Evaluasi Risiko Celah Keamanan Menggunakan Metodologi Open-Source Security Testing Methodology Manual (OSSTMM) Pada Aplikasi Web Terbaru Fakultas Ilmu Komputer UPN Veteran Jakarta

Akmal Ilmi[1], Henki Bayu Seta[2], I Wayan Widi Pradnyana[3]
Program Studi Informatika / Fakultas Ilmu Komputer
Universitas Pembangunan Nasional Veteran Jakarta
Jl. RS Fatmawati No. 1, Pondok Labu, Jakarta Selatan, DKI Jakarta 12450
[1]akmali@upnvj.ac.id, [2]henkiseta@upnvj.ac.id, [3]wayan.widi@upnvj.ac.id

Abstrak. Perkembangan teknologi berbasis aplikasi web yang semakin pesat dalam beberapa tahun terakhir sehingga digunakan untuk berbagai sektor, salah satunya sektor perguruan tinggi. Namun perkembangan ini tidak terlepas dari tingginya isu dan bahaya keamanan informasi pada web sektor perguruan tinggi. Seperti pada Web terbaru Fakultas Ilmu Komputer UPN Veteran Jakarta dengan domain http://new-fik.upnvj.ac.id. Untuk mencegah hal ini dibutuhkan sebuah evaluasi risiko celah keamanan secara komprehensif pada web tersebut. Metode yang digunakan pada penelitian ini yaitu metode OSSTMM, metode tersebut bisa menguji seberapa tinggi tingkat keamanan suatu aplikasi web dengan penilaian RAV dan STAR. Metode ini diharapkan mendapat manfaat dan luaran berupa rekomendasi yang harus dilakukan kepada IT dan developer web Fakultas Ilmu Komputer UPN Veteran Jakarta baru. Hasil penilaian yang didapatkan yakni dengan nilai *Actual Security* 74.0088, yang menunjukkan bahwa keamanan website tersebut belum baik. Oleh karena itu untuk dapat mencapai nilai 100 harus ditingkatkan dengan membuat nilai Limitation yaitu Vulnerability, Weakness dan Concern bernilai 0.

Kata Kunci: OSSTMM, *Security Testing*, RAV, STAR

1. Pendahuluan

Perkembangan teknologi informasi yang cukup pesat dan tak dapat terbendung dalam beberapa tahun terakhir. Dimana pada masa tersebut hampir dan bahkan semua sektor membutuhkan berbagai teknologi yang dimana teknologi tersebut juga digunakan untuk menggantikan pekerjaan manusia. Perkembangan ini memudahkan manusia melakukan berbagai macam aktivitas contohnya dengan adanya aplikasi berbasis web. Web merupakan sebuah tampilan pada halaman web yang berisi informasi berupa tulisan, gambar, video dan lainnya yang kemudian dapat dipergunakan sebagai pusat informasi sekaligus menyimpan data dengan menggunakan web server sehingga semua ini dapat dengan mudah ditelusuri oleh semua orang dengan menggunakan internet.

Kemudahan yang disediakan dari fitur web tersebut salah satunya digunakan oleh sektor Pendidikan perguruan tinggi, dengan menggunakan teknologi web ini semakin memudahkan mereka untuk melakukan kinerja yang cepat dan efisien seperti akademik, penyampaian informasi, promosi dan lainnya yang dimana itu semua membantu dalam menjalankan fungsinya pada setiap perguruan tinggi yang ada. UPN Veteran Jakarta merupakan salah satu perguruan tinggi negeri yang bergerak di Pendidikan tinggi.

UPN Veteran Jakarta memiliki beberapa Fakultas, salah satunya yaitu Fakultas Ilmu Komputer, Fakultas tersebut menggunakan web lama dengan domain https://fik.upnvj.ac.id, kemudian fakultas membuat web resmi yang baru dengan domain yaitu http://new-fik.upnvj.ac.id. Web ini dipergunakan sebagai media informasi yang memberikan tentang akademik, *branding* Fakultas, pembuatan surat-surat penting dan juga tentang informasi alumni.

