ANALISIS KESELAMATAN LAMAN SESAWANG MELALUI PENILAIAN KELEMAHAN DAN UJIAN PENEMBUSAN

MUHAMMAD NOOR FARIS BIN MOHAMAD NOOR

WAN FARIZA BINTI PAUZI @ FAUZI

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor Darul Ehsan, Malaysia

ABSTRAK

Keselamatan laman sesawang pada masa ini semakin terancam disebabkan terdapat pelbagai gangguan dan ancaman daripada penggodam di seluruh dunia. Kerahsiaan, integriti dan ketersediaan data di dalam laman sesawang merupakan komponen yang penting dan sentiasa dipantau oleh pentadbir keselamatan. Menurut laporan daripada Oliver Moradov (2018), laman sesawang British Airways telah diserang oleh Magecart iaitu sekumpulan penggodam berprofil tinggi yang terkenal dengan serangan skim kad kredit. Kumpulan itu telah mengeksploitasi kelemahan Skrip Silang Tapak (XSS) dalam pustaka JavaScript yang dipanggil Feedify yang digunakan oleh laman sesawang Britih Airways. Serangan yang dilancarkan oleh kumpulan penggodam ini telah menunjukkan tahap keselamatan laman sesawang ini berada dalam tahap kritikal dan mudah terdedah dengan ancaman luar. Oleh itu, objektif utama projek ini adalah untuk menguji dan membuat analisis tahap keselamatan bagi sesebuah laman sesawang menggunakan dua kaedah iatu kaedah penilaian kelemahan dan kaedah ujian penembusan. Penggunaan kedua-dua kaedah ini mempunyai tujuan yang signifikan di mana penilaian kelemahan digunakan untuk mengenalpasti dan menentukan tahap kelemahan terhadap kecacatan keselamatan dalam jangka masa tertentu. Manakala ujian penembusan pula digunakan untuk melaksanakan serangan simulasi yang dibenarkan pada sesebuah laman sesawang untuk menilai tahap keselamatannya. Penilaian kelemahan dapat dijalankan dengan menggunakan alat-alat sumber terbuka kerana lebih stabil dan selamat serta mudah dilihat dan boleh mengubahsuai sumber kod pada waktu tertentu. Antaranya ialah OWASP-ZAP, Wapiti dan Nikto. Penggunaan kepelbagaian alat ini adalah bertujuan untuk melakukan perbandingan terhadap keberkesanan alat-alat dalam menguji tahap keselamatan laman sesawang. Bagi ujian penembusan pula, metodologi yang akan digunakan ialah Projek Keselematan Aplikasi Sesawang Terbuka atau Open Web Application Security Project (OWASP). OWASP merupakan salah satu daripada 10 risiko keselamatan aplikasi sesawang yang terkenal dan membantu dalam menyerang serangan daripada serangan siber. Serangan-serangan yang digunakan mestilah memfokuskan kepada beberapa aspek seperti kata laluan, data dan servis yang disediakan oleh laman sesawang. Antara serangan yang boleh diuji ke atas laman sesawang ialah serangan Brute-force, serangan penafian perkhidmatan dan serangan pembocoran data. Oleh itu, tujuan projek ini dijalankan adalah untuk menguji dan menganalisis

tahap keselamatan laman sesawang menggunakan dua pendekatan iaitu penilaian kelemahan dan ujian penembusan.
Kata kunci: Keselamatan, Penilaian Kelemahan, Ujian Penembusan

PENGENALAN

Laman sesawang merupakan salah satu platform yang banyak diaplikasikan dan diakses sebagai sebuah medium untuk menyampaikan maklumat-maklumat yang penting, menjalankan bisnes secara atas talian dan menjadikan laman sesawang sebagai pusat sumber rujukan ilmiah untuk pelajar-pelajar dan orang awam. Laman sesawang boleh diakses melalui Internet iaitu satu rangkaian yang menghubungkan pengguna dengan pengguna lain sama ada domestik atau luar negara. Rangkaian Internet merupakan salah satu cara untuk memudahkan pengguna untuk mengakses laman sesawang dengan mudah dan efisien. Peralihan daripada cara tradisional kepada bentuk digital dalam menyampaikan maklumat dan menjalankan bisnes telah mengubah landskap dan pandangan masyarakat terhadap betapa pentingnya penggunaan laman sesawang dalam kehidupan seharian mereka. Namun begitu, peralihan ini bukan sahaja membawa impak positif kepada masyarakat tetapi telah mendedahkan masyarakat terhadap serangan-serangan siber yang dilakukan oleh penggodam-penggodam yang profesional melalui laman sesawang. Serangan ini telah mengakibatkan banyak isu berlaku seperti pembocoran data privasi, skim penipuan kad kredit, servis laman sesawang tergendala dan lain-lain lagi.

Menurut laporan yang dikeluarkan oleh Anderson (2020), sebuah laman sesawang dikendalikan oleh British Airways iaitu penerbangan kedua terbesar di United Kingdom telah mengalami pembocoran data pada tahun 2018. Kes ini telah memberi kesan kepada 380,000 transaksi tempahan antara Ogos hingga September 2018. Kes ini berjaya telah dikesan oleh penyelidik-penyelidik daripada RiskIQ yang telah melaporkan perkara ini kepada British Airways dan mereka telah menampal pembocoran ini selepas laporan ini dimaklumkan. Serangan pembocoran data telah mendapati bahawa perkara ini berkait dengan Magecart iaitu satu kumpulan penggodam yang terkenal menggunakan teknik penskiman kad kredit untuk mendapatkan maklumat sulit kad kredit daripada laman pembayaran yang tidak selamat di dalam laman sesawang yang terkenal. Proses penskiman telah dilaksanakan dengan mengeksploitasi kelemahan Skrip Silang Tapak (XSS) menggunakan pustaka JavaScript yang rosak yang dikenali sebagai Feedify. Di dalam serangan ini, fail JavaScript telah mengubahsuai rekod data pelanggan dan menghantarnya kepada pelayan penyerang iaitu “baways.com” untuk mengelak sebarang keraguan apabila pengguna-pengguna menghantar maklumat mereka. Penyerang dalam serangan ini amat licik sehingga mampu untuk membeli sijil keselamatan (SSL) untuk pelayan jahat mereka agar laman sesawang mereka dilihat selamat terhadap pengguna. Hal ini telah mengakibatkan pengguna tidak berasa ragu untuk mempercayai laman sesawang mereka untuk melakukan pembayaran sehingga kehilangan maklumat kad kredit mereka.

