ELKOMIKA | ISSN (p): 2338-8323 | ISSN (e): 2459-9638 | Vol. 6 | No. 2 | Halaman 194 - 206
DOI : http://dx.doi.org/10.26760/elkomika.v6i2.194 Mei 2018

Penerapan *Multiple Attribute Decision Making* dengan Metode *Simple Additive Weighting* untuk Pemeringkatan Kerentanan Keamanan *Website*

RIZAL MUNADI[1], MUKHROJI[2], SYAHRIAL[3], ERNITA DEWI MEUTIA[4]

[1,2,3]Program Studi Magister Teknik Elektro, Jurusan Teknik Elektro dan Komputer
[4]Program Studi Teknik Elektro, Jurusan Teknik Elektro dan Komputer
Universitas Syiah Kuala, Banda Aceh
Email: rizal.munadi@unsyiah.ac.id

Received 30 April 2018 **|** *Revised* 20 Mei 2018 **|** *Accepted* 28 Mei 2018

ABSTRAK

Pada universitas, website dibangun sebagai jendela informasi elektronik yang menyediakan informasi tentang pendidikan tinggi. Namun, adanya celah keamanan pada website berpotensi untuk dieksploitasi bagi kriminal teknologi informasi. Berdasarkan masalah ini, fokus penelitian ini ditekankan pada aspek keamanan. Dalam penelitian ini, perangkat lunak OWASP digunakan sebagai alat uji. Kemudian, evaluasi dan analisis dilakukan terhadap kerentanan website terhadap serangan. Akhirnya, dengan menggunakan teknik Multiple Attribute Decision Making dengan metode Simple Additive Weighting dilakukan proses pemeringkatan kerentanan terhadap lima website universitas negeri di Provinsi Aceh. Hasil pengujian menunjukkan bahwa potensi kerentanan yang paling tinggi terjadi pada Universitas-2 dengan nilai rata-rata kerentanan, 1,72. Kerentanan ini menunjukkan adanya celah keamanan ini yang harus segera diperbaiki segera agar informasi yang tersedia menjadi akurat.

***Kata kunci**: Website, OWASP, MADM, SAW, Kerentanan*

ABSTRACT

At the university, the website is built as a window of electronic information that provides information about higher education. However, the existence of security holes on the website has the potential to be exploited for criminal information technology. Based on this issue, the focus of this research is emphasized on the security aspect. In this study, OWASP software is used as a test tool. Then, the evaluation and analysis carried out against the vulnerability of the website against the attack. Finally, using the Multiple Attribute Decision Making technique using the Simple Additive Weighting method, vulnerability rating was made to five public university websites in Aceh Province. The test results show that the highest vulnerability potential occurs at University-2 with an average vulnerability score of 1.72. This vulnerability indicates a security hole that needs to be fixed immediately so that the information available becomes accurate.

***Keywords**: Website, OWASP, MADM, SAW, Vulnerability*

1. PENDAHULUAN

Seiring dengan perkembangan teknologi informasi dan komunikasi dewasa ini, *website* merupakan sarana informasi penting yang dapat diakses publik secara bebas dan cepat. Penggunaan *website* sebagai jendela informasi elektronik juga menjadi bagian yang terintegrasi pada sistem informasi perguruan tinggi. Sebagai wadah informasi, suatu *website* tidak saja didesain sebaik mungkin, namun integritas keamanan *website* perlu menjadi perhatian yang serius. Teknologi pembuatan *website*, baik menggunakan *Content Management System* (CMS) atau aplikasi lainnya, terus berkembang dengan berbagai fitur yang menarik. Kualitas *website* yang baik dengan penyajian informasi yang *up-to-date*, perlu diimbangai dengan keamanan. Namun berbagai teknik serangan keamanan terus bermunculan dan tindakan pencegahan perlu dilakukan agar integritas *website* tetap terjaga keberadaannya. Selain masalah keamanan, *website* juga menjadi wadah informasi yang dinilai dan dibuatkan dalam bentuk peringkat. Pemeringkatan suatu perguruan tinggi yang bersumberkan informasi yang tersajikan pada *website*, dilakukan oleh beberapa penilaian dengan kriteria dan indikator tertentu seperti *Webometrics*, *UI Greenmetrics, Times Higher Education World University Ranking* dan *Academic Ranking of World Universities* (ARWU) . Ini menunjukkan betapa pentingnya informasi yang disajikan pada suatu *website* dan layanan informasi yang disediakan.

Pada perguruan tinggi, selain untuk menyajikan informasi sebagai berita kepada publik dan civitas akademika, juga *website* diintegrasikan dengan berbagai sistem pangkalan data atau basis data (*database*). Bentuk basis data yang dibangun, disesuaikan dengan penamaan aplikasi tertentu pada *website* perguruan tinggi. Dalam era informasi dengan layanan melalui *website*, seorang mahasiswa tidak perlu datang langsung ke kampus untuk mendaftar ulang, melihat nilai matakuliah, mengisi Kartu Rencana Studi (KRS), melihat jadwal kuliah, atau bagi mahasiswa baru yang ingin mengetahui suatu jurusan atau program studi yang tersedia. Di dalam *website* kampus, terdapat banyak sekali basis data seperti data mahasiswa, data dosen, data pembayaran SPP, data jurusan dan program studi, serta data akademik lainnya. Namun disisi lain, adanya kelemahan dalam sistem informasi yang dibangun dapat menjadi celah keamanan bagi penyerang (*attacker*). Penyalahgunaan sangat mungkin dilakukan oleh pihak penyerang sehingga dapat melakukan aktivitas seperti mengambil data, menghapus data bahkan mengganti data penting *website.* Bila hal ini terjadi pada *website* kampus maka akan mengacaukan integritas sistem informasi dan dapat menimbulkan kerugian yang sangat besar.

