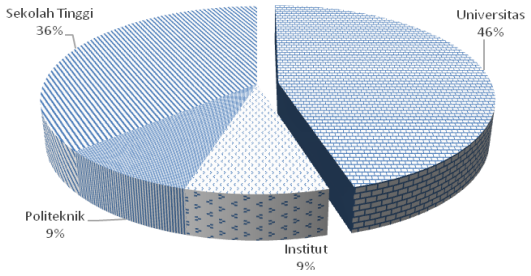
e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI : http://dx.doi.org/10.30872/jim.v14i1.1431

validasi masukan dan meneliti secara acak dalam beberapa tindakan agar konten halaman administrator aman dari serangan *SQL Injection*.Hal lain yang direkomendasikan adalah penggunaan CMS dan perlunya dilakukan pembaruan CMS secara berkala sebagai tindakan preventif.

Fokus masalah pada penelitian ini adalah menerapkan metode *Simple Additive Weighting (*SAW) pada evaluasi kerentanan untuk melihat nilai kerentanan dari *website* yang diuji.Dengan Sistem Pendukung Keputusan (SPK) yang dikembangkan menggunakan metode *Simple Additive Weighting* (SAW) dalam penentuan prioritas ini dapat mengefektifkan pengambilan keputusan yang dilakukan oleh pengambil keputusan, karena nilai setiap kriteria pada proses penentuan prioritas yang dilakukan menggunakan metode SAW telah ditentukan, sehingga proses penilaian akan lebih tepat karena didasarkan pada nilai kriteria dan bobot yang telah ditentukan. Metode *Simple Additive Weighting* ini akan menghasilkan alternatif terbaik dari sejumlah alternatif yang diberikan (Yadi Utama, 2013). Penelitian lain tentang sistem pengambilan keputusan terkait (Setiya & Fera, 2016) penentuan sistem pengambil keputusan produk unggulan. Metode yang digunakan dalam pengambilan keputusan penentuan produk unggulan adalah metode *Multiple Attribute Decision Making – Simple Additive Weighting* (MADM-SAW). Dibandingkan dengan model pengambilan keputusan yang lain, pemilihan metode MADM-SAW didasari pada kemampuannya untuk melakukan penilaian secara lebih tepat karena didasarkan pada nilai kriteria dan bobot preferensi yang sudah ditentukan, kemudian dilanjutkan dengan proses penentuan peringkat yang akan menyeleksi alternatif terbaik dari sejumlah alternatif yang ada.

2. TINJAUAN PUSAKA

Perguruan tinggi adalah satuan pendidikan penyelenggara pendidikan tinggi. Menurut jenisnya, perguruan tinggi dibagi menjadi dua, yaitu perguruan tinggi negeri yang diselenggarakan oleh pemerintah, dan perguruan tinggi swasta yang diselenggarakan oleh pihak swasta. Kedua jenis perguruan tinggi ini menjadi pilihan para mahasiswa setiap tahunnya, termasuk di Provinsi Aceh. Saat ini, ada 10 Perguruan Tinggi Negeri yang beroperasi di Aceh yang terdistribusi atas universitas (46%), institut (9%), politeknik (9%) dan sekolah tinggi (36%) seperti yang ditunjukkan pada Gambar 1.



Gambar 1. Distribusi Perguruan Tinggi Negeri di Provinsi Aceh

Dari keseluruhan PTN yang ada di Aceh, pada penelitian ini hanya diambil universitas sebagai sampel. Hal ini didasari pada dominasi sebaran fakultas dan program studi yang dikelola dalam suatu universitas. Disamping itu, universitas juga mempunyai jumlah mahasiswa yang lebih besar dibandingkan dengan PTN lain, sehingga tingkat akses informasi melalui *website* Universitas akan menjadi tinggi.

A. Simple Additive Weighting

Dari beberapa metode yang ada, *Simple Additive Weighting* (SAW) merupakan metode yang sederhana untuk pengambilan keputusan atribut jamak. Metode ini digunakan untuk menentukan suatu alternatif terbaik dari beberapa alternatif. Tahapan yang digunakan dalam penelitian ini adalah penentuan kriteria spesifik, penentuan alternatif, membuat matriks normalisasi, dan menghitung total nilai alternatif untuk mendapatkan nilai peringkat (Andri & Siti, 2014).

