Metrik Dan Indeks Penarafan Risiko Keselamatan Laman Web Bagi Institusi TVET Awam Malaysia

Sharizal bin Yusoff
sharizal.yusoff@gmail.com

Mohd Zamri bin Murah
zamri@ukm.edu.my

ABSTRAK

Laman web Institusi Latihan dan Pendidikan Teknikal dan Vokasional (TVET) Awam Malaysia berisiko untuk menghadapi ancaman keselamatan apabila wujud kesukaran untuk memilih kaedah penilaian keselamatan laman web yang berkesan, tiadanya metrik keselamatan yang boleh memberi gambaran mengenai tahap risiko keselamatan yang dihadapi, hasil pengujian keselamatan sukar difahami bagi melakukan tindakan penambahbaikan. Oleh itu, kajian ini bertujuan untuk menentukan kriteria penilaian keselamatan bersama kaedah penilaian yang bersesuaian, membangunkan metrik yang memberi keutamaan mengenai tahap risiko keselamatan yang dihadapi oleh laman web yang dinilai dan menyediakan satu indeks keselamatan laman web yang akan menentukan tahap risiko laman web yang dinilai. Pengujian yang dilaksanakan terbahagi kepada lima peringkat iaitu tinjauan, tinjauan terperinci, imbasan web, analisis data dan akhirnya pembangunan indeks. Dengan menentukan lima kriteria utama metrik keselamatan iaitu gred SSL, maklumat imbasan umum, kerentanan port rangkaian, kesesuaian sistem pengoperasian dan kerentanan aplikasi, pengujian terperinci telah dilaksanakan ke atas 76 laman web Institusi TVET Awam Malaysia. Hasil pengujian ini kemudiannya dianalisis bagi mendapatkan jumlah pemberat kumulatif mengikut kepentingan metrik berkenaan. Akhirnya, nilai ini diolah bagi menyediakan satu indeks yang membahagikan kesemua laman web yang dinilai kepada tiga kumpulan laman web dari tahap berisiko rendah hingga ke tahap berisiko tinggi. Didapati bahawa 11% dari laman web ini dinilai sebagai berisiko tinggi, 8% berisiko sederhana dan 81% berisiko rendah. Dengan tersedianya kaedah penilaian ini, kesemua objektif kajian telah berjaya dicapai bagi menyelesaikan permasalahan dalam skop kajian ini. Indeks Keselamatan ini juga boleh di implementasi dan juga diolah dalam bentuk yang lebih terperinci bagi membantu pentadbir laman web Institusi TVET Awam Malaysia dalam merancang dan menambahbaik aspek keselamatan laman web masing-masing berdasarkan hasil penilaian indeks ini.

Kata kunci—indeks penarafan risiko; metrik penarafan risiko dan keselamatan web

PENGENALAN

Keselamatan siber telah menjadi satu topik yang amat penting dan begitu banyak dibincangkan di pelbagai ruang dan medium samada pada peringkat individu mahupun organisasi [1], [2]. Dengan peningkatan kebergantungan kepada teknologi yang digambarkan dengan jumlah pengguna yang terhubung ke Internet yang meningkat dari 17% pada tahun 2005 ke 53.6% pada tahun 2019, risiko ancaman serangan siber juga turut meningkat [3].

Di Malaysia sendiri, sebanyak 10,699 kes jenayah siber telah dikesan oleh MyCERT pada tahun 2018 [4]. Jumlah ini menunjukkan peningkatan sebanyak 26% berbanding insiden pada tahun 2017

sebanyak 7,962 kes [5]. Dalam kajian yang dilaksanakan oleh syarikat penyelidik Comparitech, Malaysia merupakan salah satu negara yang menerima serangan aplikasi web dalam jumlah yang tinggi, merangkumi 3% dari jumlah keseluruhan serangan aplikasi web di peringkat global [6].

Kesemua statistik ini menunjukkan dengan jelas bahawa ancaman keselamatan kepada laman web bukanlah satu perkara yang boleh dipandang remeh dan perlu diambil serius. Antara kaedah penilaian keselamatan ini menggabungkan penilaian kerentanan dan pengujian pencerobohan atau lebih dikenali sebagai Penilaian Kerentanan dan Ujian Penembusan (VAPT). Teknik ini adalah amat berkesan untuk membolehkan pentadbir laman web untuk melakukan penilaian dan seterusnya menguji kekuatan dan kelemahan yang ada di aplikasi masing–masing [7], [8]. Maka, kajian ini membangunkan kumpulan metrik keselamatan dan seterusnya menyediakan indeks yang membolehkan penarafan laman web dilakukan mengikut kategori risiko keselamatan yang dihadapi. Sebagai kajian kes, laman sesawang rasmi dan aplikasi kritikal institusi Pendidikan Latihan Teknikal dan Vokasional (TVET) telah dipilih sebagai medium penyelidikan.

Masalah pertama yang disentuh dalam kajian ini ialah risiko serangan laman web yang semakin meningkat kerana kaedah pengurusan keselamatan laman web yang tidak berkesan. Ini ditambah pula dengan kesukaran memilih kaedah penilaian keselamatan laman web yang diperlukan. Terdapat pelbagai teknik dan instrumen yang telah dicadangkan sebelum ini dalam melaksanakan penilaian keselamatan web ini samada secara automatik atau pun manual [9]. Maka timbul persoalan mengenai piawaian yang diperlukan bagi memastikan proses penilaian ini dapat dilaksanakan dengan menyeluruh. Pelbagai garis panduan telah diperkenalkan bagi tujuan ini [10]–[12]. Oleh itu, pemilihan kaedah terbaik perlu dilakukan bagi mengatasi masalah ini.

