PENGIMBASAN APLIKASI WEB UNTUK MENGESAN KERENTANAN SEMASA MELAYARI LAMAN SESAWANG

Nur Aisyah Athirah Binti Munil Rizal

Dr. Khairul Akram Zainol Ariffin

Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Pengimbas aplikasi laman web, juga dirujuk sebagai pengimbas kelemahan aplikasi web atau pengimbas keselamatan aplikasi web, untuk melihat kelemahan dalam aplikasi web. Perisian imbasan dipanggil pengimbas aplikasi web atau pengimbas kerentanan (*vulnerability*). Selepas menganalisis semua laman web dan fail yang boleh dijumpai, pengimbas membina struktur perisian keseluruhan laman web. Alat ini yang diberi nama, pyScan pada dasarnya akan berfungsi dengan mengesan kerentanan suntikan *SQL* di kod perkhidmatan web. Serangan Suntikan SQL (SQLIA) berlaku apabila penyerang mengubah kesan yang diinginkan oleh pertanyaan SQL dengan memasukkan kata kunci atau pengendali SQL baru ke dalam pertanyaan. Kelemahan suntikan berlaku apabila data yang tidak dipercayai dihantar kepada jurubahasa sebagai sebahagian daripada perintah atau pertanyaan. Data penyerang boleh menipu jurubahasa untuk melaksanakan perintah yang tidak dijangka atau mengakses data tanpa kebenaran yang sepatutnya. Objektif kajian ini adalah untuk membangunkan sistem yang boleh mengesan suntikan SQL dan memaparkan maklumat kepada pengguna, membangunkan sistem yang berpotensi untuk menganalisis laman sesawang dengan selamat dan menguji kecekapan sistem yang dibangunkan. Secara teorinya, alat ini akan instrumen perkhidmatan web untuk melihat jika laman web yang ingin dilayari itu selamat atau tidak. Pertama sekali, pengguna perlu memasukkan alamat lamat web yang ingin dikesan pada pyScan ini. Seterusnya, pyScan akan mengesan dan memaparkan nama domain, alamat ip, nmap, fail robots.txt, dan whois. Selepas itu, pengguna akan memilih untuk mengesan blindSqli dan sqli untuk mengetahui keputusan penuh pengesanan. Akhir sekali, alat ini akan menunjukkan keputusan jika terdapat sebarang kerentanan atau masalah pada laman web tersebut. Kajian ini dilakukan untuk membina sebuah aplikasi yang menyediakan perkhidmatan untuk membantu pengguna melihat jika laman web yang ingin mereka layari selamat atau tidak. Kesimpulannya,

aplikasi ini diharapkan dapat membantu penggguna dalam menangani stress untuk menjamin kehidupan yang lebih sejahtera dan damai.

1 PENGENALAN

Laman web atau dari segi nama lainnya *World Wide Web* (WWW), merupakan sebahagian daripada *Internet* yang terdiri daripada laman-laman yang boleh diakses oleh pelayar (*browser*) web. Ramai orang menganggap bahawa laman web adalah sama seperti *Internet*, dan menggunakan istilah ini secara bergantian. Walau bagaimanapun, istilah *Internet* sebenarnya merujuk kepada rangkaian pelayan (*server*) global yang menjadikan perkongsian maklumat yang berlaku di laman web berjaya.

Aplikasi web telah menjadi salah satu saluran komunikasi yang paling penting antara pelbagai pembekal perkhidmatan dan pelanggan. Seiring dengan semakin pentingnya aplikasi Web, kesan negatif keselamatan iaitu kelemahan yang boleh didapati dalam aplikasi tersebut telah berkembang juga. Sebab utama untuk fenomena ini adalah kekangan masa dan kewangan, kemahiran pengaturcaraan terhad, atau kurangnya kesedaran keselamatan di sebahagian pemaju (Nenad Jovanovic, Christopher Kruegel, and Engin Kirda, 2006).

