eProceeding of TIK
E-ISSN: 2797-1724, P-ISSN: 3031-1454
Vol. 6 No. 1 2026 pp. 01-08

Analisis Kerentanan dan Kelemahan Keamanan Content Delivery Network (CDN) Terhadap Serangan SQL Injection Menggunakan Metode Vulnerability Assesment (VA)

Arya Saputra[1], Husaini[2*], Hari Toha Hidayat[3]

[1,2,3] Jurusan Teknologi Informasi dan Komputer, Politeknik Negeri Lhokseumawe, Indonesia

*Penulis Korespondensi: husaini@pnl.ac.id

Abstrak

Kemajuan pesat teknologi internet telah secara signifikan meningkatkan kebutuhan akan bandwidth untuk website, sehingga menyebabkan overload pada server dan penurunan kualitas layanan. Untuk mengatasi tantangan ini, teknologi Content Delivery Network (CDN) digunakan untuk mengoptimalkan kinerja website dan meningkatkan keamanan. Penelitian ini bertujuan untuk menganalisis kerentanan CDN terhadap serangan SQL Injection menggunakan metode Vulnerability Assessment (VA). Pengujian dilakukan pada 4 website menggunakan alat Acunetix Web Vulnerability Scanner dan SQLMap. Temuan menunjukkan tingkat keamanan yang bervariasi, dengan persentase keamanan antara 83,5% dan 100%. Meskipun CDN membantu meringankan beban server, kerentanan aplikasi web tetap dapat dieksploitasi oleh beberapa jenis serangan jika tidak dilindungi dengan benar. Meskipun serangan SQL Injection tidak terdeteksi dalam semua kasus, risiko yang ditimbulkan oleh direktori yang tidak terlindungi, file sensitif, dan informasi yang terekspos menyoroti pentingnya langkah-langkah keamanan yang menyeluruh. Penelitian ini menekankan kebutuhan penting bagi pengembang dan administrator web untuk meningkatkan protokol keamanan CDN, di luar perlindungan dasar dari Distributed Denial of Service (DDoS), guna melindungi dari ancaman siber yang terus berkembang. Penelitian ini memberikan wawasan berharga untuk meningkatkan pertahanan aplikasi web dan memastikan sistem CDN dikonfigurasi secara efektif untuk melindungi data pengguna serta fungsi keseluruhan website.

Kata kunci: content delivery network, SQL injection, vulnerability assessment, Cloudflare, Acunetix

1. Pendahuluan

Kemajuan internet yang pesat membawa manfaat besar dalam mencari informasi dan berkomunikasi, namun juga menyebabkan kebutuhan bandwidth meningkat sehingga server dapat mengalami overload dan menurunkan kualitas layanan. Untuk itu, diperlukan sistem yang dapat meningkatkan kualitas server agar memenuhi kebutuhan pengguna. Selain itu, keamanan website sangat penting untuk melindungi situs web dari ancaman siber, menjaga kelangsungan fungsi, serta melindungi data sensitif, privasi pengguna, dan reputasi pemilik website.

Salah satu ancaman keamanan yang sering dihadapi aplikasi web dengan CDN adalah serangan SQL Injection, yang dapat menyebabkan kebocoran data, pengambilalihan kontrol database, atau kerusakan sistem. Meskipun CDN dapat menyaring lalu lintas berbahaya, kelemahan pada aplikasi web tetap dapat dieksploitasi. Oleh karena itu, penilaian kerentanan sangat penting untuk mengidentifikasi dan mengevaluasi potensi kelemahan keamanan.

Penelitian ini bertujuan untuk menganalisis kerentanan keamanan CDN terhadap serangan SQL Injection menggunakan metode Vulnerability Assessment (VA). Penelitian ini akan mengevaluasi efektivitas CDN dalam melindungi aplikasi web serta mengidentifikasi area yang perlu diperbaiki. Hasilnya diharapkan dapat memberikan wawasan mendalam tentang keamanan CDN serta panduan bagi pengembang dan administrator web untuk meningkatkan perlindungan terhadap ancaman siber.