Seterusnya, masih tiada satu kaedah penarafan keselamatan yang menyeluruh dan berkesan untuk menggambarkan tahap keselamatan laman web yang diuji. Pada masa ini, pembangunan metrik dan indeks penarafan keselamatan yang dikemukakan hanya mengambil kira faktor teknikal terutamanya dari segi kelemahan dan ancaman yang ada pada laman web itu sendiri [13], [14]. Tanpa penggunaan metrik keselamatan yang selaras bagi pelbagai instrumen ini, hasil penilaian keselamatan yang dilaksanakan hanya akan menghasilkan implikasi penilaian secara berbeza tanpa satu keputusan yang konklusif [15]. Dengan kepelbagaian teknologi yang ada pada hari ini samada dari segi sistem pengoperasian mahupun perisian laman web, ditambah lagi dengan versi yang pelbagai bagi setiap perisian berkenaan, maka penggunaan metrik yang selaras amat diperlukan. Nilai metrik keselamatan yang dinilai juga sepatutnya mempunyai penekanan dengan kadar penilaian yang

berbeza bagi setiap penemuan pengujian memandangkan sesetengah item imbasan adalah lebih berisiko dan seharusnya dinilai memberi impak negatif yang lebih tinggi.

Oleh itu, rasional bagi menjalankan kajian ini adalah untuk menentukan kriteria penilaian keselamatan laman web dan kaedah yang bersesuaian, membangunkan metrik penilaian yang memberi keutamaan kepada tahap risiko yang ditemui dan akhirnya membina indeks keselamatan laman web yang meliputi semua aspek keselamatan dan memberi penarafan risiko yang jelas kepada laman web Institusi TVET Awam Malaysia. Sebanyak 175 laman web institusi TVET Malaysia telah dipilih sebagai skop kajian ini dimana pengujian akhir dilaksanakan kepada 76 laman web yang telah disaring berdasarkan kesesuaian skop kajian.

KAJIAN BERKAITAN

A. Kajian berkenaan tahap keselamatan 150 laman web di Arab Saudi

Pada tahun 2015, satu kajian telah dilaksanakan mengenai tahap keselamatan 150 laman web di Arab Saudi [16]. Dengan objektif untuk menilai tahap keselamatan laman web berkenaan tanpa melakukan semakan terperinci kepada kod pengaturcaraan web, kajian ini dilaksanakan dengan menggunakan perisian sumber terbuka *W3af* dan *Skipfish*. Didapati majoriti dari laman web yang dinilai mempunyai kelemahan dalam laman web mereka.

B. Kerentanan XSS dan pemalsuan input tapak silang (CSRF) pada laman web di negara Bangladesh

Dalam kajian yang dilaksanakan pada tahun 2016, penyelidikan dilakukan dengan menilai kerentanan XSS dan pemalsuan input tapak silang (CSRF) pada laman web di negara Bangladesh [13]. Sebanyak 500 laman web telah dipilih dan diuji secara manual dengan menggunakan skrip yang disediakan khusus untuk memanipulasi kerentanan XSS dan CSRF pada laman web yang ingin diuji. Dari 500 laman web yang diuji, 335 daripadanya didapati mempunyai kelemahan yang disebabkan oleh salah satu atau kedua-kedua kerentanan berkenaan

C. Penilaian terhadap tahap keselamatan laman web di Republik Mozambique

Kajian seterusnya memfokuskan penilaian terhadap tahap keselamatan laman web di Republik Mozambique dengan memberi penekanan mengenai kerentanan pendedahan maklumat oleh pelayan web dan kegunaan tetapan keselamatan HTTP [14]. Sebanyak 240 laman web telah dipilih dan dibahagikan kepada lapan kategori iaitu sektor telekomunikasi, kerajaan, akademik, bank, media, syarikat, parti politik dan organisasi lain.

D. Penilaian keselamatan laman web yang dilaksanakan oleh kerajaan Libya

Kajian seterusnya memfokuskan penilaian keselamatan laman web yang dilaksanakan oleh kerajaan Libya bagi menyediakan perkhidmatan secara dalam talian [17]. Rangka kerja pelaksanaan kajian ini dibahagikan kepada empat fasa utama iaitu Peninjauan, Pengumpulan Maklumat dan Imbasan, Penilaian Kerentanan dan Analisis Kandungan. Berdasarkan tiga faktor metrik yang diperoleh, satu model klasifikasi keselamatan web telah dicadangkan dengan empat tahap klasifikasi keselamatan. Berdasarkan hasil dari metrik yang diperoleh, satu laman web telah ditentukan pada tahap A sebagai amat tidak selamat, lapan di tahap B, enam di tahap C dan satu aplikasi di tahap D iaitu selamat.

E. Penilaian kerentanan yang berpunca dari pendedahan fail dalaman aplikasi yang tidak sah (LFD) di kalangan laman web pendidikan di Bangladesh

Pada tahun 2016, satu kajian telah dilakukan untuk menilai kerentanan yang berpunca dari pendedahan fail dalaman aplikasi yang tidak sah (LFD) di kalangan laman web pendidikan di Bangladesh [18]. 143 laman web pendidikan telah diuji secara manual bagi mengenal pasti kewujudan kelemahan yang membolehkan empat jenis serangan berdasarkan kerentanan LFD. Hasil penilaian mendapati 91% atau 130 dari 143 laman web pendidikan ini mempunyai kelemahan akibat kerentanan ini.

F. Pengujian kerentanan dilaksanakan dengan mengguna pakai fungsi carian maklumat imbasan umum yang dilakukan oleh portal Shodan

Dalam satu kajian lain, pengujian kerentanan dilaksanakan dengan mengguna pakai fungsi carian maklumat imbasan umum yang dilakukan oleh portal Shodan [19]. Eksperimen dilaksanakan ke atas 1501 perkhidmatan yang berbeza. Hasil analisis terhadap perkhidmatan yang dinilai berjaya menemukan 3922 maklumat kerentanan yang terperinci tanpa perlu melakukan ujian penembusan secara aktif terhadap perkhidmatan berkenaan.