2 PENYATAAN MASALAH

Akses ke internet lebih mudah pada masa kini dengan pada peranti yang dipegang tangan seperti telefon pintar, tablet dan lain-lain membuat kandungan web yang tersedia boleh diakses di mana-mana. Dengan pergantungan penggunna pada aplikasi web, jumlah maklumat yang sensitif dan peribadi dapat disimpan dalam pangkalan data belakang juga telah meningkat.

Suntikan adalah teknik yang digunakan oleh penyerang untuk mengeksploitasi kelemahan dalam aplikasi. Jenis serangan ini dianggap sebagai masalah utama dalam keselamatan web. Ia disenaraikan sebagai risiko keselamatan aplikasi nombor satu di OWASP (Open Web Application Security Project) Top 10 – 2017. Serangan suntikan, khususnya suntikan SQL (serangan SQLi) bukan sahaja sangat berbahaya tetapi juga meluas, terutama dalam laman web. Kelemahan suntikan berlaku apabila data yang tidak dipercayai dihantar

sebagai sebahagian daripada perintah atau pertanyaan. Data penyerang boleh menipu untuk melaksanakan perintah yang tidak dijangka atau mengakses data tanpa kebenaran yang sepatutnya.

Banyak kelemahan keselamatan aplikasi web akibat dari masalah pengesahan input generik. Antara contoh kelemahan tersebut adalah suntikan SQL dan Cross-Site Scripting (XSS). Walaupun sebahagian besar kelemahan web boleh dihalang menggunakan teknologi seperti antivirus, kebanyakan pengguna dan pemaju web mengambil mudah akan keselamatan laman web. Akibatnya, terdapat sebahagian besar bilangan aplikasi dan laman sesawang yang terdedah kepada bahaya (Stefan Kals, Engin Kirda, Christopher Kruegel, and Nenad Jovanovic, 2016).

Seiring dengan peredaran masa, pengimbas aplikasi web yang dihasilkan semakin canggih. Sepuluh tahun lalu, Query String pada akhir URL adalah seperti https://cubaan.com/xxx/yyy/?cubaan=bar. Namun begitu, pada masa kini ia telah bertukar kepada https://cubaan.com/something.ext/cubaan/bar. Hal ini telah memberikan masalah yang sangat sukar kepada pemaju pengimbas untuk mengetahui komponen dinamik permintaan HTTP. Alat yang dibangunkan ini akan menyelesaikan masalah yang dihadapi pengguna.

