ANALISIS KEAMANAN APLIKASI WEB MENGGUNAKAN ZAP

Yuswandi
Program Studi Informatika Fakultas Ilmu Komputer dan Multimedia
Universitas Islam Kebangsaan Indonesia (UNIKI) Aceh
yuswandi.mmsi@gmail.com

ABSTRAK

Ketangguhan maupun keamanan sebuah aplikasi berbasis pada web serta keamanan pada jaringannya harus benar-benar aman dan lulus dari tahap pengujian sebelum aplikasi tersebut disebarkan dan digunakan. Keamanan sebuah aplikasi berbasis web bisa dinilai dengan cara melakukan percobaan penetrasi atau penerobosan terhadap aplikasi web dimaksud, baik secara manual atau otomatis menggunakan alat bantu seperti perangkat lunak scanning. Penelitian ini berfokus pada penelusuran untuk menemukan celah atau kerentanan keamanan yang ada pada sebuah aplikasi berbasis web. Adapun objek yang menjadi sasaran dalam penelitian ini adalah aplikasi web sistem informasi toko komputer R-Komputer (tokokomputerku.com). Percobaan penetrasi yang dilakukan sebagai simulasi dalam penelitian ini dijalankan dengan menggunakan sebuah perangkat lunak khusus untuk analisa kerentanan keamanan web yang bernama Zed Attack Proxy (ZAP). Perangkat lunak ini memindai setiap komponen dalam aplikasi web tersebut dan kemudian mengumpulkan informasi tentang celah keamanan yang berhasil ditemukan. Semua informasi tentang celah keamanan yang berhasil dikumpulkan kemudian dibagi menjadi empat tingkatan, yaitu High, Medium, Low dan Informational. Hasil penelitian ini adalah rekomendasi atau saran perbaikan untuk menutup celah atau kerentanan keamanan yang berhasil ditemukan untuk peningkatan keamanan aplikasi web tersebut.

Kata Kunci: Keamanan, Scanning, Aplikasi, Web, ZAP

PENDAHULUAN

Bisnis jual beli secara online saat ini telah berkembang demikian cepat dan maju. Era perkembangan teknologi internet yang semakin pesat dewasa ini membuat persaingan bisnis dalam bidang apapun menjadi lebih variatif. Toko fisik kini dituntut agar berbenah untuk menawarkan produk yang dapat diakses konsumen secara online guna meningkatkan pelayanan agar tidak kalah oleh layanan serupa yang ditawarkan oleh toko online yang semakin digemari.

Dalam menjalankan dan mengelola bisnis penjualan yang semakin kompleks dan rumit ditengah ketatnya persaingan, maka sudah tentu dibutuhkan sebuah sistem informasi yang siap pakai, mudah diakses, dan handal guna menunjang pencapaian target dan kesuksesan usaha yang dijalankan tersebut. Dengan dorongan tuntutan keadaan yang demikian hingga akhirnya memunculkan ide pengembangan sebuah sistem informasi guna memenuhi kebutuhan tersebut. Maka oleh karena itu diwujudkanlah sebuah aplikasi web sistem informasi took komputer yang mencakup sistem pembelian, penjualan, stok, servis, kustomer, aliran kas, hingga sampai pada penggajian karyawan. Aplikasi web sistem informasi toko komputer tersebut telah diterapkan pada unit usaha toko komputer R-Komputer Lhokseumawe.

Sifat aplikasi berbasis web online yang bisa diakses kapan saja, dari mana saja, dan oleh siapa saja selain sangat memudahkan pengguna tentunya juga menjadi faktor utama terbukanya peluang terjadinya serangan atau penyusupan dari siapapun yang tidak bertanggung jawab yang dapat berakibat pada pencurian data dan informasi juga kerusakan pada aplikasi web tersebut.

Bentuk serangan paling umum yang terjadi pada sebuah aplikasi web yaitu, Malware, Penetration Testing, SQL Injection dan sebagainya. Penyebab semua kerentanan yang teridentifikasi dalam aplikasi web, masalahnya disebabkan oleh input yang tidak diperiksa

yang diakui sebagai yang paling umum. Berdasarkan data terbaru tahun 2022 dari WPScan, jumlah kerentanan baru yang ditemukan telah meningkat dalam beberapa tahun terakhir. Sampai tahun 2021, lebih dari 5600 kerentanan baru telah ditemukan. Kemudian ada tambahan lebih dari 78 kerentanan baru telah ditemukan pada tahun 2022.