Penelitian terkait (Rahman Abdillah, 2017) memformulasikan perhitungan aplikasi pendukung keputusan pada beasiswa penelitian RISPRO dengan menggunakan metode SAW. Nilai akhir yang digunakan sebagai bahan acuan pengambilan keputusan, memiliki selisih yang sedikit untuk kemudian diurutkan, sehingga pengambil keputusan dapat mengambil data beberapa peserta dengan nilai yang tinggi. Dari hasil perhitungan yang didapat, penggunaan metode ini memungkinkan pengolahan data yang lebih tepat, cepat dan akurat serta dapat memberikan rekomendasi calon peserta yang layak menerima beasiswa penelitian.

$$R_{ij} \begin{cases} \dfrac{x_{ij}}{\max x_{ii}} \\ \dfrac{\min x_{ij}}{x_{ij}} \end{cases} \qquad \text{.....(1)}$$

Dimana :

Rij : Nilai peringkat kinerja ternormalisasi

xij : Nilai atribut yang dimiliki setiap kriteria

$\dfrac{x_{ij}}{\max x_{ij}}$: Nilai terbesar dari setiap kriteria

$\dfrac{\min x_{ij}}{x_{ij}}$: Nilai terkecil dari setiap kriteria

Benefit : Jika nilai terbesar adalah terbaik

Cost : Jika nilai terkecil adalah terbaik

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI : http://dx.doi.org/10.30872/jim.v14i1.1431

Dimana *rij* adalah peringkat kinerja ternormalisasi dari alternatif *Ai* pada atribut *Ci*. i = 1,2,….,m dan *j= 1,2,…,n*. Nilai prefensi untuk alternatif (*Vi*) diberikan pada persamaan 2 sebagai berikut:

$$V_{i=} w_j \, r_{ij} \quad \text{.....(2)}$$

Dimana :
V_i : Peringkat untuk setiap alternatif
w_i : Nilai bobot dari setiap kriteria
r_i : Tingkat kinerja ternormalisasi

B. Kerentanan

Peluang terjadinya kerentanan *website* telah memberikan kesempatan untuk melakukan tindakan kejahatan dunia maya serta aktivitas negatif yang dapat dilakukan pada suatu individu, kelompok atau pemerintah seperti transaksi keuangan ilegal, pelanggaran data, pencurian identitas, pencurian properti intelektual, dan lain-lain. Serangan terhadap *website* bermula dari *phishing*, menggunakan halaman *website* untuk mengirim *malware*, sehingga serangan yang lebih kompleks dapat dilakukan yang mencakup serangan *Cross Site Scripting* (XSS), *Cookies Poisioning* dan lain-lain. Tanpa langkah-langkah keamanan *website* yang efektif, efisien dan baik, maka situs *website* akan lebih mudah untuk dilakukan serangan serta membuat sistem keamanannya menjadi kritis (Satam, Kely & Harini, 2016).

C. Open Web Application Security Project

Open Web Aplication Security Project (OWASP) adalah sebuah aplikasi komunitas terbuka (*Open Source*) yang didedikasikan untuk organisasi yang memungkinkan melakukan pengembangan, dan juga pemeliharaan. Beberapa layanan yang disediakan OWASP *free* dan *open source* antara lain tool dan standar keamanan aplikasi, buku tentang uji keamanan aplikasi, pengembangan kode, dan *review* kode keamanan, serta pengendalian keamanan dan pustaka standar, beberapa cabang lokal di seluruh dunia, riset terkini, konferensi lengkap diseluruh dunia, *mailing list*, dan banyak layanan lainnya yang dapat diakses melalui *www.owasp.org*. Seluruh *tool*, dokumen, forum diskusi OWASP bebas dan terbuka bagi yang tertarik untuk memperbaiki keamanan aplikasi web (OWASP Top Ten, 2010).

Hasil dari beberapa pengujian presisi dan tingkat pengukuran kerentanan diperoleh bahwa OWASP merupakan aplikasi paling baik dari segi presisi dan tingkat pengukuran dengan persentase rata-rata pengujian adalah 95,67 %. Hasil ini jauh lebih tinggi dibandingkan *w3af*, *BurpSuite*, *Acunetix*, dan *Wapiti* (Idrissi, Berbiche, Gueroute & Shibi, 2017).