Potensi terjadinya gangguan keamanan suatu *website* merupakan bagian dari ketidakpastian dan dapat saja terjadi kapan pun dan ini menarik banyak pihak untuk melakukan penelitian. Pada umumnya setelah aplikasi *web* selesai dibuat, sistem tersebut langsung diluncurkan untuk digunakan **(Abdullah, dkk., 2013)**. Hal seperti ini lazim terjadi dan pemantauan terhadap keamanan suatu *website*, umumnya kurang menjadi perhatian yang serius dan dilakukan secara berkelanjutan. Hal seperti inilah yang memungkinkan terjadinya penyerangan. Teknik yang dilakukan oleh pihak yang melihat adanya potensi celah keamanan cukup beragam. Aplikasi teknik serangan yang digunakan untuk mendeteksi kerentanan juga berbeda-beda. Pada penelitian yang terkait dan telah dilakukan yang dengan menggunakan aplikasi *w3af untuk* pengujian *website* instansi pemerintah (studi kasus di Aceh) **(Munadi dkk., 2013)**. Hasil yang diperoleh menunjukkan sekitar 50% *website* terdeteksi rentan terhadap *SQL Injection*. Dari serangan ini, persentase *website* yang berdampak dapat dipilah berdasarkan *platform* CMS yang digunakan dimana sekitar 87,5% menggunakan CMS Joomla. Untuk itu, diperlukan tindakan pencegahan dengan melibatkan peran administrator. Halaman akses pada *website* perlu diadakan validasi masukan dan memantau secara acak terhadap beberapa tindakan yang mungkin tidak wajar agar konten *website* admin tetap aman dari

serangan *SQL Injection.* Tindakan pencegahan lainnya yang dapat dilakukan adalah melakukan pembaruan versi CMS secara berkala. Penelitian lain tentang kerentanan keamanan *website* perguruan tinggi swasta di Jakarta juga telah dilakukan **(Mantra & Alaydrus, 2015)**. Dalam penelitian ini dilakukan analisis bagaimana suatu informasi awal terkait target yang ditentukan, dapat diperoleh dengan teknik yang umum dilakukan seperti untuk pencarian informasi, baik menggunakan *search engine* maupun *tool* yang tersedia untuk *information gathering* atau *intelligence gathering*. Namun, tidak semua *website* memiliki kelemahan yang menyebabkan informasi yang rahasia dapat diambil dengan teknik *SQL Injection*. Selain itu, tidak semua *file* yang terdapat pada *web address* atau *domain* utama *website* dapat terserang dengan *SQL Injection*. Kelemahan atau kerentanan pada tiap *website* target tersebut tidak terkait dengan cara mendapatkan informasi hanya dengan teknik *SQL Injection* saja, namun masih dapat diterapkan dengan cara yang berbeda.

Tindakan lebih lanjut akibat dari adanya kelemahan sehingga integritas informasi suatu *website* dapat terganggu dan dapat ditindaklanjuti dengan pemantauan secara berkala. Data yang terkumpul akan menjadi data agregat untuk dikaji lebih lanjut. Berdasarkan data, peta kerentanan suatu *website* dapat dikaji dan dianalisis berdasarkan teknik serangan yang digunakan seperti *SQL Injection*, *XSS* dan lainnya. Hasil kajian ini kemudian secara agregat dapat dilakukan pemeringkatan. Salah satu sistem pendukung pengambilan keputusan untuk pemeringkatan dapat diterapkan metode *Simple Additive Weighting* (SAW) dalam penentuan prioritas. Pendekatan ini diambil agar efektivitas pengambilan keputusan yang dilakukan tercapai, dimana nilai setiap kriteria pada proses penentuan prioritas didasari metode SAW, sehingga proses penilaian akan lebih tepat. Dalam suatu hasil kajian dengan SAW ini menghasilkan alternatif terbaik dari sejumlah alternatif yang diberikan **(Utama, 2013)**. Penelitian lain tentang penentuan sistem pengambil keputusan produk unggulan telah dilakukan **(Nugroho & Wulandari, 2016)**. Pada penelitian ini, metode yang digunakan dalam pengambilan keputusan penentuan produk unggulan adalah kombinasi metode *Multiple Attribute Decision Making-Simple Additive Weighting* (MADM-SAW). Pemilihan metode MADM-SAW ini disebabkan pada kemampuannya untuk melakukan penilaian secara lebih tepat dibandingkan dengan model pengambilan keputusan yang lain. Hal ini didasari pada nilai kriteria dan bobot preferensi yang sudah ditentukan, kemudian dilanjutkan dengan proses pemeringkatan yang akan menyeleksi alternatif terbaik dari sejumlah alternatif yang tersedia.

