SISTEM PRIVASI DATA DI SEKTOR KESIHATAN DARIPADA SERANGAN DDOS

[1]Muhammad Afif Irfanuddin Faizuddin, [1]Nazhatul Hafizah Kamarudin

[1]Fakulti Teknologi dan Sains Maklumat

43600 Universiti Kebangsaan Malaysia

Abstrak

Data privasi merupakan salah satu data yang penting bagi setiap manusia. Data privasi banyak digunakan di pelbagai sektor awam kerajaan terutamanya sektor pendidikan, kesihatan dan kerajaan. Di sektor kesihatan, data privasi kita bukan sahaja digunakan untuk rujukan kita sebagai pengguna pakar perubatan seperti doktor memerlukan data privasi kita sebagai rujukan mereka untuk mengenalpasti sebarang penyakit dan masalah kita sebagai pengguna dengan mudah. Namun begitu, di zaman globalisasi ini, ancaman baharu telah dikesan telah berlaku dan kini masih berleluasa merebak iaitu serangan siber. Ancaman serangan siber berbahaya kerana data privasi pengguna yang penting dicuri oleh pakar penggodam untuk digunakan sebagai kelebihan dan faedah mereka sendiri. Antara serangan yang sering terjadi pada masa kini dan masih popular yang digunakan oleh penyerang adalah serangan DDoS (DDoS Attack). Ddos attack merupakan salah satu serangan yang digunakan oleh penyerang dengan cara menghantar banyak alamat IP yang sama ke sesuatu sistem untuk melemahkan keselamatan sistem tersebut. Oleh itu, saya telah merancang serta menghasilkan satu sistem data privasi di sektor kesihatan untuk menghalang serangan DDoS daripada berlaku. Sistem ini bertujuan untuk menyimpan segala data terutamanya data privasi pengguna serta data privasi doktor dengan selamat. Sistem ini akan menyekat segala alamat IP yang sama daripada mengakses sistem ini. Sistem ini juga untuk mesra pengguna, senang digunakan serta selamat daripada ancaman luar. Sistem ini akan dibangunkan menggunakan pendekatan model AGILE bagi memastikan pembangunan secara iteratif dengan penambahbaikan berterusan boleh dilakukan kepada sistem ini. Dengan sistem ini, data privasi yang disimpan akan dapat dikukuhkan serta dapat mengelakkan daripada dibocorkan oleh para penggodam.

Kata Kunci: Distributed Denial-of-Service, Internet Protocol

Abstract

Data privacy is one of the important data for every human being. Data privacy is widely used in various public sectors of the government, especially the education, health and government sectors. In the health sector, our privacy data is not only used for our reference as users, but medical experts also such as doctors need our privacy data as their reference to easily identify any diseases and problems for us as users. However, in this era of globalization, a new threat has been detected and is now still widespread, namely cyber-attacks. The threat of cyber-attacks is dangerous because important user privacy data is stolen by hacking experts to use for their own advantage and benefit. Among the attacks that often occur today and are still popularly used by attackers is the DDoS attack. DDoS attack is one of the attacks used by attackers by sending many of the same IP addresses to a system to weaken the security of the system. Therefore, I have designed and produced a privacy data system in the health sector to prevent DDoS attacks from occurring. This system aims to store all data, especially user privacy data and doctor privacy data, safely. This system will block all the same IP addresses from accessing this system. This system is also user-friendly, easy to use and safe from external threats. This system will be developed using the AGILE model approach to ensure iterative development with continuous improvements can be made to this system. With this system, the privacy data stored will be strengthened and can be prevented from being leaked by hackers.

Keywords: Distributed Denial-of-Service, Internet Protocol

1.0 PENGENALAN

Serangan siber merupakan serangan dalam talian yang dilakukan oleh pakar pengodam atau lebih dikenali “hacker” menyerang sistem yang ditarget. Serangan siber boleh dilakukan oleh seorang pakar pengodam atau sebuah organisasi yang pakar dalam teknologi maklumat. Data privasi merupakan sesuatu data sulit setiap manusia seperti nama mereka, alamat mereka, serta data sulit yang berbahaya untuk dibocorkan seperti data bank serta data peribadi. Data privasi pada masa kini banyak digunakan oleh pelbagai sektor kerajaan seperti sektor pendidikan, sektor kesihatan dan lain-lain. Sektor seperti swasta juga memerlukan data peribadi supaya informasi untuk kegunaan semasa dapat diagihkan dengan mudah. Ini menunjukkan bahawa data privasi sangat penting untuk disimpan bagi kegunaan masa akan datang dan bebas daripada serangan kecurian daripada orang luar.