Oleh itu, kajian mengenai analisis keselamatan laman sesawang amatlah signifikan dan akan dilaksanakan di dalam projek ini dengan menjalankan penilaian kelemahan (Vulnerability

Assessment, VA) dan ujian penembusan (Penetration Testing, PT) atau lebih dikenali sebagai VAPT. Kaedah ini merupakan salah satu pendekatan ujian keselamatan komprehensif yang bertujuan untuk mengenalpasti dan menangani kelemahan keselamatan siber. Penilaian kelemahan diadakan bagi tujuan untuk mengenalpasti dan menentukan tahap keselamatan yang sedia ada terhadap kecacatan keselamatan dalam jangka masa tertentu. Penilaian kelemahan ini akan menggunakan alat-alat sumber terbuka kerana lebih selamat dan stabil dalam menilai tahap keselamatan laman sesawang seperti OSV-Scanner, sqlmap, Wapiti dan OWASP ZAP. Tambahan pula, ujian penembusan pula akan memastikan keputusan yang diperoleh daripada penilaian kelemahan ialah tulen dan boleh dipercayai. Ujian penembusan ini menggunakan metodologi OWASP kerana metodologi dapat meningkatkan kredibiliti bagi sesebuah organisasi di mana OWASP menyediakan panduan dan rangka kerja yang standard untuk pembangun terutamanya di dalam proses pengujian penembusan. Ujian penembusan juga akan menjalankan simulasi serangan yang dibenarkan terhadap laman sesawang tertentu menggunakan perisian Linux seperti XSS, suntikan SQL, serangan Brute-force dan lain-lain lagi.

Penggunaan kedua-dua penilaian kelemahan dan ujian penembusan dapat menyediakan analisis secara menyeluruh untuk mengukuhkan keselamatan siber sesebuah organisasi. Menurut Nicholls (2023), alat, taktik dan prosedur yang semakin berkembang digunakan oleh penjenayah siber untuk melanggar rangkaian menunjukkan penilaian kelemahan dan ujian penembusan amat penting untuk menguji keselamatan siber bagi sesebuah organisasi sepanjang masa. Kaedah-kaedah ini dapat membantu untuk melindungi organisasi tersebut dengan menyediakan kelemahan keselamatan yang mudah dikesan dan panduan untuk menanganinya. Kaedah ini juga penting bagi organisasi bagi mencapai pematuhan piawaian yang telah ditetapkan termasuk GDPR, ISO 27001 dan PCI DSS. Secara tuntasnya, keselamatan laman sesawang merupakan komponen yang amat penting demi memastikan kerahsiaan, integriti dan ketersediaan data dapat dijamin dan dilindungi daripada serangan siber. Oleh itu, penilaian kelemahan dan ujian penembusan perlu dilaksanakan untuk menganalisis tahap keselamatan laman sesawang.

METODOLOGI KAJIAN

Metodologi kajian merupakan komponen yang penting di dalam projek ini bagi memastikan pelaksanaan projek dapat berjalan dengan lancar dan efektif. Hal ini demikian kerana, setiap fasa dan spesifikasi di dalam projek ini perlulah terperinci agar sentiasa dipatuhi dan teratur bagi memastikan produk akhir daripada projek ini adalah efisien dan berkualiti tinggi untuk digunakan oleh pengguna. Bagi pelaksanaan analisis keselamatan laman sesawang ini, projek ini akan menggunakan metodologi Model Air Terjun atau *Waterfall Model* sepanjang projek ini dijalankan. Model Air Terjun bermula dengan pelan projek dan berakhir dengan penjagaan prototaip projek dan mendapatkan pandangan daripada pengguna terhadap prototaip projek ini.

Fasa Perancangan

Fasa perancangan merupakan fasa pertama dalam Model Air Terjun. Pada peringkat ini lebih memfokuskan kepada pembinaan dan perancangan projek dengan lebih teliti. Penyediaan jadual pelaksanaan dan garis masa yang lebih terperinci dapat memudahkan projek ini berjalan dengan lebih lancar dan sistematik. Di samping itu, pada fasa ini juga pengumpulan maklumat awal mengenai keperluan projek juga akan dijalankan bagi memastikan setiap data yang dikumpulkan dapat memperincikan lagi skop kajian projek ini serta dapat menyediakan proses-proses yang diperlukan untuk melaksanakan projek ini. Data-data yang dikumpulkan melibatkan beberapa aspek seperti maklumat mengenai alat keselamatan sumber terbuka, kajian-kajian lepas mengenai bagaimana untuk menjalankan analisis keselamatan laman sesawang dan panduan cara penggunaan alat keselamatan tersebut. Maklumat ini boleh diperoleh melalui sumber perpustakaan dan sumber atas talian seperti Google Scholar, GitHub dan TechTarget. Dengan pengumpulan maklumat daripada sumber-sumber yang dinyatakan, masalah yang terdapat pada kajian lepas dapat dikenalpasti dan penambahbaikan serta keperluan sistem dapat diperincikan semasa fasa kedua. Analisis dan perincian hasil pengumpulan maklumat akan dijalankan semasa fasa analisis keperluan.