Berdasarkan masalah celah keamanan *website* yang dikaji, analisis penelitian ini menghasilkan pemetaan potensi keamanan sehingga dapat diformulasi ke dalam pemeringkatan kerentanan keamanan *website* Perguruan Tinggi Negeri yang ada di Provinsi Aceh.

1.1. Perguruan Tinggi

Perguruan tinggi adalah satuan pendidikan penyelenggara pendidikan tinggi. Komponen penting suatu pendidikan tinggi terdiri dari peserta didik perguruan tinggi yang disebut mahasiswa, dan tenaga pendidik perguruan tinggi disebut dosen dan ditambah *supporting staff* yang membantu dalam kegiatan akademik dan administrasi. Berdasarkan pengelolaannya, perguruan tinggi dapat dibagi menjadi dua, yaitu Perguruan Tinggi Negeri (PTN) yang didanai dan diselenggarakan oleh pemerintah, dan Perguruan Tinggi Swasta (PTS) yang diselenggarakan oleh pihak swasta.

1.1.1. Perguruan Tinggi Negeri di Aceh

Aceh merupakan sebuah provinsi yang terletak di ujung pulau Sumatera, dan merupakan provinsi paling Barat di Indonesia. Sejak awal kemerdekaan, perhatian pemerintah daerah terhadap kemajuan masyarakat Aceh diarahkan salah satunya pada pembangunan sumber daya manusia melalui jalur pendidikan. Awal tahun 1960, di Provinsi Aceh telah dibangun Kota Pelajar dan Mahasiswa (Kopelma) di kawasan Darussalam, yaitu Universitas Syiah Kuala

(Unsyiah) dan Institut Agama Islam Negeri (IAIN) Ar-Raniry, sebagai jantung hati rakyat Aceh. Dalam perkembangannya, saat ini di Provinsi Aceh telah memiliki beberapa Perguruan Tinggi Negeri (PTN) yang dikategorikan kedalam Universitas, Institut, Politeknik, dan Sekolah Tinggi. Daftar nama-nama PTN yang tersebar di Provinsi Aceh, ditunjukkan pada Tabel 1.

Tabel 1. Perguruan Tinggi Negeri di Aceh

No.	Institusi Pendidikan Tinggi	Kota
1	Universitas Syiah Kuala	Banda Aceh
2	Universitas Islam Negeri Ar-Raniry	Banda Aceh
3	Universitas Malikussaleh	Lhokseumawe
4	Universitas Samudra	Langsa
5	Universitas Teuku Umar	Meulaboh
6	Institut Agama Islam Negeri Malikussaleh	Lhokseumawe
7	Politeknik Negeri Lhokseumawe	Lhokseumawe
8	Institut Agama Islam Negeri Zawiyah Cot Kala	Langsa
9	STAIN Gajah Putih	Takengon
10	STAIN Teungku Dirundeng	Meulaboh

Dalam kaitannya dalam penelitian ini, dari keseluruhan PTN yang ada di Aceh, ruang lingkup pada penelitian ini hanya diambil pada kategori universitas sebagai sampel. Dasar pertimbangan dipilihnya universitas dibandingkan jenis perguruan tinggi lainnya adalah skalabilitas akademik, dimana universitas mempunyai lebih banyak mahasiswa yang menekuni pendidikan yang tersebar pada berbagai program studi pada setiap fakultas. Selain itu, universitas mempunyai jumlah dosen dan tenaga kependidikan yang lebih banyak dibandingkan dengan kategori PTN lain.

1.2. *Multiple Attribute Decision Making*

Sistem Pendukung Keputusan (SPK) adalah bagian dari sistem informasi berbasis komputer termasuk sistem yang berbasis pengetahuan (manajemen pengetahuan) yang digunakan untuk mendukung pengambilan keputusan dalam suatu organisasi atau institusi. Juga dapat dikatakan sebagai sistem informasi berbasis komputer yang membantu *user* dalam mengatasi masalah dengan menggunakan data model. Namun, SPK tidak dimaksud untuk mengotomatisasikan pengambilan keputusan tetapi memberi peringkat interaktif yang memungkinkan pengambilan keputusan untuk melakukan berbagai analisis menggunakan model yang tersedia seperti *Multiple Attribute Decision Making* (MADM) **(Sismoro & Hartatik, 2015)**.

Multiple Attribute Decision Making merupakan suatu sistem pendukung pengambilan keputusan yang digunakan untuk mendapatkan jawaban atas suatu masalah di dalam ruang diskrit. Pada penggunaannya, proses MADM dapat dilakukan melalui beberapa tahap diantaranya penyusunan komponen kondisi, analisis serta sintesis sistem informasi. Ada beberapa metode yang dapat digunakan untuk menyelesaikan masalah MADM antara lain: *Simple Additive Weighting (SAW)*, *Weighting Product (WP)*, *ELECTRE*, *Technique for Order Preference by Similarity to Ideal Solutions (TOPSIS)*, *Analytic Hierarchy Process (AHP)*.