Untuk mencegah terjadinya isu celah keamanan, dibutuhkan sebuah evaluasi mengenai kondisi dan keadaan web tersebut. Dalam proses evaluasi tersebut maka diperlukan adanya pengecekan kerentanan dan celah keamanan pada web [1]. Metode tersebut yang bisa mencakup semua aspek dari evaluasi celah keamanan adalah OSSTMM.

OSSTMM merupakan metode pengujian mendetail, metrik untuk menilai tingkat keamanan saat ini, dan rekomendasi untuk membuat laporan akhir [3]. Metode OSSTMM memastikan bahwa semua tes yang dilakukan sesuai dengan OSSTMM rinci dan komprehensif dan hasilnya terukur dan faktual [3]. OSSTMM memiliki *framework report* serta rekomendasi yang dikemudian hari diharapkan berguna bagi tim IT.

Dikarenakan beberapa faktor dan kejadian tersebut dimana serangan siber pada aplikasi *web* semakin marak dan menyasar Fakultas Ilmu Komputer UPN Veteran Jakarta, penelitian ini dilakukan untuk melakukan evaluasi celah keamanan pada *web* Fakultas Ilmu Komputer UPN Veteran Jakarta baru dengan *domain http://new-fik.upnvj.ac.id* dengan menggunakan metodologi OSSTMM (*Open Source Security Testing Methodology Manual*) dan memberikan rekomendasi dan Langkah selanjutnya untuk melakukan penguatan serta pencegahan pada *web* tersebut untuk kedepan.

2. Tinjauan Pustaka

2.1 *Open Source Security Testing Methodology Manual* (OSSTMM)

Menurut [3] ada beberapa tahapan yang dilakukan sebelum melakukan OSSTMM, yaitu:

2.1.1 Mendefinisikan Aset

Melakukan Pendefinisian aset apa yang akan dilindungi dan akan di tes.

2.1.2 Menentukan *Engagement Zone*

Penguji menentukan tentang lingkungan aset yang mungkin ada di sekitar aset dalam bentuk mekanisme, proses, atau layanan perlindungan. Di sinilah interaksi dengan aset terjadi. Ini dikenal sebagai *Engagement zone*.

2.1.3 Mendefinisikan *Scope*

Mendefinisikan apa yang ada di luar zona keterlibatan yang dibutuhkan untuk melindungi aset. Semua ini disebut *Scope*.

2.1.4 Menentukan *Vector*

Menentukan *vector* harus dilihat dari bagaimana *scope* tersebut berinteraksi dengan *environment*. Aset-aset yang terdapat dalam *scope* dikelompokkan menurut arah interaksinya.

2.1.5 Menentukan *Channel*

Dalam menentukan Channel dapat dilakukan identifikasi peralatan yang dibutuhkan untuk menjalankan tes. Semua dikategorikan berdasarkan fungsi dan disebut *channel*. Yaitu:

1. *Human Security Channel*
2. *Physical Security Channel*
3. *Wireless Security Channel*
4. *Telecommunication Security Channel*
5. *Data Network Channel.*

2.1.6 Menentukan jenis tes.

Dalam menentukan jenis tes yang akan digunakan dalam pengujian berdasarkan informasi mengenai apa yang ingin dihasilkan dari pengujian. Jenis tes diberikan setiap kali mengikuti tes [2]. Berikut jenis tes yang ada pada metode OSSTMM.

1. *Double Blind*
2. *Blind*
3. *Gray Box*
4. *Double Gray Box*
5. *Tandem*
6. *Reversal*

2.1.7 *Rules of Engagement*

Pengujian keamanan yang telah tetapkan harus sesuai dengan *Rules of Engagement* pada *Test Process*, pedoman proses tersebut untuk memastikan proses pengujian keamanan yang tepat agar tidak menimbulkan kesalahpahaman, atau luaran yang salah.[3].