Fasa Analisis Keperluan

Fasa analisis keperluan merupakan peringkat kedua di dalam proses Model Air Terjun. Fasa ini memperincikan keperluan daripada pihak pengguna dan sistem dan perlu didokumentasikan sebagai rujukan untuk pengguna dan pembangun sistem. Pengguna yang terlibat di dalam projek ini merupakan pakar profesional keselamatan siber IT kerana pembinaan dan pelaksanaan projek ini merupakan projek secara terbuka Bagi pihak pengguna, keperluan mereka lebih memfokuskan kepada sistem atau rangka kerja bagi menjalankan ujian VAPT ini dengan lebih mudah. Penulisan skrip Shell untuk menjalan ujian VAPT secara automatik mestilah mudah difahami dan fleksibel terhadap sebarang pengubahsuaian skrip mengikut kemahuan dan keperluan pengguna. Pengubahsuaian skrip ini membenarkan pengguna untuk menjalankan ujian VAPT terhadap laman sesawang dengan lebih bebas dan efisien mengikut keperluan pengguna dan polisi sesebuah organisasi. Selain itu, pengguna juga memerlukan panduan pelaksanaan ujian VAPT yang mudah difahami dan tidak kompleks agar dapat diaplikasikan terhadap analisis keselamatan laman sesawang mereka. Di samping itu, bagi keperluan sistem atau rangka kerja mestilah menggariskan beberapa aspek seperti kemudahan mengakses rangka kerja bagi ujian VAPT dalam tempoh 24 jam pada setiap hari, kelancaran dalam memproses keputusan analisis keselamatan laman sesawang tanpa sebarang gangguan dan pembinaan rangka kerja yang bebas daripada segala kecacatan dan ralat di dalam penulisan skrip Shell.

Fasa Reka Bentuk

Fasa reka bentuk projek ini merupakan fasa ketiga yang memfokuskan mereka dan memperincikan fungsi-fungsi yang diperlukan berdasarkan keperluan pengguna dan rangka kerja menjalankan proses VAPT secara automatik dan manual. Bahagian VAPT yang menjalankan proses secara automatik menggunakan penulisan skrip Shell kerana menyediakan fungsi automatik yang lebih pantas untuk melaksanakan kod dari segi kecekapan menjalankan

kod, jimat masa dan meningkatkan ketepatan dalam menghasilkan keputusan. Pada fasa ini, gambar rajah aliran data direka terlebih dahulu berdasarkan keperluan pengguna dan sistem untuk mendapatkan gambaran awal bagi proses sistem automatik VAPT. Setiap fungsi dan elemen yang diperlukan di dalam sistem automatik akan diperincikan di dalam gambar rajah aliran data. Selepas itu, mengenalpasti metod dan fungsi yang sesuai dan direka sendiri untuk digunakan di dalam penulisan skrip Shell. Bagi penulisan panduan manual cara penggunaan ujian VAPT, penulisan panduan akan direka berdasarkan maklumat-maklumat yang diperoleh daripada sumber perpustakaan dan Internet serta keperluan pengguna dan orang awam. Penulisan panduan ini tidak memerlukan sebarang perisian dan hanya perlu didokumentasikan secara rasmi sebagai rujukan untuk pengguna.

Fasa Pembinaan dan Pembangunan

Fasa pembinaan dan pembangunan sistem di dalam projek ini merupakan fasa keempat di dalam kitaran Model Air Terjun. Fasa ini lebih menumpukan kepada penulisan kod untuk membina sistem perisian untuk projek analisis keselamatan laman sesawang. Pembinaan di dalam projek ini memfokuskan kepada pembinaan sistem automasi VAPT menggunakan skrip Shell yang boleh didapati di dalam Linux. Penggunaan skrip Shell dalam pembinaan sistem adalah bersifat mudah dan efisien serta fleksibel untuk diubahsuai mengikut keperluan spesifik yang telah digariskan semasa fasa kedua. Fasa pembangunan merupakan fasa yang kritikal kerana perlu memastikan pembangunan sistem mestilah mengikut rekaan yang telah ditetapkan berserta memastikan segala fungsi-fungsi yang mengikut keperluan pengguna dan sistem telah dimasukkan agar dapat memastikan sistem yang dibangunkan ini dapat berfungsi dengan baik dan sistematik.

Fasa Pengujian

Fasa pengujian merupakan komponen yang penting di dalam Model Air Terjun kerana fasa ini dapat memastikan sistem yang telah dibangunkan ini stabil dan selamat digunakan sebelum dilancarkan kepada pengguna. Fasa pengujian bagi projek ini hanya menggunakan satu kaedah sahaja iaitu pengujian kotak hitam *(Black Box Testing)*. Pengujian kotak hitam memfokuskan kepada pengujian terhadap sifat dalam sistem dan perisiannya untuk memastikan perisian lembut sistem ini berada dalam keadaan stabil dan mempunyai tahap prestasi dan keberkesanan pada kadar yang tinggi. Proses pengujian terhadap sistem VAPT menggunakan pengujian kotak hitam memfokuskan kepada kelancaran proses simulasi penilaian kelemahan dan ujian penembusan terhadap laman sesawang yang diuji. Hal ini untuk memastikan tiada sebarang ralat manusia berlaku yang disebabkan kesilapan konfigurasi alat-alat sumber terbuka dan kadar keberkesanan penggunaan alat-alat tersebut pada tahap yang tinggi. Seterusnya, mengenal pasti proses penggunaan sistem automatik yang relevan menggunakan carta alir. Kemudian, mengenal pasti laluan proses yang bersesuaian dan menyediakan kes ujian untuk menguji laluan proses yang telah dikenalpasti. Kes ujian menggariskan beberapa aspek yang diperlukan seperti keterangan kes ujian, data yang diuji iaitu laman sesawang, jangkaan keputusan, keputusan sebenar dan status ujian. Seterusnya, menjalankan proses pengujian mengikut carta alir yang telah dilakar dan kes ujian yang telah disenaraikan untuk mengenal

pasti sebarang ralat manusia dan kesilapan konfigurasi yang mungkin berlaku semasa fasa pembangunan.