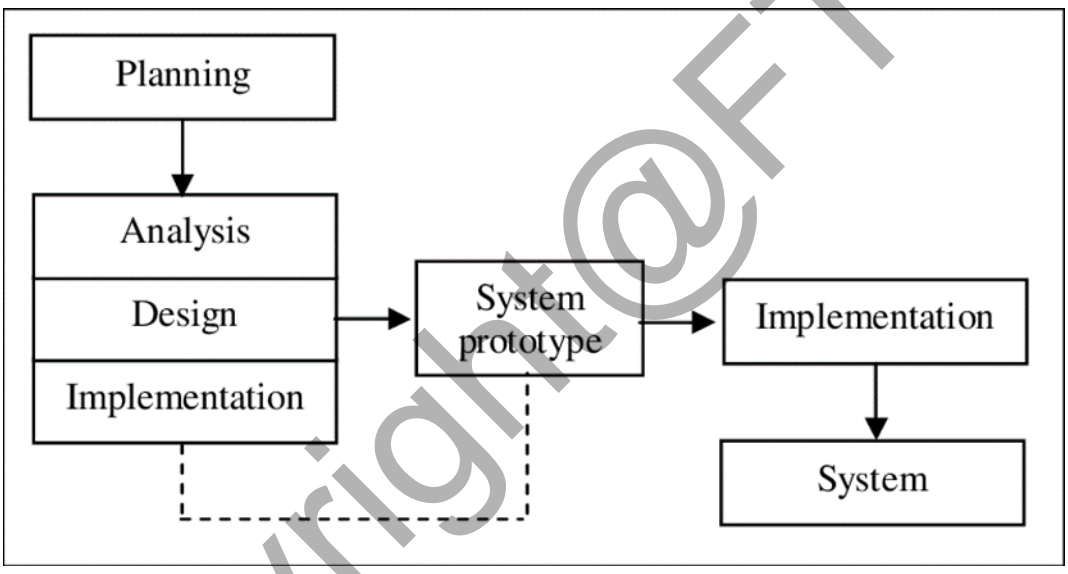
3 OBJEKTIF KAJIAN

Projek ini bertujuan untuk membangunkan satu alat yang mengesan kerentanan semasa melayari laman sesawang iaitu serangan suntikan SQL. Secara umum objektif kajian adalah menghasilkan sebuah sistem yang boleh memaparkan butiran maklumat laman sesawang kepada pengguna dan mengesan suntikan SQL.

Kertas ini membincangkan tentang projek pengimbasan aplikasi web untuk mengesan kerentanan semasa melayari laman sesawang. Pengimbasan yang dilakukan ke atas laman sesawang adalah untuk mendapatkan butiran laman web dan mengesan suntikan SQL. Pembangunan sistem PyScan yang berpotensi untuk menganalisis laman sesawang dengan selamat dibincangkan di dalam projek ini.

4 METOD KAJIAN

Penggunaan model pembangunan yang sesuai penting untuk memastikan perjalan projek berjalan dengan lancer dan menjamin hasil kerja yang berkualiti. Terdapat beberapa fasa iaitu fasa perancangan, fasa analisis, fasa implementasi, fasa prototaip sistem, fasa implementasi (selepas fasa prototaip sistem) dan fasa sistem. Metodologi yang digunakan telah diambil dari Dennis dan Wixom (2003) yang dikenali sebagai Metodologi Prototaip. Methodologi ini melaksanakan fasa analisis, reka bentuk, dan pelaksanaan secara serentak. Methodologi ini penting untuk memastikan perjalanan projek lancar dan teratur. Tiga fasa dilakukan berulang kali dalam kitaran untuk menyelesaikan projek ini seperti yang ditunjukkan dalam Rajah 1.0.



Rajah 1.0 Metodologi Prototaip

4.1 Fasa Perancangan

Fasa Perancangan adalah fasa dimana pengumpulan makluat berkaitan dengan projek ini dijalankan. Fasa ini melibatkan proses pengenalpastian masalah, objektif, persoalan kajian dan penentuan skop. Fasa ini penting untuk mengeluarkan idea dan merancang pembentukan alat ini. Maklumat dikumpul dapat dilihat dalam fasa analisis.

4.2 Fasa Analisis

Fasa yang kedua ialah fasa analisis. Fasa analisis ialah pengkajian kesusasteraan yang sedia berkait dengan kajian ini. Hal ini dapat dilihat dengan membaca kerja-kerja terdahulu sebagai rujukan dan membincangkan kajian yang bakal dilakukan terhadap pengguna untuk membangunkan perisian yang mengikut kehendak pengguna. Pembacaan, pengumpulan dan pencarian jurnal dan artikel kajian lepas bagi mencetus idea dan dijadikan garis panduan. Pengunaan internet untuk mencapai maklumat dilakukan dan laman web yang diakses mengunakan akeses dari Perpustakaan Tun Seri Lanang Universiti Kebangsaan Malaysia dilakukan. Selain daripada itu, analisis tentang perisisan juga dilakukan untuk memastikan perkakasan dan perisian yang sedia ada adalah sesuai untuk membangun projek ini.

4.3 Fasa Reka Bentuk

Dalam fasa ini, proses perancangan dan penyelesaian masalah untuk bahagian perisian akan dijalankan. Fasa ini melibatkan pembinaan reka bentuk bahagian perisian aplikasi ini. Sebagai conth, reka bentuk algorithma, reka bentuk seni bina perisian, reka konsep pangkalan data, dan definisi struktur data.

