SISTEM KESELAMATAN HALAMAN WEB DINAMIK DARI SERANGAN SUNTIKAN NOSQL DENGAN MENGGUNAKAN SKRIP JAVA

Nurul Nasuha Binti Ahmad Hidzir

Dr. Ravie Chandran Muniyandi

Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Sistem penyimpanan data NoSQL telah menjadi sangat popular kerana skalabiliti dan kemudahan penggunaanya. Projek ini meneliti kematangan NoSQL dalam langkah-langkah keselamatan pangkalan data NoSQL,bagi menangani pertanyaan baru dan mekanisma akses. Fleksibiliti dan skalabiliti bagi pangkalan data NoSQL merupakan punca besar bagi pangkalan data NoSQL menjadi popular. Malangnya, disebabkan kekurangan langkah keselamatan dan kesedaran pangkalan data NoSQL memerlukan perlindungan data. Seterusnya, disebabkan pendedahan global menyebabkan pangkalan data NoSQL terdedah kepada serangan kerana wujudnya kelemahan. Kelemahan keselamatan ini terus memberi kesan kepada web aplikasi melalui serangan suntikan yang membenarkan penyerang menyerang terus ke pangkalan data melalui suntikan kod jahat ke dalam kenyataan yang diluluskan oleh pangkalan data NoSQL. Di sini saya kemukakan cara menyerang pangkalan data dengan menggunakan nod Skrip Java. Dengan cara ini boleh menganalisis sumber kelemahan dan metadologi yang digunakan adalah untuk memperbaiki kekurangan yang ada . Metadologi yang digunakan dalam sistem ini adalah menggunakan kaedah air terjun. Kaedah ini dipilih kerana dapat mengenalpasti masalah dengan lebih awal dan dapat dibaiki dengan segera.

1 PENGENALAN

Projek ini adalah mengenai keselamatan halaman web dinamik dari serangan suntikan NoSQL dengan menggunakan nod Skrip Java. Halaman web dinamik secara umumnya dijana daripada aplikasi yang bukanya dibuat terlebih dahulu untuk diposkan kepada pelayan web. Kebiasaanya, kandungan teks akan disimpan ke pangkalan data dan kandungan yang dilihat apabila halaman itu dipaparkan boleh berubah-ubah mengikut

cara dan apabila halaman itu dipaparkan. Contoh yang boleh kita ambil adalah WordPress. WordPress boleh digunakan untuk membuat halaman web dinamik. Ianya merupakan aplikasi yang kompleks dan hanya di muat turun pada pelayan web dan ianya memerlukan pemasangan pangkalan data MySQL untuk berfungsi. Halaman web dinamik juga telah dibangunkan dengan menggunakan teknologi pelayan (*server*) yang lebih maju. Sebagai contoh, Skrip Java, PHP ataupun ASP dengan menggunakan bahasa tersebut dapatlah kita menghasilkan laman web. Web dinamik ini kebiasaanya akan disambungkan kepada pangkalan data yang lebih besar (Scott P.Randby 2019). Seperti yang anda sedia maklum, pangkalan data NoSQL adalah sokongan skala yang lebih baik, kebolehkesanaanya dan dapat mengakses data dengan lebih pantas berbanding dengan RDBMS. Seterusnya, MongoDB adalah platform yang berorientasikan dokumen yang dimiliki oleh pangkalan data NoSQL. Kebanyakan digunakan untuk permohonan peribadi dan pengurusan perusahan. MongoDB adalah contoh suntikan dan pertahanan, pengesanan, analisis bagi pangkalan data NoSQL. Suntikan ini selalunya menggunakan cara yang sama untuk menyerang pangkalan data dengan menyuntik ayat yang mengandungi kod jahat untuk dimasuki ke kod perlaksanaan daripada aplikasi ataupun perisian. Dengan cara ini penyerang akan dapat kuasa pengguna untuk memperolehi informasi daripada pangkalan data, kemaskini, ataupun membuang data dalam pangkalan data. (Boyu Hou 2016).

2 PENYATAAN MASALAH

Suntikan NoSQL akan mengancam keselamatan pangkalan data.