1.3. *Simple Additive Weighting*

Simple Additive Weighting (SAW) merupakan salah satu metode yang dapat digunakan untuk penentuan sistem pengambilan keputusan, kinerja metode ini adalah menentukan bobot pada setiap atributnya, kemudian pada tahap selanjutnya dilakukan pemeringkatan yang akan menyeleksi alternatif terbaik. Dalam metode SAW biasanya menggunakan konsep

penjumlahan terbobot dari semua atribut di setiap alternatif **(Sonata, 2015)**. Metode SAW sering juga dikenal dengan istilah metode penjumlahan terbobot. Konsep dasar metode SAW adalah mencari penjumlahan terbobot dari tingkat kinerja pada setiap alternatif pada semua atribut. Metode SAW membutuhkan proses normalisasi matriks keputusan *(X)* ke dalam suatu skala yang dapat dibandingkan dengan semua peringkat alternatif yang ada. Berikut adalah rumus peringkat kinerja ternormalisasi, seperti yang ditunjukkan pada Persamaan 1.

$$Rij \begin{cases} \dfrac{x_{ij}}{\max x_{ij}} & \text{Jika } j \text{ adalah atribut keuntungan } \textit{(benefit)} \\ \dfrac{\min x_{ij}}{x_{ij}} & \text{jika } j \text{ adalah atribut biaya } \textit{(cost)} \end{cases} \quad (1)$$

Keterangan

Rij	: Nilai peringkat kinerja ternormalisasi
xij	: Nilai atribut yang dimiliki setiap kriteria
$\frac{x_{ij}}{\max x_{ij}}$	: Nilai terbesar dari setiap kriteria
$\frac{\min x_{ij}}{x_{ij}}$	: Nilai terkecil dari setiap kriteria
Benefit	: Jika nilai terbesar adalah terbaik
Cost	: Jika nilai terkecil adalah terbaik

Dimana *rij* adalah peringkat kerja ternormalisasi dari alternatif,A_i pada atribut,C_i. Dimana:i = 1,2,...,m dan j = 1,2, ...,n. Nilai preferensi untuk alternatif (V_i) diberikan pada Persamaan 2 sebagai berikut:

$$V_i = \sum_{j=1}^{n} w_j r_{ij} \quad (2)$$

Keterangan:

V_i	: Peringkat untuk setiap alternatif
w_j	: Nilai bobot dari setiap kriteria
r_{ij}	: Nilai peringkat kinerja ternormalisasi

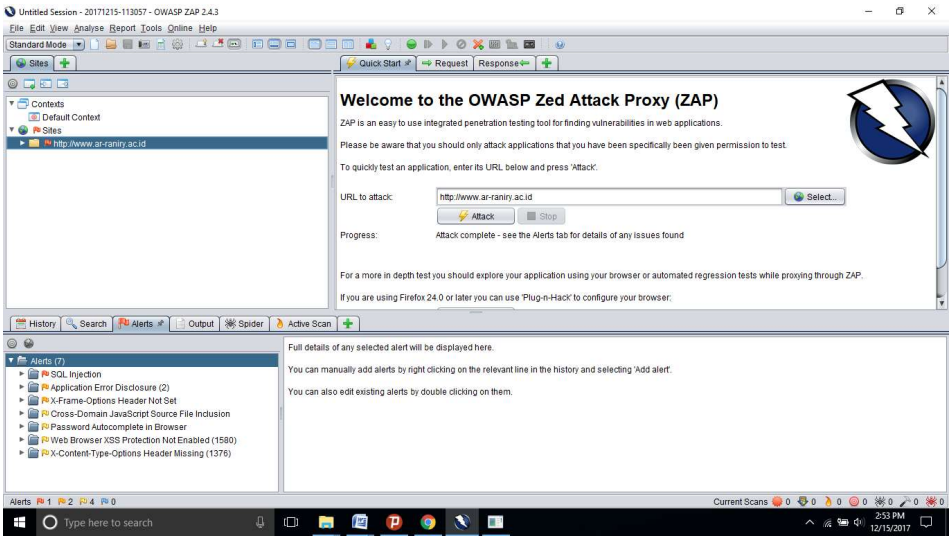
1.4. Keamanan *Website*

Munculnya teknologi informasi berbasis internet telah memberikan banyak manfaat bagi kehidupan manusia di segala bidang. Wujud batas negara semakin kabur dengan mudahnya suatu informasi menyebar dan sebagian besar transaksi di dunia ini dilakukan secara *online*. Pertukaran informasi ini, tidak terlepas dari aplikasi *website* yang sudah menjadi bagian dari kegiatan sehari-hari setiap orang dengan menggunakan peramban tertentu, seperti *Firefox, Chrome, Edge*. Setiap informasi pada *website* menyediakan layanan otentikasi pengguna yang mengacu pada *database*. Jika kerahasiaan informasi dalam basis data terungkap keluar, maka tujuan melakukan transaksi *online* akan sangat berbahaya. Oleh karena itu, penyerang *(attacker)* dapat menggunakan kesempatan itu untuk mengambil *username* dan *password* pada layanan *web*. Target, salah satu pengecer potongan harga *(discount retailer*) terbesar kedua di Amerika Serikat (setelah Walmart), mengalami korban pelanggaran keamanan yang mempengaruhi lebih dari 70 juta pelanggan. Kejadian pencurian data kartu kredit dan kartu debit terjadi antara 27 November 2013 dan 18 Desember 2013. Dalam kejadian pada perusahaan Target, 40 juta nomor kartu kredit dan debit dan 70 juta catatan informasi pribadi

dicuri **(Plachkinova & Maurer, 2018)**. Kejadian pada perusahaan Target merupakan salah satu tindak kejahatan yang terbesar terhadap penyalahgunaan akses oleh pihak yang tidak bertanggung jawab. Teknik serangan yang beragam dan salah satu serangan ini populer dikenali sebagai *SQL Injection*, suatu serangan yang mengeksploitasi *basis data* yang terhubung pada suatu aplikasi. Oleh karenanya harus dapat dideteksi dan dicegah **(Abirami, 2015)**.

