UJIAN PENGESANAN PAUTAN PELOKASI SUMBER SERAGAM PALSU

NURUL IZZAH BINTI ARMIZA

WAN FARIZA BINTI FAUZI

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

ABSTRAK

Terdapat banyak isu keselamatan data yang melibatkan masyarakat umum hari ini. Peningkatan kemahiran penggodam dalam menggunakan pengetahuan mereka untuk mengakses sistem orang lain dan mencuri maklumat telah meningkatkan kebimbangan keselamatan. Satu kaedah yang sering digunakan oleh penggodam ialah memancing data, juga dikenali sebagai "*phishing*". Kaedah ini melibatkan pemindahan lain melalui e-mel, pemesejan segera, media sosial dan platform lain untuk mendapatkan maklumat sensitif seperti maklumat pengenalan peribadi, butiran perbankan dan maklumat kad kredit.Sebagai contoh, Divya Bathi (2022), seorang pesara bank dari Mumbai, menjadi mangsa gewang data dan kehilangan sejumlah besar wang (950,000 lakh) selepas mengklik pautan yang dihantar melalui aplikasi "*Whatsapp*" selepas memfailkan aduan di laman web sesawang Union Bank di India. Oleh itu, objektif utama projek ini adalah untuk mengenal pasti perbezaan antara lokasi sumber palsu dengan tujuan untuk mencegah memancing data.Metodologi yang digunakan dalam projek ini ialah kaedah air terjun. Kaedah ini melibatkan langkah-langkah reka bentuk, analisis, pelaksanaan, pengujian, dan penyelenggaraan yang dijalankan secara berurutan. Proses ini menyediakan struktur yang kemas dan bersatu untuk melaksanakan projek dengan kemas.Projek ini mencadangkan untuk melaksanakan semakan dan penapisan pautan lokasi menggunakan pelayan proksi web seperti *ProxySite, CroxyProxy dan WinGate Proxy Server*. Ujian saringan lain akan dijalankan untuk menguji kandungan dan pautan tapak web, sambil menyekat akses kepada tapak web yang tidak diingini. Jika pengguna cuba mengakses tapak web dengan mengklik pada pautan, pautan akan dihantar ke peranti keselamatan rangkaian seperti pelayan proksi web. Alat keselamatan akan mengkategorikan pautan kepada senarai hitam atau putih berdasarkan sifat kandungan tapak web. Hasil yang dimaksudkan untuk projek ini adalah untuk meningkatkan keselamatan maklumat pengguna dengan mengurangkan potensi ancaman penipuan data. Dengan menggunakan semakan dan saringan pautan secara berkesan, ia diharap dapat mengurangkan jenayah siber dan mengekalkan privasi pengguna. Projek ini menyediakan lapisan perlindungan tambahan terhadap aktiviti pancingan data dalam talian, menjadikan persekitaran siber lebih selamat untuk orang awam.

PENGENALAN

Pancingan data atau lebih dikenali sebagai *Phishing* satu bentuk jenayah siber yang memangsakan kelemahan manusia, mengeksploitasi kepercayaan dan memanipulasi individu atau organisasi untuk mendedahkan maklumat sensitif tanpa disedari, seperti kata laluan log masuk, data peribadi atau butiran kewangan. Jenayah ini akan berlaku apabila mangsa membuka pautan yang telah direka oleh penggodam dan secara tidak langsung mangsa telah mendedahkan maklumatnya kepada penggodam. Penipuan pancingan data telah berkembang dari semasa ke semasa, menjadi lebih terperinci dan lebih sukar untuk dikesan. Sebagai contoh, penggodam kini dapat menggunakan sumber maklumat awam, seperti *Facebook*, *LinkedIn* dan *Twitter*, untuk mengumpulkan butiran peribadi mangsa, sejarah kerja, dan aktiviti yang dilakukan. Namun, mereka dapat menggunakan maklumat tersebut untuk mencipta emel pancingan data yang boleh dipercayai oleh mangsa.

Kes pancingan data dapat dikesan daripada zaman awal internet apabila komunikasi emel mula berkembang. Kejadian pancingan data yang direkodkan pertama muncul pada pertengahan 1990-an (Paul Gillin,2020) apabila penjenayah siber menyamar sebagai entiti yang dipercayai, seperti bank atau agensi kerajaan, dalam usaha untuk memperdaya pengguna supaya memberikan maklumat peribadi. Istilah "pancingan data" itu sendiri adalah permainan pada perkataan "memancing," yang melambangkan tindakan melontar mata kail untuk memancing mangsa yang tidak curiga.