Suntikan boleh menyebabkan kebocoran akaun peribadi dan informasi syarikat terdedah. Penggodam boleh mengambil kuasa pengguna sebenar ataupun membuat apa sahaja dengan suntikan yang menghasilkan pengaruh yang sangat negatif terhadap keselamatan maklumat. Oleh itu, perlulah menambah fungsi pertahanan untuk meningkatkan keselamatan. Sebagai pertahanan kita akan membincangkan bagaimana untuk mengelak suntikan kotak input dalam halaman web

3 OBJEKTIF KAJIAN

Sistem ini dibangunkan bagi memenuhi beberapa objektif yang berikut:

I. Untuk membangunkan sistem yang boleh menyimpan data dan memperbaiki antaramuka (*interface*) agar lebih selamat dengan menggunakan sistem

dinamik.

II. Untuk memastikan data yang terdapat dalam pangkalan data NoSQL itu tidak terdedah kepada orang lain dengan adanya fungsi *bcrypt*.

III. Untuk mengekalkan tahap keselamatan pangkalan data daripada ancaman suntikan NoSQL dengan *penggunaan Vega*.

4 METOD KAJIAN

Sistem Keselamatan Halaman Web Dinamik Dari Serangan suntikan NoSQL dengan menggunakan Skrip Java ini menggunakan metadologi dikenali sebagai Air Terjun(Waterfall Model). Model Air Terjun dipilih kerana model ini mudah digunakan kerana jika terdapat masalah semasa mebangunkan sistem kita oleh mengundur kembali dan membetulkan apa yang salah. Selain itu, Model Air Terjun di pilih kerana kebanyakan pembangun sistem banyak menggunakan model ini , ini kerana ianya terdiri daripada lima tahap pemperosesan yang jelas dari satu ke satu peringkat disebabkan itu pembangun dapat menambahbaikan dari semasa ke semasa.

4.1 Fasa Perancangan

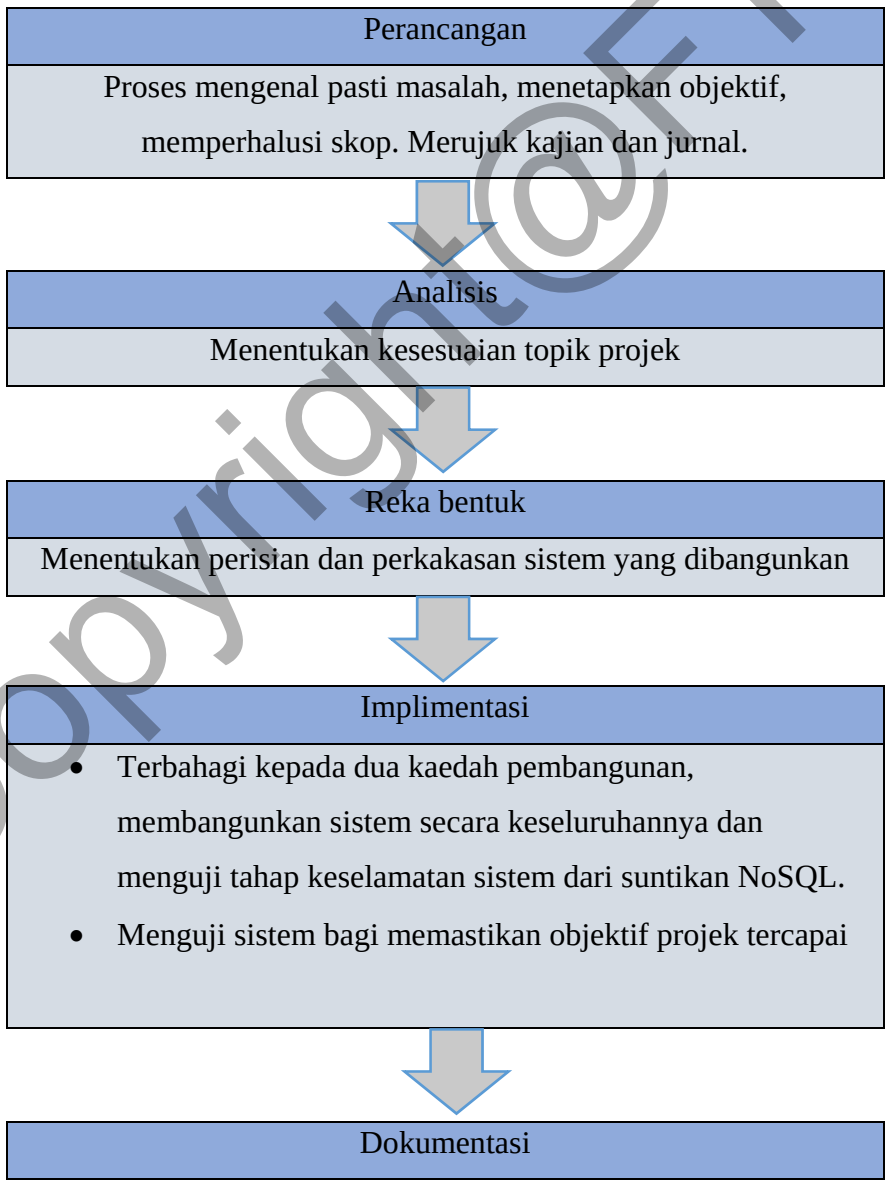
Fasa perancangan ini melibatkan proses mengenalpasti masalah, cadangan penyelesaian masalah, mencari objektif kajian dan menentukan skop kajian dalam menjalankan projek ini. Langkah seterusnya melibatkan kajian kusasteraan yang melibatkan pengumpulan, pencarian dan pembacaan jurnal dan kajian-kajian lepas bagi mencetus idea untuk pembangunan yang ingin dijalankan. Contoh topik yang yang berkaitan akan dikaji terutamanya tentang konsep MongoDB dan pangkalan-pangkalan data NoSQL yang diguna pakai oleh sistem terdahulu. Maklumat dikumpul, distruktur dan di analisis untuk diperjelaskan secara kreatif dan inovatif pada fasa analisis.