A. Content Delivery Network (CDN)

CDN adalah sistem server yang terhubung, di mana setiap server yang berfungsi sebagai pengganti memiliki salinan data dari server utama. Ini memungkinkan data yang diminta oleh pengguna saat mengunjungi sebuah situs web disampaikan tidak langsung dari server pusat, tetapi melalui server CDN yang paling dekat dengan pengguna tersebut [1].

CDN bekerja dengan menyimpan salinan konten web di server yang tersebar di berbagai lokasi. Saat pengguna mengakses konten, CDN mengarahkan mereka ke server terdekat, sehingga mempercepat pengiriman dan mengurangi waktu respons. Web atau aplikasi memiliki server pusat yang menyimpan data, dan saat pengguna mengaksesnya, komputer mereka mengirim permintaan ke server pusat, yang kemudian memprosesnya dan mengirimkan data yang diminta, seperti halaman web, video, atau gambar.

Proses permintaan dan pengiriman data membutuhkan waktu, dan kecepatannya dipengaruhi oleh beberapa faktor, termasuk jarak antara server dan perangkat pengguna. Semakin besar jarak tersebut, semakin lama waktu yang dibutuhkan. Oleh karena itu, untuk meningkatkan kecepatan akses dari berbagai lokasi di seluruh dunia, diperlukan server tambahan yang tersebar di berbagai wilayah. Server ini dikenal sebagai CDN (Content Delivery Network), yang menyimpan salinan data dari server utama. Ketika pengguna mengakses situs web, CDN terdekat akan menyediakan data, sehingga proses akses menjadi lebih cepat dibandingkan dengan jika data dikirim langsung dari server utama.

Cloudflare adalah salah satu CDN (Content Delivery Network) yang dapat membuat situs web lebih cepat. Fungsi utama CDN adalah untuk menjaga situs web, pertahanan pertama melawan serangan hacker, serangan DDoS, serta perlindungan dari ancaman lain. Cloudflare memiliki beberapa server di seluruh dunia [2].

B. Website

Website adalah salah satu bentuk media informasi di internet. Selain berfungsi sebagai sarana penyebaran informasi, website juga dapat digunakan untuk berbagai tujuan, termasuk membangun toko online. Sebuah website terdiri dari berbagai halaman yang biasanya tergabung dalam satu domain atau subdomain. Semua ini berada di World Wide Web (WWW) di internet [3].

Website adalah platform di internet yang menghubungkan berbagai dokumen, yang disebut webpage, melalui tautan (hypertext). Link ini dapat menghubungkan halaman di server yang sama atau berbeda di seluruh dunia, dan dapat diakses melalui browser web seperti Google Chrome atau Mozilla Firefox. Website dihosting di server web dan diakses melalui URL, dengan domain sebagai identifikasi alamat. Website bisa berupa situs statis, dengan konten tetap, atau dinamis, dengan konten yang diperbarui secara otomatis. Dengan kemajuan teknologi, website juga dapat berfungsi sebagai aplikasi web interaktif yang lebih kompleks.

C. Cloudflare

Cloudflare adalah perusahaan yang menyediakan layanan keamanan dan kinerja web, seperti DNS, proteksi DDoS, dan CDN untuk mempercepat waktu pemuatan situs web. Cloudflare bertindak sebagai proxy yang menghubungkan website dengan pengunjung, sehingga mempercepat loading dan meningkatkan keamanan website.

Cloudflare merupakan jaringan untuk pengiriman konten, di mana jaringan Cloudflare berperan sebagai proxy untuk menghubungkan website dengan pengunjung. Dengan kata lain, CloudFlare berperan sebagai penghubung antara server website dan pengunjung. Banyak orang tertarik untuk menggunakan CloudFlare karena bisa menjadikan loading website lebih cepat dan juga meningkatkan keamanan sebuah website [4].

Fitur utama Cloudflare adalah firewall aplikasi web (WAF) yang memantau lalu lintas dan mencegah ancaman sebelum mencapai server aslinya. Cloudflare juga mengoptimalkan kinerja melalui kompresi data, caching konten, dan manajemen lalu lintas, serta menyediakan layanan DNS yang cepat dan aman. Secara keseluruhan, Cloudflare meningkatkan keamanan, kecepatan, dan keandalan layanan situs web, sehingga membantu perusahaan mengurangi biaya operasional dan memberikan pengalaman pengguna yang lebih baik.

