SISTEM PENGIMBASAN KERENTANAN BERASASKAN WEB

RUEBESH A/L PASUPATHY
DR. KHAIRUL AKRAM ZAINOL ARIFFIN

Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Virus dan malware semakin maju dan berbahaya kerana boleh membuat kita kehilangan data berharga kita. Selama bertahun-tahun, banyak laman web telah di "hack" dan dieksploitasi, bahkan di server bank yang paling selamat. Penggodam akan selalu mencari jalan untuk memintas keselamatannya dan mengaut data berharga untuk tebusan atau sebab lain yang tidak baik. Oleh itu, ujian keselamatan aplikasi web dan telefon penyemak imbas web sangat penting dalam dunia masa kini yang penuh dengan teknologi. Pengemaskinian sistem web haruslah dijalankan dari semasa ke semasa untuk memastikan keselamatan sesebuah sistem web dijamin selamat. Daripada itu, idea pembangunan sebuah sistem web pengimbas kerentanan didapati. Pengimbas kerentanan berasaskan web adalah sistem automatik yang mengimbas aplikasi web, biasanya dari luar, untuk mencari kelemahan keselamatan yang berbahaya.

Perancangan pembangunan sebuah sistem pengimbasan kerentanan berasaskan web ini telah dilakukan untuk mengesan masalah seperti perisian pelayan yang sudah lapuk, HTTP header yang tidak selamat, tetapan "cookies" yang tidak selamat dan beberapa yang lain. Pengesanan yang lebih kuat seperti pengesanan *SQL Injection, XSS, Local File Inclusion, OS Command Injection* dan banyak lagi juga akan dimasukkan ke dalam sistem ini. Mereka juga dikenali sebagai sistem pengujian penembusan web yang akan berusaha menembus keselamatan system untuk melihat sejauh mana ia dapat menembus dan seberapa rentan sistem anda yang sedia ada. Ini sangat penting dan berguna bagi banyak pelayar web untuk sentiasa menjaga privasi dan keselamatan data dan sistem kita.

1 PENGENALAN

Pengimbas Kerentanan berasaskan Web adalah sistem web yang mengimbas aplikasi web untuk mencari kerentanan keselamatan seperti *XSS scripting, SQL Injection, Command Injection, Path Traversal* dan konfigurasi server yang tidak selamat. Sistem web kategori ini sering disebut sebagai Sistem Perisian Pengujian Keselamatan Aplikasi Dinamik. Sebilangan besar sistem pengujian kerentanan ini mempunyai kekuatan dan kelemahan masing-masing. Penilaian kerentanan adalah proses mengenal pasti, mengukur, dan mengutamakan kerentanan dalam sistem. Sistem-sistem pengujian ini digunakan dalam pengenalpastian dan pengesanan

kerentanan yang timbul dari salah konfigurasi atau program yang tidak betul dalam “network-based aset” seperti firewall, router, server web, server aplikasi, dan lain-lain.

Projek ini dibangunkan dalam PHP dan MYSQL. Seperti yang kita ketahui, pelanggaran data berprofil tinggi semakin meningkat dalam organisasi-organisasi yang besar sejak sedekad yang lalu. Sebilangan besar ini berlaku melalui serangan suntikan (*injection attacks*), iaitu merupakan suntikan kod jahat (*malicious code*) ke dalam aplikasi web. Sesungguhnya, Projek Keselamatan Aplikasi Web Sumber Terbuka atau lebih dikenali sebagai *Open Source Web Application Security Project (OWASP),* organisasi terkemuka dalam bidang keselamatan aplikasi web menyatakan bahawa "Cara input data dikendalikan oleh aplikasi Web merupakan aspek keselamatan yang paling penting." Ada dua faktor yang meningkatkan kepentingan perjuangan sekuriti siber. Secara taktikal dan operasi, peningkatan ketergantungan kepada kemajuan teknologi moden pada rangkaian dan sistem maklumat mewujudkan serta membawa pelbagai jenis kelemahan dan kerentanan yang dapat dimanfaatkan oleh penggodam-penggodam topi hitam. Selain itu, sebagai masyarakat moden termasuk tentera terus berkembang dan semakin bergantung pada serangkaian "infrastruktur kritikal" yang banyak serta besar dan semakin rentan untuk berfungsi dengan berkesan. Infrastruktur ini tidak hanya menjadi lebih cekap dalam hari ke hari di hampir setiap bahagian masyarakat moden, tetapi juga memperkenalkan pelbagai jenis kerentanan baru yang mampu dieksploitasi oleh penggodam-penggodam.

Oleh itu, pengesanan kerentanan dalam sesebuah sistem mesti dilakukan dari masa ke masa untuk mengesan kelemahan-kelemahan sistem tersebut dan kemudiannya haruslah diperbaiki supaya dapat mengelakkan pelanggaran data yang mampu membawa kerugian yang besar kepada organisasi-organisasi yang penting dalam masyarakat. Dalam zaman teknologi yang ketara ini, sistem-sistem yang mempunyai data dan rangkaian yang penting haruslah sentiasa berada dalam keadaan selamat. Dengan ini, projek tahun akhir ini dibangunkan untuk mencipta sebuah sistem pengimbas kerentanan berasaskan web yang kuat dengan antara muka yang jelas dan mudah difahami oleh pengguna-pengguna sistem ini.

2 PENYATAAN MASALAH

Setiap sistem ataupun aplikasi yang dibangunkan bermula dari beberapa masalah yang tidak boleh diselesaikan. Oleh itu, terdapat beberapa masalah yang terdapat sebelum pembangunan sistem web pengimbas kerentanan ini. Antaranya, menurut sebuah artikel dalam laman web IBM, kebanyakan sistem pengimbas kerentanan akan menemui kelemahan atau kerentanan keselamatan yang palsu dalam sesuatu sistem web. Oleh itu, sistem web tersebut tidak mempunyai jaminan yang kukuh bahawa sistem tersebut tidak mudah dieksploitasi. Ini adalah salah satu masalah yang besar dalam semua jenis sistem pengimbasan kerentanan kerana sesebuah sistem tidak akan mengesan sesetengah kelemahan/kerentanan merupakan risiko yang tinggi dan dapat dieksploitasi oleh penggodam.

Selain itu, sebuah sistem pengimbas kerentanan harus mempunyai pengemaskinian sistem yang berterusan supaya kerentanan-kerentanan yang baharu dan berpotensi untuk menjadi peluang eksploitasi penggodam-penggodam dapat dikesan oleh sistem web pengimbas kerentanan ini. Oleh itu, pembangun haruslah peka terhadap kelemahan- kelemahan baharu yang telah muncul dalam dunia teknologi.