4.2 Fasa Analisis

Fasa ini melibatkan analisis dan tafsiran mengenai kelemahan dan permasalahan yang dihadapi dari semasa ke semasa. Fasa ini menganalisis kajian- kajian yang sedia ada bagi dikaji semula untuk dibuat rujukan dalam pembanguna sistem ini. Tujuan tersebut adalah untuk membangun sistem yang dapat memenuhi keperluan pengguna dan kehendak pengguna. Selain itu, kaedah pengujian wujud dalam sistem ini bagi menganalisis tahap keselamatan yang perlu diperhalusi oleh sistem ini.

4.3 Fasa Reka Bentuk

Fasa ini melibatkan proses merangka reka bentuk antara muka halaman sistem yang ingin dibangunkan. Fasa ini menerangkan setiap pautan yang diguna pakai termasuk fungsi setiap butang, carta alir dan rajah-rajah yang berkaitan. Fasa ini juga mengambil kira perisian dan perkakasan yang digunakan bagi menghasilkan satu sistem yang dapat berfungsi dengan baik dan berjaya. Untuk menghasilkan reka bentuk yang efektif dan berkualiti *Data Flow Diagram(DFD)*, carta aliran harus dibuat terlebih dahulu supaya dapat melihat gambaran yang lebih jelas. Tambahan pula, penggunaan *Entity Relationship Diagram(ERD)* yang telah memaparkannya secara jelas dan terperinci cara pembinaannya, ini memberi kemudahan dalam fasa implimentasi kelak.



Melaporkan keseluruhan projek Membuat kesimpulan dan menganalisis kelemahan dan kekuatan sistem

Rajah 1 Model pembangunan sistem halaman web dinamik dari serangan suntikan NoSQL dengan menggunakan Skrip Java.

4.4 Fasa Implimentasi

Fasa ini adalah fasa bermulanya sesebuah pembangunan. Proses ini penting dalam memastikan sama ada fungsi yang dipersembahkan berfungsi dengan baik sama seperti yang dirancang dalam fasa reka bentuk. Dalam fasa ini juga kita akan nampak dengan jelas kelemahan dan kelebihan sistem yang dibina. Kelamahan perlulah dibaiki dalam fasa ini bagi memudahkan urusan kelak.