1.5. *Open Web Aplication Security Project*

Setiap pasar teknologi yang dinamis membutuhkan sumber informasi yang tidak bias mengenai praktik terbaik serta badan yang aktif mengadvokasi standar terbuka. Dalam kaitannya dengan keamanan aplikasi, salah satu dari kelompok tersebut adalah *Open Web Aplication Security Project* (OWASP). OWASP menawarkan sebuah aplikasi komunitas terbuka *(Open Source)* yang didedikasikan untuk organisasi yang memungkinkan untuk dilakukan pengembangan, dan juga pemeliharaan. Beberapa layanan yang disediakan OWASP secara terbuka antara lain *tool* dan standar keamanan aplikasi, buku tentang uji keamanan aplikasi, pengembangan kode, dan *review* kode keamanan, kendali keamanan dan pustaka standar, cabang lokal di seluruh dunia, riset terkini, konferensi lengkap diseluruh dunia, *mailing list*, dan banyak layanan lainnya yang dapat diakses melalui *https://www.owasp.org*. Berikut adalah tampilan OWASP yang ditampilkan seperti pada Gambar 1 **(Open Web Aplication Security Project, 2010)**.



Gambar 1. Tampilan Aplikasi OWASP Saat Pengujian

Pada penelitian yang menggunakan OWAPS, dilakukan perbandingan beberapa aplikasi *vulnerability scanner* **(Idrissi dkk., 2017)**. Dari hasil beberapa pengujian yang presisi dan tingkat pengukuran kerentanan disebutkan bahwa OWASP merupakan aplikasi paling baik dengan rata-rata pengujian adalah 95,67 %. Hasil ini jauh lebih tinggi dibandingkan *w3af*, *BurpSuite*, *Acunetix*, dan *Wapiti*.

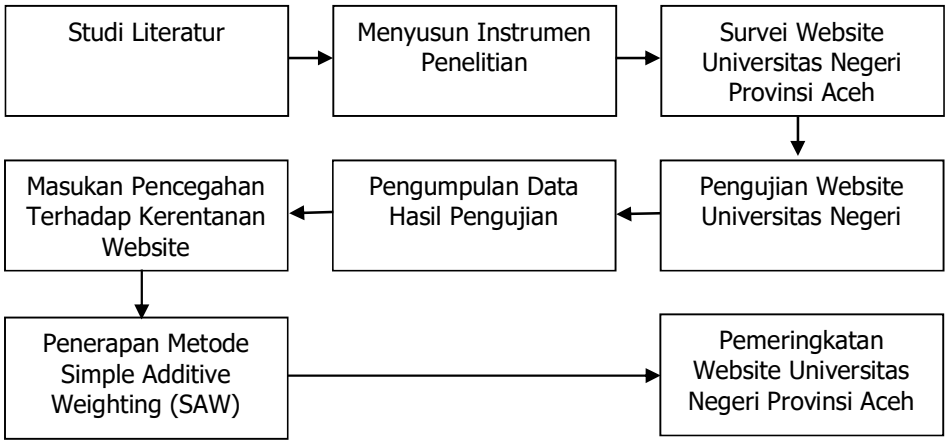
2. METODOLOGI PENELITIAN

Pada penelitian ini dilakukan pengujian kerentanan keamanan *website* menggunakan OWASP, dan kemudian hasil survei kerentanan dievaluasi untuk menentukan peringkat keamanan terhadap kerentanan *website* dengan menerapkan metode *Simple Additive Weighting* (SAW). Terdapat 5 *website* universitas negeri yang ada di Provinsi Aceh yang dijadikan target uji

dengan 4 parameter level kerentanan yang didefinisikan OWASP antara lain *Informational, Low, Medium*, dan *High*. Pengujian kerentanan *website* menggunakan *software* OWASP dilakukan sebanyak 5 kali untuk setiap *website* Universitas, dimana target yang diuji ada 5 *website*, maka total proses pengujian kerentanan adalah sebanyak 25 kali. Pengujian dilakukan secara bertahap, ada 5 siklus pengujian dalam pengujian ini, satu siklus pengujian adalah 5 *website* Universitas yang akan diuji, rentang waktu yang dihabiskan dalam 1 siklus pengujian berkisar antara 3 hari sampai 5 hari, tergantung pada kecepatan dan kestabilan jaringan internet. Sedangkan sistem pendukung pengambilan keputusan dengan MADM dalam proses pemeringkatan menggunakan metode SAW dilakukan setelah total siklus pengujian telah selesai. Hasil evaluasi uji kerentanan kemudian diproses melalui tahapan normalisasi matriks dan perkalian bobot untuk mendapatkan hasil pemeringkatan kerentanan *website*.