Di samping itu, antara muka sistem pengimbas kerentanan yang kurang menarik juga merupakan salah satu masalah. Kebanyakan pengimbas kerentanan yang sedia ada lebih kepada anatara muka yang sangat teknikal serta hanya boleh difahami oleh sesetengah orang yang mahir dalam skop pengetahuan sekuriti siber. Sekiranya terdapat apa-apa kerentanan dalam sistem web yang diimbas, kadangkala sukar untuk pekerja-pekerja syarikat operasi perniagaan yang kurang berpengetahuan dalam ini untuk menilai dan memahami hasil laporan pengimbasan di sebaliknya. Sistem-sistem pengimbasan automatik seperti ini tidak akan memberitahu atau menerangkan kelemahan dan kerentanan sistem. Oleh itu, ini memerlukan seorang pentadbir sistem seperti seorang pegawai keselamatan siber yang biasanya akan lebih fokus pada aspek teknikal kerentanan.

3 OBJEKTIF KAJIAN

Projek yang dibangunkan ini adalah untuk tujuan mencipta sebuah sistem pengimbasan kerentanan web mesra pengguna yang mampu mengesan kelemahan sesebuah sistem dengan cepat, efisien, dan secara mendalam.

Objektifnya adalah seperti berikut:

- Untuk mencipta sebuah sistem pengimbas kerentanan web untuk pembangun web yang amatur dan baharu dalam bab sistem web secara percuma.
- Untuk menjadikan sistem web pengimbas mesra pengguna serta senang dan lebih difahami oleh pengguna tentang kelemahan sistem dengan teliti
- Mencipta sebuah sistem yang mampu mengekalkan keselamatan sesuatu sistem dengan sentiasa mengemas kini pangkalan data sistem pengimbas tersebut dengan data yang diperlukan untuk mengelakkan penggodam-penggodam mencari kelemahan baharu untuk mengancam keselamatan sistem tersebut.

4 METOD KAJIAN

Dalam pembangunan projek ini, metodologi merupakan perkara yang sangat penting. Selepas beberapa tinjauan dan analisis dibuat, saya telah mengambil keputusan untuk menggunakan metodologi System Development Life Cycle (SDLC) kerana metodologi ini sesuai untuk pembangunan sistem ini. SDLC dapat membantu mengurangkan kerumitan dalam perkembangkan sistem web ini dari awal pembangunan serta dalam kerangka fasa berstruktur yang dapat membantu membentuk projek dan menguruskannya dengan mudah. Secara amnya, Metodologi SDLC akan dijalankan seperti berikutnya:

a) Sistem-sistem pengimbas web sedia ada yang berkaitan serta sama dengan projek yang dibangunkan patutlah ditinjau dan dibandingkan kekuatan dan kelemahan serta perbezaan untuk mengenal pasti kelemahan dan kekurangan yang ada pada sistem-sistem pengimbas yang tersedia ada. Hal ini boleh dikaji selidik dalam internet serta pensyarah yang ada pengalaman dan ilmu tentang projek tersebut.
b) Perancangan untuk keperluan jaminan kualiti dan pengenalpastian risiko yang berkaitan dengan projek juga dilakukan pada tahap perancangan. Hasil kajian kemungkinan teknikal adalah untuk menentukan pelbagai pendekatan teknikal yang dapat diikuti untuk melaksanakan projek dengan berjaya dengan risiko minimum. Hal ini dapat menambah baik segala kekurangan dan kelemahan yang terada pada sistem-sistem pengimbas yang sedia ada.
c) Sistem pengimbas yang baharu yang telah diusul akan direka dengan betul. Rekaan sistem pengimbas ini merangkumi operasi pengimbasan, perkakasan, pengaturcaraan serta isu-isu keselamatan.

d) Pembangunan sistem pengimbas yang baharu menjadi permulaan. Setiap pengaturcaraan dan program yang diperlukan akan dilakukan. Latihan untuk menguji penggunaan sistem pengimbas harus dijalankan oleh pengguna supaya dapat mengetahui semua aspek prestasi sistem tersebut dengan baik. Penambahbaikan boleh dijalankan pada awal-awal peringkat ini jika ada masalah ataupun kekurangan dalam sistem pengimbas tersebut.

e) Sistem pengimbas akan digunakan untuk mengimbas pelbagai sistem yang sedia ada dalam pelbagai cara seperti sistem-sistem yang lain, masa, lokasi serta keadaan rangkaian.

f) Penilaian akan dilakukan atas sistem pengimbas kerentanan dengan kadar terperinci. Di samping itu, penyelenggaraan yang ketat akan dilakukan atas sistem pengimbas kerentanan pada sepanjang masa. Pengguna sistem pengimbas tersebut haruslah dimaklumkan tentang perubahan dan pembaharuan yang terkini dalam sistem pengimbas tersebut.

RAJAH 4.1: METODOLOGI SDLC

4.1 Fasa Perancangan

Fasa pertama dalam metodologi ini. Dalam fasa ini, pengenalan projek, pernyataan masalah, objektif, skop dan cara untuk membina sistem ini akan dikenal pasti. Pada peringkat ini, kumpulan maklumat yang komprehensif mengenai apa yang diperlukan oleh projek ini dilakukan. Di samping itu, carta gantt telah disusun supaya tempoh pembangunan sistem tersusun dan mengikut jadual yang telah ditetapkan.

Projek Sistem Pengimbasan Kerentanan berasaskan Web ini bertujuan untuk memberi data dan informasi kepada pengguna untuk mengesan kelemahan/kerentanan sistem web yang dibangunkan. Sistem ini dibangunkan menggunakan PHP dan MySQL serta CSS dan JavaScript tertentu. Ianya juga akan dibangunkan untuk menjana laporan pengimbasan yang telah dilakukan atas sesebuah laman sesawang. Skop kajian adalah:

- Sistem pengimbas kerentanan mampu digunakan oleh pembangun web baharu yang ingin menguji keselamatan sistem web yang telah dibangunkan.
- Tertumpu kepada syarikat-syarikat, institusi-institusi, serta organisasi perniagaan kecil-kecilan yang menggunakan sistem web dan sistem-sistem teknologi rangkaian

4.2 Fasa Analisis

Fasa analisis merupakan fasa yang seterusnya selepas fasa perancangan. Fasa ini melibatkan analisis dan tafsiran maklumat yang telah dikumpulkan dalam fasa sebelumnya iaitu fasa perancangan. Kerja-kerja analisis dilakukan dalam fasa ini untuk mengenal pasti masalah dan menentukan penyelesaian masalah. Sistem sedia ada yang telah dikaji akan dijadikan sebagai rujukan untuk menentukan ralat-ralat dan penyelesaian masalah untuk ralat-ralat tersebut. Selain itu, analisis tentang perisian yang digunakan juga dijalankan untuk memastikan perisian yang diguna dan sedia ada merupakan perisian yang sesuai untuk diguna pakai dalam pembangunan projek ini. Perbandingan sistem akan dilakukan untuk mendapatkan ciri-ciri sistem yang akan dibangunkan dalam projek ini.