2.2 *Risk Assessment Value* (RAV)

RAV adalah pengukuran untuk zona permukaan serangan seperti yang didefinisikan oleh OSSTMM (*Open Source Security Testing Methodology Manual*). Sebuah RAV dari 100 mencerminkan keseimbangan sempurna antara perlindungan dan titik serangan [6].

Tabel 1. Nilai RAV [2]

Hasil	Keterangan
100	*Security* stabil/sempurna.
<100	*Security* masih lemah. Dan kurang
>100	*Security* berlebihan atau *over protective*

Tabel 2. Kategori RAV

OPSEC		*Visibility*
		Access
		Trust
Controls	*Class A –Interactive*	*Authentication*
		Indemnification
		Resilience
		Subjugation
		Continuity
	Class B – Process	*Non-Repudiation*
		Confidentiality
		Privacy
		Integrity
		Alarm
Limitations		*Vulnerability*
		Weakness
		Concerns
		Exposures
		Anomalies

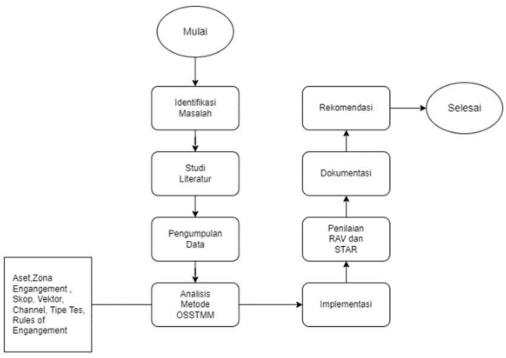
2.3 *Security Testing Audit Report* (STAR)

Menurut [3] STAR merupakan laporan tes yang menampilkan detail dari apa saja yang dilakukan pada penelitian yaitu berupa dokumen.

3. Metodologi Penelitian

3.1 Tahapan Penelitian

Tahapan dalam penelitian yang dilakukan dalam melakukan evaluasi celah risiko keamanan *web* terbaru FIK UPN Veteran Jakarta dengan metode OSSTMM yang digambarkan dalam gambar *flowchart* sebagai berikut:



Gambar 1. *Flowchart* Tahapan Penelitian

3.1.1 Identifikasi Masalah

Pada tahap pertama ini yang pertama kali dilakukan adalah mencari permasalahan yang berhubungan dengan topik yang akan diteliti. Dilakukan pencarian beragam ide yang baru untuk memetakan dan memecahkan masalah yang ditemukan pada tahap ini.

3.1.2 Studi Literatur

Studi literatur dilakukan untuk mendapatkan pengetahuan dan kerangka acuan seperti prosedur, tahapan dan laporan yang sesuai pada metodologi OSSTMM

3.1.3 Pengumpulan Data

Pengumpulan data dilakukan dengan melakukan wawancara dengan pihak IT dan *developer* yang memegang dan bertanggungjawab pada *web* terbaru FIK UPN Veteran Jakarta, kemudian melakukan observasi dan pengumpulan informasi secara pasif pada *hardware* dan *software*

3.1.4 Analisis Metode OSSTMM

Melakukan testing terdapat 7 poin dalam mendefinisikan *security testing* dalam metode OSSTMM yaitu Aset (apa yang akan diproteksi), *Engagement Zone* (lingkungan di sekitar aset), *Scope* (lingkungan diluar *Engagement Zone* yang diperlukan), *Vector* (arah dari interaksi scope), *Channel* (kanal pengujian), Tipe tes, dan *Rules of Engagement.*

3.1.5 Implementasi

Implementasi tersebut dilakukan dengan menggunakan OS Kali Linux 2021.3 64 bit, dengan dibantu aplikasi bawaan yang *pre-install* seperti Nmap, Nessus, Whois, Wireshark dan sebagainya. Semua pengetesan keamanan ini menggunakan tahapan *ethical hacking*

3.1.6 Penilaian RAV dan STAR

Setelah semua pengetesan keamanan telah dilakukan, kemudian hasil dan temuan dari pengetesan tersebut digunakan untuk membuat penilaian yang berbentuk *Risk Assessment Value* (RAV) dan *Security Testing Audit Report* (STAR)