Adapun salah satu alasan menggunakan aplikasi OWASP dalam penelitian ini adalah sifatnya yang *open source* dan mudah digunakan *(friendly)*. OWASP juga dapat mendeteksi 10 peringkat teratas risiko keamanan yang rentanan menyerang *website* dan dapat memberi informasi URL yang rentan terserang, menjelaskan penyebabnya dan dan memberi solusi untuk mencegah kerentanan tersebut. Beberapa aplikasi yang serupa dengan OWASP adalah *Burb Suite, Nikto, w3af, Paros Proxy, Acunetix, SQL Map, Sqiptish, Appscan* dan *Netpaker*.

3. METODE PENELITIAN

Proses penelitian ini diawali dengan mengkaji teori yang relevan melalui buku referensi, hasil penelitian- penelitian sejenis yang pernah dilakukan sebelumnya serta dari jurnal dan publikasi ilmiah untuk mendapatkan landasan teori mengenai penelitian yang akan diteliti. Secara diagram, alur proses penelitian seperti ditunjukkan pada Gambar 2.

Gambar 2. Alur Proses Penelitian

Pengujian dilakukan dengan menguji kerentanan menggunakan aplikasi *Open Web Application Security Project* (OWASP). Pengujian dilakukan terhadap 5 *website* Universitas Negeri di Provinsi Aceh untuk mengetahui seberapa rentan *website* tersebut terhadap serangan. Hasil pengujian kerentanan berupa nilai *alerts* akan diproses menggunakan metode *Simple Additive Weighting* (SAW) untuk mendapatkan pengurutan nilai kerentanan pada setiap *website* yang diuji. Cara kerja metode SAW adalah menjumlah setiap perkalian bobot dari rating kerja pada setiap atribut, metode SAW membutuhkan proses normalisasi matriks keputusan (X) ke suatu skala yang dapat diperbandingkan dengan semua rating alternatif yang ada, tujuannya adalah agar mendapatkan nilai alternatif tertinggi diantara alternatif yang lain sebagai acuan untuk pengurutan nilai kerentanan *website* yang diuji

4. HASIL DAN PEMBAHASAN

Pada bagian ini akan menjelaskan hasil dari pengolahan dan analisa data berdasarkan metode penelitian yang telah dikemukakan. Pembahasan terfokus pada permasalahan pengujian kerentanan *website* Universitas Negeri di Aceh, dan evaluasi kerentanan akan diimplementasikan pada metode *Simple Additive Weighting* (SAW) untuk mendapatkan nilai kerentanan.

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI : http://dx.doi.org/10.30872/jim.v14i1.1431

A. Data Universitas Negeri di Provinsi Aceh

Terdapat 5 Universitas Negeri yang ada di Provinsi Aceh. Ada 2 Universitas yang terletak di ibu kota provinsi, kemudian 2 Universitas terletak pada bagian timur Provinsi Aceh, yang terakhir adalah terletak di bagian barat Provinsi Aceh. Dan berdasarkan data *Content Management System* (CMS) yang diambil dari aplikasi *Wappalyzer* (*add on*) yang di-*download* pada *browser chrome*, ada 3 universitas yang menggunakan CMS *Joomla*, 1 universitas menggunakan CMS *WordPress*, dan 1 universitas lagi tidak menggunakan CMS. Berikut rincian datanya akan ditampilkan pada Tabel 1.

Tabel 1. Data Universitas Negeri di Provinsi Aceh

Inisial PTN	CMS
Universitas 1	Joomla
Universitas 2	Non CMS
Universitas 3	Joomla
Universitas 4	WordPress
Universitas 5	Joomla

B. Pengujian Kerentanan Website

Pengujian kerentanan website dilakukan dengan menggunakan aplikasi OWASP, hasil keluaran dari pengujian tersebut berupa nilai kerentanan dari masing-masing website yang diuji. Data pengujian berupa hasil uji dari OWASP akan dituangkan dalam tabel kerentanan yang sudah diimplementasikan metode *Simple Additive Weighting*.

C. Pembobotan

Penelitian terkait pembobotan diberikan antara nilai 0 sampai dengan 1 (Dian, Fitro & Achmad, 2014). Apabila kriterianya ada 4 diasumsikan pembaginya setara (*equal*) sehingga pembobotan diberikan dari bobot terendah sampai bobot tertinggi yaitu 0,25, 0,5, 0,75, dan 1. Dan apabila kriterianya ada 5, maka pembobotan terendah sampai tertinggi adaah 0,2, 0,4, 0,6, 0,8, dan 1. Berdasarkan definisi penelitian diatas, maka pembobotan pada penelitian ini ditentukan berdasarkan level kerentanan yang terdapat pada Tabel 2 terdapat 4 level kerentanan antara lain *informational* merupakan level paling rendah dengan pemberian nilai bobot 0,25, *low* merupakan level rendah satu tingkat di atas *informational* dengan nilai bobot 0,50, *medium* merupakan level sedang dengan nilai bobot 0,75, dan *high* merupakan level tinggi dengan nilai bobot 1.

