KAJIAN KERENTANAN WEB DAN PENGUJIAN TEMBOK API APLIKASI WEB DALAM MELINDUNGI APLIKASI WEB RENTAN

Sharifah Aminah binti Said Mohamed

Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Aplikasi web rentan merupakan aplikasi web yang mempunyai kerentanan. Kerentanan web ini boleh menyebakkan aplikasi web diserang oleh orang yang berniat hasad. Akibat daripada serangan itu, pelbagai informasi dan maklumat sensitif daripada aplikasi web terdedah kepada pihak yang tidak bertanggungjawab. Tembok api aplikasi web bertanggungjawab dalam memainkan peranan melindungi aplikasi web daripada diserang oleh pihak luar. Kajian tentang kerentanan-kerentanan web yang paling popular telah dijalankan melalui pembacaan. Antara kerentanan web yang kerap terjadi ialah suntikan SQL, penskripan tapak silang, tatarajah salah sekuriti, pengesahan putus dan pengurusan sesi, rujukan objek secara langsung yang tidak selamat, permintaan palsu tapak silang, simpanan kriptografi tidak selamat, kegagalan untuk menyekat akses URL, perlindungan lapisan pengangkutan yang tidak mencukupi, dan ubah hala dan perantaian ke depan yang tidak selamat. Tembok api aplikasi web daripada sumber terbuka iaitu *Mod Security* dan *Shadow Daemon* telah dipilih untuk dilakukan pengujian dan perbandingan daripada segi peraturan, pemasangan dan penyediaan. Hasil daripada projek ini, ujian penembusan telah dilakukan dalam dua fasa. Antara ujian penembusan yang dilakukan ialah suntikan SQL, penskripan tapak silang, memuat naik fail, eksploitasi FTP dan akses pintu belakang. Tembok api *Mod Security* juga telah berjaya diuji untuk melindungi aplikasi web rentan melalui ujian penembusan.

1. PENGENALAN

- Situasi kebocoran maklumat adalah maklumat penting atau maklumat peribadi telah terbocor secara tidak sengaja kepada penggodam. Penggodam boleh menyalah gunakan maklumat pengguna web aplikasi untuk kepentingan peribadi kita (Joe,2018). Contohnya, laman web bank palsu yang seakan-akan laman web bank yang sebenar. Penggodam akan menggunakan laman web itu untuk memancing pengguna

menggunakan laman web itu. Apabila pengguna memasukkan nama pengguna dan kata laluan mereka, penggodam akan menggunakan maklumat itu untuk menggodam akaun bank kita.

- Pada 20 Julai 2018, BBC News telah menulis berita tentang data peribadi rakyat Singapura hampir sebanyak 1.5 juta telah berjaya dicuri oleh penggodam. Data mereka dicuri melalui sistem Kesihatan Singapura. Bahkan, rekod kesihatan Perdana Menteri Singapura iaitu Mr Lee juga telah didedahkan kepada pihak umum. Mr Lee dikatakan telah dikatakan berjaya selamat daripada penyakit kanser selama 2 kali. Sistem kesihatan Singapura telah bocor kerana salah satu komputer kepunyaan SingHealth telah dijangkiti *malware* yang dihantar oleh penggodam (BBC,2018).

2. PENYATAAN MASALAH

- Organisasi yang menyediakan perkhidmatan web aplikasi seharusnya menggunakan tembok aplikasi web untuk menjaga dan melindungi keselamatan web aplikasi mereka. Hal ini demikian kerana, penggodam akan lebih mudah menggodam web aplikasi jika web aplikasi tidak ditambah perlindungan. Apabila web aplikasi mereka digodam oleh penggodam, penggodam akan dapat melihat segala data-data dan menggunakan maklumat-maklumat penting atau rahsia yang diakses daripada web aplikasi organisasi untuk kepentingan mereka.
- Ter pelbagai tembok api sumber terbuka dan komersial. Namun begitu, tembok api komersial adalah mahal dan perusahaan-perusahaan kecil dan atau sederhana (SME) tidak mampu membelinya. Manakala, tembok api jenis terbuka pula walaupun percuma adalah lebih sukar untuk persediaan(*setup*) dan dikonfigurasikan. Kefungsian untuk setiap tembok api terbuka pula adalah berbeza dan berlainan. Bahkan garis panduan untuk melaksana(*implement*) setiap tembok api juga sangat terhad

3. PENYELESAIAN MASALAH

- Tembok api aplikasi web adalah satu perisian yang akan berada di antara web pelanggan (*client web*) dan pelayan web (*web server*). Tembok api aplikasi web menggunakan peraturan (*rules*) tertentu yang digunakan dalam perbualan protokol HTTP (Lawrence Koved dan Lin Luo 2016).
- Tujuan tembok api aplikasi web ini adalah mengawal laluan keluar masuk trafik antara web aplikasi dan Internet, melindungi web aplikasi daripada serangan berniat jahat dan

memastikan maklumat yang dimasukkan pengguna selamat daripada ancaman luar dan lain-lain (Rezaduty, 2019). Berdasarkan peraturan-peraturan tertentu yang dilaksanakan dalam tembok api aplikasi web, tembok api akan menolak kemasukan kepada tetamu yang tidak memenuhi peraturan dan melaksanakan laluan trafik yang pernah disahkan.