2.1. Objek dan Alur Penelitian

Objek yang dikaji pada penelitian ini adalah kerentanan *website* Universitas Negeri di Provinsi Aceh dan dilakukan pemeringkatan terhadap *website* yang paling rentan terhadap serangan. Alur penelitian ini memiliki beberapa tahapan seperti Gambar 2 di bawah ini.



Gambar 2. Diagram Alir Penelitian

Tahapan awal dari penelitian ini adalah melakukan studi literatur sesuai dengan teori yang relevan dan hasil penelitian-penelitian sejenis yang pernah dilakukan. Kemudian dilakukan pengujian serangan terhadap 5 *website* universitas negeri di Provinsi Aceh. Dalam penelitian ini, akan dilakukan pengujian *website* menggunakan *software* OWASP untuk mendapatkan keakurasian nilai kerentanan masing-masing *website.* Tahapan berikutnya, data hasil uji menggunakan *software* OWASP diimplementasikan ke dalam *Multiple Attribute Decision Making* (MADM) dengan menggunakan metode *Simple Additive Weighting* (SAW) untuk menilai pemeringkatan kerentanan *website* dari universitas yang paling rentan terhadap serangan.

3. HASIL DAN PEMBAHASAN

3.1. Data Universitas Negeri di Provinsi Aceh

Berdasarkan sumber data yang disajikan pada pangkalan data perguruan tinggi negeri, *https://forlap.ristekdikti.go.id/perguruantinggi*, ada 5 universitas negeri di Provinsi Aceh. Secara geografis, letak setiap universitas ini tersebar: di ibu kota provinsi terdapat 2 universitas, kemudian masing-masing 1 universitas terletak di Aceh Timur, Aceh Utara dan Aceh Barat. Dengan menggunakan aplikasi *Wappalyzer* diperoleh data jenis *Content Management System* (CMS) yang digunakan oleh tiap universitas: 3 universitas yang

menggunakan CMS *Joomla*, 1 universitas menggunakan CMS *Wordpress*, dan 1 universitas lagi tidak menggunakan CMS. Berikut rincian datanya seperti yang ditampilkan pada Tabel 2.

Tabel 2. Data Universitas Negeri di Provinsi Aceh

NO	PTN	CMS
1	Universitas-1	Joomla
2	Universitas-2	Non CMS
3	Universitas-3	Joomla
4	Universitas-4	Wordpress
5	Universitas-5	Joomla

3.2. Evaluasi Penerapan Metode *Simple Additive Weighting* terhadap *Website Universitas Negeri di Aceh*

Dari hasil pengujian kerentanan *website* yang dilakukan sebanyak 5 *website* dalam 1 siklus pengujian dengan menggunakan persamaan 1. Nilai yang diperoleh kemudian dilakukan proses normalisasi. Nilai Vektor bobot dibagi dalam skala yang sama dengan interval 0,25 dengan rentang maksimumnya adalah 1. Matriks keputusan, *X*, dibangun untuk kemudian dilakukan normalisasi dengan menggunakan persamaan 1. Alternatif diperoleh dengan menggunakan Persamaan 2. Berikut diuraikan prosesnya penyelesaiannya:

1. Langkah-langkah Penyelesaian

   a) Vektor bobot : W= [1, 0,75, 0,5, 0,25]
   b) Matrik Keputusan X

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

   c) Normalisasi matriks X menggunakan Persamaan 1

Alternatif A1

$$r11 = \frac{4}{\text{Max } (2;1;3;4;2)} = 0{,}5$$

$$r12 = \frac{2}{\text{Max } (2;2;1;2;2)} = 2$$

$$r13 \quad \frac{0}{\text{Max } (0;1;0;0;0)} = 0$$

Alternatif A4

$$r41 = \frac{8}{\text{Max } (2;1;3;4;2)} = 1$$

$$r42 = \frac{2}{\text{Max } (2;2;1;2;2)} = 1$$

$$r43 = \frac{0}{\text{Max } (0;1;0;0;0)} = 0$$

Alternatif A2

$$r21 = \frac{4}{\text{Max } (2;1;3;4;2)} = 0,5$$

$$r22 = \frac{2}{\text{Max } (2;2;1;2;2)} = 1$$

$$r23 = \frac{1}{\text{Max } (0;1;0;0;0)} = 1$$

Alternatif A5

$$r51 = \frac{5}{\text{Max } (2;1;3;4;2)} = 0,6$$

$$r52 = \frac{2}{\text{Max } (2;2;1;2;2)} = 1$$

$$r53 = \frac{0}{\text{Max } (0;1;0;0;0)} = 0$$

Alternatif A3

$$r31 = \frac{2}{\text{Max } (2;1;3;4;2)} = 0,25$$

$$r32 = \frac{1}{\text{Max } (2;2;1;2;2)} = 0,5$$

$$r33 = \frac{0}{\text{Max } (0;1;0;0;0)} = 0$$

Dari hasil perhitungan di atas maka didapat matriks ternomalisasi,*R* sebagai berikut :

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

d) Mencari alternatif terbaik menggunakan Persamaan 2
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 ke-2, *V2* menunjukkan nilai tertinggi yang berarti alternatif ke-2 merupakan *website* paling rentan keamanannya dan alternatif ke-3, *V3* diperoleh hasil dengan nilai terendah yang berarti alternatif ke-3 merupakan *website* yang

paling aman dibandingkan semua alternatif pada pengujian ini. Hasil dari lima kali pengujian dari semua siklus pengujian dengan penerapan metode *Simple Additive Weighting* (SAW) akan disajikan pada Tabel 3 dan Tabel 4 berikut.