4.3 Fasa Reka Bentuk

Fasa reka bentuk merupakan fasa yang amat penting dalam pembangunan sesebuah projek. Fasa ini bertujuan untuk menentukan rekaan sistem web serta visualisasi sistem web yang akan

digunakan. Dalam fasa ini juga akan menentukan kerentanan-kerentanan yang akan digunakan untuk mengimbas kerentanan dalam sesebuah laman web. Pelbagai perkara perlu dipilih iaitu penggunaan bahasa, perisian yang akan digunakan, warna latar belakang sistem web dan lakaran awal dan akhir sistem yang akan dilaksanakan. Antara muka sistem dan laman web direka bentuk supaya lebih mesra pengguna dan mudah digunakan untuk pengguna permulaan. Selain itu, dalam fasa ini penyediaan bahan seperti data dan maklumat dalam pangkalan data yang perlu serta akan dimasukkan.

4.4 Fasa Implementasi

Fasa implementasi dalam modul ini bertujuan untuk menambahbaikkan bahan-bahan modul yang sedia diukur, diuji dan dilaksanakan seperti mana ianya perlu fungsi.

4.4 Fasa Pengujian

Fasa ini bertujuan untuk menguji sistem web pengimbas yang telah dibangunkan pada fasa reka bentuk untuk kebolehgunaan sistem tersebut. Sistem juga akan diuji kecekapannya. Sekiranya sistem web yang dibangunkan gagal mencapai objektif utama projek ini, penyelarasan harus dilakukan serta pengimbasan kembali ke fasa analisis supaya dapat melakukan penambahbaikan kajian secara mendalam.

5 HASIL KAJIAN

Bahagian ini akan membincangkan hasil yang didapati daripada pembangunan sistem web pengimbasan kerentanan. Oleh itu, penerangan secara mendalam tentang reka bentuk, implementasi dan pengujian sistem web tersebut akan diperihalkan dalam bahagian ini. Dalam pembangunan sesebuah sistem web, fasa reka bentuk dan pengujian sistem tersebut merupakan fasa yang sangat penting kepada sistem web tersebut. Dalam pembangunan projek ini, Adobe Dreamweaver, Google Chrome, Notepad++,Sublime Text, dan XAMPP digunakan untuk mereka bentuk model sistem web pengimbas kerentanan serta CSS yang sesuai. Seterusnya, pengujian terhadap reka bentuk dan kefungsian sistem web yang dibangun dijalankan untuk memastikan hasil pembangunan sistem web ialah selaras dengan objektif yang telah ditetapkan sebelum ini.

5.1 Modul Reka Bentuk

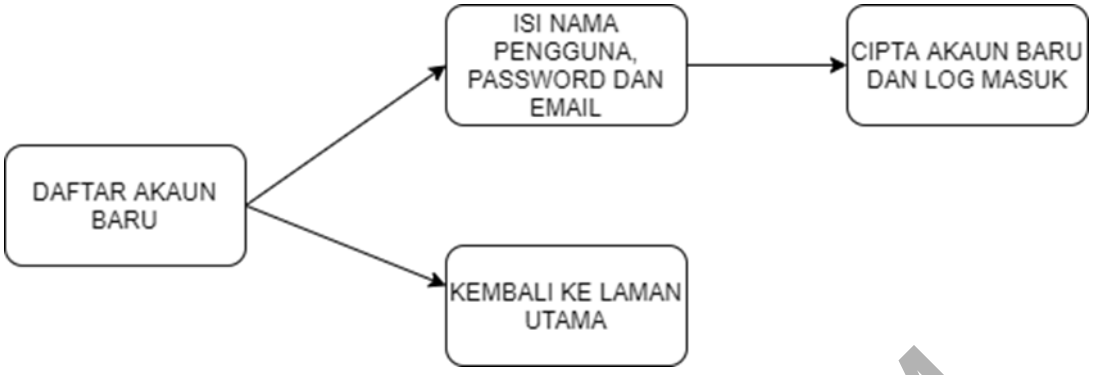
Reka bentuk seni bina adalah sebuah proses yang menerangkan tentang koleksi komponen perkakasan dan perisian serta antara muka untuk mewujudkan rangka kerja bagi pembangunan sistem komputer. Melalui reka bentuk ini, ia juga menunjukkan hubungan antara proses spesifikasi dan reka bentuk yang dijalankan secara selari dengan aktiviti spesifikasi yang lain.

Dalam sistem web yang akan dibangunkan, Seni Bina Pelanggan-Pelayan (Client-Server Architecture) digunakan untuk sistem web pengimbas kerentanan ini. Seni Bina Pelanggan-Pelayan (Client-Server Architecture) adalah model pengkomputeran di mana pelayan menjadi hos, menyampaikan dan menguruskan sebahagian besar sumber dan perkhidmatan yang akan digunakan oleh pelanggan.

Seni bina pelanggan / pelayan juga dikenal sebagai model pengkomputeran rangkaian kerana semua permintaan dan layanan disampaikan melalui rangkaian. Dalam sistem web yang bakal dibangunkan, pengguna menggunakan komputer dan kemudahan internet untuk menyambung ke pelayan/server melalui pelayar web (web browser). Setelah pengesahan, sistem web pengimbas dapat dikendalikan serta fungsi lain seperti pengumpulan maklumat rangkaian dan penjelajahan maklumat juga dapat digunakan.

i. MODUL DAFTAR AKAUN BARU

Rajah 1.2 menunjukkan modul untuk pendaftaran akaun baharu di mana pengguna yang ingin menggunakan sistem pengimbas web ini boleh mencipta akau. Dalam paparan pendaftaran akaun baharu, pengguna ada pilihan untuk mengisi nama pengguna (username), kata laluan (password) dan e-mel pengguna untuk mendaftar akaun baharu dan kemudian, log masuk ke dalam sistem tersebut. Di samping itu, jika pengguna tersilap tekan atau tidak mahu mendaftar akaun baharu, pengguna boleh meneruskan ke laman utama sistem untuk perkara lain.