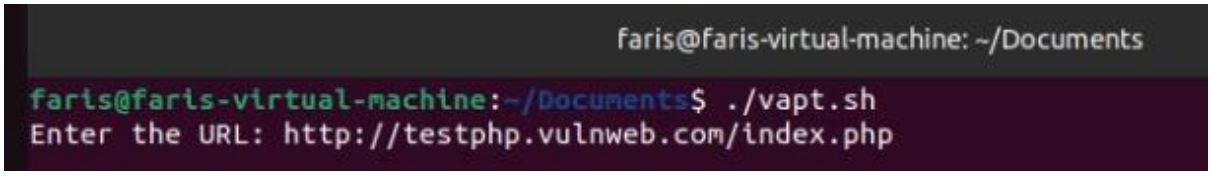
Fasa Penggunaan

Fasa penggunaan merupakan fasa kelima di dalam Model Air Terjun. Fasa ini merupakan fasa yang membenarkan pengguna dapat menggunakan sistem perisian yang telah diuji oleh pembangun dan pengguna awal. Fasa ini akan melibatkan pengumpulan maklum balas daripada pengguna untuk dijadikan sebagai rujukan untuk menambah baik sistem dan membaiki segala kecacatan kecil yang ada di dalam sistem ini. Pengguna akan menggunakan sistem automatik VAPT untuk menganalisis tahap keselamatan laman sesawang mereka dan mendapatkan keputusan yang lebih efektif untuk membuat perbandingan terhadap alat keselamatan yang sedia ada dengan alat keselamatan yang lain.

KEPUTUSAN DAN PERBINCANGAN

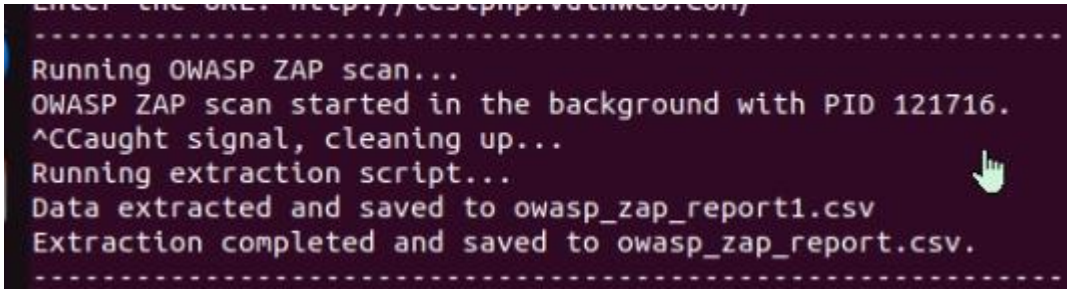
Sistem penilaian kelemahan dan ujian penembusan (VAPT) telah berjaya dibangunkan dan semua dokumentasi dan keperluan telah dilengkapkan. Semasa proses pembangunan, pembinaan skrip Shell sebagai satu metod untuk mengautomasi proses pengesanan kelemahan ke atas laman sesawang yang telah diuji bagi setiap alat penilaian kelemahan iaitu OWASP-ZAP, Wapiti dan Nikto. Selain itu, penggunaan kod Python sebagai satu kaedah untuk mengekstrak maklumat daripada laporan yang dijana oleh ketiga-tiga alat penilaian kelemahan tersebut dan digabungkan menjadi laporan tunggal yang terdiri daripada 10 kelemahan teratas OWASP, skor kebolehpercayaan, bilangan kelemahan yang dijumpai, nilai pemberat dan tahap risiko. Penghasilan laporan tunggal ini telah dapat memudahkan pengguna untuk menganalisis dan merujuk laporan tersebut bagi tujuan ujian penembusan.

Proses penilaian kelemahan menggunakan skrip Shell dimulakan dengan melaksanakan arahan *./vapt.sh* pada antara muka arahan dan mesej meminta pautan telah dipaparkan kepada pengguna untuk meminta pengguna untuk memasukkan pautan URL laman sesawang yang ingin diuji menggunakan format HTTP atau HTTPS sebagai input untuk melaksanakan proses pengesanan seperti yang tertera pada rajah 1.



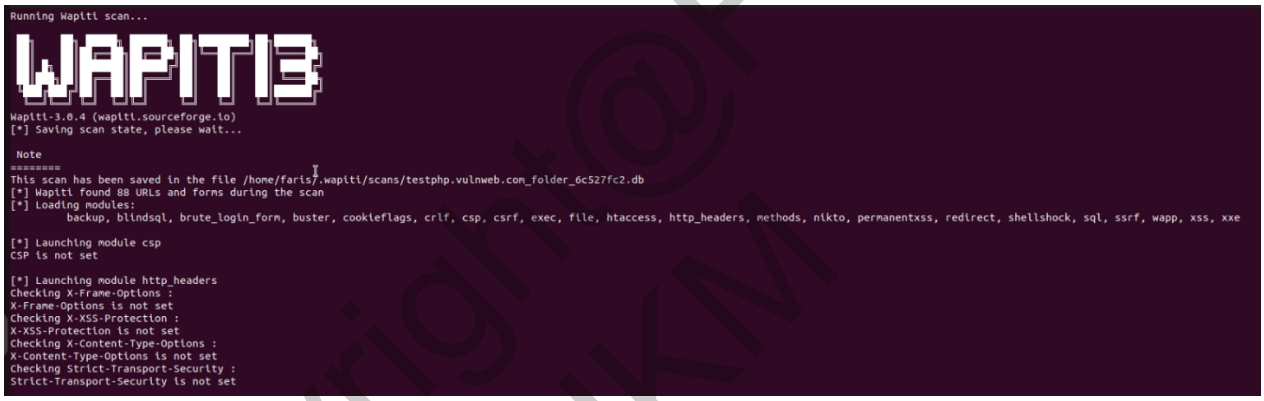
Rajah 1 Memasukkan Pautan URL Laman Sesawang

Setiap proses pengesanan telah dilaksanakan satu per satu bermula daripada proses pengesanan menggunakan OWASP-ZAP. Selepas proses pengesanan menggunakan alat ini tamat, laporan OWASP-ZAP telah dijana dan disimpan ke dalam direktori *Documents* seperti yang tertera pada rajah 2.