3.1.7 Dokumentasi

Web yang sudah berhasil menghadapi implementasi pengujian keamanan serta penilaian STAR dan RAV akan dilakukan dokumentasi dengan berisi *template* perhitungan kalkulator RAV yang telah disediakan oleh metode OSSTMM

3.1.8 Rekomendasi

Hasil dari penilaian dari RAV dan STAR akan dijadikan tabel yang berisi poin Jenis kerentanan, *Severity*, *Impact*, *Affected* URL dan Rekomendasi.

4. Hasil dan Pembahasan

4.1 Analisis

Dalam melakukan *security testing* diharuskan dianalisa dan ditentukan poin-poin yang dibutuhkan dalam

penelitian terlebih dahulu. Poin yang dimaksud adalah sebagai berikut ini:

4.1.1 Mendefinisikan Aset

Pada penelitian ini, Aset yang akan dilakukan evaluasi risiko celah keamanan adalah aplikasi *web* terbaru Fakultas Ilmu Komputer UPN Veteran Jakarta.

4.1.2 Menentukan *Zone Engagement*,

Proses menentukan *Zone Engagement* dibangun di sekitar Jakarta yang sudah didefinisikan, dalam hal ini terdapat dua poin yaitu mekanisme proteksi dan proses/layanan yakni sebagai berikut:

1. Mekanisme Proteksi dalam sistem aplikasi *web* terbaru Fakultas Ilmu Komputer UPN Veteran Jakarta yang telah dikumpulkan pada pengumpulan data adalah dari segi protokol yang menggunakan protokol HTTP, TLS versi 1.0 dan TLS versi 1.1, kemudian CMS Wordpress *login*.
2. Proses/layanan yang dapat diberikan berupa *website* perkenalan profil Fakultas Ilmu Komputer serta form pengajuan surat dari mahasiswa.

4.1.3 Mendefinisikan *Scope*

Beberapa hal yang mempengaruhi dalam scope adalah sebagai berikut:
1. Energi Listrik aset menggunakan energi listrik untuk beroperasi pada *web server*.
2. Kebijakan/regulasi dari Jakarta menggunakan kode etik mahasiswa serta UU ITE.
3. Hosting dan Bandwith Internet menggunakan jalur *website*.

4.1.4 Menentukan *Vector*

Penelitian ini melakukan pengetesan dari satu arah yaitu pengetesan keamanan melalui jaringan internet ke sistem target.

4.1.5 Menentukan Channel

Dalam metode OSSTMM terdapat lima Channel untuk diobservasi, pada penelitian ini menggunakan *Channel Data Network Security*, pengujian ini mengenai evaluasi risiko celah keamanan dan uji penetrasi terhadap kerentanan yang ditemukan pada aplikasi *web* terbaru Fakultas Ilmu Komputer UPN Veteran Jakarta

4.1.6 Menentukan tipe tes

Tipe tes yang digunakan harus sesuai kondisi yang tepat bagi peneliti dalam melakukan penelitian, Oleh karena itu tipe tes yang digunakan dan yang tepat untuk penelitian ini berupa *greybox testing*

4.1.7 Menentukan *Rules of Engagement* beberapa aturan agar pengujian ini tidak membuat luaran

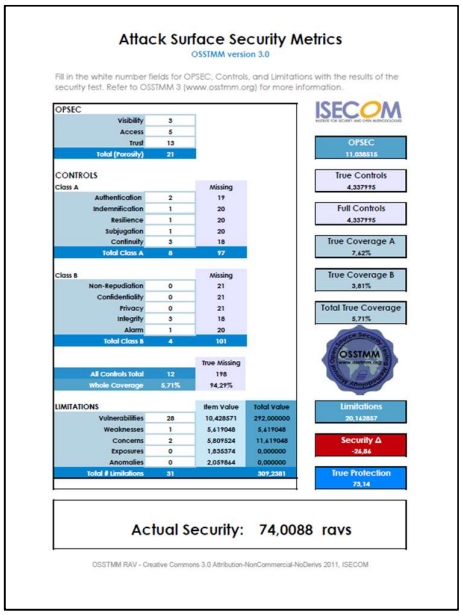
4.2 Implementasi

Setelah melakukan security testing terhadap semua task yang ada maka dirangkum semua nilai tersebut yakni sebagai berikut:

Tabel 3. Rangkuman Temuan

Visibilty (P_v)	No	Keterangan	Jumlah
	1	Melalui domain utama	1
	2	Internet Service Provider (ISP)	1
	3	*Web Server*	1
	Total		3
Access (P_A)	No	Keterangan	Jumlah
	1	*Port* berstatus open berjumlah 5 yaitu 21,22,80,443,5432	5
	Total		5
Trust (P_T)	No	Keterangan	Jumlah
	1	*Cross-site Request* dengan 13 domain	13
	Total		13
Authentication (LC_{Au})	No	Keterangan	Jumlah
	1	Sistem login user pada CMS Wordpress	1
	2	Sistem login pada SSH	1

	Total		2
Indemnification (LC_{Id})	No	Keterangan	Jumlah
	1	Aset menggunakan TLSv1.1	1
		Total	1
Resilience (LC_{Re})	No	Keterangan	Jumlah
	1	Penolakan *access* login apabila *username*/*password* tidak benar	1
	Total		1
Subjugation (LC_{Su})	No	Keterangan	Jumlah
	1	Satu *access* URL http://new-fik.upnvj.ac.id/wp-login.php untuk *access* login	1
	Total		1
Confidentiality (LC_{Cf})	No	Keterangan	Jumlah
	1	Aplikasi *web* menggunakan TLSv1.0 dan TLSv1.1	2
	2	SSL Certificate	1
	Total		3
Integrity (LC_{It})	No	Keterangan	Jumlah
	1	Aplikasi *web* menggunakan TLSv1.0 dan TLSv1.1	2
	2	SSL Certificate	1
	Total		3
Alarm (LC_{Al})	No	Keterangan	Jumlah
	1	Login attempt berlebihan mendapatkan pemblokiran dan peringatan dari aplikasi *web*	1
	Total		1
Vulnerability (L_v)	No	Keterangan	Jumlah
	1	Kerentanan *Cross-origin resource sharing:arbitrary origin Trust*ed pada 3 URL	3
	2	Kerentanan *Cross Site Scripting (Reflected)*, XSS Reflected pada 25 URL	25
	Total		28
Weakness (L_W)	No	Keterangan	Jumlah
	1	Ditemukan kerentanan Cleartext Submission pada 1 url	1
	Total		1
Concerns (L_C)	No	Keterangan	Jumlah
	1	TLSv1.0 yang sudah usang	1
	2	TLSv1.1 yang sudah usang	1
	Total		2



Gambar 2. Nilai RAV

Dari temuan diatas dapat ditemukan, hasil Akhir berupa *Actual Security* adalah sebesar 74.0088, dengan hasil RAV yang merujuk pada Gambar 2. Nilai RAV penilaian RAV tersebut, dapat dikategorikan <100 dan masuk pada penilaian *Security* masih lemah. Untuk bisa mencapai *Actual Security* bernilai 100 maka semua nilai limitations yakni *Vulnerability*, *Weakness* dan *Concern* harus bernilai mendekati 0 maka seluruh kondisi yang menyebabkan naiknya nilai Limitation harus diperbaiki. Sedangkan untuk kontrol harus tetap dipertahankan.