Maka dari itu, penelitian ini dikhususkan dan dibatasi dengan tujuan untuk mendapatkan informasi tentang celah atau kerentanan keamanan pada aplikasi web yang menjadi sasaran. Adapun teknik yang dipakai dalam penelitian ini bersifat otomatis dengan menggunakan sebuah perangkat lunak khusus untuk analisa kerentanan keamanan web yang bernama Zed Attack Proxy (ZAP) yang dibuat oleh organisasi nirlaba dalam bidang jasa keamanan web yang bernama OWASP. Sebagai hasil dari penelitian ini adalah saran dan rekomendasi perbaikan untuk menutup celah atau kerentanan keamanan tersebut yang berguna sebagai solusi untuk peningkatan ketangguhan dan keamanan aplikasi web tersebut pada masa yang akan datang.

METODE PENELITIAN

Penulis dalam penelitian mendapatkan data-data yang dibutuhkan dengan cara studi literatur, yaitu data dihasilkan dari studi kepustakaan dengan pencarian pada sistus-situs internet, jurnal-jurnal yang membahas tema yang serupa, dan juga buku-buku digital yang sesuai dengan tema dan tujuan penelitian ini. Metode berikutnya adalah observasi langsung, yaitu mendapatkan data-data dengan melihat dan mencatat segala aktivitas aplikasi web tersebut yang khusus berhubungan dengan penelitian ini. Perangkat yang dipakai dalam penelitian ini berupa perangkat keras (hardware) dan juga perangkat lunak (software). Selengkaptnya adalah sebagai berikut:

Perangkat Keras (Hardware); Satu unit komputer laptop yang terinstal dua sistem operasi yang difungsikan sebagai penyerang dengan detail sebagai berikut:

1. Laptop MacBook Air 2014,
2. Processor Intel® Core™ i7-5650U CPU @ 2.20GHz,
3. RAM 8.00 GB,
4. Harddisk SSD 500GB.

Perangkat Lunak (Software); Yaitu semua program atau perangkat lunak yang terpasang dalam komputer laptop tersebut yang dijalankan untuk melakukan pengujian dalam penelitian ini adalah sebagai berikut:

1. Sistem Operasi MacOS Catalina dan Windows 10 Pro 64-bit, x64-based processor,
2. Zed Attack Proxy (ZAP) versi 2.11.1.

HASIL DAN PEMBAHASAN

Setelah data dan informasi perangkat sasaran diketahui, maka tahapan selanjutnya adalah proses pemindaian (scanning) untuk mencari dan menemukan segala kerentanan yang ada dalam aplikasi web tokokomputerku.com yang dilakukan dengan menggunakan perangkat lunak ZAP versi 2.11.1. Tahapan ini telah dijalankan pada tanggal 18 Januari 2022. Proses awal tahapan pemindaian memperlihatkan progress kemajuan proses pemindaian disertai dengan alamat URL atau file yang sedang diperiksa.

Proses pemindaian selesai dalam waktu sekitar 15 sampai 20 menit dan menghasilkan laporan bahwa ditemukan total sejumlah 32 celah bahaya, yaitu dengan 13 celah tingkat menengah (Medium), 14 celah tingkat rendah (Low), 5 yang bersifat informasi (Informational), dan tidak ada celah tingkat tinggi (High). maka didapatkan jumlah persentase tingkat celah bahaya keamanan pada aplikasi web tokokomputerku.com adalah terlihat bahwa persentase jumlah celah paling besar yang ditemukan adalah 44 persen yaitu untuk bahaya tingkat rendah (Low),

kemudian jumlah celah terbesar kedua yaitu 40 persen untuk bahaya tingkat menengah (Medium), diikuti oleh bahaya tingkat rendah Low) sebesar 16 persen, dan 0 persen untuk bahaya tingkat tinggi (High).

Kemudian dari penemuan jumlah celah bahaya tersebut dapat diperincikan lagi berdasarkan jenis celah bahaya yang ditemukan, yaitu bahwa jenis celah bahaya terbanyak yang ditemukan adalah Directory Browsing yaitu sebesar 34,4 persen, kemudian X-Content-Type-Options Header Missing sebesar 31,2 persen, *Information Disclosure-Suspicious Comments* sebesar 15,6 persen, dan diikuti oleh jenis X-Frame-Options Header Not Set, Absence of Anti-CSRF Tokens, dan Cookie without SameSite Attribute masing-masing sebesar 6,2 persen.