2. Pengujian

Data siklus pengujian pertama berupa hasil uji dari OWASP dirangkum ke dalam tabel kerentanan yang sudah diimplementasikan metode *Simple Additive Weighting* seperti yang ditunjukkan pada Tabel 3 berikut. Pada hasil pengujian tidak ditemukan kerentanan pada kategori *informational*.

Tabel 3. Data Matrik Pengujian

Bobot (w_j)	**0,25**	**0,50**	**0,75**	**1**
Alternatif / Kriteria	**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

Data matriks diproses melalui tahapan normalisasi dengan mengambil nilai pembagi paling besar pada kolom matriks ($max\, x_{ij}$) kemudian dibagi dengan matriks pada kolom tersebut (x_{ij}) sehingga didapatkan hasil normalisasi matriks. Setelah mendapatkan nilai normalisasi matriks, kemudian dilakukan pemeringkatan (V_i) kerentanan keamanan *website* dengan menggunakan Persamaan 2, berikut adalah hasil proses normalisasi matriks dan pemeringkatan yang ditampilkan pada Tabel 4.

Tabel 4. Data Normalisasi Matriks Pengujian

Pembagi ($max\, x_{ij}$)	**0**	**8**	**2**	**1**	**Hasil (V_i)**
Normalisasi (R_{ij})					
Universitas-1	0	0,50	1,00	0	1,00
Universitas-2	0	0,50	1,00	1,00	2,00
Universitas-3	0	0,25	0,50	0	0,50
Universitas-4	0	1,00	1,00	0	1,25
Universitas-5	0	0,62	1,00	0	1,10

Berdasarkan hasil pengujian pertama, penerapan metode SAW memberikan hasil *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* universitas lainnya berada dalam rentang 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. Ini menunjukkan walau ada *website* yang dibangun dengan CMS yang sama, namun hasil kerentanan berbeda.

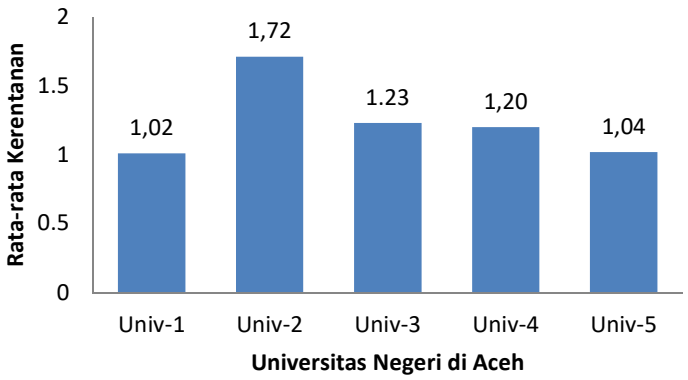
3.3. Rekapitulasi Keseluruhan Hasil Pengujian

Rekapitulasi keseluruhan hasil uji pada penelitian ini terdapat lima bagian, yaitu pengujian pada siklus pengujian pertama sampai pengujian pada siklus pengujian ke-5. Hasil yang didapat dari rekapitulasi adalah pemeringkatan kerentanan seluruh pengujian, dan nilai rata-rata dari hasil kerentanan siklus pengujian pertama sampai siklus pengujian ke-5 yang ditunjukkan pada Tabel 5. P_i, merupakan Total Nilai Kerentanan Pengujian, dimana i= 1, 2, 3, 4, 5.

Tabel 5. Rekapitulasi Keseluruhan Hasil Uji

Nama Universitas	Pengujian Ke					Total	Rata-Rata
	P1	P2	P3	P4	P5		
Universitas-1	1,00	0,75	1,70	0,68	0,97	5,10	1,02
Universitas-2	2,00	1,22	1,75	1,68	1,97	8,62	1,72
Universitas-3	0,50	1,61	0,85	1,34	1,86	6,16	1,23
Universitas-4	1,25	1,25	1,00	1,25	1,25	6,00	1,20
Universitas-5	1,10	0,89	1,25	0,82	1,14	5,20	1,04

Berdasarkan rekapitulasi hasil uji dari keseluruhan siklus pengujian, didapati hasil total kerentanan: Universitas-1 mendapatkan total nilai kerentanan 5,10 dengan rata-rata nilai kerentanan 1,02. Evaluasi untuk universitas lainnya, Universitas-2 mendapatkan total nilai kerentanan 8,62 dengan rata-rata nilai kerentanan 1,72. Nilai yang diperoleh pada Universitas-2 merupakan hasil yang paling besar nilai kerentanannya. Universitas-3 mendapatkan total nilai kerentanan 6,16 dengan rata-rata nilai kerentanan 1,23. Universitas-4 mendapatkan total nilai kerentanan 6 dengan rata-rata nilai kerentanan 1,20. Dan terakhir, Universitas-5 mendapatkan total nilai kerentanan 5,20 dengan rata-rata nilai kerentanan 1,04. Hasil total rata-rata kerentanan ditunjukkan pada Gambar 3.