Fasa ini merupakan fasa yang penting. Dalam fasa ini, penggunaan perisian telah disenaraikan ketika fasa analisis. Dalam aplikasi pengimbasan laman web ini dari aspek perisisan, pembangunan menggunakan perisian Sublime Text, PyCharm, Xampp dan w3af.

4.4 Fasa Implementasi

Fasa Implementasi ini adalah di mana kod sebenar ditulis dan disusun menjadi aplikasi yang beroperasi dan fail pangkalan data dicipta. Struktur kod dibangunkan menggunakan perisian PyCharm dan Sublime Text. Pembinaan struktur kod untuk proses memaparkan maklumat mengenai laman sesawang dan pengesanan suntikan SQL dilakukan di PyCharm dan mengunakan bahasa Python. Manakala, struktur kod untuk pembangunan laman web PyScan pula dibina di Sublime Text menggunakan bahasa HTML dan PHP.

Terdapat 5 komponen yang diperlukan dalam memaparkan butiran laman sesawang iaitu nama domain, alamat ip, nmap, fail robots.txt, dan whois. Maklumat ini dapat diperoleh dengan

membina struktur kod di Python dan Kali Linux. Bagi mengibas serangan suntikan SQL pula, PyScan telah mengunakan w3af. W3af adalah sebuah rangka kerja yang diwujudkan untuk membantu pengguna meningkatkan keselamatan aplikasi web dengan mencari dan mengeksploitasi semua kelemahan aplikasi web.

Oleh itu, sebahagian daripada *plugins* telah digunakan. *Plugin* sangat penting untuk w3af, mereka memperluas kerangka dengan pelbagai cara seperti mencari kerentanan baru, mengenal pasti URL baru dan menulisnya ke pelbagai jenis fail. *Plugin* diselaraskan oleh strategi teras dan menggunakan ciri inti. Terdapat satu *plugins* yang digunakan didalam PyScan iaitu, *Audit*. Jenis *Audit* yang digunakan didalam alat ini adalah, *blind_sql* dan *sqli*.

4.5 Fasa Prototaip Sistem

Dalam fasa ini, proses untuk memeriksa adakah alat ini telah memenuhi keperluan dan spesifikasi asal serta mencapai tujuan yang ditetapkan. Para pengguna juga akan diberi ujian seperti *paper testing* untuk melihat jika terdapat sebarang kekurangan yang boleh diubah sebelum aplikasi ini dibagunkan sepenuhnya. Sekiranya menghadapi masalah, penyelarasan perlu dijalanakan atau imbas kembali fasa analisis bagi membuat penambahbaikan ke atas kajian ini.

Keperluan perkakasan dan perisian perlu dipilih dengan cermat dan mampu berfungsi dengan baik apabila hasil projek diuji. Hal ini supaya projek tidak mengalami masalah di pertengahan jalan.

4.6 Fasa Implementasi (Selepas Fasa Prototaip Sistem)

Fasa implementasi ini adalah fasa di mana proses menyelenggaraan selepas pembetulan alat ini dibangunkan untuk membaiki ralat dan meningkatkan prestasi dan kualiti sebelum digunakan oleh pengguna.

Spesifikasi keperluan perisian yang diguna untuk membangun projek ialah Perisian Sublime Text, PyCharm, Xampp dan w3af. Aplikasi ini tidak mengunakan pangkalan data

untuk menyimpan data. Dengan bantuan Xampp dan Sublime Text, hal ini dapat memudahkan pembangunan laman sesawang yang dibina. Dalam proses pengujian, perisian PyCharm dari kebolehupayaan mengesan serangan suntikan sql dan pengujian terhadap paparan antara muka juga dilakukan untuk memastikan data dan fungsi projek dibangunkan dengan betul.