Rajah 5.1 – Modul Daftar Akaun Baru

ii. MODUL LOG MASUK KE DALAM SISTEM

Rajah 1.3 melibatkan modul untuk log masuk ke dalam Sistem Pengimbas Kerentanan Web. Dalam modul ini, pengguna boleh log masuk dalam sistem untuk menggunakan sistem pengimbasan kerentanan web ini. Untuk log masuk ke dalam sistem, pengguna perlu mengisi nama pengguna (username) dan kata laluan (password) serta tekan butang "LOG IN" di bawah ruang kotak yang diisi. Dengan ini, pengguna akan dialihkan ke laman utama secara pengguna sistem web tersebut dengan akaun yang didaftar untuk menggunakan fungsi pengimbasan sistem tersebut. Jika pengguna ingin kembali ke laman utama, pengguna boleh menekan butang "Home".

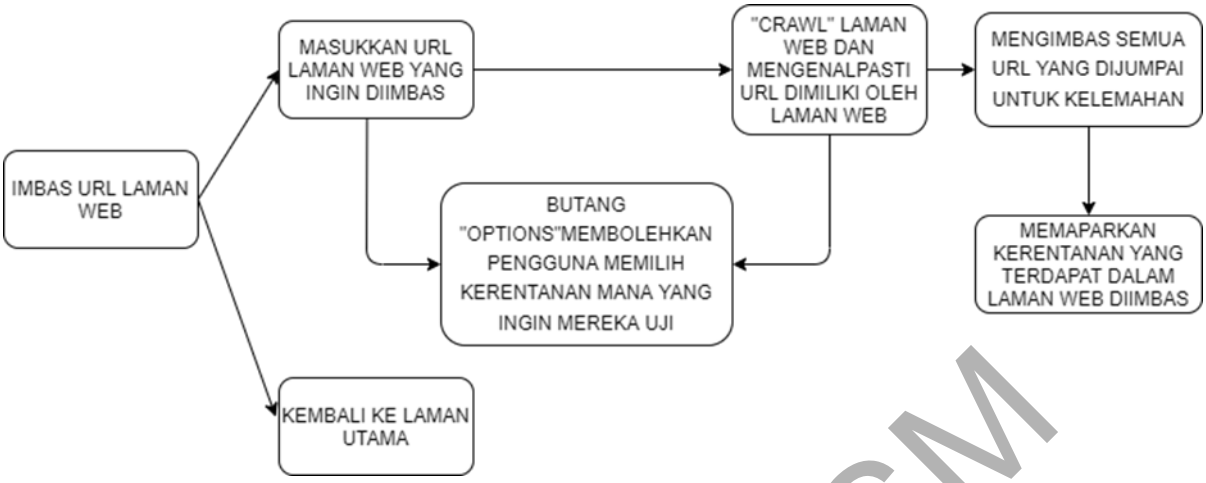
Rajah 5.2 – Modul Log Masuk ke dalam Sistem

iii. MODUL IMBAS URL LAMAN WEB

Dalam Rajah 1.4, terdapat modul untuk imbas URL laman web di halaman web sistemnya. Dengan ini, pengguna yang telah log masuk, boleh mengimbas laman web yang diingini. Pengguna perlu memasukkan URL laman web yang ingin diimbas. Sistem web pengimbasan ini juga ada perkara "OPTION" di bawah ruang kotak URL untuk membolehkan pengguna memilih kerentanan mana yang ingin diuji atas laman web yang diimbas. Antara pengimbasan kerentanan yang telah dibangunkan dalam sistem ialah:

- XSS Scripting Tercermin (Reflected)
- Suntikan SQL Standard
- Sijil SSL tidak dipercayai
- Pengalihan Tidak Sah
- Autocomplete yang Diaktifkan pada Medan Kata Laluan
- XSS Scripting yang Disimpan (Stored)
- Pendedahan Banner HTTP
- Pengesahan yang rosak menggunakan SQL Injection
- Penyenaraian Direktori Diaktifkan (Directory Listing)
- Rujukan Objek Langsung Berpotensi Tidak Selamat (Insecure Direct Object References)

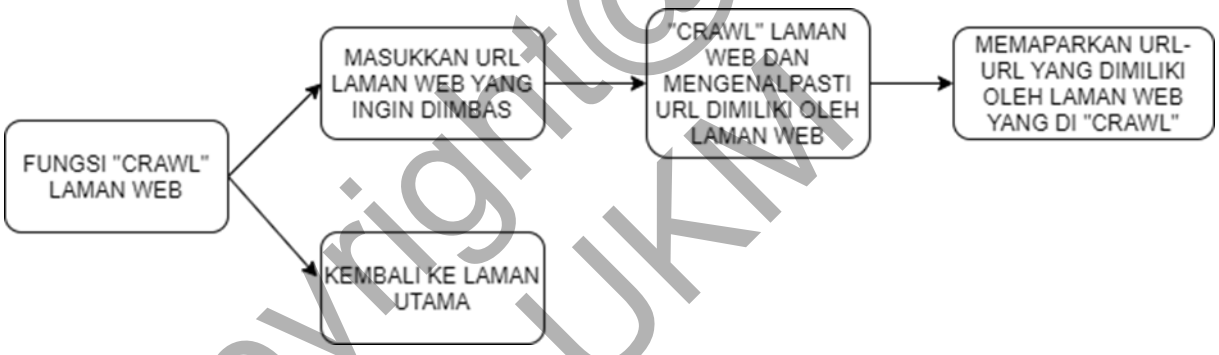
Selepas memilih, sistem akan mengenal pasti semua URL yang dimiliki laman web tersebut. Kemudian, sistem akan mengimbas semua URL yang telah dikenal pasti untuk mana-mana kelemahan yang ada. Selepas selesai, sistem akan memaparkan laporan kerentanan laman web yang telah diimbas.



Rajah 5.3 – Modul Imbas URL Laman Web

iv. MODUL FUNGSI "CRAWL" LAMAN WEB

Rajah 1.5 menunjukkan modul fungsi "crawl" laman web. Fungsi "crawl" adalah untuk mengimbas URL-URL yang dimiliki oleh sesebuah laman web.