- Seterusnya, saya bercadang untuk mengkaji dan melakukan perbandingan antara beberapa tembok api aplikasi web(WAF) daripada segi garis panduan, konfigurasi, pemasangan (*installation*), penetapan (*setting-up*), kefungsian dan mesra pengguna.

4. OBJEKTIF

Antara objektif projek Tembok api Aplikasi Web ini ialah:

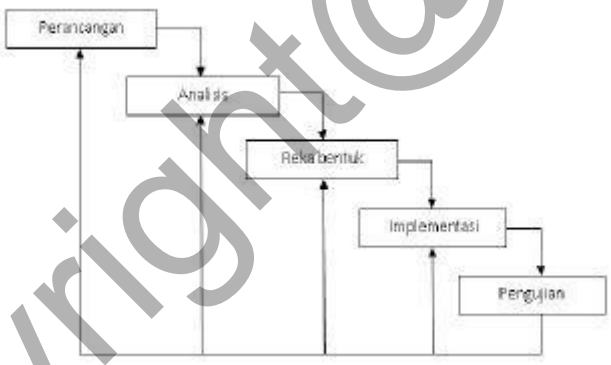
i. Memahami dan mengkaji pelbagai jenis ancaman kerentanan sistem aplikasi web.

ii. Melakukan perbandingan antara tembok api aplikasi web daripada sumber terbuka.

iii. Melakukan pengujian terhadap fungsi tembok api aplikasi web daripada sumber terbuka.

5. METODOLOGI

Kaedah pembangunan yang akan digunakan untuk menjayakan projek Tembok api Aplikasi Web ini ialah Model Air Terjun. Pemilihan model Air Terjun adalah disebabkan setiap fasa akan dilakukan mengikut turutan. Selain itu, model ini lebih mudah digunakan untuk memantau perkembangan projek dari semasa ke semasa. Rajah 1.1 ini menggambarkan carta alir metodologi mengikut fasa.



Rajah 1.1 Metodologi

i. Fasa Perancangan

Fasa Perancangan merupakan fasa yang pertama dan penting dalam mengkaji dan melakukan pengujian terhadap tembok api aplikasi web daripada sumber terbuka ini. Dalam Fasa Perancangan ini, kajian awal akan dilakukan melalui perancangan rangkaian maya(*virtual network*). Selain itu, faktor-faktor serangan aplikasi web juga akan dikaji.

ii. Fasa Analisis

Selepas Fasa Perancangan, Fasa Analisis ini akan digunakan untuk menganalisis latar belakang dan fungsi tembok api aplikasi web. Kerentanan-kerentanan web yang paling kerap dan popular turut akan dianalisis.

iii. Fasa Reka bentuk

Fasa Rekabentuk adalah proses reka bentuk untuk sesuatu sistem atau aplikasi. Pada fasa ini, rangkaian maya akan dibina dalam aplikasi kotak maya(*virtual box*). Kotak maya VMWare akan digunakan untuk pemasangan sistem operasi, pelayan web, dan aplikasi-aplikasi yang berkaitan dengan pengujian tembok api aplikasi web sumber terbuka. Sistem operasi sistem yang akan digunakan ialah *Kali Linux*, manakala pelayar web pula ialah *Metasploitable*.

iv. Fasa Implementasi

Dua tembok api aplikasi web sumber terbuka akan diimplementasikan dalam aplikasi web yang terdapat beberapa kerentanan dan mudah terdedah kepada serangan internet. Peraturan-peraturan akan diletakkan dalam tembok api untuk menentukan langkah keselamatan meenghadapi serangan internet disebabkan kerentan-kerentanan yang terdapat pada aplikasi web tersebut. Perbandingan dan penambahbaikan akan dilakukan dalam fasa ini juga. Fasa implementasi ini akan melibatkan pemasangan aplikasi web yang mempunyai kerentanan pada pelayan web. Ujian penembusan peringkat pertama akan dilakukan terhadap aplikasi web rentan tersebut.

v. Fasa Pengujian

Fasa ini merupakan fasa web aplikasi yang telah dipasang tembok api akan diuji. Pada fasa ini, kedua-dua tembok api aplikasi web ini akan dipasang pada aplikasi web tersebut. Ujian penembusan peringkat 2 akan dilakukan untuk menguji keberkesanan dan kecekapan tembok api aplikasi web dalam melindungi aplikasi web rentan tersebut daripada serangan

6. Hasil Kajian

- Kerentanan-kerentanan web yang paling kerap terjadi telah dikenalpasti iaitu suntikan SQL, penskripan tapak silang, tatarajah salah sekuriti, pengesahan putus dan pengurusan sesi, rujukan objek secara langsung yang tidak selamat, permintaan palsu tapak silang, simpanan kriptografi tidak selamat, kegagalan untuk menyekat akses URL, perlindungan lapisan pengangkutan yang tidak mencukupi, dan ubah hala dan perantaian ke depan yang tidak selamat.
- Kemahiran ujian penembusan seperti suntikan SQL, penskripan tapak silang, memuat naik fail, eksploitasi FTP dan akses pintu belakang.
- Tembok api aplikasi web iaitu *Mod Security* telah berjaya dipasang, disediakan dan diuji keberkesannya dalam melindungi aplikasi web rentan.