Perkakasan dan perisian yang diguna untuk membangunkan projek harus dipilih dengan teliti. Perkakasan dan perisian yang berfungsi sepenuhnya dengan baik dapat memberi impak dalam pelancaran membina sistem keselamtan web dinamik ini. Spesifikasi keperluan perkakas untuk sistem ini adalah sesebuah komputer. Senarai spesifikasi keperluan perkakas adalah seperti berikut:

Jadual 1 keperluan perkakasan

Perkakasan	**Penerangan**
Komputer riba	HP
Pemprosesan	Intel core i5 8th Gen
Ram	1 TB
Jenis sistem	64-bit

Seterusnya, keperluan perisian yang digunakan untuk membangunkan sistem keselamatan web dinamik yang berasaskan platform web ini hendaklah meghasilkan sistem yang boleh menyimpan data dan maklumat dengan selamat agar pengguna ada keyakinan dalam menggunakan sistem ini. Dibawah menunjukkan spesifikasi keperluan perisian yang menjadi tuntas utama dalam pembikinan projek ini.

Jadual 2 keperluan perisian

Kriteria	**Spesifikasi**

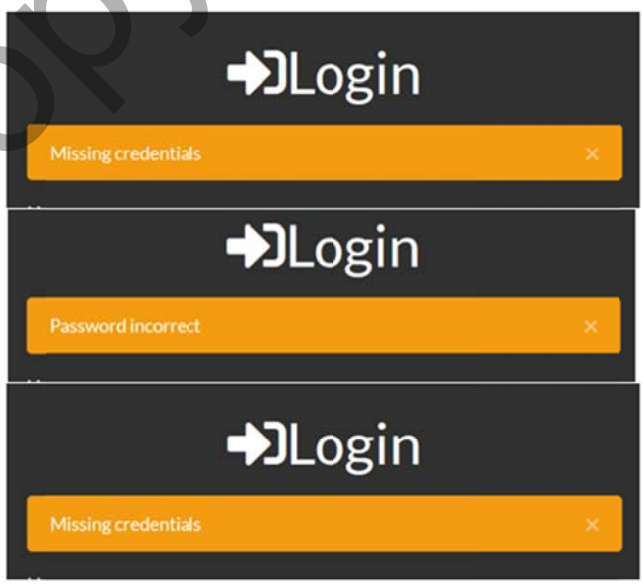
Sistem pengoerasian	Microsoft window 10
Enjin carian	Mozilla firefox
Perisian pembangunan	Sublime,Command Prompt,Nod Java Skrip
Perisian pangkalan data	MongoDB
Perisian pengujian	Vega

5 HASIL KAJIAN

Fasa ini membincangkan hasil daripada proses pembangunan yang di buat pada fasa implimentasi. Penerangan yang lebih terperinci tentang bagaimana sesuatu bahagian itu berfungsi ianya akan dijelaskan dalam bahagian ini. Fasa reka bentuk adalah fasa yang penting dalam pembangunan sesuatu projek. Dalam projek ini perisian sublime dan Nod Java Skrip adalah merupakan tunggak utama bagi melihat hasil sistem keselamatan web dinamik ini. Pengujian yang ditunjukkan adalah untuk memastikan pembangunan dihasilkan selaras dengan objektif kajian. Antara fungsi yang memainkan peranan penting untuk menjayakan projek ini berlandaskan objektif adalah fungsi *bcrypt*. Rajah – rajah dibawah menunjukkan hasil penggunaan fungsi bcrypt ke dalam sistem bagi mengekalkan keselamatan. Penggunaan bcrypt juga dapat mengelakkan suntikan yang terhasil.