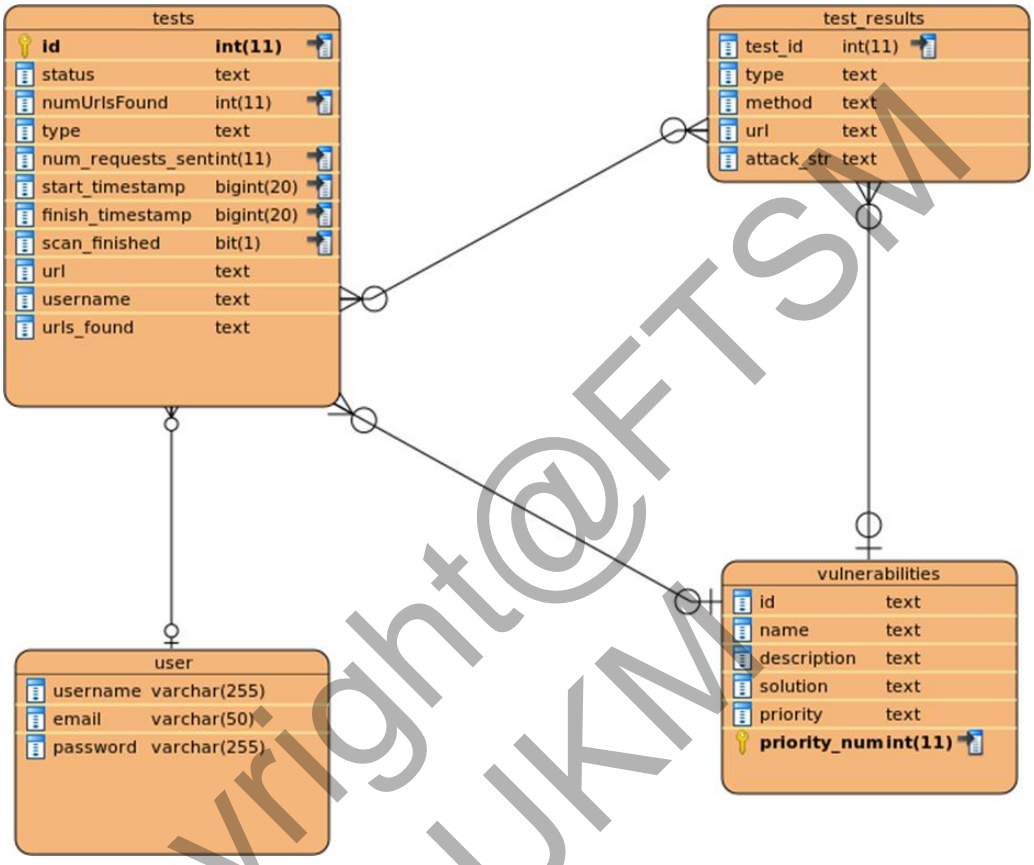


Rajah 5.4 – Modul Fungsi "Crawl" Laman Web

v. Modul Reka Bentuk Pangkalan Data

Reka bentuk pangkalan data adalah bahagian yang paling penting dalam fasa reka bentuk sistem. Dalam persekitaran pangkalan data, data yang umum haruslah tersedia supaya dapat digunakan oleh pelbagai pengguna dalam sesebuah sistem. Daripada mengehadkan data untuk pengguna-pengguna tersendiri, pengguna biasa tidak dapat mengakses data-data privasi pengguna yang lain serta tidak boleh menggodam sistem pangkalan data. Reka bentuk pangkalan data merupakan suatu proses dalam menghasilkan modul data secara terperinci. Di samping itu, reka bentuk pangkalan data ini juga memainkan peranan yang penting dalam menentukan aliran data. Rajah 1.6 iaitu rajah hubungan entiti (ERD - Entity

Relationship Diagram) telah dicipta dan digunakan dalam projek ini untuk menerangkan reka bentuk pangkalan data yang ada dalam Sistem Pengimbasan Kerentanan Web yang dibangunkan ini.



Rajah 5.5 – Rajah Hubungan Entiti bagi Sistem Pengimbasan Kerentanan Web

Meja “vulnerabilities” dalam pangkalan data ini memainkan peranan yang sangat penting kerana ia merupakan sumber utama sistem web ini untuk mendapatkan maklumat tentang kerentanan yang sedia ada untuk mengimbas serta mengenal pasti kerentanan yang ada pada laman web yang diimbas. Meja “users” menyimpan data pengguna-pengguna yang telah daftar dalam sistem, iaitu nama pengguna, kata laluan serta emel. Meja “tests” dalam pangkalan data pula menyimpan data tentang pengimbasan seperti masa pengimbasan telah mula dan tamat serta maklumat-maklumat lain tentang pengimbasan. Meja “test_results” juga memainkan peranan yang sama.

5.2 Implementasi Sistem Web

Seterusnya, proses implementasi akan dijalankan setelah proses reka bentuk berjaya dihasilkan untuk membangunkan sistem web pengimbas kerentanan ini. Dalam pembangunan web sistem pemeriksaan kerentanan ini, bahasa pengaturcaraan yang digunakan ialah PHP, HTML/CSS dan JavaScript. Pangkalan data yang digunakan adalah MySQL dan klien pelayar XAMPP. Perisian yang digunakan untuk membangunkan rangka sistem web ini adalah Sublime Text serta Adobe Dreamweaver.

Selain itu juga, bab ini bertujuan untuk menguji sistem web ini seperti mana yang telah dirancang pada fasa sebelum ini. Perancangan yang dilaksanakan dapat membantu dalam memenuhi matlamat dan objektif yang ditetapkan pada peringkat awal.