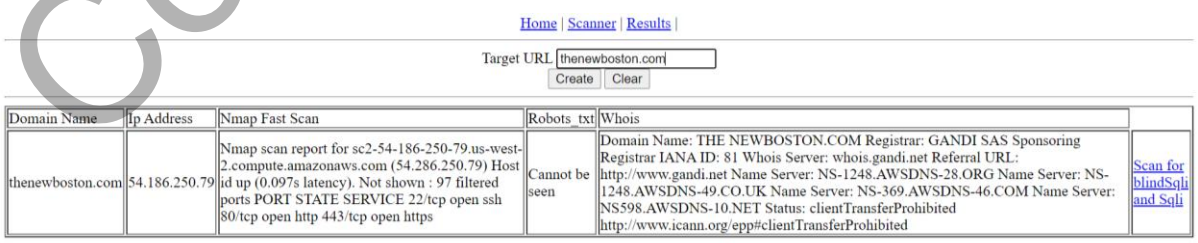
4.7 Fasa Sistem

Fasa terakhir atau ialah fasa sistem adalah dimana hasil daripada kajian ini iaitu pyScan telah dibangunkan sepenuhnya dan menepati objektif kajian dan semua komponen yang terlibat boleh berfungsi dengan baik.

5 HASIL KAJIAN

Bahagian ini membincang hasil daripada proses pembangunan pengimbasan aplikasi web untuk mengesan kerentanan semasa melayari laman sesawang. Penerangan yang mendalam tentang pengesanan suntikan SQL dan antara muka PyScan diperihal. Dalam projek ini terdapat beberapa komponen penting yang dikaji.

Antara salah satu fungsi utama PyScan adalah memaparkan butiran laman sesawang iaitu nama domain, alamat ip, nmap, fail robots.txt, dan whois. Dengan membina struktur kod di Python, maklumat yang ingin diperoleh boleh dicapai dengan mudah.



Rajah 1.1 Antara muka PyScan (1)

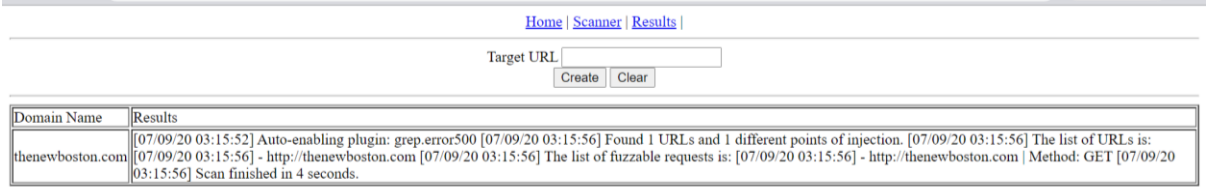
Nama domain ialah nama kepada laman sesawang tersebut. Ia juga merupakan alamat dimana pengguna Internet boleh mengakses laman web tersebut. Nama domain digunakan untuk mencari dan mengenali computer di internet. Nama domain dapat berupa kombinasi huruf dan angka, dan dapat digunakan dalam kombinasi berbagai ekstensi nama domain, seperti .com, .net dan banyak lagi. Disini hanya struktur nama domain dan domain *Top-level* sahaja yang di ambil.

Alamat Protokol Internet (alamat IP) adalah label berangka yang diberikan kepada setiap peranti yang disambungkan ke rangkaian komputer yang menggunakan Protokol Internet untuk komunikasi. Alamat IP melayani dua fungsi utama: pengenalan antara muka host dan rangkaian dan alamat lokasi. Hanya alamat IP yang paling atas akan dipaparkan.

Nmap (Network Mapper) adalah pengimbas rangkaian sumber terbuka dan bebas. Nmap digunakan untuk mencari hos dan perkhidmatan di rangkaian komputer dengan menghantar paket dan menganalisis tindak balas. Untuk alat PyScan ini, kaedah yang diguna untuk mengesan adalah *fast scan* supaya tidak mengambil masa yang lama dan hanya melihat di *port* yang penting sahaja.

Fail robots.txt ialah dimana pembina laman sesawang akan menyimpan atau menyenaraikan fail yang tidak boleh diakses atas kerana keselamatan dan sekuriti. Apabila melakukan pengimbasan terhadap isu sekuriti pada laman web, perkara pertama yang akan diimbas adalah fail robots.txt. Oleh itu, PyScan tidak dapat melihat kandungan fail robots.txt tapi dapat melihat senarai fail robots.txt sahaja.