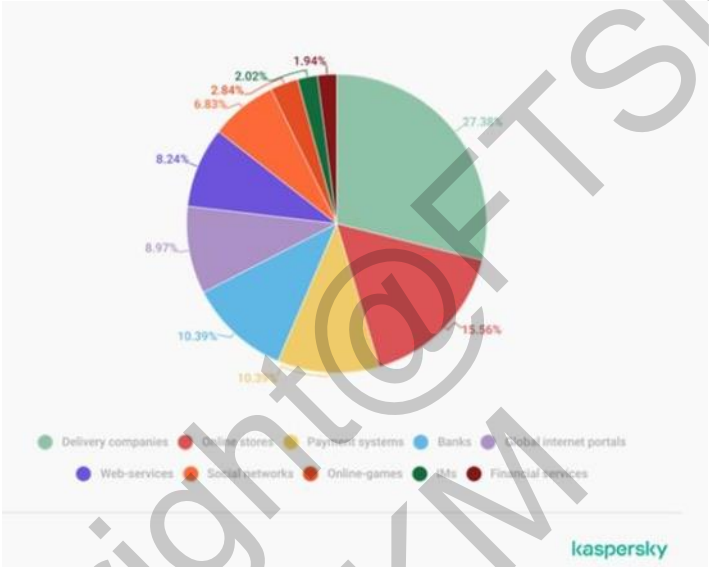
Jadual **Error! No text of specified style in document.**.1 Nombor itu mewakili pautan berniat jahat yang disekat oleh *Kaspersky*

Negara	2022
Indonesia	4931367
Malaysia	8267013
Filipina	4559288
Singapura	1556232
Thailand	6283745
Vietnam	17847857

Sumber: *Kaspersky* 2022

Menurut artikel di *Cybersecurity Asean* (2023), *Kaspersky* yang merupakan sebuah sistem keselamatan siber dan anti-virus mengatakan sebanyak 8,267,013 emel termasuk pautan palsu yang telah disekat di Malaysia pada tahun 2022. Malaysia kekal sebagai tiga teratas

dalam kalangan Asia Tenggara dari segi emel berniat jahat yang disekat oleh *Kaspersky*. Jenayah ini penting untuk diambil perhatian bahawa trend pancingan data yang meningkat diperhatikan bukan sahaja di Malaysia malah, di seluruh dunia. Di peringkat global, bilangan serangan pancingan data meningkat dengan ketara pada tahun lepas. Sistem *Anti-Phishing Kaspersky* telah menghalang 507,851,735 percubaan untuk mengikuti pautan pancingan data.



Rajah **Error! No text of specified style in document.**.1 Carta Pai Yang Menunjukkan Faktor Berlakunya Pancingan

Sumber: Kaspersky,2022

Carta pai diatas telah membutikan bahawa pada 2022, halaman yang menyamar sebagai perkhidmatan penghantaran mempunyai peratusan tertinggi klik pada pautan pancingan data iaitu (27.38%). Seterusnya, kedai dalam talian sebanyak (15.56%) yang banyak tertipu ketika pandemic. Akhir sekali, tempat ketiga yang banyak tertipu dengan pautan ialah sistem pembayaran (10.39%) dan bank (10.39%). Melalui maklumat yang diperolehi ini memberi penerangan tentang taktik penjenayah siber yang sentiasa berkembang kerana penggodam menyesuaikan diri dengan situasi semasa, aliran ekonomi dan kelemahan yang dijumpai. Oleh itu, penting bagi individu dan organisasi untuk terus berwaspada, kekal bermaklumat dan menerima pakai langkah keselamatan siber yang teguh untuk melindungi daripada serangan pancingan data dan melindungi maklumat sensitif dalam dunia yang semakin digital. Dengan adanya pengesahan pautan pelokasi sumber seragam palsu ini, pengguna dapat mengelakkan berlakunya pancingan data melalui pemeriksaan dan penapisan pautan pelokasi yang boleh memeriksa dan menyekat pautan berniat jahat yang terkandung di dalam emel.

METODOLOGI KAJIAN

Metodologi kajian ialah satu set kaedah yang digunakan untuk mendapatkan maklumat, dan bahan untuk memastikan kajian berjalan dengan lancar dan teratur. Melalui kajian ini, kaedah yang digunakan ialah kaedah Model Air Terjun. Kaedah ini merupakan pendekatan kepada pembangunan perisian yang memfokuskan pada peringkat berjujukan dan linear.