Dalam sektor kesihatan seperti hospital, banyak privasi data yang disimpan didalam sistem seperti data doktor, data jururawat, data pekerja hospital serta data pesakit. Namun begitu, data privasi yang disimpan oleh pihak berkuasa seperti hospital kini menjadi semakin membimbangkan tentang tahap keselamatan yang dilaksanakan. Di era teknologi pada masa kini, serangan siber kini menjadi salah satu masalah umum yang berlaku di seluruh negara termasuk negara kini, Malaysia. Data besar (big data) merujuk kepada set data yang banyak serta komplek yang melebihi keupayaan pengiraan, penyimpanan dan komunikasi yang sedia ada dan juga sistem konvensional. Data yang disimpan didalam sektor hospital boleh diklasifikasi sebagai data besar kerana banyak data yang komplek disimpan di dalam sistem kesihatan seperti data peribadi, data kesihatan, data ubatan dan lain-lain. Beberapa dekad yang lepas menunjukkan bahawa terdapat pertambahan pelanggaran data di sektor kesihatan. Pada 2023, laporan siasatan daripada Verizon melaporkan bahawa terdapat siasatan forensik dan masalah sekuriti yang telah diperoleh berkaitan isu sekuriti dan sebanyak 91% pelanggaran data telah didapati benar (Verizon, 2024) Seterusnya, kajian tentang data privasi pesakit dan data sekuriti menunjukkan bahawa 94% telah diserang oleh pelanggaran data sekurang-kurangnya sekali dalam tempoh 2 tahun. Hal ini menunjukkan kebimbangan dalam penyimpanan data privasi di sektor yang penting seperti sektor kesihatan. Namun begitu, serangan ini kebiasaannya berlaku daripada serangan dalam berbanding serangan luar. Serangan luar asalkan bermula di negara seperti China, Amerika Syarikat dan Eropah Timur.

Serangan DDoS atau lebih dikenali sebagai DDoS Attack (Distributed Denial of Service Attack) merupakan salah satu serangan siber yang bertujuan untuk mengganggu keperluan fungsian dan bukan keperluan fungsian sesuatu sistem yang disasarkan, seperti lam web atau pelayan, menghantar alamat IP yang tidak diperluan serta permintaan yang tidak diperlukan bagi melemahkan trafik sistem. Pada era teknologi masa kini, serangan DDoS merupakan salah satu serangan siber yang masih popular digunakan oleh penyerang. Masalah ini haruslah dielakkan daripada berlaku di dalam sesebuah sistem. Ini dapat memastikan bahawa setiap data yang disimpan di dalam sesebuah sistem dapat disimpan tanpa sebarang masalah daripada serangan siber. Justeru itu, setiap sistem yang dilaksanakan harus mempunyai dilindungi dengan baik daripada sebarang serangan siber. Privasi mempunyai akar sejarah yang dalam (Pritts, 2008; Westin, 1967).

Kesimpulannya, kajian ini dicadangkan kerana terdapat beberapa cabaran dalam melakukan simulasi serangan DDoS. Selain itu, sistem penyimpanan data privasi di sektor kesihatan haruslah selamat daripada serangan DDoS. Sistem ini akan menggunakan RBAC

bagi mengawal serta mengehadkan akses pengguna serta alamat IP daripada serangan DDoS yang diterima akan disekat bagi memastikan data privasi yang disimpan selamat tanpa sebarang isu. Pendekatan ini dilaksanakan supaya tahap keselamatan siber dalam menangani serangan siber seperti serangan DDOS yang bertujuan mencuri data privasi dapat dielakkan dan juga menolong staf di sektor kesihatan seperti doktor dan jururawat dapat menjamin keselamatan data pesakit serta data staf sendiri. Hasil akhir kajian adalah kami akan dapat memahami dan mengelakkan serangan siber daripada berlaku.

2.0 KAJIAN LITERATUR

Kajian Algoritma Kawalan Akses Berasaskan Peranan (RBAC)

Kajian Algoritma Kawalan Akses Berasaskan Peranan (RBAC) merupakan kajian algoritma yang paling digunakan untuk menjaga data privasi di sektor kesihatan. Kajian pertama iaitu kajian oleh (Baihan, M. Shaya 2022) merupakan satu kajian yang menggunakan RBAC. Kajian ini bertujuan untuk mempersembahkan penyelesaian Kawalan Capaian Berasaskan Peranan (RBAC) untuk memintas semua permintaan GraphQL di dalam sektor kesihatan. Sumber data yang digunakan di dalam kajian ini ialah HAPI FHIR. Kajian ini mengunakan tiga senario yang berbeza dan dibandingkan tahap kelajuan untuk mendapatakan data yang diminta.

Keputusan kajian ini telah menunjukkan bahawa purata masa yang digunakan untuk mengatasi kelemahan daripada (BOLA) dan (BFLA) dengan mengunakan RBAC lebih berkesan berbanding dengan tidak menggunakan RBAC. Purata masa yang dapat disimpan dengan menggunakan RBAC dapat dijimatkan sebanyak 6%. Ini menunjukan bahawa penggunakan RBAC dapat memudahkan serta mengurangkan masa yang digunakan untuk mendapatkan data yang dimohon.

Kajian seterusnya oleh (R. Cai, L. Chen, Y. Zhu 2024) juga menggunakan algoritma Kawalan Akses Berasaskan Peranan (RBAC). Kajian ini bertujuan untuk menfokus tentang isu keselamatan data privasi di sektor kesihatan terutamanya pengunaan (Cloud). Kajian ini juga bertujuan untuk mengabungkan RBAC dengan protokol PSI untuk mengukuhkan tahap keselamatan data privasi di dalam Cloud di sektor kesihatan. Sumber data yang digunakan di dalam kajian ini adalah daripada data pengguna yang disimpan di Cloud.