G. Pembangunan indeks dan metrik bagi keselamatan laman sesawang institusi pengajian tinggi awam (IPTA) Malaysia

Pada 2018, kajian berkaitan pembangunan indeks dan metrik bagi keselamatan laman sesawang institusi pengajian tinggi awam (IPTA) Malaysia telah dilaksanakan [20]. Dalam kajian ini, sebanyak 229 IPTA yang mengandungi Universiti, Politeknik dan kolej telah disenaraikan untuk dinilai. Proses kajian ini terbahagi kepada tiga fasa utama iaitu fasa tinjauan, fasa analisis dan fasa

indeks. Keputusan akhir kajian ini menunjukkan 63% atau 62 dari 98 laman web IPTA berada di tahap berisiko rendah, 23% berisiko sederhana dan 14% atau 13 laman web IPTA berada di tahap berisiko tinggi.

H. Kaedah Penilaian Laman Web Sedia Ada

Terdapat pelbagai teknik dan instrumen yang telah dicadangkan sebelum ini dalam melaksanakan penilaian keselamatan web ini samada secara automatik atau pun manual [9]. Kedua-dua kaedah ini mempunyai kebaikan dan kekurangan masing-masing. Bagi memastikan hasil penilaian adalah menyeluruh dan memberikan maklumat yang selaras bagi mana-mana entiti yang dinilai, penggunaan beberapa instrumen atau kaedah yang saling melengkapi adalah amat diperlukan [21].

Pada masa yang sama, kaedah pengujian juga perlu mengambil kira garis panduan teknikal atau piawaian sedia ada. Empat garis panduan utama telah dikenal pasti dan dirumuskan seperti berikut:

JADUAL 1 SKOP PENILAIAN, KEPERLUAN PENGLIBATAN DAN TEMPOH PERLAKSANAAN PENILAIAN

Garis Panduan	Skop Penilaian	Penglibatan	Tempoh masa jangkaan pelaksanaan
NIST 800-115	Polisi, sumber manusia dan proses keseluruhan	Keseluruhan organisasi	Lama kerana melibatkan keseluruhan organisasi
OWASP WSTG	Kerentanan aplikasi	Pasukan khusus	Lama kerana melibatkan keseluruhan proses dari pembangunan sehingga pengujian aplikasi setelah selesai
EC Council EH	Maklumat ancaman umum, kerentanan rangkaian, sistem operasi dan aplikasi	Pasukan khusus	Pendek ke sederhana mengikut skop penilaian
MCMC SPA TC	Kerentanan rangkaian dan sistem operasi	Pasukan khusus	Pendek ke sederhana mengikut skop penilaian

I. Metrik Dan Indeks Keselamatan Laman Web

Terma metrik sering digunakan untuk merujuk kepada proses pengukuran prestasi entiti, namun sebenarnya metrik dan pengukuran adalah dua perkara yang berbeza [22]. Dari sudut lain, metrik didefinisikan dengan menyatakan ia adalah satu sistem pengukuran berdasarkan kepada nilai yang boleh dikira [23]. Metrik yang berkesan seharusnya dibangunkan dengan ciri-ciri spesifik seperti boleh diukur, tidak mustahil untuk dicapai dan boleh digunakan semula. Secara mudah, pengukuran adalah data asas yang dikumpul secara objektif dan metrik adalah terjemahan atau interpretasi yang dicapai menggunakan data asas berkenaan.

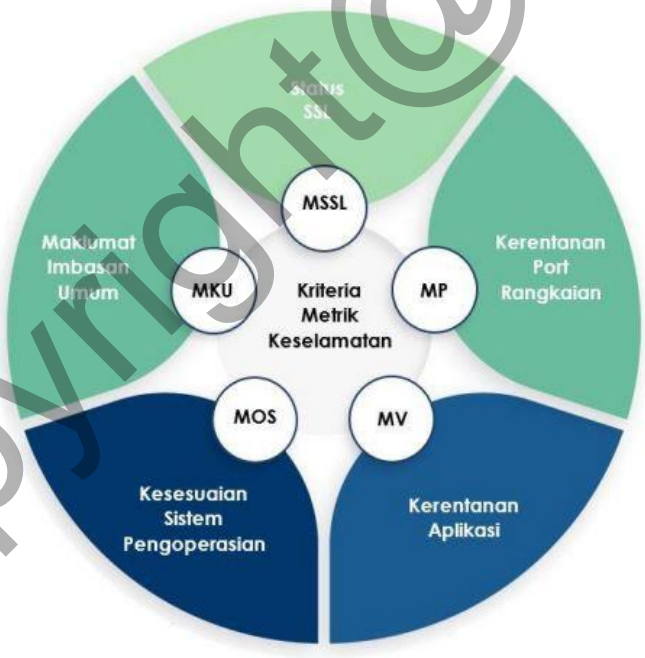
Menurut kamus Oxford, indeks adalah nilai di dalam sistem atau skala yang mempersembahkan nilai purata bagi item yang spesifik berbanding mana-mana nilai rujukan bagi item berkenaan [24].

Indeks diperolehi dengan menggunakan kaedah pengiraan kumulatif dari nilai metrik yang dikumpul semasa penilaian.

PENDEKATAN KAJIAN

Setelah melihat kepada kelebihan dan kekurangan garis panduan penilaian keselamatan sedia ada [10]–[12], [25] seperti di jadual 1, kajian ini akan menggunakan rangka kerja pengujian yang merujuk kepada garis panduan penggodaman beretika [10] memandangkan skop pengujian yang lebih meluas iaitu mengambil kira maklumat ancaman umum, kerentanan rangkaian, sistem pengoperasian dan aplikasi.