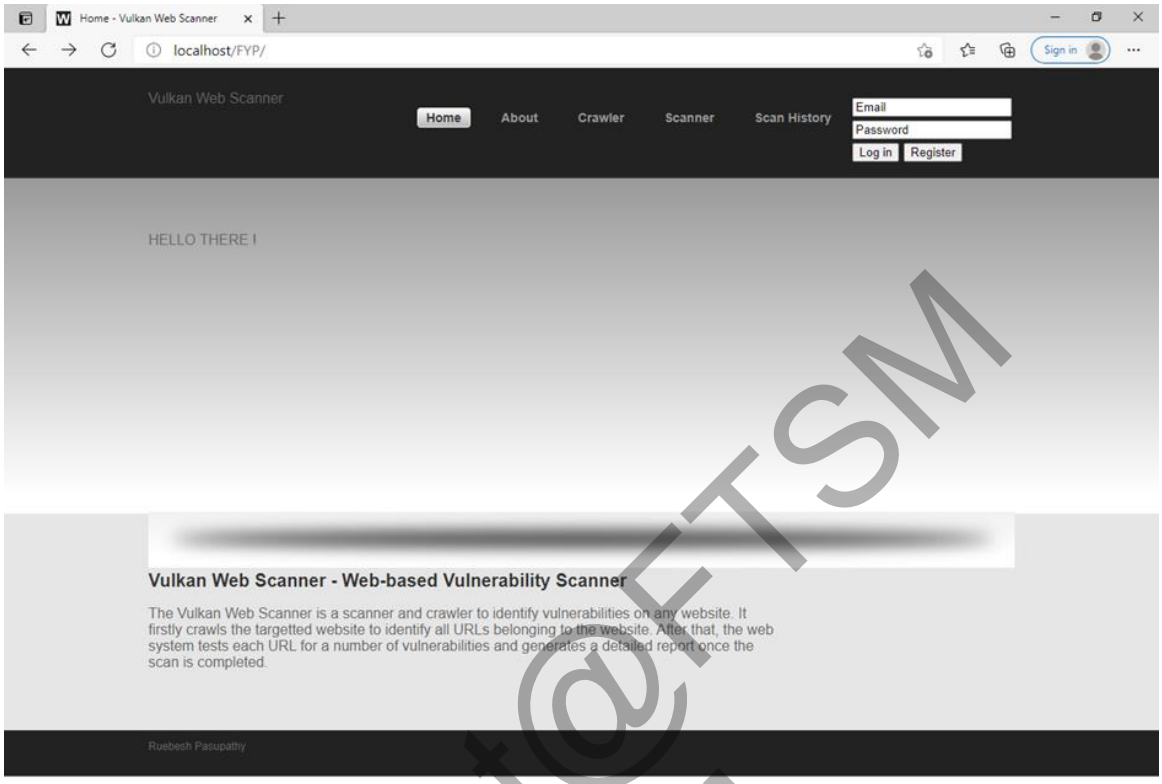
i. Proses Pembangunan

Sistem Pemeriksaan Kerentanan Berasaskan Web ini mempunyai 2 bahagian yang utama iaitu SCAN, dan CRAWL untuk mengenal pasti kerentanan yang ada pada sesebuah laman web. Proses pembangunan asas adalah merangkumi pembangunan proses pendaftaran profil pengguna, fungsi SCAN/CRAWL dan laman utama. Proses-proses ini dibangunkan terlebih dahulu sebelum proses utama dijalankan.

ii. Pembinaan Antara Muka Sistem

Antara muka sistem merupakan medium interaksi antara pengguna dan sistem web serta kefungsiannya. Oleh itu, antara muka yang mesra pengguna amat penting supaya dapat memastikan pengguna boleh menggunakan sistem web pengimbasan kerentanan ini dengan mudah dan berkesan.

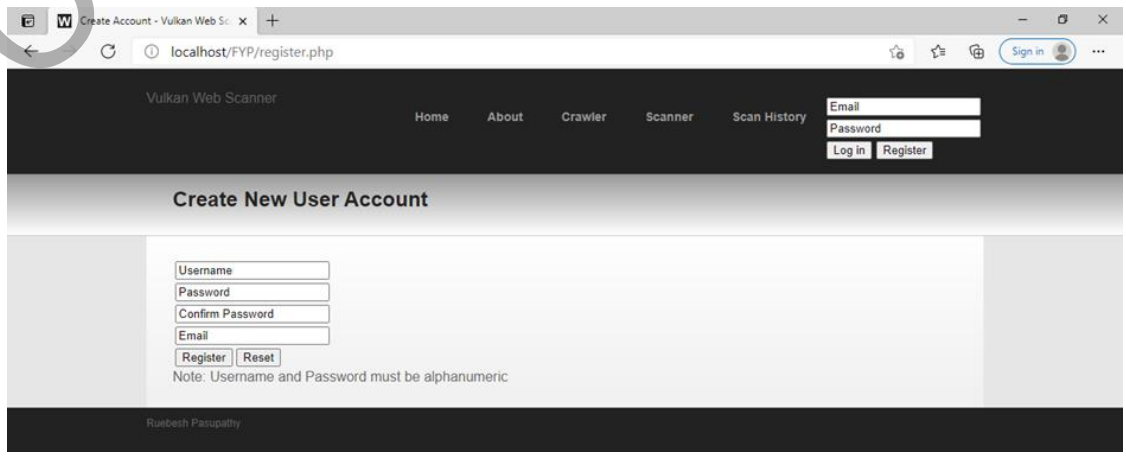
a) Antara Muka Laman Utama



Rajah 5.6 Laman Utama Sistem Pemeriksaan Kerentanan berasaskan Web

Sistem Pemeriksaan Kerentanan Berasaskan Web bermula dengan laman web utama. Laman web ini dibangunkan dengan menggunakan PHP, HTML dan CSS yang kemas supaya pengguna dapat memahami fungsi serta memberikan penampilan sistem web ini dengan senang.

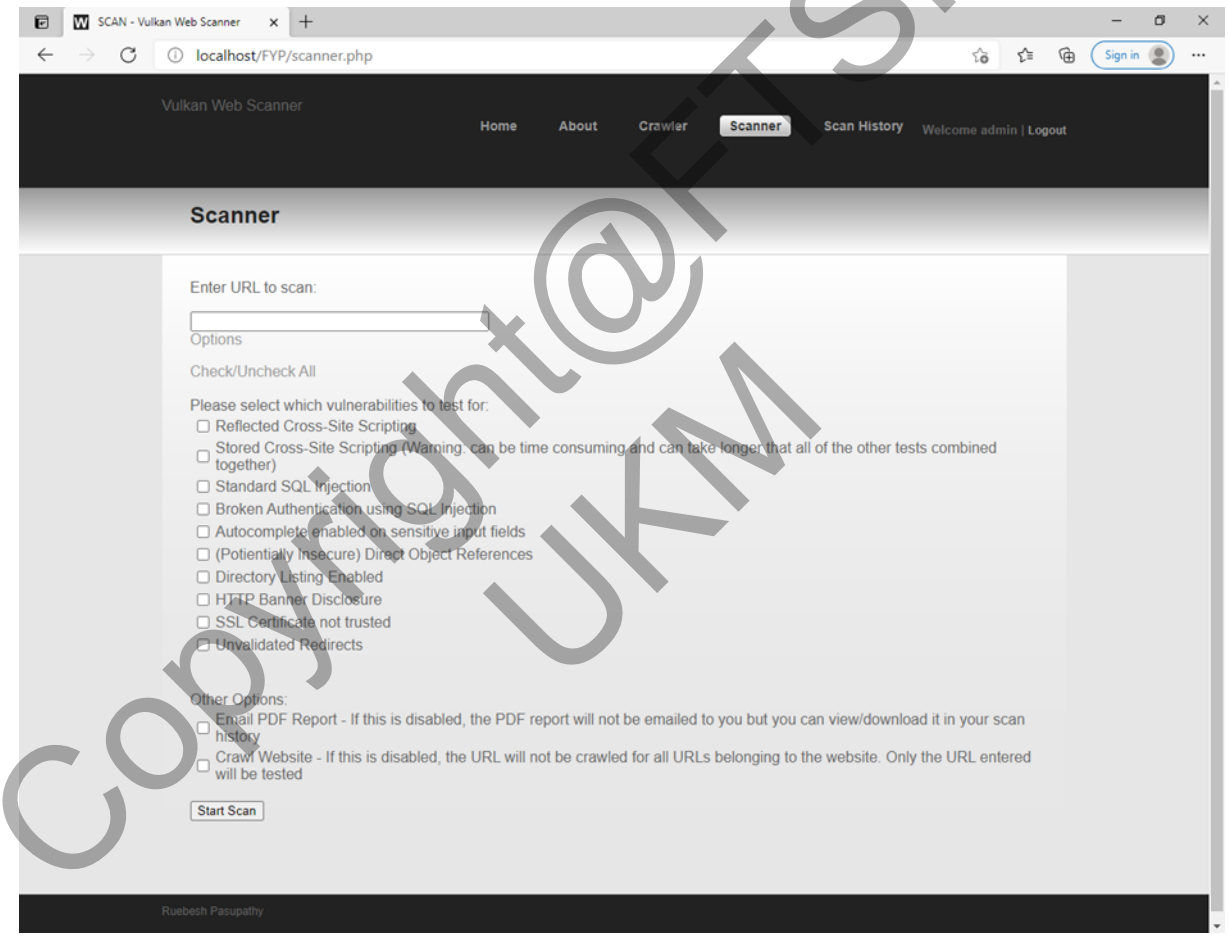
b) Antara Muka Pendaftaran Profil Pengguna