Rajah 2 Proses Pengesanan Menggunakan OWASP-ZAP

Selepas laporan OWASP-ZAP dijana, proses pengesanan kelemahan menggunakan alat Wapiti telah juga dilaksanakan secara automasi tanpa mengulangi proses memasukkan input pautan URL laman sesawang seperti yang tertera pada rajah 3. Proses pengesanan ini telah berlangsung dan apabila proses ini tamat, suatu mesej dipaparkan kepada pengguna untuk memasuki kekunci yang sepatutnya untuk menjana laporan Wapiti dan disimpan di dalam direktori *Documents*.



Rajah 3 Proses Pengesanan Menggunakan Wapiti

Selepas Wapiti telah tamat melakukan proses pengesanan kelemahan, alat Nikto terus melakukan proses pengesanan kelemahan ke atas laman sesawang yang sama. Selepas proses pengesanan kelemahan menggunakan Nikto tamat, suatu mesej dipaparkan kepada pengguna untuk memasukkan kekunci untuk menjana laporan Nikto dan disimpan ke dalam direktori *Documents* seperti yang tertera pada rajah 4.

Rajah 4 Proses Pengesanan Menggunakan Nikto

Kemudian, suatu mesej dipaparkan kepada pengguna untuk memasukkan kekunci sama ada *yes* atau *no* untuk menjana laporan berintegrasi. Apabila pengguna memasukkan kekunci *yes*, laporan berintegrasi terus dijana secara automasi dan memaparkan jadual data kepada pengguna pada antara muka arahan (CLI). Hasil laporan berintegrasi telah disimpan di dalam direktori *Documents* berserta graf bar sebagai visual kepada skor kebolehpercayaan yang boleh didapati di dalam laporan tersebut seperti yang tertera pada rajah 5 dan 6.

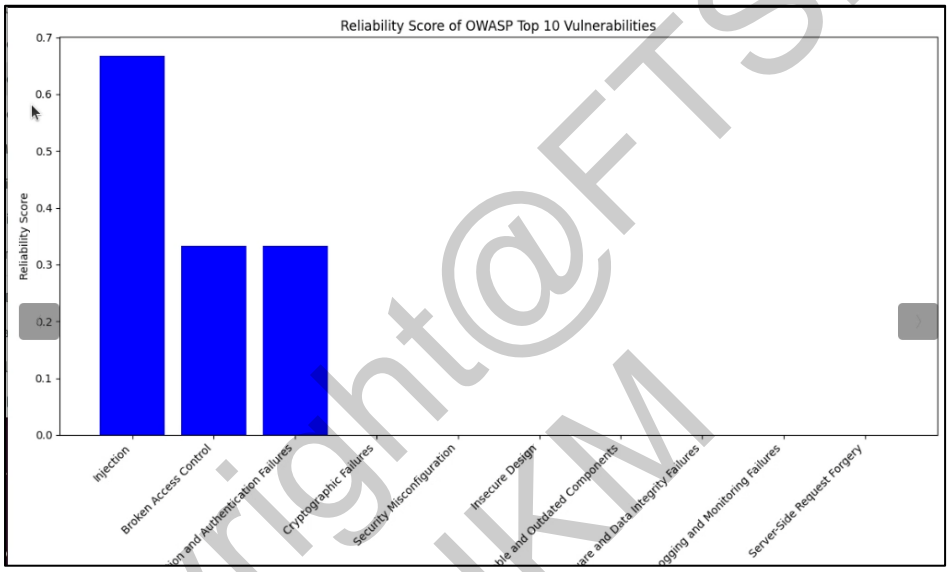
File Edit View Insert Format Styles Sheet Data Tools Window Help

Liberation Sans 10 pt

A1 Vulnerability

	A	B	C	D	E	F	G	H	I	J
1	Vulnerability	Reliability Score	Nikto Count	Wapiti Count	OWASP Count	OWASP Risk Level	Wapiti Risk Level	Weighted Score	Final Risk Level	Risk Label
2	Injection	0.667	0	2	2	0	1	0	1	Low
3	Broken Access Control	0.333	0	0	2	0	0	0	0	Informational
4	Identification and Authentication Failures	0.333	0	0	1	0	0	0	0	Informational
5	Cryptographic Failures	0	0	0	0	0	0	0	0	Informational
6	Security Misconfiguration	0	0	0	0	0	0	0	0	Informational
7	Insecure Design	0	0	0	0	0	0	0	0	Informational
8	Vulnerable and Outdated Components	0	0	0	0	0	0	0	0	Informational
9	Software and Data Integrity Failures	0	0	0	0	0	0	0	0	Informational
10	Security Logging and Monitoring Failures	0	0	0	0	0	0	0	0	Informational
11	Server-Side Request Forgery	0	0	0	0	0	0	0	0	Informational
12										
13										

Rajah 5 Laporan Berintegrasi



Rajah 6 Graf Skor Kebolehpercayaan

Pengujian Berfungsi dan Tidak Berfungsi

Pengujian berfungsi merupakan salah satu proses pengujian untuk menguji setiap komponen dan fungsi yang telah dibangunkan di dalam skrip Shell bermula daripada menerima pautan URL laman sesawang sehingga dapat menjana laporan berintegrasi. Beberapa kes ujian telah disediakan bagi menguji setiap komponen tersebut dengan memasukkan beberapa input. Tujuan pengujian berfungsi adalah untuk memastikan setiap fungsi dan komponen dapat berjalan dengan lancar dan memenuhi keperluan dan objektif projek ini. Di samping itu, pengujian tidak berfungsi bagi projek ini memfokuskan kepada ujian penembusan secara manual untuk mengesahkan kelemahan yang telah dikesan adalah benar-benar menunjukkan keberadaan kelemahan tersebut di dalam laman sesawang. Tujuan pengujian ini dijalankan untuk memastikan sistem VAPT yang dibangunkan dapat mengesan kelemahan secara efisien dan efektif.