D. Hosting dan Domain

Hosting adalah layanan internet yang menyediakan sumber daya server untuk disewakan, sehingga memungkinkan organisasi atau individu menempatkan informasi di internet dalam berbagai bentuk, seperti HTTP, FTP, EMAIL, atau DNS. Hosting melibatkan penyimpanan file dan data situs web di server yang terhubung ke internet, dengan penyedia hosting yang menawarkan ruang server, bandwidth, keamanan, serta dukungan teknis. Tipe hosting bervariasi dari shared hosting, di mana beberapa situs berbagi sumber daya, hingga dedicated hosting untuk satu situs. Layanan tambahan seperti manajemen database dan pemantauan kinerja juga tersedia, sehingga memudahkan pemilik situs untuk fokus pada pengembangan konten. Sementara itu, domain adalah alamat unik yang mengidentifikasi sumber daya di internet, seperti "example.com" dalam alamat www.example.com.

Hosting merupakan tempat penyimpanan data website dimana didalamnya meliputi kapasitas penyimpanan, bandwith yang merupakan sebuah kapasitas yang di gunakan untuk mengukur jumlah pengunjung website serta database [5].

Domain merupakan sebuah string pengenal yang digunakan untuk mengidentifikasi sebuah server seperti webserver atau mail server pada sebuah jaringan komputer ataupun internet agar mudah untuk diakses oleh user [6].

E. Vulnerability Assessment

Vulnerability Assessment adalah proses identifikasi, evaluasi, dan klasifikasi tingkat kerentanan pada sistem keamanan dalam ekosistem teknologi informasi. Hasil identifikasi, evaluasi, dan klasifikasi melalui Vulnerability Assessment akan memberikan pandangan kepada entitas yang melakukan proses tersebut agar entitas tersebut mengetahui adanya celah yang dapat disalahgunakan oleh pihak yang tidak bertanggung jawab terkait data penting entitas tersebut [7].

Vulnerability Assessment akan dilakukan dengan melakukan pemeriksaan secara terperinci dan sistematis pada infrastruktur komputasi suatu bisnis atau perusahaan untuk menentukan kelemahan atau celah yang mungkin dapat ditembus oleh pihak tidak bertanggung jawab dalam desain, implementasi, atau praktik.

F. SQL Injection

SQL injection (SQLi) adalah teknik serangan siber yang memanfaatkan kerentanan dalam aplikasi berbasis web untuk mengganggu basis data yang mendasarinya. Serangan ini terjadi ketika penyerang berhasil menyuntikkan kode SQL berbahaya ke dalam input yang diterima oleh aplikasi web, misalnya melalui formulir login, kolom pencarian, atau URL. Jika aplikasi tidak memvalidasi dan membersihkan input tersebut dengan benar, kode SQL yang disusupi dapat dieksekusi oleh server database.

SQL Injection merupakan sebuah teknik pengeksploitasian sebuah aplikasi web memakai data yang diberikan atau yang disisipkan dalam query SQL. Cara kerja dari SQL injection adalah dengan cara memasukkan query SQL atau juga perintah (command) sebagai input yang dimungkinkan melalui halaman web atau command prompt [8].

G. Acunetix Web Vulnerability Scanner

Acunetix adalah perangkat lunak keamanan web yang dirancang untuk mendeteksi dan membantu memperbaiki kerentanan pada aplikasi dan situs web. Perangkat lunak ini melakukan pemindaian otomatis yang mendalam untuk menemukan berbagai ancaman keamanan seperti SQL Injection, Cross-Site Scripting (XSS), CSRF (Cross-Site Request Forgery), dan banyak lagi. Acunetix dapat memindai aplikasi web modern, termasuk Single Page Applications (SPA) yang menggunakan teknologi seperti Angular, React, dan Vue, serta menganalisis konten dinamis dan JavaScript untuk mengidentifikasi kerentanan yang mungkin terlewat oleh pemindai tradisional.

Acunetix Web Vulnerability Scanner juga telah menjadi alat pilihan bagi banyak pelanggan di pemerintahan, militer, pendidikan, telekomunikasi, perbankan, keuangan, dan perusahaan E-Commerce, termasuk perusahaan-perusahaan besar lainnya dari berbagai negara [9].