Whois ialah alat digunakan untuk mengetahui siapa yang mendaftar nama domain. Ia juga merupakan protokol pertanyaan dan tindak balas yang banyak digunakan untuk membuat pertanyaan pangkalan data yang menyimpan pengguna berdaftar atau penerima sumber Internet, seperti nama domain, blok alamat IP atau sistem autonomi, dan lebih banyak maklumat lain lagi.



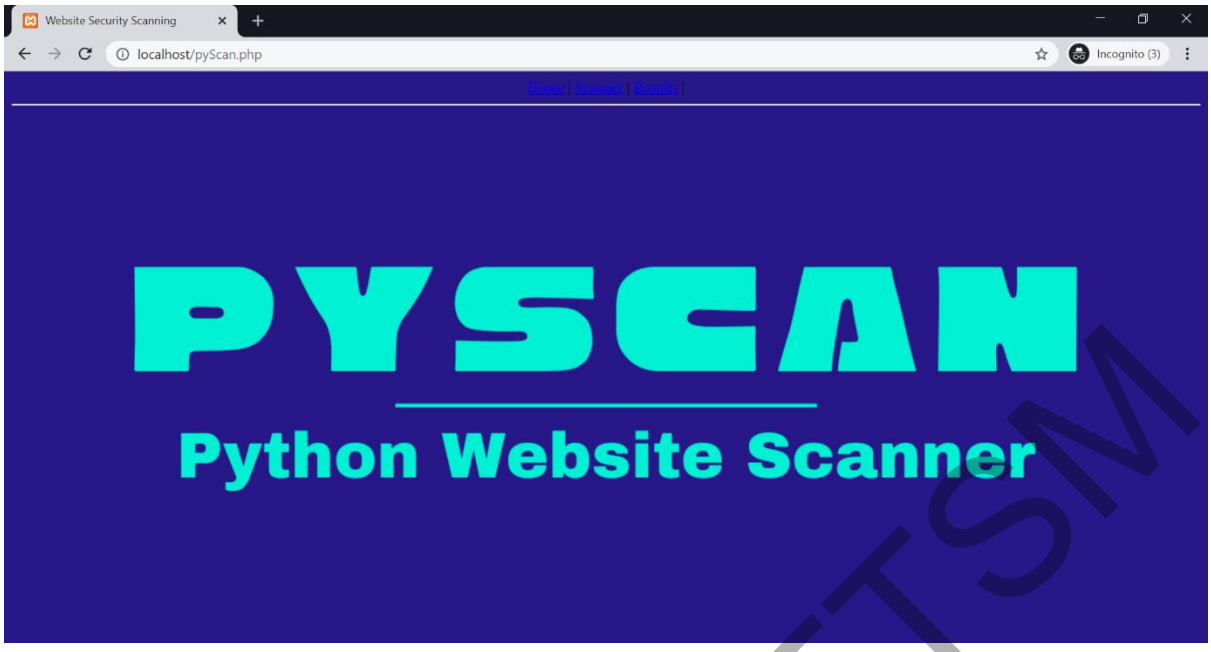
Rajah 1.2 Antara muka PyScan (2)

Seterunya ialah bahagian mengimbas serangan suntikan SQL. Bagi mengibas serangan suntikan sql ini. PyScan telah mengunakan w3af. W3af adalah sebuah rangka kerja yang diwujudkan untuk membantu pengguna meningkatkan keselamatan aplikasi web dengan mencari dan mengeksploitasi semua kelemahan aplikasi web.