7. Kesimpulan

Kesimpulannya, melalui projek ini saya telah mempelajari pelbagai jenis kerentanan aplikasi web. Kerentanan-kerentanan web itu akan menyebabkan aplikasi web mudah diserang oleh penyerang yang berniat buruk. Akibat daripada serangan itu, kebocoran maklumat-maklumat sensitif boleh terjadi. Selain itu, saya juga dapat mempelajari kemahiran ujian penembusan yang menggunakan Kali Linux. Antara ujian penembusan yang saya telah pelajari ialah akses pintu belakang, suntikan SQL, dan penskripan tapak silang. Saya juga telah memasang, menyediakan, dan menguji keberkesanan perlindungan yang disediakan oleh *Mod Security*.

RUJUKAN

Aaron O'Keeffe, A. 2017. Host-Based vs Network-Based Firewalls https://www.aussiebroadband.com.au/blog/host-based-vs-network-based firewalls/?fromwideband [20 Oktober 2019]

Anon, 2019. What are Cloud Firewalls https://www.barracuda.com/glossary/cloud-firewall. [20Oktober 2019]

Anon, 2018. Singapore personal data hack hits 1.5m, health authority says https://www.bbc.com/news/world-asia-44900507 [3 Oktober 2019]

Anon, 2019. What is a Firewall? https://www.cloudflare.com/learning/security/what-is-a-firewall/ [5 Disember 2019]

Anon, 2016. 5 Open Source Web Application Firewall for Better Security. https://geekflare.com/open-source-web-application-firewall [20 Oktober 2019]

Anon, 2019. Pentration Testing https://www.imperva.com/learn/application-security/penetration-testing/ [5 Disember 2019]

Anon. What is a Trojan Virus? https://www.kaspersky.com/resource-center/threats/trojans [3 Oktober 2019]

Anon, 2019. What Can ModSecurity Do? https://www.modsecurity.org/about.html [3 Oktober 2019]

Anon, 2019. ModSevurity Evaluation Framework https://www.owasp.org/index.php/OWASP_ModSecurity_rule_evaluation_framework [5 Disember 2019]

Anon, 2019. Introduction
https://shadowd.zecure.org/overview/introduction/ [20 Oktober 2019]

Anon, 2019 Malaysia Airlines warns of fake websites
https://www.thestar.com.my/business/business-news/2019/01/14/malaysia-airlines-warns-of-fake-websites/ [3 Oktober 2019]

Anon (n.d.). About ModeSecurity
https://www.modsecurity.org/about.html [20 Oktober 2019]

Anon, 2015. Web Application Firewall.
https://vulnerablelife.wordpress.com/tag/web-application-firewall/ [20 Oktober 2019]

Fruhlinger, J. 2019 .What is a Trojan horse? How this tricky malware works
https://www.csoonline.com/article/3403381/what-is-a-trojan-horse-how-this-tricky-malware-works.html [3 Oktober 2019]

Joe, 2018 What Is Information Leakage ?
https://affinity-it-security.com/what-is-information-leakage/ [20 Oktober 2019]

Kashefi, Iman & Kassiri, Maryam & Shahidinejad, Ali. 2013. A Survey on Security Issues in Tembok apis: A New Approach for Classifying Tembok api Vulnerabilities. International Journal of Engineering Research and Applications (IJERA) 2248-9622. 3. 585-591. [3 Oktober 2019]

Koved, L., & Luo, L. (2016). U.S. Patent No. 9,473,457. Washington, DC: U.S. Patent and Trademark Office

Ortega, J., 2017. What is a Website Vulnerability and How Can it be Exploited?
https://www.sitelock.com/blog/what-is-a-website-vulnerability/ [5 Disember 2019]

Prasanthi Eati. 2019. 10 Most Common Web Security Vulnerabilities https://www.guru99.com/web-security-vulnerabilities.html [20 Oktober 2019]

Rezaduty. 2019. Complete Web Application Firewall Guide https://medium.com/schkn/web-application-firewall-guide-125645343beb [5 Disember 2019]

Rouse, M., & Bacon, M. 2019. What is a Web Application Firewall? - Definition from WhatIs.com https://searchsecurity.techtarget.com/definition/Web-application-firewall-WAF [20 Oktober 2019]