H. UML (Unified Modeling Language)

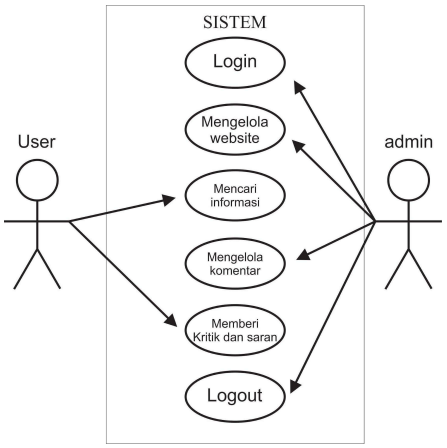
UML atau Unified Modeling Language adalah bahasa visual yang digunakan untuk memodelkan sistem perangkat lunak. UML menyediakan cara untuk menggambarkan, memvisualisasikan, dan mendokumentasikan aspek-aspek sistem perangkat lunak melalui berbagai diagram. Ini membantu para pengembang, arsitek, dan pemangku kepentingan lainnya memahami, merancang, dan berkomunikasi tentang sistem perangkat lunak secara lebih efektif.

UML adalah salah satu tool atau model untuk merancang dan mengembangkan software berbasis object-oriented. UML juga memberikan standar penulisan blueprint sistem yang meliputi konsep proses bisnis, penulisan kelas-kelas dalam bahasa pemrograman tertentu, skema basis data, serta komponen yang diperlukan dalam sistem perangkat lunak [10].

2. Metode

A. Diagram Sistem

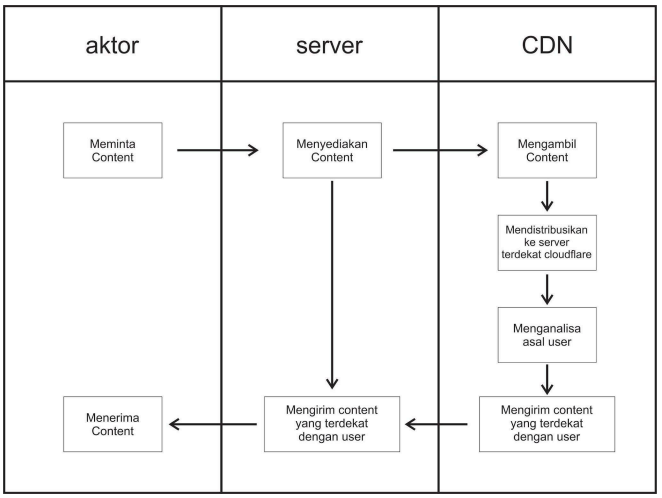
Dalam penelitian ini, implementasi terhadap sistem yang nantinya akan diterapkan membutuhkan rancangan agar implementasi dapat berjalan tanpa gangguan dan kendala yang signifikan. Oleh karena itu, berikut rancangan sistem yang nantinya akan diimplementasikan dalam penelitian ini. Adapun use case pada website dapat dilihat pada Gambar 1.



Gambar 1. Digram use case pada website tugasku.site

Untuk memperjelas alur use case pada Gambar 1, website yang dibuat hanya berupa blog yang berisi informasi umum. Peran pengguna terbatas pada mencari informasi seputar teknologi informasi dan memberikan kritik atau saran yang akan dikirimkan kepada admin. Admin memiliki akses penuh, termasuk login, mengelola konten (menghapus, menambah informasi, mengubah tema, serta menambahkan atau menghapus gambar), serta mengelola kritik dan saran pengguna (menghapus, menyetujui, atau membalas komentar). Admin juga dapat login dan logout untuk menjaga kualitas dan operasional website.

Agar penelitian ini dilaksanakan secara lebih sistematis dan jelas, dibutuhkan perancangan sistem. Perancangan diagram activity CDN dalam penelitian ini dapat dilihat pada Gambar 2.



Gambar 2. Diagram Activity CDN

B. Aktor

Ketika seorang pengguna membuka halaman web atau meminta file dari sebuah website, permintaan tersebut dikirim melalui jaringan internet ke sistem yang akan menyediakannya. Permintaan ini dapat berupa permintaan halaman HTML, gambar, video, file CSS, file JavaScript, dan lainnya. Setelah semua proses selesai, pengguna akan menerima konten yang diminta. Karena konten dikirim dari edge server CDN yang terdekat, pengguna mendapatkan konten lebih cepat dibandingkan dengan jika konten tersebut harus dikirim langsung dari web server yang mungkin berlokasi jauh dari pengguna.