Fasa keperluan

Fasa keperluan ini dikendalikan dengan mengumpul maklumat dan menganalisis masalah melalui Pustaka dan *Google Scholar* dalam artikel dan jurnal berkaitan sumber data lain melalui aplikasi *Telegram*, *X* dan *Whatsapp*. Seterusnya, kajian-kajian tersebut telah dikumpul dan dianalisis bagi memenuhi objektif yang dihasratkan dalam objektif tersebut. Melalui bacaan ini, ia boleh membantu menyesuaikan algoritma memancing data yang sedang dibangunkan. Selain itu, analisis ini dijalankan untuk menyiasat percubaan memancing data seperti kaedah salah nyata yang melibatkan lokasi sumber seragam (URL) dan penggunaan saluran komunikasi popular sebagai medium untuk aktiviti berniat jahat. Sepanjang fasa ini, proses dokumentasi diperincikan untuk memastikan setiap analisis direkodkan dengan sewajarnya.

Fasa reka bentuk

Fasa reka bentukini memberi tumpuan yang utama kepada reka bentuk yang digunakan dalam kajian ini untuk mengenalpasti fungsi kajian. Oleh itu, sebuah prototaip yang mempunyai fungsi dan ciri yang dikemukan dibina untuk mengesan URL pancingan data yang berkesan dalam platform *Telegram*. Matlamat utama fasa ini ialah untuk membina prototaip yang bukan sahaja merangkumi elemen teknikal namun untuk menggariskan reka bentuk asas pengesan pautan pelokasi sumber seragam (URL) pancingan data yang melibatkan pengimbasan pautan pelokasi sumber seragam (URL), pengecaman corak, analisis kandungan mesej platfrom.

Fasa pelaksanaan

Fasa perlaksanaan ini memberi tumpuan terutamanya pada pembangunan dan ujian prototaip yang direka bentuk sebelum ini. Pertama sekali, langkah awal dalam pelaksanaan ini ialah pembangunan prototaip yang melibatkan penulisan kod dan penyepaduan elemen fungsi yang telah dikenal pasti dalam fasa reka bentuk. Prototaip ini bertujuan untuk melaksanakan pengimbasan URL dan keupayaan analisis kandungan mesej dalam platform *Telegram*. Tambahan pula, penyepaduan dengan API ialah langkah penting untuk mengembangkan operasi dan memastikan akses lancar kepada sumber luaran, termasuk pangkalan data pancingan data yang diperlukan untuk keberkesanan API. Proses penyepaduan ini memerlukan kepakaran teknikal untuk memastikan pertukaran maklumat yang lancar antara prototaip dan sumber luaran. Selain itu, ujian kefungsian ialah peringkat seterusnya, di mana prototaip diuji untuk memastikan setiap fungsi berfungsi sebagaimana objektif kajian. Melalui fasa pelaksanaan yang sistematik dan berstruktur, projek pembangunan projek ini boleh berjalan dengan lancar, memberikan hasil yang berkualiti tinggi dan memenuhi jangkaan

pengguna.

Fasa pengesahan

Dalam fasa ini, pengujian dilakukan menggunkan sebahagian kod telah selesai. Proses ini membolehkan pengecaman awal dan pembetulan kecacatan sistem yang berpotensi. Ujian ini merangkumi penilaian fungsi yang tidak dapat digunakan bagi memastikan pengesan mengenai pautan pautan pelokasi sumber seragam (URL) pancingan data dengan tepat dalam *Telegram* sambil memenuhi prestasi dan kebolehan di objektif. Scenario yang disimulasi untuk menguji keupayaan ialah pengesanan menggunakan *Mobile Language Model* yang memeriksa dan bandingkan pautan pelokasi sumber seragam (URL) pautan tersebut dengan tapak web yang berniat jahat. Seterusnya ujian diteruskan dengan memastikan pautan pelokasi sumber seragam (URL) penapisan berfungsi sebagai alat yang menyekat akses kepada pancingan data. Dengan ini dapat memastikan maklumat pengguna lebih selamat dan terjaga daripada ancaman penggodam. Ujian ini juga diadakan untuk memastikan sistem yang dihasilkan dapat memperoleh pencapaian yang dinyatakan di dalam objektif.

Fasa Penyelenggaraan

Fasa Pelaksanaan ini ialah peringkat kritikal dalam kitaran hayat perisian, di mana tumpuan utama adalah pada pengurusan, penyelenggaraan dan penambahbaikan berterusan API yang dibangunkan. Selepas melalui fasa pembangunan dan pengesahan, fasa pelaksanaan menjadi tanggungjawab untuk memastikan kelancaran sistem dan mengekalkan tahap prestasinya. Beberapa aspek utama dalam fasa ini melibatkan pengurusan kod sumber yang menjadi keutamaan.Selain itu, memantau dan menyelenggara sistem adalah langkah penting untuk memastikan prestasi API kekal pada tahap yang dikehendaki. Pemantauan sistematik dijalankan untuk mengesan sebarang masalah atau penurunan prestasi, manakala tindakan penyelenggaraan diambil untuk mengekalkan kebolehpercayaan sistem mengikut objektif. Dengan melalui fasa pelaksanaan ini secara sistematik, projek Pembangunan API Pengesanan Pancingan Data URL boleh dikekalkan pada tahap prestasi yang tinggi dan kekal relevan dengan keperluan semasa pengguna.