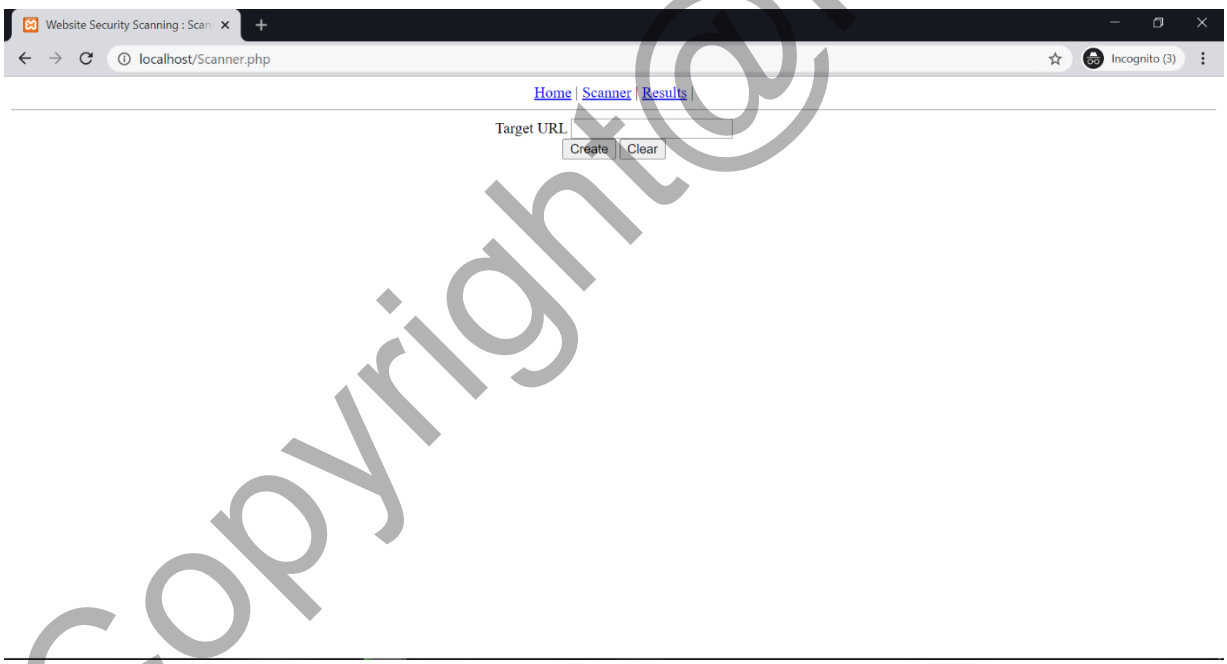
Oleh itu, sebahagian daripada *plugins* telah digunakan. *Plugin* sangat penting untuk w3af, mereka memperluas kerangka dengan pelbagai cara seperti mencari kerentanan baru, mengenal pasti URL baru dan menulisnya ke pelbagai jenis fail. Plugin diselaraskan oleh strategi teras dan menggunakan ciri inti.

Terdapat satu jenis plugins yang digunakan didalam PyScan iaitu, *Audit*. Jenis *Audit* yang digunakan didalam alat ini adalah, blind_sql dan sqli. *Plugin* ini mencari suntikan SQL mengunakan dua teknik iaitu *time delays* dan *true or false response comparison*. Hanya satu parameter yang boleh dikonfigirasi iaitu eq_limit.

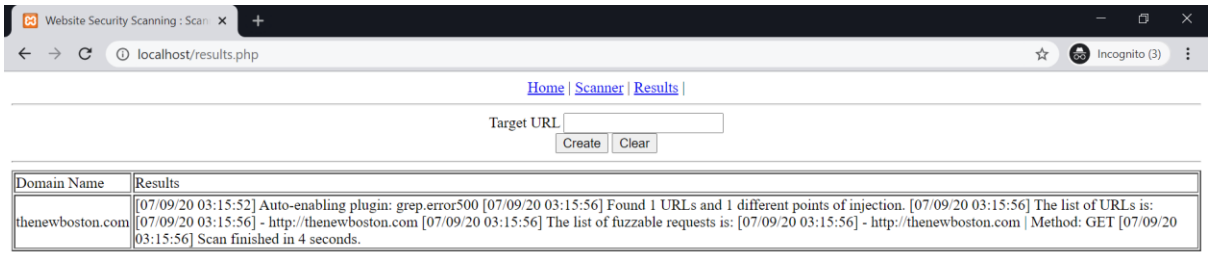
Setelah selesai pembinaan struktur kod untuk menepati objektif projek ini, pembangunan laman web PyScan pula dilakukan untuk menghasilkan paparan yang lebih jelas. Parameter, objek dan gambar yang diperlukan telah diimport. Terdapat 3 halaman yang boleh didapati pada laman web ini iaitu laman web *Home*, *Scanner* dan *Results*.