Hasil keputusan kajian ini telah menunjukkan bahawa hasil penggabungan sistem RBAC dan protokol PSI di Cloud untuk kegunaan sektor kesihatan dapat berlaku kebocoran data oleh pelawat yang menggunakan sistem Cloud.

Kajian Serangan DDoS

Kajian Serangan DDoS merupakan satu kajian lepas yang dilakukan oleh (M. Dey, S. Sharma 2023). Kajian ini bertujuan untuk mencadangkan kaedah pengedaran yang memelihara privasi untuk mengesan serangan DDoS dengan menganalisis corak aktiviti peranti IoT. Ia juga dapat melaksanakan simulasi serangan DDoS bagi menyekat serangan tersebut di dalam IoT. Metod yang digunakan bagi kajian ini adalah memantau aktivitiperanti IoT dan melakukan ujian CPD (Change Point Detection)

Hasil yang telah diterima adalah penyelesaian memelihara data privasi untuk mengesan serangan DDoS dengan menganalisis peranti merentas rangkaian IoT yang diedarkan telah dapat dibuktikan dengan berkesan, terutamanya dalam persekitaran dengan bilangan pengguna adalah sederhana.

3.0 METEDOLOGI

Bahagian ini merangkumi analisis keperluan, merangka reka bentuk model konseptual, pembangunan aplikasi, pengujian kebolehgunaan dan hasil yang diperoleh daripada kajian ini. Metodologi menerangkan kaedah bagi mengatasi masalah yang dikenal pasti serta menerangkan proses kajian yang dilakukan.

3.1 Analisis Keperluan

Keperluan Pengguna amat penting untuk dicadangkan bagi menunjukkan segala perkhidmatan yang disediakan oleh sistem kepada pengguna untuk digunakan. Ini boleh dijadikan sebagai panduan untuk pembangunan sistem ini selaras dengan keperluan pengguna dan objektif pembinaan sistem ini. Sebarang keperluan yang menentukan apa yang perlu dilakukan oleh sistem (Reqtest 2023). Keperluan fungsian merupakan satu keperlukan yang diperlukan di dalam sistem. Sekiranya pengguna tidak memenuhi syarat yang diperlukan, sistem ini tidak dapat dijalankan. Antara keperluan fungsian bagi sistem untuk menjaga data privasi pengguna di sektor kesihatan daripada serangan DDoS adalah sistem ini har Setiap pengguna haruslah

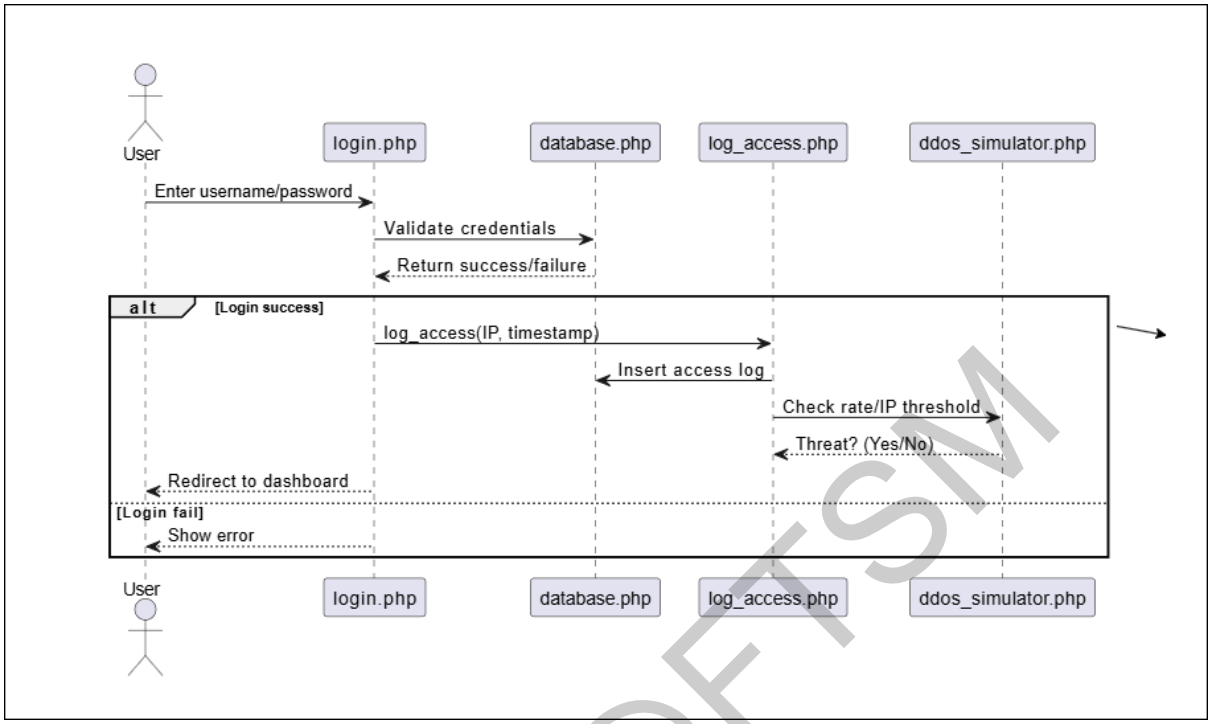
mempunyai tag nama yang istimewa dan hanya satu tag nama bagi setiap pengguna untuk melanggan masuk sistem ini uslah mempunyai data-data privasi pengguna yang menggunakan sistem ini untuk dilindungi, sistem ini haruslah diimplikasi sistem menyekat alamat IP yang berbahaya daripada serangan DDoS selaras dengan objektif kajian dan Simulasi serangan DDoS dapat dilakukan dengan baik dan berjaya disekat. Rajah 1 dibawah menunjukkan hasil yang dicadangkan untuk diperoleh apabila sistem ini telah berjaya dibangunkan. Sistem yang telah dibangunkan untuk sistem ini adalah **HeathGuard**.