Rajah 5.6 Laman Pendaftaran Profil Pengguna Baharu

Proses pendaftaran profil pengguna bermula dengan reka bentuk yang agak ringkas dan senang untuk difahami oleh semua jenis pengguna. Pengguna yang ingin mendaftar profil baharu perlu mengisi maklumat seperti nama pengguna (username), kata laluan (password), pengesahan password (confirm password) serta emel (email). Kata laluan perlulah ada ciri "alphanumeric" yang bermaksudnya kata laluan yang diisi perlu ada abjad dan angka dalamnya. Contohnya seperti "abc123".

c) Antara Muka Fungsi SCAN

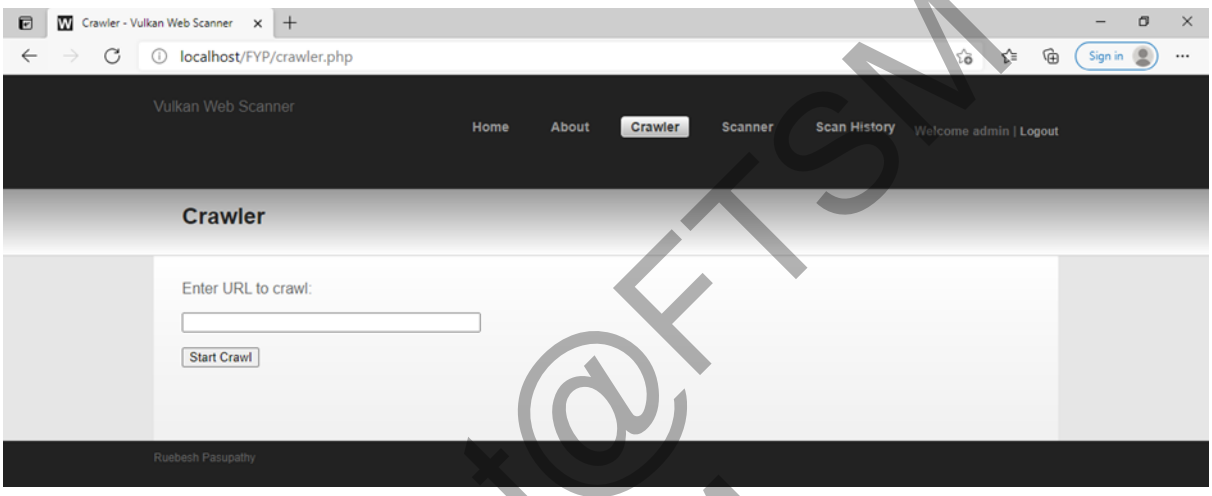


Rajah 5.7 Laman SCAN Sistem Pengimbasan Kerentanan Web

Fungsi SCAN digunakan untuk mengimbas URL-URL untuk mengesan kerentanan yang ada pada sistem web yang menggunakan domain tersendiri. Fungsi SCAN dilakukan dengan menggunakan dua kod yang merangkumi fungsi untuk mengimbas data XML sesebuah sistem web. Seterusnya, ianya akan mendapati data dan mengimbas dengan menggunakan sesuatu fungsi yang dipanggil "Simple HTML DOT Parser".

Kemudiannya, fungsi “PHPCrawl” digunakan untuk mengesan laman web yang dimasukkan secara mendalam. Selepas itu, fungsi-fungsi yang lain akan digunakan untuk mengesan kerentanan yang ada pada data yang didapati dalam laman web yang telah dimasukkan untuk pengujian.

d) Antara Muka CRAWL



Rajah 5.8 Laman CRAWL Sistem Pengimbasan Kerentanan Web

Fungsi CRAWL pula tidak begitu canggih seperti fungsi SCAN. Fungsi CRAWL hanya digunakan untuk mengesan URL-URL yang dimiliki oleh sesebuah laman web. Hal ini dilakukan dengan menggunakan fungsian “PHPCrawl” untuk mengesan suatu laman web secara keseluruhannya serta mendapatkan data dan senarai URL-URL yang dimiliki oleh laman web tersebut. Setelah mengimbas dan mendapatkan URL-URL tersebut, sistem web akan memaparkan semua URL-URL tersebut.

5.3 Pengujian Sistem Web

Selepas proses implementasi telah berjaya selesai, proses pengujian untuk sistem web pengimbas kerentanan ini akan dijalankan. Pengujian sistem web ini dijalankan untuk memastikan sistem web yang dibangunkan ini menemui keperluan dan mampu berfungsi seperti mana yang dijangkakan tanpa sebarang masalah yang kritikal. Selain itu, proses ini harus dilakukan untuk mengurangkan ralat dalam sistem web ini supaya sistem web tersebut dapat memenuhi keperluan teknikal dengan cekap.

i. Pengujian Fungsian

Kes pengujian menjelaskan dengan lebih terperinci terhadap apa yang perlu diuji dan cara pengujian untuk sesebuah kes dijalankan. Spesifikasi kes pengujian ini juga digunakan untuk menentukan bahawa adanya ralat serta untuk menguji kefungsian sistem yang betul.