Rajah 1.3 Halaman utama PyScan (Home)



Rajah 1.4 Halaman kedua PyScan (Scanner)



Rajah 1.5 Halaman terakhir PyScan (Results)

Pengujian aplikasi perlu dijalankan selepas pembangunan aplikasi untuk memastikan aplikasi berfungsi dengan baik dan menepati spesifikasi yang ditetapkan, Pengujian pertama adalah pengujian kebolehan mengesan serangan suntikan SQL. Bagi memastikan serangan suntikan sql dapat dikesan. Sebuah eksperiment telah dijalankan melibatkan beberapa laman sesawang. Laman sesawang tersebut terdiri daripada www.thenewboston.com, www.ftsm.ukm.my dan www.reddit.com. Selain daripada itu, pengujian antara muka penting juga dilakukan bagi memastikan pengguna memahami setiap komponen di dalam antara muka.

5 KESIMPULAN

Pengimbas aplikasi laman web ini diharap dapat memenuhi kehendak pengguna yang megalami masalah berkaitan keselamatan ketika melayari Internet terutamanya daripada serangan penceroboh dan perisian hasad. Projek ini telah dibangunkan mengikut perisian dan aplikasi yang akan membantu pembinaan aplikasi ini. Penggunaan bahasa Python dalam projek ini memudahkan kerja mengekstrak data dan pembinaan struktur kod. Bahasa Python yang mudah difahami dan mudah diaplikasikan. Terutama sekali apabila terdapat pelbagai library yang telah disediakan digunakan sepanjang pembinaan projek ini.

Pemahaman mengenai kepentingan spesifikasi keperluan sistem untuk membangunkan sesebuah sistem. Selain itu, kehendak perkakasan serta perisisan juga telah dikupas dengan terperinci. Secara keseluruhannya, pada era yang semakin berkembang luas ini teknologi rangkaian semakin penting dalam hidup masyarakat masa kini untuk menghadapi perjalanan seharian. Demikian itu, diharapkan aplikasi ini dapat memenuhi kepuasan dan kehendak pengguna semasa menggunakannya.

7 RUJUKAN

Radka Nacheva. Prototyping Approach In User Interface Development. In 2nd Conference on Innovative Teaching Teaching Methods (ITM 2017). 2017.

Blake Ross, Collin Jackson, Nicholas Miyake, Dan Boneh, and John C. Mitchell. Stronger Password Authentication Using Browser Extensions. In P. McDaniel, editor, 14th USENIX Security Symposium. 2005.

Christensson, P. WHOIS Definition. Dicapai pada 5 Disember 2019.

Dudley, Tonia. "Stop That Phish". SANS.org. Dicapai pada 4 Disember 2019.

H. Liu and H. B. Kuan Tan, “Covering code behavior on input validation in functional testing,” Information and Software Technology. 2009.

Rachna Dhamija and J. D. Tygar. The battle against phishing: Dynamic security skins. In SOUPS ’05: Proceedings of the 2005 symposium on Usable privacy and security, pages 77–88, New York, NY, USA. 2005.

OWASP Foundation, 2017, http://www.owasp.org/index.php/Top_10_2017

Jose Nazario. PhoneyC: A Virtual Client Honeypot. 2009.

Jesse Russell and Ronald Cohn. W3af. 2012.

Emre Ertuk and Angel Rajan. Web Vulnerability Scanners: A Case Study. 2017.