Gambar 3. Grafik Rata – Rata Kerentanan

Berdasarkan Gambar 3, terlihat jelas pemeringkatan kerentanan keamanan *website* universitas negeri di Aceh dengan menempatkan Universitas-1 dengan skor yang paling rendah atau paling kurang rentan dibandingkan universitas lainnya. Sebaliknya, *website* Universitas-2

mendapatkan skor nilai kerentanan yang tertinggi dengan nilai 1,72. Hasil ini menunjukkan *website* Universitas-2 adalah yang paling rentan dibandingkan tingkat keamanan *website* universitas lainnya. Kerentanan ini mengindikasikan potensi adanya celah yang dapat disalahgunakan dan oleh karena itu perlu dilakukan pembenahan dan audit keamanan *website*. Salah satu solusinya untuk *website* Universitas-1 adalah penerapan salah satu CMS daripada mempertahankan *website* yang telah dibangun tanpa menggunakan *Content Management System (CMS)*. Berdasarkan nilai kerentanan yang telah diperoleh, pada Tabel 6 disajikan indeks peringkat *website* universitas negeri di Aceh.

Tabel 6. Indeks Peringkat Kerentanan Universitas yang Diuji

Nama Universitas	Total	Rata-Rata	Peringkat
Universitas-1	5,10	1,02	**1**
Universitas-5	8,62	1,72	**2**
Universitas-4	6,16	1,23	**3**
Universitas-3	6,00	1,20	**4**
Universitas-2	5,20	1,04	**5**

4. KESIMPULAN

Berdasarkan hasil pengujian dan analisis dalam penelitian ini, dapat disimpulkan:

1. Proses pengujian dengan menggunakan OWASP sebagai *tool* evaluasi kerentanan telah dilakukan terhadap lima *website* universitas negeri yang ada di Provinsi Aceh.
2. Penerapan MADM dengan metode SAW diperoleh peringkat yang paling rentan adalah *website* Universitas-2 sedangkan *website* Universitas-1 menjadi yang paling rendah kerentanan dari 5 *website* universitas yang diuji.
3. Hasil menunjukkan bahwa penggunaan CMS lebih baik dibandingkan *website* yang dibangun tanpa menggunakan CMS.
4. Penggunaan CMS untuk pembuatan *website* memberikan proteksi keamanan yang lebih baik dan audit keamanan perlu dilakukan secara berkala dengan melakukan penyesuaian dengan pembaruan versi CMS yang tersedia.

DAFTAR RUJUKAN

Abdullah, R. K., Zaini, A., & Christyowidiasmoro. (2013). Simulasi Celah Keamanan Aplikasi Web dengan Kerangka Kerja OWASP, *Jurnal Teknik POMITS, 2*(1), 1-6.

Munadi, R., Fajri, T.S., Meutia, E.D., & Elizar. (2013). Analysis of SQL injection attack in web service (a case study of *website* in Aceh province).*Proc. of 2013 3rd Int. Conf. on Instrumentation, Communications, Information Technol., and Biomedical Engineering:*

Science and Technology for Improvement of Health, Safety, and Environment, ICICI-BME 2013, (pp. 431-435).

Mantra, I. G. N., & Alaydrus, M. (2015). Analisis Kerentanan Keamanan (VA) Web Perguruan Tinggi Swasta Jakarta. *Prosiding SENATEK 2015*, (pp. 1-6).

Utama, Y. (2013). Sistem Pendukung Keputusan Untuk Menentukan Prioritas Penanganan Perbaikan Jalan Menggunakan Metode Saw Berbasis Mobile Web. *Jurnal Sistem Informasi (JSI)*, *5*(1), 566–579.

Nugroho, S., & Wulandari, F. T., (2016). Penerapan Metode MADM-SAW Dalam Penentuan Produk Kerajinan Unggulan Kabupaten Klaten. *Jurnal SIMETRIS, 7*(1), 163-168.

Sismoro, H. (2013). Multiple Attribute Decision Making-Penggunaan Metode SAW dan WPM Dalam Pemilihan Proposal UMKM. *Jurnal DASI, 14*(1), 29-34.

Sonata, F. (2016). Implementasi Metode Simple Additive Weighting (SAW) Dengan Proses Fuzzifikasi Dalam Penilaian Kinerja Dosen. *Jurnal Teknologi Informasi Dan Komunikasi*, *5*(2), 71–80.

Plachkinova, M. & Maurer, C. (2018). Teaching Case: Security Breach at Target. *Journal of Information Systems Education, 29*(1), 11-20.

Abirami, J.Devakunchari, R., & Valliyammai, C. (2015). A Top Web Security Vulnerability SQL Injection Attack-Survey. *The Seventh International Conference on Advanced Computing (ICoAC),* (pp. 1-6).

Open Web Application Security Project (OWASP). (2018, Januari 23). *OWASP Top Ten 2010*. Retrieved from https://www.owasp.com

Idrissi, S.E., Berbiche, N., Guerouate, F., & Shibi, M., (2017). Performance Evaluation of Web Application Security Scanners for Prevention and Protection against Vulnerabilities. *International Journal of Applied Engineering Research, 12*(21), 11068-11076.