Jadual berikut menunjukkan KP1, iaitu pengimbasan CRAWL laman web

ID Kes Pengujian	KP1		
ID Keperluan	F001		
No.	Input	Jangkaan Keputusan	Keperluan Prosedur Khas
1	Enter URL: "http://www.ftsm.ukm.my/" Tekan "Start CRAWL"	Laman web mengimbas laman web tersebut dan memaparkan keputusan CRAWL iaitu laman-laman URL yang lain yang dimiliki oleh URL yang diinput setelah selesai mengimbas.	Tiada
2	Enter URL:	"Please enter a valid URL	Tiada

Jadual 5.1 Kes Ujian Pengimbasan CRAWL

Jadual berikutnya menunjukkan KP2, iaitu fungsi pengimbasan SCAN laman web

ID Kes Pengujian	KP2		
ID Keperluan	F002		
No.	Input	Jangkaan Keputusan	Keperluan Prosedur Khas

1	Enter URL: “http://www.ftsm.ukm.my/” Tekan “Start SCAN”	Laman web mengimbas laman web tersebut dan memaparkan keputusan SCAN yang menunjukkan kerentanan yang ada pada laman web URL yang telah diinput setelah selesai mengimbas.	Tiada
2	Enter URL:	“Please enter a valid URL	Tiada

Jadual 5.2 Kes Ujian Pengimbasan SCAN

Jadual berikut menunjukkan KP3, iaitu fungsi pemaparan keputusan ujian imbasan SCAN/CRAWL masa lalu.

ID Kes Pengujian	KP3		
ID Keperluan	F003		
No.	Input	Jangkaan Keputusan	Keperluan Prosedur Khas
1	Tekan butang “VIEW” pada mana-mana keputusan yang ada di SCAN HISTORY	Laman web akan memaparkan keputusan masa lalu yang telah dipilih.	Tiada

Jadual 5.3 Kes Ujian Pemaparan Keputusan Imbasan

Jadual 5.4 menunjukkan keputusan log pengujian Sistem Pengimbasan Kerentanan berasaskan Web. Pengujian ini dilakukan oleh mahasiswa UKM secara manual di tempat masing-masing melalui komputer riba atau telefon bimbit. Mengikut jadual ini, ia boleh dikatakan bahawa pengujian yang dilakukan terhadap fungsi-fungsi dalam Sistem Pengimbasan Kerentanan berasaskan Web ini semuanya lulus.

ID KEPERLUAN	ID KES PENGUJIAN	ID PROSEDUR UJIAN	JENIS UJIAN	ALATAN	LULUS/GAGAL	ID INSIDEN PENGUJIAN	CATATAN
F001	KP01	TPS-01-01	FUNGSIAN	MANUAL	LULUS	-	-
F002	KP02	TPS-02-01	FUNGSIAN	MANUAL	LULUS	-	-
F003	KP03	TPS-03-01	FUNGSIAN	MANUAL	LULUS	-	-

Jadual 5.4 Keputusan Log Pengujian

6 KESIMPULAN

Setelah menjalani beberapa fasa pembangunan bagi projek Sistem Pengimbas Kerentanan berasaskan Web ini, maka, dalam bab ini akan menjelaskan secara ringkas dan menyeluruh mengenai projek ini. Bab ini juga merupakan bab yang terakhir dalam dokumentasi laporan pembangunan projek Sistem Pengimbas Kerentanan berasaskan Web. Sehubungan dengan itu, kekangan yang dihadapi dan cadangan penambahbaikan sistem pada masa hadapan akan diterangkan. Hal ini disebabkan cadangan penambahbaikan sangat dititikberatkan untuk membaiki kelemahan dan meningkatkan kemampuan sistem web ini yang dibangunkan pada masa akan datang.

Terdapat beberapa kekangan dan masalah yang telah dikenal pasti semasa Sistem Pengimbas Kerentanan berasaskan Web dibangunkan. Kekangan pertama berlaku ketika ingin mengumpul data untuk membangunkan data yang akan digunakan untuk mengimbas pelbagai jenis kerentanan dalam sesebuah laman sesawang. Hal ini disebabkan sistem web pengimbas kerentanan tidak akan dapat mengesan kerentanan sesebuah sistem web atau laman sesawang dengan cekap dan efisien. Seterusnya, sistem ini hanya ditawarkan berasaskan web.

Sistem Pengimbas Kerentanan berasaskan Web merupakan versi ringkas dan mesra pengguna. Justeru itu, penambahbaikan perlulah dilakukan dari masa ke semasa supaya dapat sentiasa mengesan kerentanan dalam laman sesawang yang berisiko tinggi. Cadangan yang dapat dibuat bagi menyelesaikan masalah mengenai sistem ini ialah melalui mengemaskini informasi pangkalan data dari masa ke semasa agar kerentanan yang moden dan baharu dapat dikesan oleh Sistem Pengimbas ini. Seterusnya, pembangunan aplikasi untuk telefon pintar yang menggunakan sistem operasi Android dan iOS. Oleh hal yang demikian, lebih ramai

pengguna memperolehi manfaat daripada Sistem Pengimbas Kerentanan berasaskan Web ini. Mereka tidak perlu menggunakan komputer riba atau komputer meja untuk mengimbas dan mengesan kerentanan sesebuah sistem web malah boleh berbuat demikian di mana-mana tempat dengan syarat ada akses ke internet.

7 RUJUKAN

Castillo, Carlos (2004). Effective Web Crawling (PhD thesis). University of Chile.

http://chato.cl/research/crawling_thesis

Cho, Junghoo, "Crawling the Web: Discovery and Maintenance of a Large-Scale Web Data", PhD dissertation, Department of Computer Science, Stanford University, November 2001

http://oak.cs.ucla.edu/~cho/papers/cho-thesis.pdf

Nuno Antunes (August 2017) Designing vulnerability testing tools for web services: approach, components, and tools

https://eden.dei.uc.pt/~mvieira/2016_IJIS_Tools.pdf

Sommerville, Software Engineering, 10 ed., Chapter 6

https://cs.ccsu.edu/~stan/classes/CS410/Notes16/06- ArchitecturalDesign.html

McGraw, G. (2006). Software Security: Building Security In, Adison Wesley Professional

http://docshare01.docshare.tips/files/19233/192333876.pdf

False Positives Management (IBM)

https://www.ibm.com/support/knowledgecenter/SS42VS_7.4/com.ibm.qradar.doc/c_qvm_false_positive_vulns.html