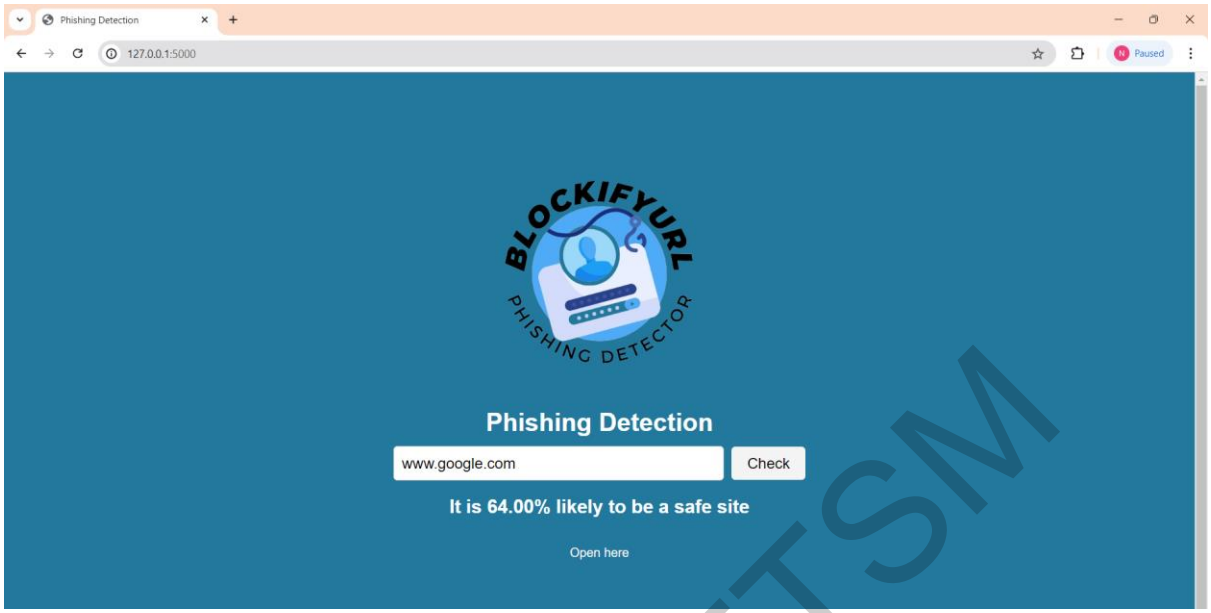
KEPUTUSAN DAN PERBINCANGAN

Pengesan Pautan Pelokasi Sumber Seragam BlockifyURL telah berjaya dibangunkan dan semua dokumentasinya telah dilengkapkan. Semasa proses pembangunan, pengesan pautan ini dibangunkan menggunakan teknologi Flask yang berfungsi sebagai bahagian belakang sistem yang dibangunkan di persekitaran Anaconda. Pembinaan model ini juga dibina dengan mengguna Machine Learning Language bagi menganalisis pautan pancingan data.

Apabila memasuki laman hadapan BlockifyURL, pengguna dapat memuat naik pautan yang ini dianalisis pada kotak teks.

Rajah 1 Antara Muka Notifikasi

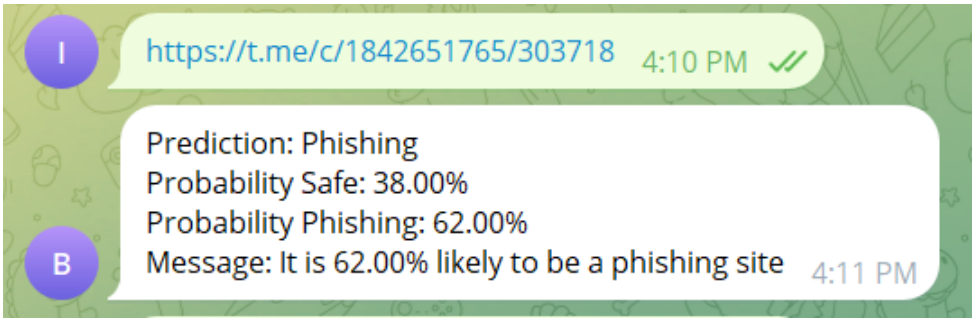
Apabila pengguna memasukkan pautan yang ingin dianalisis, paparan notifikasi akan memberi tahu sama pautan tersebut adalah selamat atau pacingan data. Rajah 2 menujukkan antara muka notifikasi sekiranya pautan adalah selamat dan Rajah 3 memaparkan notifikasi yang menunjukkan pautan tersebut adalah pancingan data.