Jadual 1 Hasil Pengujian Berfungsi

ID Kes Ujian	Hasil Pengujian	Lulus/Gagal

TC1	Dapat menghantar pautan URL laman sesawang daripada skrip Shell utama kepada setiap skrip Shell alat penilaian kelemahan menggunakan *parsing.*	Lulus
TC2	Dapat mengendalikan pautan URL laman sesawang yang tidak mengikuti format yang betul iaitu format HTTP atau HTTPS.	Lulus
TC3	Dapat menjana laporan berintegrasi dengan menggabungkan ketiga-tiga laporan yang telah dijana menggunakan kod Python iaitu *generate_vapt_report.py*	Lulus
TC4	Dapat merekod dan mempamerkan proses pengesanan yang sedang berjalan secara masa nyata dan disimpan di dalam fail log di direktori *Documents*	Lulus

Jadual 1 menunjukkan hasil pengujian berfungsi berdasarkan 4 kes ujian antaranya kes ujian ke atas penerimaan URL laman sesawang dan menghantar pautan tersebut kepada skrip Shell alat penilaian kelemahan. Seterusnya, kes ujian dalam mengendalikan sebarang ralat pautan URL laman sesawang dimana pengguna memasukkan beberapa pautan yang tidak mengikuti format HTTP dan HTTPS. Kemudian, kes ujian ketiga adalah menguji kemampuan kod Python untuk menjana laporan tunggal dengan mengekstrak ketiga-tiga laporan penilaian kelemahan dan disatukan menjadi laporan berintegrasi. Di samping itu, kes ujian keempat memfokuskan kepada kemampuan sistem untuk merekod segala proses pengesanan kelemahan ke dalam fail log dan dapat diakses oleh pengguna secara masa nyata. Hasil pengujian bagi keempat-empat kes ujian ini menunjukkan lulus sekaligus sistem VAPT yang telah dibangunkan dapat mengendalikan setiap fungsi dan komponen tanpa sebarang ralat yang besar.

Jadual 2 Hasil Pengujian Tidak Berfungsi

Kelemahan	Keputusan Penilaian Kelemahan	Keputusan Ujian Penembusan	Positif Benar / Positif Palsu

Suntikan SQL	Dapat Dikesan	Dapat Dikesan	Positif Benar
Serangan Skrip Silang Tapak (XSS)	Dapat Dikesan	Dapat Dikesan	Positif Benar
Pendedahan Maklumat Sensitif	Dapat Dikesan	Tidak Dapat Dikesan	Positif Palsu

Jadual 2 menunjukkan hasil pengujian tidak berfungsi di mana ujian penembusan secara manual telah dijalankan untuk menguji setiap kelemahan yang dikesan menggunakan teknik yang terkawal dan mengikut prosedur yang ditetapkan oleh OWASP. Terdapat tiga ujian penembusan yang telah dijalankan iaitu suntikan SQL, serangan skrip silang tapak dan pendedahan maklumat sensitif. Tujuan menjalankan ujian penembusan hanya ke atas ketiga-tiga ujian penembusan adalah disebabkan ketiga-tiga kelemahan ini adalah yang sering yang dijumpai setelah menjalankan proses pengesanan kelemahan ke atas beberapa laman sesawang yang berbeza. Ujian penembusan secara manual ini dijalankan ke atas laman sesawang yang dibenarkan iaitu Acuart kerana laman sesawang ini ialah khas untuk menjalankan penilaian kelemahan dan ujian penembusan. Hasil pengujian tidak berfungsi menunjukkan 2 daripada 3 kelemahan menunjukkan positif benar di mana kelemahan ini benar-benar dijumpai di dalam laman sesawang Acuart. Oleh itu, keputusan pengujian ini menunjukkan sistem VAPT mencapai keberkesanan yang optimum dan boleh dipercayai untuk digunakan untuk mengesan kelemahan di dalam laman sesawang.

Cadangan Penambahbaikan

Cadangan penambahbaikan kajian di masa hadapan adalah dengan meningkatkan penggunaan alat penilaian kelemahan kepada beberapa jenis seperti Nessus, nmap, Acunetix dan lain-lain lagi untuk meningkatkan keberkesanan sistem VAPT dalam mengesan kelemahan dengan lebih komprehensif. Selain itu, pembangunan sistem VAPT ini juga boleh ditambahbaik dengan membangunkan sistem yang boleh digunakan pada persekitaran lain seperti Windows dan MacOS agar sistem ini boleh digunakan secara lebih meluas untuk mengesan kelemahan laman sesawang. Di samping itu, penjanaan laporan berintegrasi perlu ditambahbaik dengan memasukkan elemen-elemen lain seperti risiko pada aset, risiko pada data, senarai kelemahan yang tertakluk selain daripada 10 teratas kelemahan OWASP dan pelbagai lagi untuk memudahkan pengguna untuk merujuk dan melaksanakan ujian penembusan secara manual. Kemudian, meningkatkan fleksibiliti sistem VAPT dimana pengguna boleh memilih mana-mana alat untuk dikonfigurasi dan digunakan untuk mengesan kelemahan dengan hanya

menggunakan skrip Shell dan platform yang telah disediakan. Akhir sekali, sistem VAPT boleh juga ditambahbaik dengan menyediakan antara muka pengguna grafik atau *Graphic User Interface (GUI)* yang terdiri daripada pelbagai alat keselamatan dan fungsi-fungsi tambahan yang tidak begitu kompleks agar dapat meningkatkan keberkesanan dan mengurangkan masa proses pengesanan kelemahan dalam mana-mana laman sesawang yang ingin diuji.