Bagi mengelakkan gangguan atau kerosakan kekal kepada laman web yang akan diuji, maka kajian ini akan mengguna pakai kaedah pengujian secara kotak hitam [8] di mana pengujian hanya dilakukan di luar skop persekitaran rangkaian laman web yang diuji. Berdasarkan kajian kesusasteraan yang telah dilakukan, maka lima kriteria utama metrik keselamatan telah dikenal pasti bagi kajian ini seperti berikut:



RAJAH 1 KRITERIA METRIK KESELAMATAN LAMAN WEB

Kriteria Status SSL (MSSL), Kerentanan Port Rangkaian (MP), Kesesuaian Sistem Pengoperasian (MOS) dan Kerentanan Aplikasi (MV) adalah merupakan elemen penting yang meliputi keselamatan web dari segi infrastruktur rangkaian dan juga perisian yang digunakan. Manakala kriteria Maklumat Imbasan Umum (MKU) pula merupakan elemen penilaian bagi

mengukur pendedahan maklumat jejak digital laman web yang berpotensi disalahguna oleh penjenayah siber.

Untuk mendapatkan maklumat yang tepat dan sahih berkenaan kriteria yang telah ditentukan ini, rangka kerja pengujian yang dicadangkan sebelum ini telah diperincikan supaya bersesuaian dengan kriteria kajian yang akan dilaksanakan. Berdasarkan keperluan maklumat, lima peringkat pengujian telah dikenal pasti bagi dilaksanakan dalam kajian ini merangkumi 11 proses seperti berikut:

JADUAL 2 FASA PELAKSANAAN KAJIAN

Peringkat Pengujian	**Proses**	**Penerangan Proses**
Tinjauan Asas	Kueri Maklumat Domain Kueri penggunaan SSL	Kueri menggunakan skrip *Python* bagi mendapatkan maklumat domain dan status penggunaan SSL
Tinjauan Terperinci	Penilaian gred SSL laman web Pengumpulan maklumat imbasan umum	Penilaian Gred SSL bagi kriteria MSSL dan pengumpulan maklumat imbasan umum bagi kriteria MKU
Imbasan Web	Imbasan Port Rangkaian dan Sistem Operasi Imbasan ZAP Imbasan Acunetix	Imbasan port rangkaian (Kriteria MP) dan sistem operasi (Kriteria MOS) serta imbasan kerentanan (Kriteria MV)
Analisis Data	Analisis hasil dan pemberian pemberat Penetapan Metrik	Hasil pengujian setiap kriteria akan dianalisis dan diberi nilai pemberat kualitatif. Nilai ini dijumlah sebagai nilai metrik keseluruhan (AM)
Pembangunan Indeks	Analisis Metrik dan Penetapan Pembolehubah Pembangunan Indeks	Penormalan nilai AM dan pembangunan Indeks Keselamatan akhir

A. Tinjauan Asas

Pada peringkat ini, maklumat asas berkaitan kumpulan sasar iaitu 175 laman web institusi TVET akan dikumpul dan disediakan menggunakan kaedah berikut:

i. Kueri Maklumat Domain

Setiap item di dalam kumpulan sasar akan diselidik melalui enjin carian seperti enjin carian web Google bagi mendapatkan maklumat asas mengenai sasaran. Kueri yang digunakan adalah “Laman web (Nama Institusi)”, “Laman Web (Nama Institusi)” dan “Portal (Nama Institusi).

ii. Kueri penggunaan SSL

Dengan menggunakan senarai lengkap domain yang disediakan pada proses sebelumnya yang mengandaikan semua laman web ini menggunakan teknologi HTTP, ujian

pengesanan status penggunaan teknologi HTTPS akan dilaksanakan mengguna pakai skrip pengaturcaraan python. Status penggunaan SSL adalah ditetapkan berdasarkan kos respon sama ada 200, 300 atau 500.

B. Tinjauan Terperinci

Pada peringkat ini, maklumat spesifik berkaitan kumpulan sasar akan dikumpul dan disediakan bagi tujuan imbasan. Maklumat terperinci yang ditentukan adalah status perkhidmatan kritikal seperti berikut:

i. Penilaian gred SSL laman web

Setelah senarai lengkap status penyediaan SSL diperoleh melalui proses sebelum ini, portal Qualys SSL akan digunakan bagi menyemak konfigurasi SSL bagi setiap alamat Internet dan perincian mengenai sijil. Hasil akhir penilaian adalah gred penarafan berkenaan tetapan teknologi SSL yang digunakan oleh laman berkenaan.

ii. Pengumpulan maklumat imbasan umum

Melalui portal Shodan, tahap pendedahan maklumat kepada umum dapat dinilai dengan melakukan carian menggunakan alamat IP laman web berkenaan. Hasil akhir adalah maklumat umum kerentanan bagi laman berkenaan.

C. Imbasan Web

Setelah kesemua alamat Internet dan alamat IP kumpulan sasar dimuktamadkan, maklumat ini seterusnya digunakan bagi pelaksanaan proses imbasan web. Peringkat ini terbahagi kepada tiga jenis imbasan iaitu imbasan port, sistem pengoperasian dan kerentanan aplikasi.

Perisian sumber terbuka *nmap* akan digunakan untuk mengimbas status penggunaan port pada pelayan aplikasi, perkhidmatan yang terbuka untuk capaian umum, nama dan versi sistem pengoperasian yang digunakan. Seterusnya, imbasan menggunakan perisian sumber terbuka OWASP ZAP dan Acunetix akan lebih tertumpu kepada kerentanan pada sistem operasi, aplikasi pelayan web dan pangkalan data sedia ada, kelemahan dalam kod aplikasi dan persekitaran aplikasi yang membolehkan serangan dilakukan pada aplikasi. Imbasan hanya dilakukan dengan memfokuskan kepada kerentanan XSS dan suntikan SQL sahaja. Kesemua hasil penemuan proses imbasan ini akan digunakan untuk membangunkan metrik dan menentukan pemberat kuantitatif yang bersesuaian bagi metrik berkenaan.