Rajah 2 Antara Muka Selamat

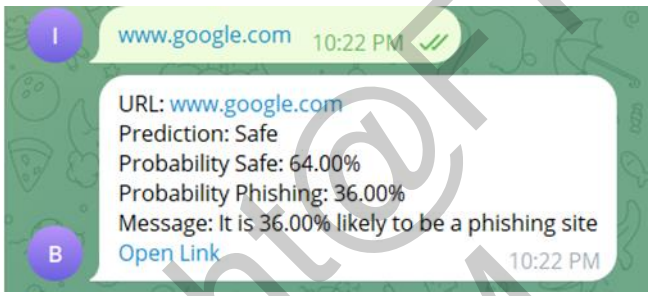
Rajah 3 Antara Muka Pancingan Data

Bagi pengguna yang ingin menggunakan Bot Telegram, Rajah 4 menunjukkan bahawa reka bentuk antara muka notifikasi di Telegram kepada pengguna sekiranya pautan yang dimuat naik adalah pancingan. Notifikasi ini dipaparkan selepas pengguna menghantar pautan yang ingin dianalisis ke bot Telegram.

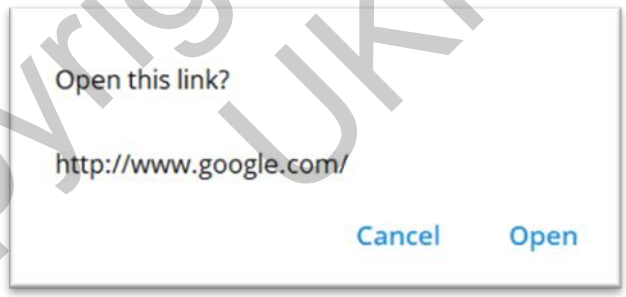


Rajah 4 Antara Muka Pancingan Data di Bot Telegram

Rajah 5 menunjukkan paparan di Bot Telegram selepas pautan yang dikenal pasti sebagai selamat. Pengguna juga dapat menekan pautan hiper untuk meneruskan ke tapak web dengan menekan ‘open link’ dan akan mendapat pertanyaan yang dipaparkan di Rajah 6.



Rajah 5 Antara Muka Selamat di Bot Telegram



Rajah 6 Pautan Hiper ke Tapak Web

PENGUJIAN KEBOLEHGUNAAN

Ujian kebolehgunaan ialah proses di mana pengguna dan pihak yang berminat menjalankan ujian akhir untuk memastikan permainan serius yang dibangunkan memenuhi fungsi yang diperlukan sebelum dikeluarkan kepada umum. Tujuan ujian kebolehgunaan adalah untuk menilai kebolehgunaan sistem, mengumpul data kuantitatif, dan menilai tahap kepuasan pengguna.

Jadual 1 menunjukkan keputusan pengujian yang dijalankan pada BlockifyURL dengan menggunakan senarai pautan pancingan daripada Github(mitchellkrogza) dan Telegram.

Jadual 1 Jadual Keputusan Pancingan data

Pautan	**Hasil pengujian di BlockifyURL**	**Lulus/Gagal**
https://t.me/c/1842651765/303718	63% Phishing	Lulus
https://tg1.leetgems.h1n.ru	51% Phishing	Lulus
https://sameerniz00.github.io/wasif	99% Phishing	Lulus
https://t.me/c/1506013568/5175	62% Phishing	Lulus
https://swapt.pages.dev/undefined	54% Phishing	Lulus
https://t.me/c/1584623096/328871	62% Phishing	Lulus
https://www.jshxnyjx.com	90% Phishing	Lulus
https://reviwesamazon.shop	59% Phishing	Lulus
https://rehaman20.github.io/Netflix	54% Phishing	Lulus
https://recibirtrasfiyabancolombia2124211.brizy.site	92% Phishing	Lulus
https://rawthot.github.io/facebook-clone	58% Phishing	Lulus
https://pubgmobile.info.vn	54% Phishing	Lulus
https://antriksh16b.github.io/Netflix-UI-clone	57% Phishing	Lulus
https://assetfix.vercel.app	92% Phishing	Lulus
https://att-mail-109008.weeblysite.com	82% Phishing	Lulus
https://br0q1nh67z2c.xzf.my.id	88% Phishing	Lulus

1) Ujian Kebolehgunaan

Ujian kebolehgunaan ialah proses di mana produk atau perkhidmatan diuji oleh pengguna sebenar untuk menilai sejauh mana ia mudah digunakan, intuitif dan memenuhi keperluan pengguna. Proses ini melibatkan pemantauan dan menganalisis cara pengguna berinteraksi dengan produk, dengan tujuan untuk mengenal pasti sebarang masalah atau halangan di *BlockifyURL* yang mungkin menghalang pengalaman pengguna yang positif.