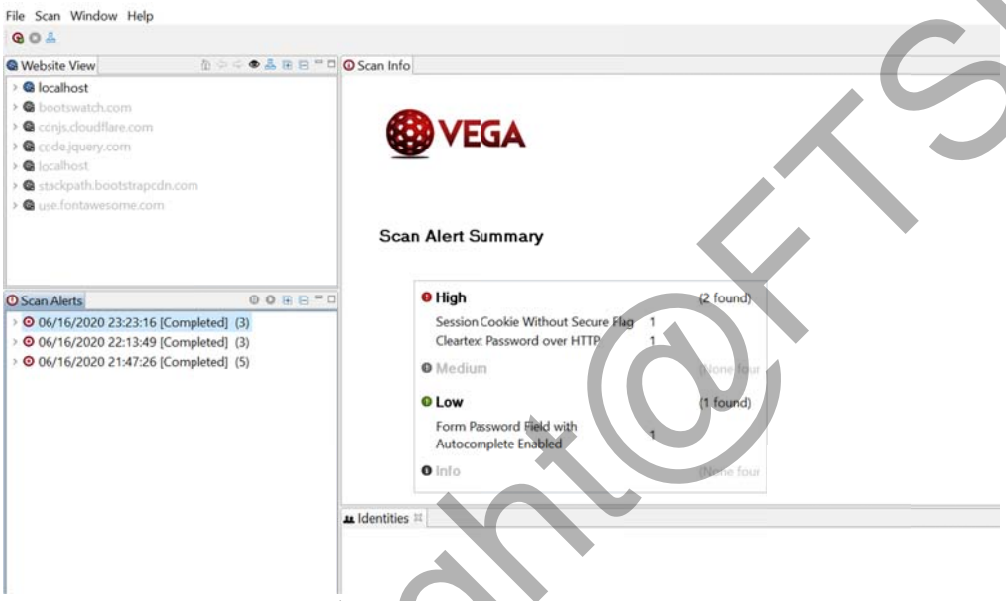

```
_id: ObjectId("5e91e3c8235d900a9cf0d1f7")
name: "nasuha"
email: "nurul@gmail.com"
password: "$2a$10$9hEalU1cGn/JjqOSPmRByOS4x2Yt.xSO.OOAIPL10QbKS3qaju.XO"
date: 2020-04-11T15:35:36.479+00:00
__v: 0
```


Rajah 2 kata laluan dapat disulitkan



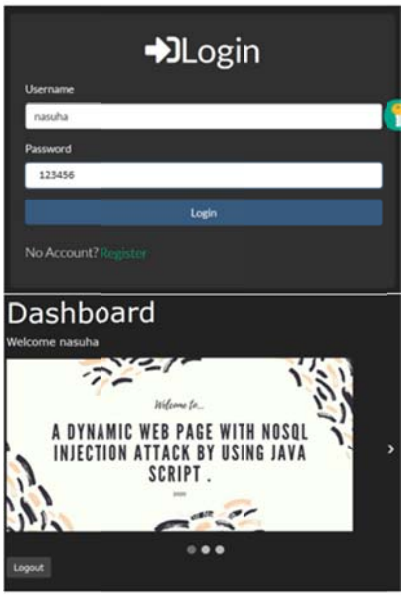
Rajah 3 halaman sistem yang ditolak selepas suntikan dijalankan

Kedua, penggunaan Vega sebagai web aplikasi imbasan menjadikannya salah satu hasil ujian yang terpenting bagi mengekalkan tahap keselamatan sistem halaman web dinamik. Rajah dibawah menunjukkan peggunaan vega bagi sistem web dinamik.



Rajah 4 penggunaan vega

Akhir Sekali, menunjukkan halaman sistem yang berjaya di masuki pengguna tanpa dikenakan suntikan NoSQL.



Rajah 5 log masuk

6 KESIMPULAN

Sistem keselamatan halaman web dinamik ini dapat membantu menyulitkan data yang dimasuk oleh pengguna. Kemudahan ini dapat membantu masalah jenayah siber yang semakin berleluasa pada era moden ini. Ini kerana terdapatnya satu sistem yang dilengkapi dengan tahap keselamatan yang tinggi.

Penggunaan Sublime, Nod Java Skrip dan juga pangkalan data NoSQL mongoDB sebagai medium utama pembangunan projek ini yang membantu menyelesaikan masalah projek ini. Namun , akibat masalah kemahiran dalam aspek tertentu menyebabkan proses menyiapkan projek ini agak lama. Masalah yang dikenalpasti menjadi punca utama adalah penguasaan Bahasa pengaturcaraan menyebabkan pembangunan tidak dapat dikuasai sepenuhnya.