D. Analisis Data

Pada peringkat ini, kesemua hasil tinjauan asas, terperinci dan imbasan web akan dikumpulkan mengikut kriteria masing-masing. Data ini akan dianalisis untuk membolehkan proses klasifikasi data dilakukan. Klasifikasi ini akan mengambil kira perbandingan pemboleh ubah pada hasil imbasan untuk membolehkan satu nilai kuantitatif diberikan pada setiap kriteria bagi membina penanda aras bagi metrik keselamatan aplikasi. Pemberian pemberat yang akan ditentukan adalah berdasarkan justifikasi kepentingan kriteria berkenaan kepada pelaksanaan operasi perkhidmatan laman web berkenaan secara langsung atau tidak langsung.

i. Analisis MSSL

Berdasarkan pematuhan setiap komponen ini, gred penarafan yang bersesuaian akan diberikan pada akhir pengujian yang terbahagi kepada enam tahap iaitu gred A, B, C, D, E dan F. Pemberat metrik Gred SSL (MSJ) bagi setiap gred ini adalah ditentukan seperti berikut:

JADUAL 3 PEMBERAT MENGIKUT GRED PENARAFAN SSL

Gred Penarafan	**Pemberat**
A	0
B	1
C	2
D	3
E	4
F	5

ii. Analisis MKU.

MKU merupakan nilai metrik bagi status penemuan kerentanan umum laman web berdasarkan carian di portal Shodan. Nilai 1 akan diberikan jika laman web berkenaan mempunyai maklumat kerentanan dan nilai 0 akan diberikan bagi laman web tidak mempunyai maklumat berkenaan.

iii. Analisis MP

Bagi penilaian keselamatan port, port dikategorikan kepada dua kumpulan iaitu port sasaran utama mengikut penarafan *nmap* [26] sebagai P_{HR} dan port selain dari yang tersenarai di kumpulan sebelumnya sebagai P_T. P_{HR} ini akan diberikan pemberat 3 bagi setiap port manakala P_T pula diberikan nilai 1 bagi setiap port. Manakala port 80 dan port

443 akan dikeluarkan dari senarai penemuan port dan tidak akan dikira. Oleh itu, persamaan bagi pengiraan keseluruhan metrik port (MP) ini adalah seperti berikut:

$$MP = 3\ (P_{HR}) + P_T$$

iv. Analisis MOS

Bagi kriteria ini, nilai kuantitatif akan diberikan secara perbandingan bagi versi sistem pengoperasian yang digunakan. Jadual markah ini adalah seperti berikut:

JADUAL 4 PEMBERAT BAGI METRIK KESELAMATAN SISTEM PENGOPERASIAN

Usia Sistem Pengoperasian Nilai metrik	**Usia Sistem Pengoperasian Nilai metrik**
Kurang 4 tahun 0	Kurang 4 tahun 0
4 – 6 tahun 2	4 – 6 tahun 2
Lebih 6 tahun 4	Lebih 6 tahun 4

v. Analisis MV

Bagi kajian ini, imbasan kerentanan yang dilakukan menumpukan kepada tiga aspek utama : kerentanan umum persekitaran pelayan web, kerentanan skrip tapak silang dan kerentanan suntikan SQL. Untuk tujuan pembangunan metrik, nilai kuantitatif perlu diberikan kepada lima tahap ini untuk membolehkan perbezaan tahap ini diambil kira dalam metrik yang akan digunakan bagi mendapatkan indeks di fasa terakhir. Maka, nilai berikut telah ditentukan bagi setiap tahap:

JADUAL 5 NILAI PEMBERAT BAGI TAHAP RISIKO

Tahap Risiko	**Nilai Pemberat**
Tinggi (T_T)	3
Sederhana (T_S)	2
Rendah (T_R)	1
Info (T_I)	0

Setelah diberikan nilai, metrik kerentanan aplikasi (MV) akan dikira berdasarkan persamaan berikut:

$$MV = (T_T \times 3) + (T_S \times 2) + (T_R \times 1) + (T_I \times 0)$$

vi. Membina Metrik Keseluruhan (AM)

Setelah kesemua nilai metrik keselamatan yang dinilai sebelum ini ditentukan, maka jumlah akhir bagi metrik ini (AM) akan dikira dengan mengambil kira kesemua nilai berkenaan mengikut persamaan berikut:

$$AM = MSSL + MKU + MP + MOS + MV$$

E. Membina Indeks

Peringkat akhir dalam melaksanakan penilaian keselamatan ini adalah untuk membangunkan satu indeks keselamatan berdasarkan nilai metrik keselamatan yang diperoleh sewaktu analisis data dilakukan sewaktu peringkat sebelumnya. Kesemua nilai metrik ini akan melalui proses penormalan statistik untuk mendapatkan julat indeks yang rasional. Akhirnya nilai yang telah dinormalkan ini akan disusun mengikut nilai akhir indeks bagi menyediakan jadual dan senarai institusi yang dinilai mengikut tahap risiko yang ditemui.

Setelah kesemua nilai Indeks Keselamatan ini diperoleh melalui proses penormalan akhir, maka nilai indeks ini akan digunakan bagi menentukan penarafan keselamatan laman web mengikut kategori risiko berikut:

JADUAL 6 KATEGORI RISIKO MENGIKUT NILAI INDEKS KESELAMATAN

Kategori Risiko	Nilai indeks
Rendah	<0.00
Sederhana	0.00-1.00
Tinggi	>1.00

F. Instrumen Kajian

Terdapat lima instrumen utama yang digunakan dalam melaksanakan kajian ini iaitu Qualys SSL, Shodan, nmap, OWASP ZAP dan Acunetix. Setiap instrumen ini mempunyai fungsi dan kekuatan tersendiri yang telah diperakui dalam kajian sebelum ini.