Rajah 1: Akses Disekat

3.2 Reka Bentuk Model Konseptual

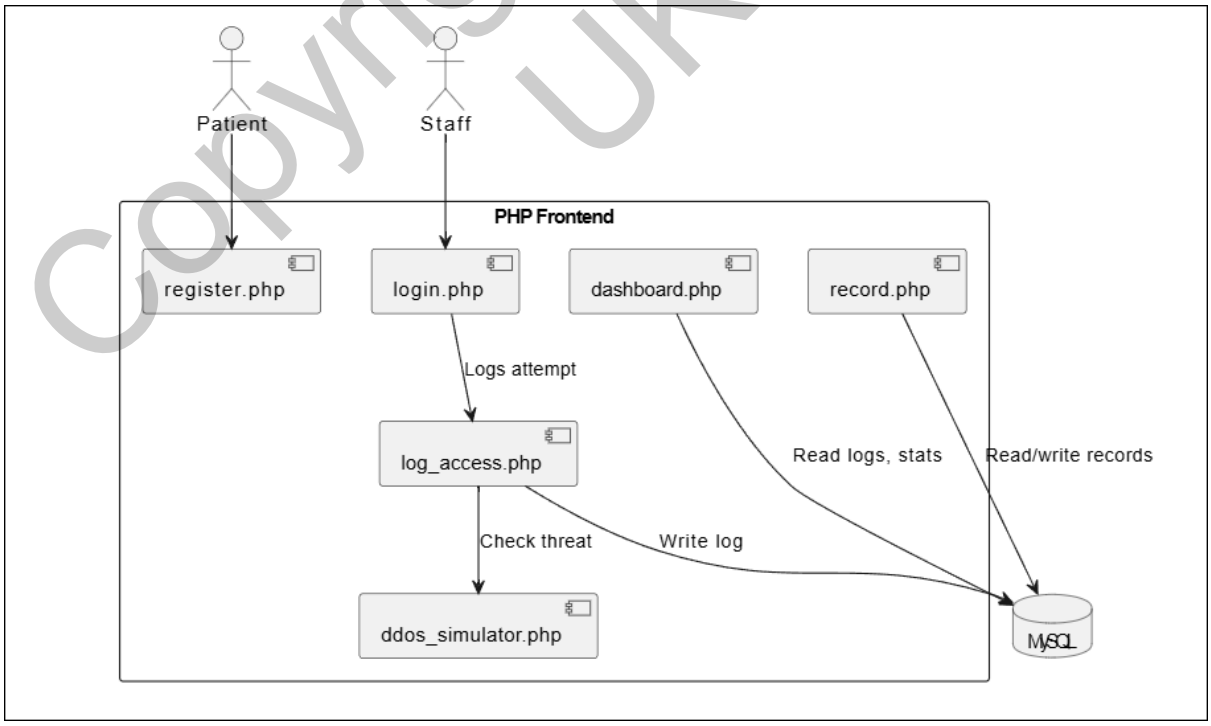
Reka bentuk interaksi setiap komponen pada sistem **HealthGuard** ini menerapkan sistem penyimpanan data privasi yang selamat dan mesra pengguna. Komponen bagi sistem ini terdiri daripada penyimpanan data pengguna, pengesanan DDoS serta mengekat akses sistem.

Rajah 2 dibawah menunjukkan interaksi yang berlaku apabila pengguna log masuk ke dalam sistem dan serangan DDoS diperiksa berlaku ataupun tidak. Pengesanan DDoS akan mengekat akses alamat IP tersebut berdasarkan kadar permintaan yang tinggi.



Rajah 2: Pengguna log masuk ke dalam sistem

Rajah 3 pula ialah rajah komunikasi data. Rajah ini bertujuan untuk menunjukkan interaksi yang berlaku semasa RBAC berlaku di antara pesakit dan stafs semasa log masuk ke sistem. Rajah ini akan menunjukkan tahap akses yang boleh dilihat oleh pengguna dan staf.



Rajah 3: RBAC di antara Pengguna dan Staf

4.0 HASIL

4.1 Pembangunan Sistem

Pada proses Pembangunan sistem, terdapat beberapa keperluan perisian yang diperlukan dalam membangunkan sistem ini. Keperluan perkakasan dan perisian amatlah penting bagi memastikan proses pembangunan sistem ini dapat dijalankan dengan lancar dan tiada masalah serta menghasilkan sistem yang mencapai objektif projek ini. Keperluan perkakasan penting untuk mengenalpasti kekuatan perkakasan yang digunakan untuk mereka bentuk sistem ini. Selain itu, perisian yang canggih dapat menyokong keperluan khusus projek, menyediakan kemudahan pengintegrasian dan memastikan keselamatan data yang optimum. Jadual di bawah menunjukkan keperluan perkakasan dan perisian bagi sistem ini.