Walaupun masih terdapat kelemahan pada sistem ini, diharapkan pada masa hadapan dapat penambahbaikan sistem ini agar dapat digunakan secara meluas oleh masyarakat.

7 Rujukan

Boyu Hou. (2016). Article from IEEE MongoDB NoSQL Injection Analysis and Detection. Department of CS Pace University New York, USA ltao@pace.edu Jigang

Liu Department of ICS Metropolitan State University St. Paul, MN

Celeb Garling. (2012). Amazon Goes Back to the Future with 'NoSQL' Database https://www.wired.com/2012/01/amazon-dynamodb/

David L. Prowse. CompTIA Security+ SY0-401 Cert Guide, Deluxe Edition: Comp Security SY04 Cert .https://books.google.com.my/books?id=bv8PBAAAQBAJ&pg=PT301&lpg=PT301&dq=brute+force+attack+and+nosql+injection+same&source=bl&ots=K74ctyHwIC&sig=ACfU3U2pL-pOHk5LIjB1vQ83u45hsyUiDw&hl=en&sa=X&ved=2ahUKEwjHrvjzipjqAhWbzTgGHYP0AUIQ6AEwAnoECAwQAQ#v=onepage&q=brute%20force%20attack%20and%20nosql%20injection%20same&f=false

Dan Arias. (2018). Hashing in Action: Understanding bcrypt. https://auth0.com/blog/hashing-in-action-understanding-bcrypt/

Digicert. What is SSL,TLS,HTTPS. https://www.websecurity.digicert.com/security-topics/what-is-ssl-tls-https

Eassa, A.M., Al-Tarawneh, O.H., El-Bakry, H.M.,and Salama, A.S., (2017) NoSQL racket: a testing tool fordetecting NoSQL injection attacks in web applicationss, Int. J. Adv. Comput. Sci. Appl., 2017, vol. 8,no. 11, pp. 614–622.

Google Cloud database. Cloud BigTable. https://cloud.google.com/bigtable/

Github.(2019). Static Web Page Vs Dynamic Web App. http://pconrad-webapps.github.io/topics/webpage_vs_webapp/

Guru99. Node.js MongoDB Tutorial with Example. https://www.guru99.com/node-js-mongodb.html

Kristof kovacs. (2001). Cassandra **vs** MongoDB **vs** CouchDB **vs** Redis **vs** Riak **vs** HBase **vs** Couchbase **vs** OrientDB **vs** Aerospike **vs** Neo4j **vs** Hypertable **vs** ElasticSearch **vs** Accumulo **vs** VoltDB **vs** Scalaris **vs** RethinkDB **comparison**. https://kkovacs.eu/cassandra-vs-mongodb-vs-couchdb-vs-redis

Lucas Olivera. (2019). Everything you need to know about NoSQL databases"https://dev.to/lmolivera/everything-you-need-to-know-about-nosql-databases-3o3h#adv

ScaleGrid. (2019). 2019 Database Trends- SQL vs NoSQL Top Database ,single vs Multiple Database Use http://highscalability.com/blog/2019/3/6/2019-database-trends-sql-vs-nosql-top-

Sverre H.Huseby. (2005). Common security problems in the code of dynamic web application. Version 1.0 .http://www.webappsec.org/projects/articles/062105.shtml

Subgraph. 2014. Using the Vega Scanner. https://subgraph.com/vega/documentation/Vega-Scanner/index.en.html

Shivang. Facebook Database [Updated] – A Thorough Insight Into The Databases Used @Facebook. https://www.8bitmen.com/what-database-does-facebook-use-a-1000-feet-deep-dive/

Scott P.Randby. (2019). Dynamic and Static Website Security. Made with GNU Emacs 26.1 and org 9.2. https://srandby.org/digital-writing/index.html

Tomaz Andrzej. (2020). NoSQL Injection and How to Avoid them. https://www.acunetix.com/blog/web-security-zone/nosql-injections/

Uladzislau Murashka. (2019).Vega https://www.scanforsecurity.com/scanners/vega.html