Tabel 2. Bobot Kriteria

Kriteria	C1	C2	C3	C4
Bobot	0,25	0,5	0,75	1

D. Penyelesaian

Data matriks akan melalui tahapan normalisasi dengan mengambil nilai pembagi paling besar pada kolom matriks kemudian dibagi dengan matrik pada kolom tersebut barulah didapatkan hasil normalisasi matrik. Setelah mendapatkan nilai normalisasi matriks, dilakukan pencarian hasil kerentanan keamanan *website* dengan menggunakan persamaan 2 yang telah dijelaskan sebelumnya.

Tahap 1

Tentukan matriks X dari hasil pengujian menggunakan OWASP sebagai nilai dari kriteria dan alternatif.

$$X = \begin{Bmatrix} 4 & 2 & 0 \\ 4 & 2 & 1 \\ 2 & 1 & 0 \\ 8 & 2 & 0 \\ 5 & 2 & 0 \end{Bmatrix}$$

Tahap 2

Matriks X dari pengujian kerentanan melalui tahapan normalisasi dengan menggunakan persamaan 3 karena manfaat dari seluruh atribut adalah keuntungan, berikut adalah hasil normalisasi matriks:

$$R_{ij} = \begin{Bmatrix} 0,5 & 1 & 0 \\ 0,5 & 1 & 1 \\ 0,25 & 0,5 & 0 \\ 1 & 1 & 0 \\ 0,6 & 1 & 0 \end{Bmatrix}$$

Tahap 3

Setelah mendapatkan matriks ternormalisasi, tiap baris matrik pada alternatif dikalikan dengan bobot yang telah ditentukan pada Tabel 2 menggunakan persamaan berikut:

$$V_i = W_j \; R_{ij} \quad \text{..............................(3)}$$

V1= (0,5x0.5)+(0.75x1)+(1x0)= 1
V2= (0,5x0.5)+(0.75x1)+(1x1)= 2
V3= (0,5x25)+(0.75x0.5)+(1x0)= 0.5
V4= (0,5x1)+(0.75x1)+(1x0)= 1.25
V5= (0,5x0.6)+(0.75x1)+(1x0)= 1.1

Dari hasil pengujian diatas, alternatif kedua menunjukkan nilai tertinggi yang berarti alternatif kedua merupakan *website* paling rentan keamanannya, dan alternatif ketiga menunjukkan nilai terendah yang berarti alternatif ketiga merupakan *website* yang paling aman dibandingkan kelima alternatif pada pengujian ini.

Tahap 4

Setelah mendapatkan hasil pengujian, selanjutnya data pada hasil pengujian akan dimasukkan ke dalam tabel, tujuannya adalah untuk memudahkan dalam memahami proses penerapan metode SAW. Berikut data hasil pengujian ditampilkan dalam Tabel 3 dan Tabel 4.

e-ISSN 2597-4963 dan p-ISSN 1858-4853 DOI : http://dx.doi.org/10.30872/jim.v14i1.1431

Tabel 3. Data Matrik Pengujian

Kriteria/ Alternatif	Informational	Low	Medium	High
Universitas 1	0	4	2	0
Universitas 2	0	4	2	1
Universitas 3	0	2	1	0
Universitas 4	0	8	2	0
Universitas 5	0	5	2	0

Tabel 4. Data Normalisasi Matrik

	Normalisasi (R_{ij})				Hasil (V_i)
Universitas-1	0	0.5	1	0	1
Universitas-2	0	0.5	1	1	2
Universitas- 3	0	0.25	0.5	0	0.5
Universitas-4	0	1	1	0	1.25
Universitas-5	0	0.62	1	0	1.1

Pada Tabel 4 dijelaskan, nilai pembagi adalah nilai tertinggi yang ada pada matriks hasil pengujian seperti dipaparkan pada Tabel 3. Nilai pembagi ini akan dikalikan dengan nilai matriks dari hasil pengujian ini disebut dengan normalisasi matriks. Hasil normalisasi matriks akan dikalikan dengan setiap bobot yang dimikiki oleh kriteria, untuk pembobotan sudah dijelaskan pada Tabel 2. Hasil dari perkalian tersebut akan dijumlahkan sehingga didapatkan nilai alternatif terbaik sebagai perbandingan.