Kriteria	Spesifikasi
Pemproses	AMD Ryzen™ 7 7735HS Mobile Processor
Pemacu keadaan pepejal	512GB
Memori Capaian Rawak (RAM)	16GB
Sistem Operasi	Windows 11
Unit Pemprosesan Grafik (GPU)	NVIDIA® GeForce RTX™ 4050

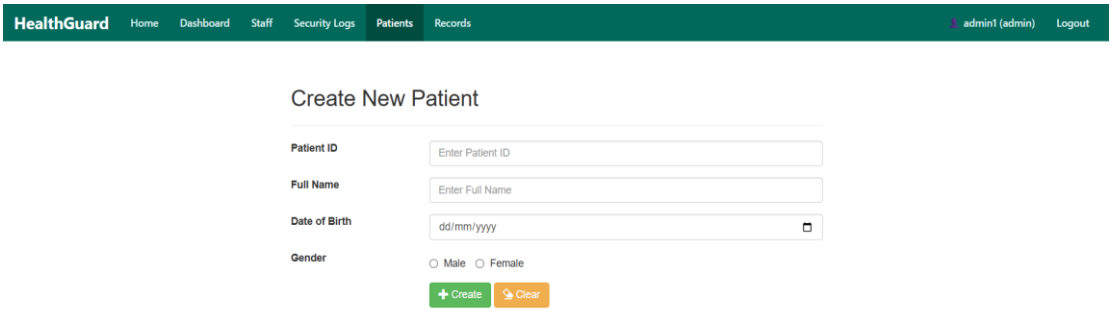
Jadual Keperluan Perisian

Perisian	Perincian
Microsoft Word	Menulis laporan ilmiah projek akhir tahun
Microsoft Excel	Tempat simpanan maklumat dan data
SublimeText	Tempat untuk mereka bentuk sistem ini dan melakukan simulasi serangan DDoS
Google Chrome	Laman web yang digunakan untuk mencari maklumat dan tinjauan kesusasteraan
MySQL	Tempat segala data akan disimpan

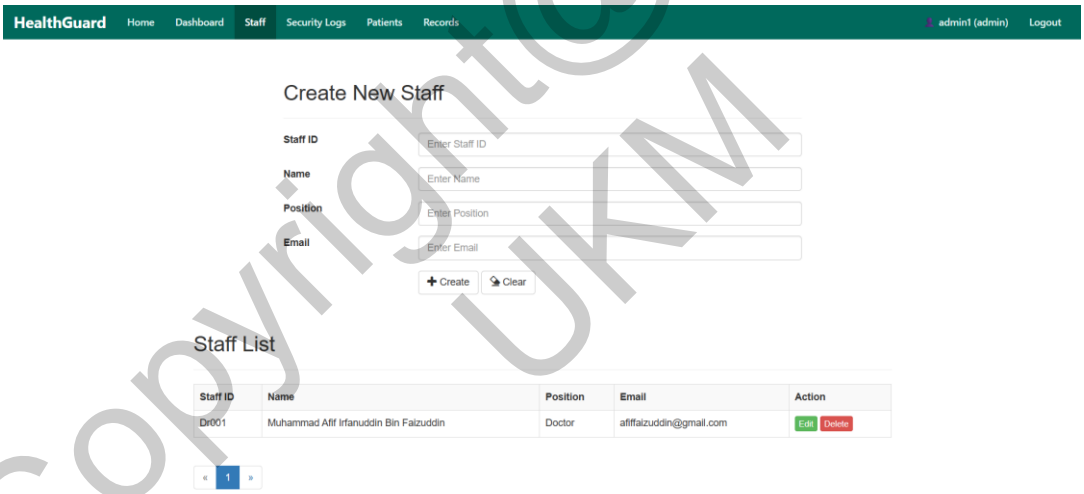
Jadual Keperluan Perisian

Terdapat beberapa fungsi yang dapat dilihat di dalam sistem HealthGuard ini. Pertama, sistem ini mempunyai sistem log masuk yang selamat bagi membahagikan tahap akses pengguna. Selain itu, sistem ini juga memenuhi objektif dalam penyimpanan data privasi pengguna di sektor Kesihatan. Pengguna dan Staf dapat melihat dan menambah data privasi dan rekod Kesihatan di dalam sistem. Seterusnya, laman log keselamatan juga dapat memastikan admin dapat mengetahui jenis penyerang yang menyerang sistem ini. Di samping itu, Laman Papan Pemuka Trafik dan Keselamatan juga akan menunjukkan bilangan akses yang dihantar oleh penyerang mengikut masa dunia nyata. Akhir sekali, simulasi DDoS berjaya dilakukan dengan menghantar permintaan yang banyak pada sesuatu masa.