KESIMPULAN

Secara keseluruhannya, sistem VAPT ini telah berjaya dibangunkan dengan menggunakan data yang telah dikaji dan diperolehi. Objektif kajian dan keperluan yang telah ditetapkan sebelum ini telah berjaya dicapai. Walaupun terdapat beberapa halangan, ia berjaya diatasi menggunakan pelbagai cara. Diharapkan sistem VAPT ini dapat meningkatkan kesedaran kepada pengguna mengenai kepentingan keselamatan laman sesawang mereka.

Kekuatan Sistem

Kekuatan sistem penilaian kelemahan dan ujian penembusan ini adalah lebih kepada pembangunan skrip Shell yang boleh melaksanakan proses pengesanan secara automatik tanpa melibatkan konfigurasi yang kompleks. Sistem VAPT ini juga hanya melibatkan alat penilaian kelemahan yang terbuka dan percuma sahaja menunjukkan bahawa sistem ini boleh dibangunkan tanpa melibatkan kos yang tinggi dan alat penilaian keselamatan yang terlalu kompleks untuk difahami dan konfigurasi serta mempunyai cabaran untuk menggunakan skrip Shell. Sistem ini juga menggunakan persekitaran yang terbuka iaitu Linux dimana pengubahsuaian skrip Shell boleh dibangunkan menunjukkan sistem ini bersifat fleksibel dan mudah diadaptasi jika terdapat berlakunya penambahbaikan. Di samping itu, sistem ini juga mampu menjana laporan yang menggabungkan ketiga-tiga laporan yang telah diekstrak kepada satu laporan tunggal serta dapat menghasilkan visualisasi sebagai rujukan tambahan kepada pengguna.

Kelemahan Sistem

Namun begitu, terdapat juga kekangan semasa membangunkan sistem ini dimana pemilihan alat penilaian keselamatan yang percuma sukar dijumpai kerana kebanyakan alat pada masa ini mempunyai pelan tahunan yang perlu dilanggan untuk menggunakan alat tersebut. Di samping itu, pemilihan alat penilaian keselamatan juga agak sukar kerana perlu mencari alat yang bersesuaian dan boleh dikonfigurasi hanya menggunakan CLI sahaja. Kekangan ini menyukarkan pembangunan skrip Shell kerana objektif projek ini mahu membangunkan persekitaran yang mudah dan tidak kompleks serta tidak memiliki sebarang butang fungsi yang perlu difahami. Kemudian, alat penilaian kelemahan ini juga mengambil masa yang panjang untuk menjana laporan dan menyukarkan lagi semasa proses pengujian sedang dilaksanakan. Akhir sekali, sistem yang dibangunkan ini terhad kepada persekitaran Linux sahaja dan masih belum diuji pada persekitaran perisian lain seperti Windows atau MacOS.

PENGHARGAAN

Alhamdulillah dan syukur kepada ALLAH SWT dengan izin-Nya saya dapat menyiapkan kajian ini bagi memenuhi keperluan Ijazah Sarjana Muda Sains Komputer. Dengan limpah dan kurnia-Nya, saya dapat menyiapkan kajian ini dengan lancar.

Saya ingin mengucapkan setinggi-tinggi penghargaan kepada penyelia saya, Ts. Dr. Wan Fariza Fauzi, atas tunjuk ajar dan nasihat yang diberikan sepanjang proses pengajian ini dilaksanakan. Terima kasih kepada Dr. atas perkongsian ilmu dan tunjuk ajar yang berharga. Terima kasih kepada Dr. dalam menghalang saya daripada pemahaman terhad tentang dunia keselamatan siber, saya kini mempunyai pemahaman yang lebih mendalam tentang aspek luas sains keselamatan siber. Perkhidmatan Dr amat saya menghargainya, dan tanpa bimbingan beliau, saya tidak akan dapat menyiapkan kajian ini. Namun, tidak lupa juga kepada keluarga saya. Terima kasih di atas kasih sayang yang mereka curahkan sehingga saya mampu sampai ke tahap ini. Tanpa sokongan, doa dan redha mereka, saya mungkin tidak akan sampai ke tahap ini.

Selain itu, saya juga ingin mengucapkan terima kasih kepada rakan-rakan seperjuangan di atas nasihat dan tunjuk ajar yang mereka kongsikan semasa proses kajian ini. Nasihat dan sokongan yang saya terima daripada semua rakan sahabat amat membantu saya dalam menyiapkan tugasan ini. Akhir kata, saya ingin merakamkan ucapan terima kasih yang tidak terhingga kepada semua pihak yang terlibat sama ada secara langsung dan tidak langsung sepanjang proses menyiapkan kajian ini. Tanpa kehadiran anda, tidak mungkin kajian ini berjalan dengan lancar dan mencapai kejayaan.

RUJUKAN

Acunetix. t.th. Introduction to Acunetix. https://www.acunetix.com/support/docs/introduction [11 Disember 2023].

Adam, R. 2023. 10 Advantages & Disadvantages of Quantitative Research. https://helpfull.com/blog/10-advantages-disadvantages-of-quantitative-research [15 Disember 2023].

Anderson, B. 2020. 3 Dangerous Cross-Site Scripting Attacks of the Last Decade. https://readwrite.com/3-dangerous-cross-site-scripting-attacks-of-the-last-decade/ [1 November 2023].

Baker, K. 2023. Penetration Testing (Pen Testing) https://www.crowdstrike.com/cybersecurity-101/penetration-testing/ [25 Disember 2023].

cjvcntev. 2022. The Pros and Cons of Manual and Automated Penetration Testing. https://amatas.com/resources/the-pros-and-cons-of-manual-and-automated-penetration-testing/ [16 Disember 2023].

Dodds, M. 2022. The Dangers of Not Having a Security Policy. https://www.linkedin.com/pulse/dangers-having-security-policy-mark-dodds/ [15 Disember 2023].