Informasi di atas juga dapat diperincikan lagi sampai terlihat jelas lokasi tempat dimana celah bahaya yang ditemukan berada, yaitu bahwa jenis celah bahaya *Directory Browsing* terletak pada lokasi directory assets, sedangkan untuk jenis X-Frame-Options Header Not Set terletak pada top-level domain https://tokokomputerku.com. Perincian jenis celah bahaya Information Disclosure-Supicious Comments, memperlihatkan celah kerentanan terdapat dalam 3 buah file javascript yang berektensi .js yang terletak didalam directory assets/js, assets/vendor/bootstrap/js, dan juga directory assets/vendor/jquery/jquery.min.js. Perincian jenis celah bahaya Absence of Anti-CSRF Tokens, Cookie without SameSite Attribute, dan X-Content-Type-Options Header Missing; memperlihatkan jenis celah Absence of Anti-CSRF Tokens dan Cookie without SameSite Attribute terletak pada top-level domain, dan untuk jenis celah X-Content-Type-Options Header Missing selain juga ada pada top-level domain, sebagian besar ada dalam directory assets.

PENUTUP

Setelah melalui serangkaian pemindaian pada aplikasi web tokokomputerku.com, dapat disimpulkan bahwa penelitian ini telah berhasil dan sukses menemukan celah atau kerentanan keamanan dan kelemahan dalam aplikasi web tersebut dengan tingkat bahaya menengah (Medium). Celah kritis utama yang ditemukan adalah pada sistem directory browsing, dimana siapapun bisa membuka dan melihat isi directory yang seharusnya hanya bisa dilihat oleh superuser (root). Kelemahan ini bisa dengan mudah dieksploitasi hanya dengan cara mengetikkan alamat atau lokasi directory tersebut berada pada web browser.

Sebagai saran yaitu perlu adanya penambahan baris script khusus (Options -Indexes) dalam file. htaccess yang berfungsi sebagai penutup akses menuju directory tersebut. Kemudian perbaikan untuk jenis kerentanan X-Content-Type-Options Header Missing juga dengan cara penambahan baris script khusus yaitu (header ("X-Frame-Options: DENY")) dalam file index.php yang terletak pada root directory. Saran lainnya adalah agar dilanjutkan dengan melakukan pengujian menggunakan metode-metode pengujian lainnya yang lebih baik dan efektif.

DAFTAR PUSTAKA

Barry Buzan, Lenen Hansen, 2009. *The Evolution of International Security Studies,* United Kingdom: Cambridge University Press, 2009.

Gordon B Davis, 2013. *Kerangka Dasar Sistem Informasi Manajemen*, Palembang: Maxikom.

Richardus Eko Indrajit, Konsep Dasar Sistem dan Teknologi Informasi. Koleksi Pustaka, *The Preinexus,* 26 September 2016.

Akhyar Lubis, Avinanta Tarigan, Security Assessment of Web Application Through Penetration System Techniques. *International Journal of Recent Trends in*

Engineering & Research (IJRTER), Volume 03, Issue 01, January 2017, ISSN (Online): 2455-1457, @IJRTER, 2017.

Ankita Gupta, Kavita, Kirandeep Kaur. Vulnerability Assessment and Penetration Testing. *Computer Science Department, PEC University of Technology, India. Electronics and Electrical Communication Department, PEC University of Technology, India. IJETT,* Vol 4 Issue 3-2013.

Hiroyuki Okamura, Masataka Tokuzane, Tadashi Dohi, Optimal Security Patch Release Timing under Non-homogeneous Vulnerability-Discovery Processes. *Researchgate*, 120-128. 10.1109/ISSRE. 2009.19, 2009.

Jai Narayan Goel, BM Mehtre, Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. *Elsevier B.V., Science Direct, Procedia Computer Science*, 57 710-715, 2015.

T. Pandikumar, Tseday Eshetu, Detecting Web Application Vulnerability using Dynamic Analysis with Penetration Testing. *International Research Journal of Engineering andTechnology (IRJET)*, e-ISSN: 2395-0056, p-ISSN: 2395- 0072, Volume: 03 Issue: 10 | Oct-2016, www.irjet.net, 2016.

URL: https://owasp.org/, 18 Januari 2022.

URL: https://www.w3.org/People/Frystyk/thesis/WWW.html, 18 Januari 2022.

URL: https://www.w3.org/Submission/wadl/#x3-20001.1, 18 Januari 2022.

URL:https://wpscan.com/statistics?cf_chl_f_tk=xJNZpo526InlD.YvroUTvBONaoAaDUuElAbaqX._zGU-1642484044-0-gaNycGzNCNE, 18 Januari 2022.