Keputusan hasil kebolehgunaan sistem pengesan pautan pelokasi *BlockifyURL* mempengaruhi faktor umur dan tahap pendidikan responden. Keputusan ini menceritakan tahap pendedahan pendidikan teknologi kepada umur responden sama ada tua atau muda.

a. Kebolehgunaan

Mengikut Jadual 2 menunjukkan soalan yang dinyatakan pada tinjauan. Bagi kebolehgunaan, soalan ini dinilai untuk mengetahui pengguna dapat menggunakan fungsi dengan baik tanpa sebarang masalah.

Jadual 2 Kebolehgunaan Fungsi

Soalan
Saya dapat menggunakan antara muka *BlockifyURL* dengan mudahnya
Saya dapat menggunakan *Telegram* Bot dengan baik
Saya dapat menganalisis pautan dengan mudah dan cepat

b. Keberkesanan Fungsi

Mengikut Jadual 3 menunjukkan soalan yang dinyatakan pada tinjauan mengenai keberkesanan fungsi terhadap sistem. Soalan ini dinilai untuk mengetahui sistem *BlockifyURL* dan *Telegram* Bot ini berjaya dalam melindungi pengguna daripada ancaman phishing dan pautan berbahaya di internet.

Jadual 3 Keberkesanan Fungsi

Soalan
Sistem ini membenarkan memuat naik pautan di laman hadapan *BlockifyURL* dan *Telegram* Bot
Sistem ini dapat mengeluarkan laman hadapan *BlockifyURL* dan *Telegram* Bot
Sistem ini memaparkan notifikasi pautan selamat atau pancingan

c. Kebolehpercayaan Fungsi

Mengikut Jadual 4 menunjukkan soalan yang dinyatakan pada tinjauan mengenai kebolehpercayaan terhadap sistem. Soalan ini ditanya untuk mengetahui sistem *BlockifyURL* dan *Telegram* Bot ini berjaya dalam mengenal pasti ancaman phishing dan pautan berbahaya di internet

Jadual 4 Kebolehpercayaan Fungsi

Soalan
Sistem ini memberi keputusan yang tepat
Sistem ini dapat mengesan pautan yang selamat
Sistem ini dapat mengesan pautan yang pancingan
Sistem ini dapat menghantar permintaan dari Postman

d. Umur Responden

Jadual 5 menunjukkan kategori bagi umur responden iaitu yang paling muda ialah 20 tahun ke bawah, umur 30 tahun ke atas dan 21 hingga 30 tahun.

Jadual 5 Umur Responden

Umur Responden
20 tahun ke bawah
21-30 tahun
30 tahun ke atas

e. Tahap Pendidikan

Jadual 6 menunjukkan kategori bagi tahap pendidikan iaitu yang pendidikan menengah, pendidikan pra-universiti dan pendidikan pengajian tinggi.