EC-Council University. 2022. What is web application security, and why is it important?. https://www.eccu.edu/blog/technology/what-is-web-application-security-and-why-is-it-important/ [5 Disember 2023].

Fathurrachman. 2023. Pengujian Kerentanan Log4shell Pada Website E-Commerce Menggunakan Metode Vulnerability Assessment And Penetration Testing (Vapt) Life Cycle. 1-107. https://repository.uinjkt.ac.id/dspace/handle/123456789/71211 [23 November 2023].

Geeksforgeeks. 2022. What is Burp Suite. https://www.geeksforgeeks.org/what-is-burp-suite [13 Disember 2023].

Hamilton, T. 2023a. What is Reliability Testing? (Example). https://www.guru99.com/reliability-testing.html [2 Januari 2024].

Hamilton, T. 2023b. What is Vulnerability Testing? VAPT Scan Assessment Tool. https://www.guru99.com/vulnerability-assessment-testing-analysis.html [12 Disember 2023].

Homola, I. 2023. OWASP Zap: 8 Core Features (Pros & Cons). https://www.codiga.io/blog/owasp-zap/ [10 Disember 2023].

Hossein, A. 2022. Black Box vs. White Box Testing: Understanding 3 Key Differences. https://www.spiceworks.com/tech/devops/articles/black-box-vs-white-box-testing/ [9 Julai 2024].

Jordan, S. 2021. Online Presence Management Tips for Small Businesses. https://topdesignfirms.com/web-design/blog/online-presence-management [5 Disember 2023].

Klepuszewski, P. 2023. NetCat. https://www.linkedin.com/pulse/netcat-piotr-klepuszewski [13 Disember 2023].

Kumar, B.S. 2023. Understanding True Positive, True Negative, False Positive, False Negative, and Benign Results in Cybersecurity. https://www.linkedin.com/pulse/understanding-true-positive-negative-false-benign-results-kumar/ [13 Disember 2023].

Marousis, A. 2021. Cybersecurity training lags, while hackers capitalize on COVID-19. https://www.talentlms.com/blog/cybersecurity-statistics-survey/ [6 Disember 2023].

NJ. 2023. How Many Websites Are There in the World? https://siteefy.com/how-many-websites-are-there/ [8 Disember 2023].

Nicholls, M. Vulnerability Assessment and Penetration Testing. https://www.redscan.com/services/penetration-testing/vapt/ [1 November 2023].

OWASP. t.th. OWASP Top Ten. https://owasp.org/www-project-top-ten/ [6 Disember 2023].

Packetlabs. 2021. 3 Reasons to Review the OWASP Web Security Testing Guide. https://www.packetlabs.net/posts/owasp-web-security-testing-guide/ [7 Disember 2023].

Pahuja, A. 2023. What is Security Testing and Why is it important? https://www.getastra.com/blog/security-audit/what-is-security-testing/ [23 Disember 2023].

Secret Double Octopus. t.th. Meterpreter. https://doubleoctopus.com/security-wiki/threats-and-tools/meterpreter/ [13 Disember 2023].

Sharp, K. 2021. 6 Reasons Why Companies Don’t Update Their Technology. https://www.perillon.com/blog/6-reasons-why-companies-dont-update-their-technology [23 Disember 2023].

SilentSignal. 2023. Log4Shell Scanner. https://portswigger.net/bappstore/b011be53649346dd87276bca41ce8e8f [13 Disember 2023].

Simplilearn. 2023. What is Metasploit: Overview, Framework, and How is it Used. https://www.simplilearn.com/what-is-metaspoilt-article [10 Disember 2023].

Şivka, Ö. 2021. What is Netsparker? Netsparker Vulnerability Severity – Netsparker Installation. https://www.systemconf.com/2021/01/20/what-is-netsparker/ [15 Disember 2023].

Software Testing Help. 2023. What Is Efficiency Testing And How To Measure Test Efficiency. https://www.softwaretestinghelp.com/efficiency-testing/ [2 Januari 2024].

The Security Company. 2023. Why employees avoid reading policies and how you can change this? https://www.linkedin.com/pulse/why-employees-avoid-reading-policies-how-you-can-change-gunve/ [20 Disember 2023].

Varshney, S. 2022. Types Of Virtual Networks In VMware Virtualization Concepts? https://www.c-sharpcorner.com/article/types-of-virtual-networks-in-vmware-virtualization-concepts/ [21 Januari 2024].

Ventura, R, Franco, D.J, Omar Khasro Akram. 2023. A Novel Vapt Algorithm: Enhancing Web Application Security Trough Owasp Top 10 Optimization. 13-27. https://www.researchgate.net/publication/375485650_A_NOVEL_VAPT_ALGORITHM_ENHANCING_WEB_APPLICATION_SECURITY_THROUGH_OWASP_TOP_10_OPTIMIZATION [20 November 2023].

Williams, T. 2021. Why Is Quantitative Research Important?. https://www.gcu.edu/blog/doctoral-journey/why-quantitative-research-important [15 Disember 2023].

WsCubeTech Jaipur. 2023. What is the Advantage and Disadvantage of Nmap?. https://techfygeeks.wixsite.com/blog/post/what-is-the-advantage-and-disadvantage-of-nmap [16 Disember 2023].

Yolanda Hafitzhah, Umar Yunan Kurnia Septo Hediyanto, Muhammad Fathinuddin. 2023. Strategi Security Mitigation Dengan VAPT Pada Website Rekruitasi Asisten Praktikum. *Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)* 8(2): 627-639. https://ejurnal.tunasbangsa.ac.id/index.php/jurasik/article/view/646 [20 November 2023].

Muhammad Noor Faris bin Mohamad Noor (A188846)
Ts. Dr. Wan Fariza binti Pauzi @ Fauzi
Fakulti Teknologi & Sains Maklumat
Universiti Kebangsaan Malaysia