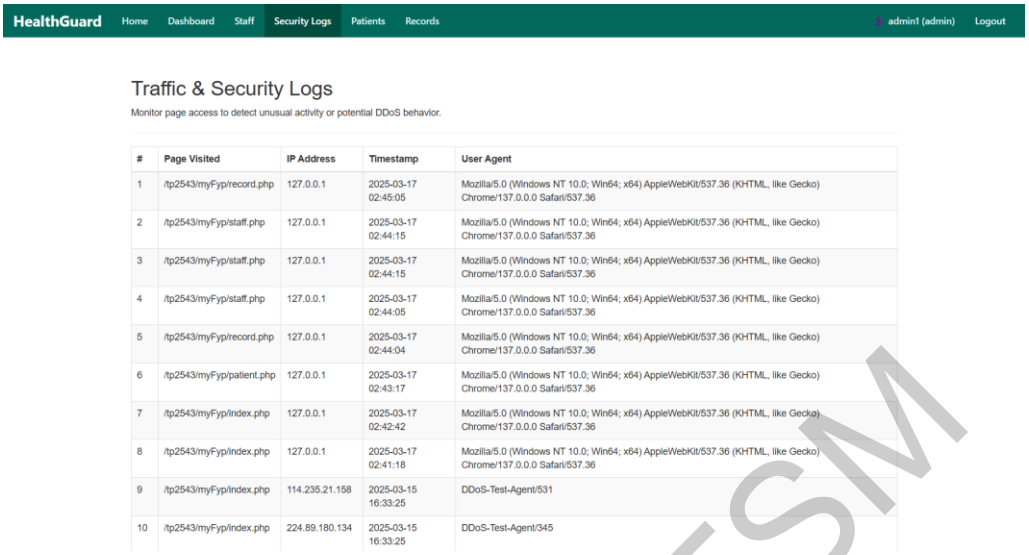
Laman Log Masuk



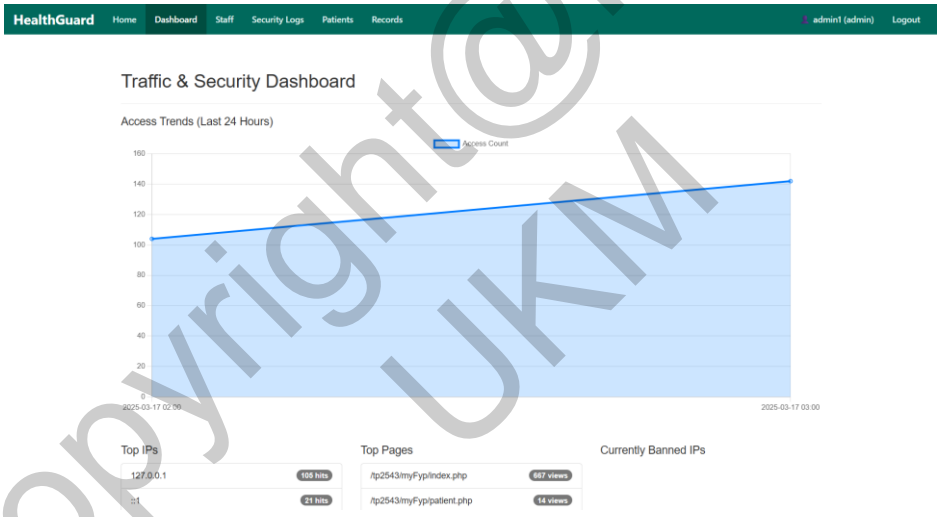
Laman Data Pesakit



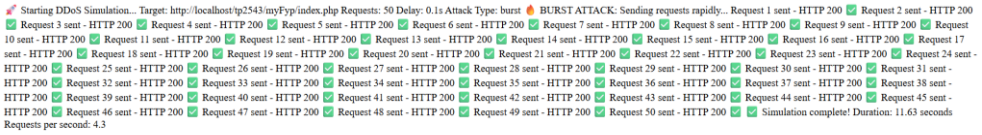
Laman Data Staf



Laman Keselamatan Log dan Trafik Masa Nyata



Laman Papan Pemuka Trafik dan Keselamatan



Simulasi Serangan DDoS

4.2 Penilaian Sistem

Penilaian sistem telah dilakukan bagi menguji tahap kekuatan dan hasil akhir bagi mengenal pasti sebarang kekurangan yang dilihat daripada sistem ini. Jadual di bawah menerangkan tentang tahap pengujian fungsian dan bukan fungsian.

i. Pengujian Fungsian

ID Kes Ujian	Penerangan	Langkah	Data Ujian	Hasil yang diharapkan	Kriteria Lulus / Gagal
TC-F-01	Log Masuk Pengguna	1. Buka laman web sistem 2. Masukkan nama pengguna dan kata laluan 3. Ketik log masuk	nama pengguna dan kata Laluan	Pengguna disahkan dan diarahkan ke papan pemuka	Pengguna dapat log masuk dan melihat papan pemuka
TC-F-02	Tambah Data Pesakit	1. Log masuk sebagai Staf 2. Navigasi ke Data Pesakit 3. Tambah Butiran Pesakit 4. Simpan	ID Pesakit Nama, Tarikh Lahir, Jantina	Data Pesakit akan muncul di dalam sistem dan disimpan di MySQL dan PHP	Data disimpan dengan selamat
TC-F-03	Tambah Data Staf	1. Log masuk sebagai Staf 2. Navigasi ke Data Staf 3. Tambah butiran Staf 4. Simpan	ID Staf Nama, Jawatan, Emel	Data Staff akan muncul di dalam sistem dan disimpan di MySQL dan PHP	Data disimpan dengan selamat
TC-F-04	Tambah Data Rekod	1. Log masuk sebagai Staf 2. Navigasi ke Data	ID Rekod ID Pesakit, ID Staf,	Rekod Kesihatan akan muncul	Data disimpan dengan selamat