4.3 Rekomendasi

Berikut dibawah ini rangkuman tabel rekomendasi yang dibuat, sebagai berikut:

Tabel 4. Rekomendasi

No	Jenis Kerentanan	*Severity*	Rekomendasi
1	*Cleartext submission of password*	*High*	Aplikasi *web* harus menggunakan enkripsi SSL atau TLS untuk melindungi semua komunikasi sensitif yang lewat antara client dan *server*. Komunikasi yang harus dilindungi termasuk mekanisme login dan fungsionalitas terkait, dan fungsi apa pun di mana data sensitif dapat di*access*. Area ini harus menggunakan mekanisme penanganan sesi sendiri, dan token sesi yang digunakan tidak boleh dikirimkan melalui komunikasi yang tidak terenkripsi. Jika *cookie* HTTP digunakan untuk mentransmisikan token sesi, maka secure flag harus disetel untuk mencegah transmisi melalui *clear-text* HTTP Referensi: CWE-319: Cleartext Transmission of Sensitive Information
2	*Cross-site scripting (reflected)*	*High*	Input pengguna harus HTML-encoded dimana input tersebut disalin ke dalam respons aplikasi. Semua metakarakter HTML, termasuk < > " ' dan =, harus diganti dengan entitas HTML yang sesuai (< > dll). diperlukan untuk mengurai HTML yang disediakan untuk memvalidasi bahwa itu tidak menggunakan sintaks yang berbahaya

			Referensi: CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS), CWE-116: Improper Encoding or Escaping of Output, CWE-159: Improper Handling of Invalid Use of Special Elements, CWE-319: Cleartext Transmission of Sensitive Information
3	*Cross-origin resource sharing: arbitrary origin Trusted*	*High*	Gunakan *web* domain *whitelisting* pada domain yang tepercaya. Kemudian hindari menggunakan header Access-*Controls*-Allow-Origin: null. Referensi: CWE-942: Permissive Cross-domain Policy with Untrusted Domains

5. Kesimpulan dan Saran

5.1 Kesimpulan

Hasil evaluasi pengujian menggunakan metode OSSTMM menunjukkan luaran nilai berupa Actual Security sebesar 74,0088 sehingga dapat disimpulkan nilai tersebut kurang dari 100 dan memiliki kekurangan nilai 25,99 sehingga security pada web terbaru Fakultas Ilmu Komputer UPN Veteran Jakarta masih kurang baik dan harus segera diperbaiki.

5.2 Saran

Berdasarkan penelitian yang dilakukan, peneliti menyarankan agar kerentanan yang ditemukan pada web tersebut agar diperbaiki secepatnya agar tidak dieksploitasi dan disalahgunakan, perbaikan tersebut berfokus pada Limitations dengan poin Vulnerability, Weakness serta Concerns dengan membuat nilai poin tersebut mendekati nilai 0. Dengan skenario poin perbaikan tersebut menyebabkan nilai *Actual Security* dapat mencapai 100 (*Security* sempurna)

Referensi

[1] Caselli, M., & Kargl, F. (2016). A *security* assessment methodology for critical infrastructures. 8985, 332–343. doi:10.1007/978-3-319-31664-2_34.

[2] Fernando, Y. I., & Abdillah, R. (2016). *Security* Testing Sistem Penerimaan Mahasiswa Baru Universitas XYZ Menggunakan *Open Source Security Testing Methodology Manual*(OSSTMM). https://issn.lipi.go.id/terbit/detail/1489459246.

[3] Herzog, P. (2010). *The Open Source Security Testing Methodology ManualBook.* Dipetik November 1, 2021*,* dari https://www.isecom.org/research.html/.

[4] Metivier, B. (2017, April 17). Fundamental Objectives of *Information Security*: The CIA Triad. *The CIA Triad*, hal. 1. Dipetik November 18, 2021, dari https://www.tylercyber*security*.com/blog/fundamental-objectives-of-*Information-security*-the-cia-triad.

[5] Narvaez, A. E. (2019). ANALISIS DE VULNERABILIDADES PARA LA RED LAN DE LA EMPRESA "HIDROMAG", BAJO LA METODOLOGIA "OSSTMM". http://repositorio.uisrael.edu.ec/handle/47000/2044

[6] Risk Assessment Value (RAV). (2021, 1 Juni). Dipetik pada November 18, 2021, dari https://www.oneconsult.com/en/glossary/rav/