HASIL PENGUJIAN

A. Hasil Peringkat Tinjauan Asas

Didapati 101 laman web dalam tiga kumpulan mempunyai alamat IP yang sama. Penggunaan IP yang sama menunjukkan bahawa laman web berkenaan beroperasi menggunakan pelayan web yang sama dan akan mempunyai tahap kerentanan yang sama. Keadaan ini membuatkan pengujian tidak relevan untuk dilaksanakan pada laman web dalam kumpulan IP yang sama. Maka hanya satu laman web dipilih bagi mewakili setiap kumpulan IP berkenaan. Keputusan pengujian juga mendapati satu laman web tidak lagi beroperasi dan dikeluarkan dari senarai sasaran kajian ini. Oleh itu, hanya 76 laman web ditentukan sebagai jumlah akhir laman web yang akan digunakan sebagai sasaran bagi pelaksanaan fasa seterusnya. Pengujian yang sama juga memberikan hasil bagi subproses Kueri Penyediaan SSL di mana hasil ujian telah mendapati hanya 11 dari 76 laman web yang diuji memberikan keputusan '*valid'* iaitu dikesan menggunakan teknologi SSL.

B. Hasil Peringkat Tinjauan Terperinci

Dari kesemua 76 laman web yang diuji, 20 pelayan laman web yang dikesan menyokong teknologi SSL ini mengikut hasil pengujian dan diberikan gred yang bersesuaian iaitu empat dari laman web ini mendapat gred A, lima dengan gred B, satu dengan gred C dan satu dengan gred F. Bagi imbasan portal Shodan pula, 48 laman web dikesan mengandungi kerentanan berdasarkan hasil imbasan portal Shodan dan 28 laman web tidak mengandungi kerentanan.

C. Hasil Peringkat Imbasan Web

Dari hasil imbasan menggunakan instrumen nmap, didapati 42 alamat IP laman web yang diuji tidak memberikan maklum balas terhadap imbasan dan hanya 34 alamat IP yang memberikan maklumat mengenai port rangkaian atau sistem pengoperasian yang digunakan oleh pelayan web berkenaan. Imbasan OWASP ZAP mendapati 26 laman web yang tidak dapat diimbas atau dikesan tidak mempunyai sebarang kerentanan. Dari 50 laman web yang berjaya diimbas, 45 dikesan mempunyai kerentanan XSS dan 24 dikesan mempunyai kerentanan suntikan SQL. Imbasan *Acunetix* pula mendapati dari 76 laman web yang diimbas, 42 laman web mempunyai kerentanan skrip tapak silang dan 28 laman web mempunyai kerentanan suntikan SQL. Baki sebanyak tujuh laman web tidak berjaya diimbas kerana tiada maklum balas dari pelayan web berkenaan atau dikesan tidak mempunyai sebarang kerentanan.

D. Analisis Data

Setelah kesemua kriteria metrik diberikan nilai pemberat yang bersesuaian dan dijumlahkan, jumlah ini kemudiannya ditentukan sebagai nilai metrik keseluruhan dan digunakan dalam fasa berikutnya.

E. Pembangunan Indeks

Di peringkat awal, penentuan outlier dilakukan dengan mengguna pakai kaedah statistik. Setelah selesai pengiraan, hasil akhir mendapati 10 laman web telah dikenal pasti sebagai *outlier* kerana nilai metrik keselamatan yang diperoleh laman web ini adalah melebihi nilai sempadan data bagi kuartil tertinggi iaitu 577.

JADUAL 7 LAMAN WEB YANG DIKENAL PASTI SEBAGAI OUTLIER

Laman Web	Nilai Metrik Keselamatan
w35	604
w72	741
w69	771
w68	833
w61	1029
w11	1180
w34	2392
w52	3408
w23	4895
w3	11948

Oleh kerana penilaian hanya mengambil kira 76 laman web setelah ditapis pada peringkat pertama, maka semakan semula alamat internet dengan alamat internet asal perlu dilakukan untuk mendapatkan jumlah sebenar laman web mengikut kategori risiko masing-masing. Setelah disemak, kesemua tiga alamat internet yang mewakili baki 99 laman web dari 175 laman web yang dikeluarkan sebelum ini adalah termasuk di dalam kategori berisiko rendah. Maka, jumlah keseluruhan laman web yang berisiko rendah adalah sebanyak 142. Hasil akhir menunjukkan 81% laman web institusi TVET yang diuji adalah berada pada kategori berisiko rendah, 8% pada kategori berisiko sederhana dan 11% pada kategori berisiko tinggi seperti berikut:

JADUAL 8 JUMLAH LAMAN WEB MENGIKUT KATEGORI RISIKO

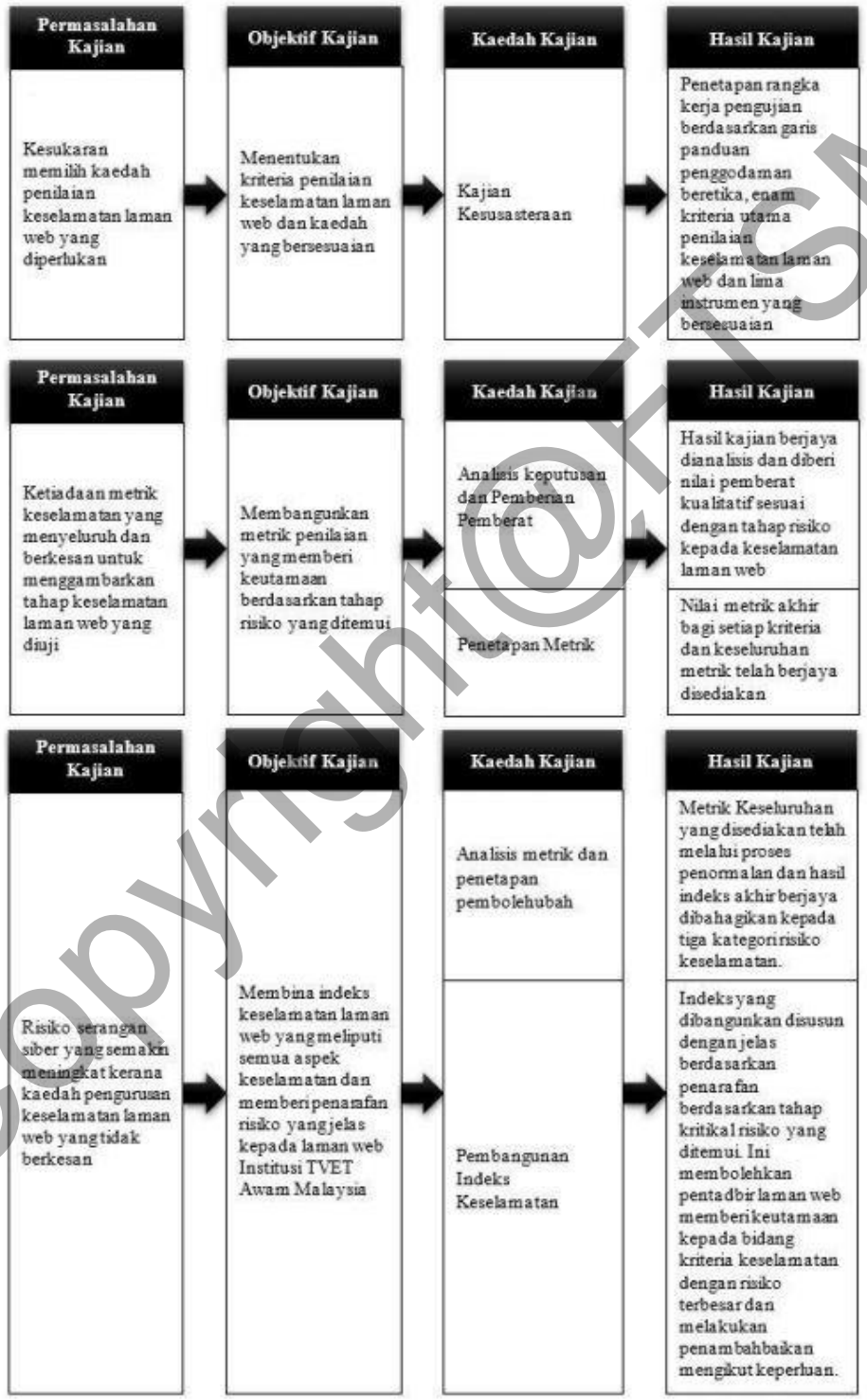
Kategori Risiko	Jumlah laman web	Peratus (%)
Rendah	142	81
Sederhana	13	8
Tinggi	20	11

Hasil ini dengan jelas menyatakan bahawa lebih separuh laman web institusi TVET yang dinilai berada pada kategori berisiko rendah dan memberi gambaran bahawa kesemua institusi berkenaan adalah mengambil berat berkenaan keselamatan laman web mereka selaku peneraju industri pendidikan di negara ini. Namun, 11% pula dari laman web institusi TVET yang dinilai berada pada kategori berisiko tinggi. Dengan kepentingan institusi TVET ini bagi pembangunan negara dan jelasnya ancaman siber terhadap infrastruktur ICT institusi ini, maka jumlah ini tidak seharusnya diambil mudah kerana penjenayah hanya memerlukan satu sasaran yang mempunyai masalah risiko keselamatan yang tinggi bagi membolehkan mereka melakukan pencerobohan dan memberi implikasi yang negatif kepada keseluruhan institusi TVET di negara ini.

KESIMPULAN

A. Rumusan dan penemuan

Kajian yang dijalankan telah berjaya menjawab persoalan kajian yang telah digariskan seterusnya membolehkan objektif kajian dipenuhi seperti di rajah berikut:



RAJAH 2 PENCAPAIAN OBJEKTIF KAJIAN SECARA KESELURUHAN

B. Sumbangan

Kajian ini telah berjaya menghasilkan dua (2) sumbangan utama iaitu lima kriteria metrik yang bersesuaian bagi penilaian keselamatan laman web dan pembangunan metrik beserta indeks keselamatan yang berupaya mengkategorikan laman web dalam kumpulan risiko masing-masing berdasarkan nilai pemberat kuantitatif yang mudah diukur dan difahami. Tindakan boleh diambil oleh pentadbir laman web berkenaan dengan mengguna pakai hasil penemuan kajian ini yang boleh di implementasi dengan pelbagai kaedah berlainan berdasarkan kriteria pembangunan indeks keselamatan ini secara berasingan untuk mendapatkan pemahaman mengenai risiko keselamatan dengan lebih terperinci. Pendekatan ini juga membolehkan pentadbir laman web untuk merancang proses penambahbaikan dengan lebih berkesan.

C. Cadangan dan Kajian Masa Depan

Kajian ini meletakkan enam kriteria utama bagi pembangunan Indeks Keselamatan laman web. Kriteria ini adalah bersifat asas dan mencukupi pada ketika ini bagi mencapai objektif kajian. Namun, penyelidikan lanjut dan lebih mendalam mengenai kriteria lengkap bagi memastikan keselamatan laman web dapat dicapai dengan sepenuhnya adalah amat penting dan berguna supaya Indeks Keselamatan yang dihasilkan nanti adalah lebih relevan dan dapat memberi gambaran risiko yang lebih realistik bagi laman web berkenaan.