Berdasarkan hasil pengujian, penerapan metode SAW memberikan hasil pengurutan nilai *website* paling rentan terhadap serangan adalah *website* Universitas-2 dengan nilai 2, dan *website* paling aman adalah Universitas-3 dengan nilai kerentanan paling rendah yaitu 0,5, sedangkan *website* paling aman di urutan ke 2 adalah Universitas-1 dengan nilai 1, urutan ke 3 adalah Universitas-5 dengan nilai 1,1, dan yang ke 4 adalah Universitas-4 dengan nilai 1,25.

5. KESIMPULAN

Penelitian yang telah dilakukan dapat disimpulkan bahwa penerapan metode SAW pada hasil pengujian kerentanan *website* Universitas Negeri di Aceh berhasil dilakukan dan dapat memberikan gambaran terhadapt kerentanan *website* pada universitas negeri di Aceh. Pengujian kerentanan *website* dengan menggunakan aplikasi OWASP telah menunjukkan hasil kerentanan, namun implementasi metode SAW lebih menambah keakurasian nilai kerentanan sehingga didapatkan hasil dengan penentuan alternatif yang paling rentan sesuai dengan hasil pengujian. Hasil menunjukkan website pada Universitas-2 yang tidak dibangun dengan CMS adalah yang paling rentan dari segi keamanan.

6. DAFTAR PUSTAKA

Andri Pranolo, Siti Muslimah Widyastuti., 2014.Simple Additive Weighting Method on Intelligent Agent for Urban Forest Health Monitoring.*IEEE International Conference on Computer, Control, Informatics and Its Applications (IC3INA).*

Dermawan Baginda Napitupulu., 2016.Evaluasi kualitas website universitsa XYZ dengan pendekatan Webqual.Buletin Pos dan Telekomunikasi.14 (1),51-64. https://DOI: 10.17933/bpostel.2016.140105

Dian Novita Handayani, Fitro Nur Hakim, Achmad Solechan., 2014. Sistem Pendukung Keputusan untuk Pemilihan Jurusan Menggunakan Fuzzy Multiple Atribute Decision Making dengan Metode SAW Studi Kasus Pada SMA Islam Sultan Agung 1. JurnalTransformatika. 11 (2).

Rahman Abdillah., 2017. Implementasi Fuzzy Simple Additive Weighting (SAW) Sebagai Pendukung Keputusan Pada Beasiswa Penelitian. Jurnal String. 2 (1).

Munadi, Rizal; Fajri, T. Surya; Meutia, Ernita Dewi; Elizar., 2013. Analysis Of SQL Injection Attack In Web Service (A Case Study Of Website In Aceh Province). 3rd International Conference on Instrumentation, Communications, Information Technology.

Open Web Aplication Security Project (OWASP), Owasp Top Ten 2010. [Online] Available at: https://www.owasp.com [Accessed 23 Januari 2018]

Riska Kurnianto Abdullah, Ahmad Zaini, Christyowidiasmoro., 2013. Simulasi Celah Keamanan Apliasi dengan Kerangka Kerja OWASP, Jurnal Teknik POMITS. 2 (1).

Satam, Pratik; Kelly, Douglas; Hariri, Salim., 2016. Anomaly Behavior Analysis of Website Vulnerability and Security. International Conference of Computer Systems and Applications (AICCSA), IEEE..

Setiya Nugroho, Fera Tri Wulandari., 2016. Penerapan Metode MADM-SAW Dalam Penentuan Produk Kerajinan Unggulan Kabupaten Klaten. Jurnal SIMETRIS Volume 7 (1).

S.EI Idrissi, N.Berbiche, F.Guerouate, M.Shibi., 2017. Performance Evaluation of Web Application Security Scanners for Prevention and Protection against Vulnerabilities. International Journal of Applied Engineering Research ISSN 0972-4562. 12 (21).

Yadi Utama., 2013. Sistem Pendukung Keputusan untuk Menentukan Prioritas Penanganan Perbaikan Jalan Menggunakan Metode SAW Berbasis Mobile Web",Jurnal Sistem Informasi (JSI), 5(1).