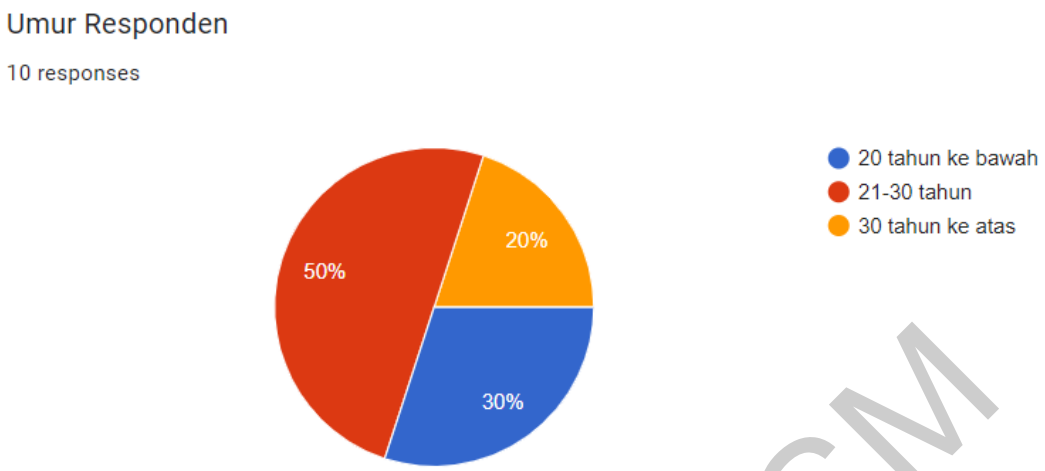
Jadual 6 Tahap Pendidikan

Tahap Pendidikan
Pendidikan Menengah
Pendidikan Pra-Universiti
Pengajian Tinggi

2) Hasil Pengujian Kebolehgunaan

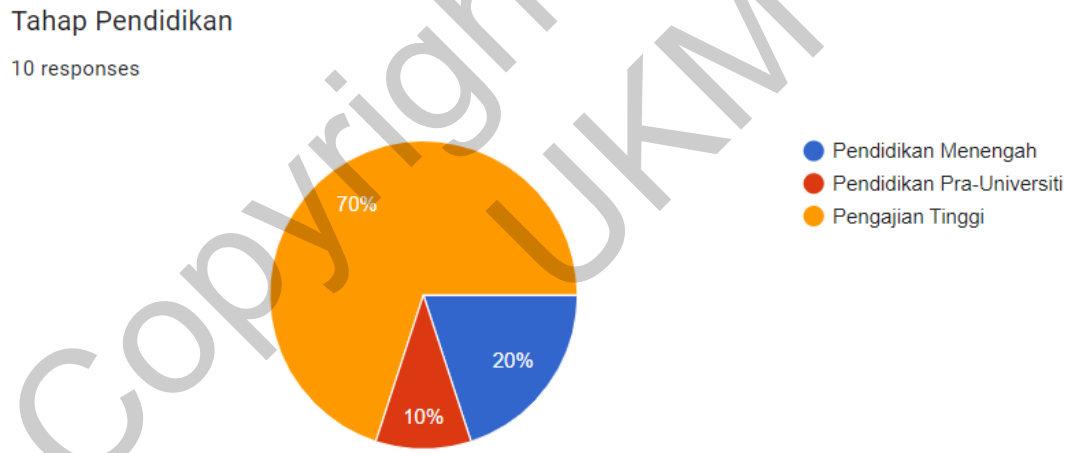
Setelah tinjauan yang dilakukan, keputusan maklum balas yang dikumpul bermula dari umur responden dan di akhiri dengan kebolehpercayaan fungsi. Terdapat 10 pengguna yang dikenal pasti dalam menganalisis sistem pengesan pautan *BlockifyURL* .

Berdasarkan Rajah 7 menunjukkan terdapat 0% bagi umur yang 21-30 tahun, 30 % bagi umur yang 30 tahun ke atas dan 20% bagi yang berumur 20 tahun yang ke bawah



Rajah 7 Umur Responden

Menurut Rajah 8 menunjukkan tahap pendidikan majoriti daripada responden mempunyai 70 % bagi responden yang pengajian tinggi. Bagi tahap pendidikan menengah pula seramai 20% dan 20% bagi yang pra-universiti.



Rajah 8 Tahap Pendidikan

Seterusnya, bagi bahagian yang pertama diuji adalah kebolehgunaan fungsi seperti Jadual 7 . Soalan ini dibagi dalam menilai pengguna dapat menggunakan fungsi dengan baik tanpa sebarang masalah. Nilai yang dinyatakan adalah nilai dari skala tertinggi iaitu “Sangat baik”.

Jadual 7 Nilai Kebolehgunaan Fungsi

Soalan	Nilai
Saya dapat menggunakan antara muka *BlockifyURL* dengan mudahnya	60%
Saya dapat menggunakan *Telegram* Bot dengan baik	40%
Saya dapat menganalisis pautan dengan mudah dan cepat	30%

Aspek yang kedua ialah keberkesanan fungsi terhadap sistem di Jadual 8. Soalan ini digunakan bagi mengetahui sistem BlocifyURL dan *Telegram* Bot ini berjaya dalam melindungi dari ancaman di internet.

Jadual 8 Nilai Keberkesanan Fungsi

Soalan	Purata
Sistem ini membenarkan memuat naik pautan di laman hadapan *BlockifyURL* dan *Telegram* Bot	70%
Sistem ini dapat mengeluarkan laman hadapan *BlockifyURL* dan *Telegram* Bot	80%
Sistem ini memaparkan notifikasi pautan selamat atau pancingan	60%
Sistem ini dapat menghantar permintaan dari Postman	30%

Aspek yang terakhir yang dinilai kebolehpercayaan fungsi seperti di Jadual 9. Soalan ini bertujuan untuk mengetahui sistem *BlockifyURL* dan *Telegram* Bot ini berjaya dalam mengenal pasti ancaman phishing dan pautan berbahaya di internet.