Skop kerentanan juga boleh diperluaskan lagi dengan mengambil kira samada berdasarkan skop kerentanan yang diperincikan oleh OWASP atau pun mengguna pakai sepenuhnya pangkalan data kerentanan yang disediakan oleh instrumen penilaian kerentanan yang dipilih. Akhirnya, fasa imbasan juga boleh dipertimbangkan untuk dilaksanakan dengan menggunakan konsep kotak putih, di mana proses imbasan dilaksanakan secara terus dari dalam rangkaian laman web yang diimbas kerana imbasan menggunakan kaedah ini lebih berpotensi untuk menemui lebih banyak kerentanan yang ada pada laman web berkenaan

RUJUKAN

[1] E. Ernst and Young, “Is cybersecurity about more than protection?,” 2018.

[2] E. Ernst and Young, “Under cyber attack EY’s Global Information Security Survey 2013 Insights on governance, risk and compliance,” 2013.

[3] International Telecommunication Union, “Measuring digital development,” 2019.

[4] C. S. M. MyCERT, “mycert-incident-statistics 2018.pdf,” 2018.

[5] C. S. M. MyCERT, “mycert-incident-statistics 2017.pdf,” 2017.

[6] R. Spiess, “Black hats, hacks and cyber attacks,” 2019. [Online]. Available: https://southeastasiaglobe.com/how-southeast-asia-ranks-in-cybersecurity/. [Accessed: 14-Nov-2019].

[7] P. S. Shinde and S. B. Ardhapurkar, “Cyber security analysis using vulnerability assessment and penetration testing,” in *IEEE WCTFTR 2016 - Proceedings of 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare*, 2016.

[8] I. Yaqoob, S. A. Hussain, S. Mamoon, N. Naseer, J. Akram, and A. ur Rehman, “Penetration Testing and Vulnerability Assessment,” *J. Netw. Commun. Emerg. Technol.*, vol. 7, no. 8, pp. 10–18, 2017.

[9] L. Dukes, X. Yuan, and F. Akowuah, “A case study on web application security testing with tools and manual testing,” in *Conference Proceedings - IEEE SOUTHEASTCON*, 2013.

[10] E. Council, “What is Ethical Hacking | Types of Ethical Hacking | EC-Council,” 2020. [Online]. Available: https://www.eccouncil.org/ethical-hacking/. [Accessed: 14-May-2020].

[11] M. T. S. F. B. MTSFB, “MCMC MTSFB TC G016:2018 TECHNICAL CODE INFORMATION AND NETWORK SECURITY-SECURITY POSTURE ASSESSMENT (SPA) MCMC MTSFB TC G016:2018 Development of technical codes,” 2018.

[12] K. Scarfone, M. Souppaya, A. Cody, and A. Orebaugh, “Special Publication 800-115 Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology,” 2008.

[13] T. Farah, M. Shojol, M. Hassan, and D. Alam, “Assessment of vulnerabilities of web applications of Bangladesh: A case study of XSS & CSRF,” in *2016 6th International Conference on Digital Information and Communication Technology and Its Applications, DICTAP 2016*, 2016, pp. 74–78.

[14] A. P. Vumo, J. Spillner, and S. Kopsell, “Analysis of Mozambican websites: How do they protect their users?,” in *2017 Information Security for South Africa - Proceedings of the 2017 ISSA Conference*, 2018, vol. 2018-Janua, pp. 90–97.

[15] N. Mendes, H. Madeira, and J. Duraes, “Security benchmarks for web serving systems,” in

Proceedings - International Symposium on Software Reliability Engineering, ISSRE, 2014, pp. 1–12.

[16] M. S. Al-Sanea and A. A. Al-Daraiseh, "Security evaluation of Saudi Arabia's websites using open source tools," in *2015 1st International Conference on Anti-Cybercrime, ICACC 2015*, 2015.

[17] A. Ahmed and M. Z. Murah, "Web Assessment of Libyan Government e-Government Services," *Int. J. Adv. Comput. Sci. Appl.*, 2018.

[18] M. Hassan, T. Bhuiyan, S. Biswas, and M. M. Hassan, "An Investigation of Educational Web Applications in Bangladesh: A Case Study on Local File Disclosure Vulnerability," *Eng. Technol. Comput. Basic Appl. Sci.*, vol. 933, pp. 11–16, 2016.

[19] B. Genge and C. Enăchescu, "ShoVAT: Shodan-based vulnerability assessment tool for Internet-facing services," *Secur. Commun. Networks*, vol. 9, no. 15, pp. 2696–2714, Oct. 2016.

[20] M. N. bin Omar, "Metrik dan Indeks keselamatan laman sesawang : satu kajian kes terhadap institusi pengajian tinggi awam di Malaysia," Universiti Kebangsaan Malaysia, 2018.

[21] B. Mburano and W. Si, "Evaluation of web vulnerability scanners based on OWASP benchmark," in *26th International Conference on Systems Engineering, ICSEng 2018 - Proceedings*, 2019.

[22] J. G. Voeller, P. E. Black, K. Scarfone, and M. Souppaya, "Cyber Security Metrics and Measures," in *Wiley Handbook of Science and Technology for Homeland Security*, John Wiley & Sons, Inc., 2008.

[23] D. Juneja, K. Arora, and S. Duggal, "Developing Security Metrics For Information Security Measurement System," *Int. J. Enterp. Comput. Bus. Syst.*, vol. 1, no. 2, 2011.

[24] Oxford, "Index | Definition of Index by Lexico," *Oxford University Press*, 2020. [Online]. Available: https://www.lexico.com/en/definition/index. [Accessed: 06-Feb-2020].

[25] OWASP, "OWASP Web Security Testing Guide," 2020.

[26] G. Lyon, "Chapter 4. Port Scanning Overview | Nmap Network Scanning," 2020. [Online]. Available: https://nmap.org/book/port-scanning.html#most-popular-ports. [Accessed: 26-Feb-2020].