		Rekod 3. Tambah butiran Rekod 4. Simpan	Diagnosis dan Tarikh Rekod	di dalam sistem dan disimpan di MySQL dan PHP	
TC-F-05	Simulasi Serangan DDoS	1. Kod Simulasi DDoS ditetapkan di dalam file 2. Link http://localhost/tp2543/myFyp/ddos_simulator_advanced.php akan dijalankan 3. Kod dapat dilakukan dengan baik	-	Permintaan Serangan DDoS dapat dijalankan	Data alamat IP daripada DDoS akan muncul di Log Trafik & Keselamatan dan Papan Pemuka Trafik & Keselamatan.
TC-F-06	Alamat IP Disekat akses	1. Simulasi Serangan DDoS dilakukan 2. Alamat IP disekat 3. Akses ke laman pesakit, staf dan rekod akan disekat	-	Akses melayari laman di sistem akan disekat	Akses ke sistem tidak dapat dilakukan

ID Kes Ujian	**Penerangan**	**Langkah**	**Hasil Yang Diharapkan**	**Kriteria Lulus/Gagal**
TC-NF-01	Ujian Keselamatan	Log Masuk dengan nama pengguna dan kata laluan yang tidak sah	Akses untuk log masuk disekat	Tidak mendapat akses

TC-NF-02	Ujian Kebolehgunaan	Pengguna, Staf dan Admin dapat melihat laman selaras dengan kehendak yang ditetapkan	Pengguna dan Staf dapat melihat laman UI	Maklum balas positif dari pengguna

ii. Pengujian Kebolehgunaan

Pengujian kebolehgunaan penting bagi memastikan sistem ini memenuhi segala keperluan pengguna berdasarkan objektif kajian. Rajah di bawah menunjukkan hasil terakhir hasil pengujian kebolehgunaan.

Kes Ujian	**Hasil**	**Catatan**
TC-F-01	Lulus	Log masuk berjaya untuk pengguna yang sah
TC-F-02	Lulus	Data Pesakit dapat ditambah serta disimpan dengan baik
TC-F-03	Lulus	Data Staf dapat ditambah serta disimpan dengan baik
TC-F-04	Lulus	Data Rekod Kesihatan dapat ditambah serta disimpan dengan baik
TC-F-05	Lulus	Simulasi Serangan DDoS dapat dijalankan dengan baik
TC-F-06	Lulus	Alamat IP yang berbahaya dapat disekat dengan kuat
TC-NF-01	Lulus	Akses tidak sah akan dihalang

TC-NF-02	Lulus	Pengguna dapat menggunakan serta memahami sistem dengan baik.

5.0 KESIMPULAN

Semasa fasa pengujian sistem HealthGuard, terdapat beberapa cabaran yang telah dilalui. Pertama, terdapat banyak amaran session_start() apabila log_access.php telah dimasukkan ke dalam banyak kod. Semakan status sesi ditambah sebelum memulakan sesi bagi mengelakkan masalah ini dari terjadi. Masalah yang seterusnya adalah kadangkala, pengguna sah disekat semasa fasa pengujian. Solusi yang dilakukan adalah mengehadkan parameter kadar larasan (20 permintaan/minit) bagi memastikan sistem ini seimbang dari segi keselamatan dan kebolehgunaan.

Manakala, dari segi pencapaian keseluruhan, semua kes ujian yang dilakukan telah berjaya dilaksanakan dengan keputusan yang diharapkan. Keputusan Ujian Penerimaan Pengguna (UAT) yang diterima daripada pengguna yang terlibat iaitu pesakit, staf dan admin menunjukkan bahawa HealthGuard dapat memenuhi kehendak dan ekspektasi pengguna. Simulasi serangan DDoS juga berjaya menunjukkan bahawa alamat IP yang disekat tidak dapat melihat data privasi pengguna. Cadangan penambahbaikan bagi sistem ini adalah untuk menyekat serangan siber daripada serangan lain selain daripada serangan DDoS seperti serangan DoS (Denial-of-Service Attack), Suntikan SQL (SQL Injection) dan lain-lain.

6.0 PENGHARGAAN

Nazhatul Hafizah Kamarudin, Fakulti Teknologi dan Sains Maklumat

7.0 RUJUKAN

1) Rajalakshmi, R. (2024). Cybersecurity in the Healthcare Sector: Protecting Patient Data and Medical Devices. International Journal for Science Technology and Engineering, 12(8), 842–848.

2) Verizon. (2024). 2024 Data Breach Investigations Report. Verizon.

3) Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule; Nass, S. J., Levit, L. A., & Gostin, L. O. (2009). Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. National Academies Press.