Jadual 9 Nilai kebolehpercayaan Fungsi

Soalan	Nilai
Sistem ini memberi keputusan yang tepat	90%
Sistem ini dapat mengesan pautan yang selamat	70%
Sistem ini dapat mengesan pautan yang pancingan	80%

KESIMPULAN

Secara kesuluruhannya, permainan serius 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 permainan serius ini dijadikan titik kajian untuk kajian lain pada masa hadapan.

Kekuatan Sistem

Kekuatan permainan serius ini ialah ia menawarkan kebolehan untuk meneruskan permainan mereka pada komputer lain. Ini juga bermaksud sekiranya pemain membuang permainan ini daripada komputer mereka dan memuat turun semula, mereka boleh menyambung progres permainan mereka selagi mereka ingat emel dan kata laluan akaun mereka. Dari segi pembangunan, projek ini mempunyai kekuatan dalam mempunyai perkakasan yang mencukupi, termasuk alat pengawal permainan yang diperlukan untuk pengujian.

Kelemahan Sistem

Kebolehan untuk menyambung permainan di komputer yang berbeza telah membawa kepada kekangan permainan ini, iaitu ia bergantung kepada talian internet walaupun permainan ini merupakan “multiplayer” tempatan. Dari segi pembangunan pula, terdapat beberapa kelemahan seperti kekurangan pakar ADHD untuk memberi tunjuk ajar semasa pembangunan permainan. Selain itu, sumber tutorial atau pembelajaran yang komprehensif adalah terhad, menjadikannya sukar untuk memperoleh pengetahuan dan kemahiran yang diperlukan untuk membangunkan permainan ini. Akhir sekali, integrasi pangkalan data awan ke dalam permainan serius ini menimbulkan masalah teknikal. Fungsi ini penting untuk memastikan pemain dapat menyambung permainan mereka di komputer lain. Namun, semua kekangan yang dinyatakan telah dapat diatasi.

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 ketahap 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

API security testing with Postman and OWASP Zap. (2022). The Test Therapist. https://thetesttherapist.com/2022/02/13/api-security-testing-with-postman-and-owasp-zap/comment-page-1/ [23 Disember 2023]

Easydmarc . (n.d.). Phishing link and URL checker | *Easydmarc* . https://*Easydmarc*.com/tools/phishingURL#:~:text=are%20used%20worldwide.,How%20to%20Check%20Link%20Safety%20With%20*Easydmarc*%3F,containing%20links%20into%20the%20box. [23 Disember 2023]

Editor. (2022). What is an API: Definition, Types, Specifications, Documentation. *AltexSoft*. https://www.altexsoft.com/blog/what-is-api-definition-types-specifications-documentation/. [23 Dismber 2023]

GeeksforGeeks. (2018). Software Engineering | Iterative Waterfall Model. https://www.geeksforgeeks.org/software-engineering-iterative-waterfall-model [25 Januari 2024]

Irwin, L. (2023). The 5 most common types of phishing attack. https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack [12 Januari 2024].

Khonji, M., Iraqi, Y. & Jones, A. 2013. Phishing detection: A literature survey. IEEE Communications Surveys and Tutorials

Molloy, J. (2023). Guide to client-server architecture or model. https://www.liquidweb.com/blog/client-server-architecture/ [2 Januari 2024]

Muhammad Hafis Nawawi. (2023). Hati-hati dengan mesej pautan bantuan Rahmah di *Telegram*. https://www.hmetro.com.my/mutakhir/2023/10/1016221/hati-hati-dengan-mesej-pautan-bantuan-rahmah-di-*Telegram* [13 Disember 2023]

Phishing URL Checker: Check a link for phishing in seconds. (n.d.). https://threatcop.com/phishing-URL-checker [20 Disember 2023]

Phishdetect. (n.d.). GitHub - phishdetect/phishdetect: PhishDetect is a library to help identify phishing pages. GitHub. https://github.com/phishdetect/phishdetect [14 Januari 2024]

Sahingoz, O.K., Buber, E., Demir, O. & Diri, B. 2019. Machine learning based phishing detection from URLs. *Expert Systems with Applications 117*: 345–357.

SecureWorld News Team & By SecureWorld News Team. (2020). 5 Smishing Attack Examples Everyone Should See. https://www.secureworld.io/industry-news/5-smishing-attack-examples-everyone-should-see [14 Januari 2024]

URL*Void*, (n.d.) Check if a Website is Malicious/Scam or Safe/Legit | URL*Void*. URL*Void*.com. https://www.URL*Void*.com/ [23 Disember 2023]

Woods, E. (2022). The most common examples of phishing emails. *usecure*. https://blog.usecure.io/the-most-common-examples-of-a-phishing-email

Nurul Izzah binti Armiza (A188420)
Wan Fariza binti Fauzi
Fakulti Teknologi & Sains Maklumat
Universiti Kebangsaan Malaysia