4) Ferraiolo, D. F., & Kuhn, D. R. (1992). Role-Based Access Control (RBAC). Diambil daripada https://en.wikipedia.org/wiki/Role-based_access_control

5) Suganthy, A., & Venkatesan, V. P. (2019). An introspective study on dynamic role-centric RBAC models. IEEE International Conference on System, Computation, Automation and Networking (ICSCAN), 1–6. https://doi.org/10.1109/ICSCAN.2019.8878827

6) Kupwade Patil, H., & Seshadri, R. (2014). Big data security and privacy issues in healthcare. IEEE International Congress on Big Data, 762–765. https://doi.org/10.1109/BigData.Congress.2014.112

7) Bonagiri, K., M. V. S., N., Gopalsamy, M., I. A., Helan R., R. H., & S. J., S. S. (2024). AI-driven healthcare cyber-security: Protecting patient data and medical devices. IEEE International Conference on Intelligent Cyber Physical Systems and IoT (ICoICI), 107–112. https://doi.org/10.1109/ICoICI62503.2024.10696183

8) Jadon, & Kumar, S. (2023). Leveraging generative AI models for synthetic data generation in healthcare: Balancing research and privacy. IEEE SmartNets, 1–4. https://doi.org/10.1109/SmartNets58706.2023.10215825

9) Jayanthilladevi, K. S., & Balamurugan, E. (2020). Healthcare biometrics security and regulations. IEEE Conference on Emerging Smart Computing and Informatics (ESCI), 244–247. https://doi.org/10.1109/ESCI48226.2020.9167635

10) Baihan, M. S. (2022). Role-based access control solution for GraphQL-based FHIR health APIs. IEEE HealthCom, 1–6. https://doi.org/10.1109/HealthCom54947.2022.9982782

11) Cai, R., Chen, L., & Zhu, Y. (2024). Privacy-preserving access control model for e-medical systems. IEEE BDPC, 63–68. https://doi.org/10.1109/BDPC59998.2024.10649051

12) Panwar, N., Kumar, N., Kumar, M. S., Rafeeq, M., Rajeswari, P., & Meenakshi, S. (2024). AI-driven healthcare infrastructure for smart cities. IEEE ICCCNT, 1–6. https://doi.org/10.1109/ICCCNT61001.2024.10725216

13) Tammina, M. R., Posinasetty, B., Nair, P. S., Kumar, S., G., P., & Kaur, H. (2024). Machine learning enabled healthcare balancing patient privacy and data utility. IEEE ICONSTEM, 1–6. https://doi.org/10.1109/ICONSTEM60960.2024.10568855

14) Rastogi, P., Singh, D., & Singh Bedi, S. (2022). Design of a blockchain-based security algorithm for IoT in healthcare. IEEE ICACITE, 2209–2214. https://doi.org/10.1109/ICACITE53722.2022.9823466

15) Ravikumar, S., Tasneem, S., Sakib, N., & Islam, K. A. (2024). Securing AI of healthcare: A selective review. IEEE ORSS, 75–78. https://doi.org/10.1109/ORSS62274.2024.10697946

16) Almusawi, M., et al. (2023). Cryptography-based privacy-preserving data analysis. IEEE ICTEASD, 92–98. https://doi.org/10.1109/ICTEASD57136.2023.10584998

17) Brocoders. (n.d.). How to write an SRS document: Definition, steps, and examples. Diambil daripada https://brocoders.com/blog/how-to-write-srs-document/

18) ReQtest. (n.d.). Functional vs. non-functional requirements: Key differences. Diambil daripada https://reqtest.com/en/knowledgebase/functional-vs-non-functional-requirements/

19) ASUS. (n.d.). ASUS Vivobook 16 M1605Y AMB424WS. Diambil daripada https://shop.asus.com/my/asus-vivobook-16-m1605y-amb424ws.html

20) GeeksforGeeks. (n.d.). MVC Framework Introduction. Diambil daripada https://www.geeksforgeeks.org/mvc-framework-introduction/

21) IBM. (n.d.). Network Topology. Diambil daripada https://www.ibm.com/think/topics/network-topology

22) GeeksforGeeks. (n.d.). What is Hybrid Topology?. Diambil daripada https://www.geeksforgeeks.org/what-is-hybrid-topology/

23) Visual Paradigm. (n.d.). What is Class Diagram?. Diambil daripada https://www.visual-paradigm.com/guide/uml-unified-modeling-language/what-is-class-diagram/

24) GeeksforGeeks. (n.d.). Unified Modeling Language (UML) Sequence Diagrams. Diambil daripada https://www.geeksforgeeks.org/unified-modeling-language-uml-sequence-diagrams/

25) YouTube. (n.d.). YouTube - Video Sharing Platform. Diambil daripada https://www.youtube.com/

26) jQuery. (n.d.). A Touch-Optimized Web Framework. Diambil daripada https://jqueryui.com/

27) Cloudflare. (n.d.). What is rate limiting? | Rate limiting and bots. Diambil daripada https://www.cloudflare.com/learning/bots/what-is-rate-limiting/

28) Cloudflare. (n.d.). OWASP Top 10. Diambil daripada https://www.cloudflare.com/learning/security/threats/owasp-top-10/

29) Fortinet. (n.d.). DDoS Attack. Diambil daripada https://www.fortinet.com/resources/cyberglossary/ddos-attack

30) Usersnap. (n.d.). User Acceptance Testing (UAT). Diambil daripada https://usersnap.com/blog/user-acceptance-testing-right/