C. *Server*

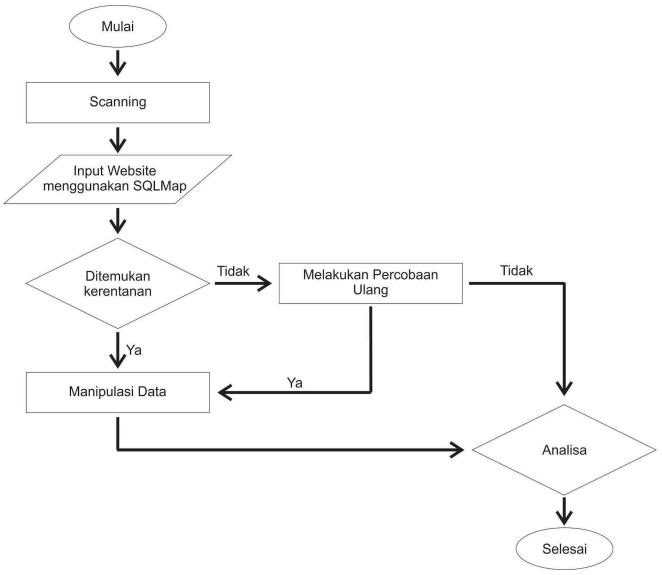
Server adalah server yang menyimpan konten website. Ketika CDN tidak memiliki salinan konten yang diminta dalam cache, CDN akan meminta konten tersebut dari web server. Web server kemudian menyediakan konten tersebut kepada CDN.

D. CDN (Content Delivery Network)

Setelah CDN menerima permintaan dari pengguna, langkah pertama adalah mengambil konten tersebut dari server asal (web server). CDN memiliki server proxy yang akan memeriksa apakah konten sudah tersedia di cache. Jika belum, CDN mengambil konten dari server web asli. Konten yang diambil dari web server kemudian disimpan di CDN (Content Delivery Network) atau yang paling dekat dengan lokasi pengguna, karena CDN

(Content Delivery Network) adalah teknologi yang telah disediakan oleh Cloudflare. Server ini dikenal sebagai "edge server". Penyimpanan ini disebut "caching", dan tujuan utamanya adalah untuk mengurangi waktu pengiriman konten ke pengguna di masa mendatang. Setelah itu, CDN menganalisis asal geografis permintaan pengguna. Ini melibatkan penggunaan teknologi seperti GeoIP untuk menentukan lokasi pengguna berdasarkan alamat IP mereka. Setelah lokasi pengguna dianalisis, CDN mengirimkan konten dari edge server yang paling dekat dengan pengguna. Hal ini meminimalkan latensi (waktu tunda) dan mempercepat pengiriman konten.

Adapun ilustrasi flowchart serangan hacker menggunakan SQL Injection dapat dilihat pada Gambar 3 berikut.



Gambar 3. Ilustrasi Serangan SQL Injection

E. Scanning

Pada proses ini, peneliti akan mencoba melakukan scanning menggunakan aplikasi bantuan, yaitu Acunetix Web Vulnerability Scanner, dengan tipe scan SQL Injection. Agar dapat mencoba untuk melakukan serangan SQL Injection, peneliti membuthkan hasil positif dari hasil scanning menggunakan aplikasi acunetix web vulnerability scanner. Scanning yang dilakukan menggunakan 4 website

F. Input Website Menggunakan SQLMap

Pada proses ini peneliti akan mencoba memasukkan perintah SQLMap untuk menguji keamanan website menggunakan sistem operasi kali linux, walaupun hasil yang di dapatkan dari hasil scanning tidak mendapatkan hasil, peneliti akan tetap mencoba memasukkan perintah SQLMap guna untuk mencoba mendapatkan hasil yang maksimal.

G. Kerentanan ditemukan

Pada proses ini, peneliti akan melihat hasil pemindaian SQLMap pada sistem operasi Kali Linux. Peneliti dapat melihat hasil berupa id dan password dari pemilik website tersebut.

H. Mencoba melakukan percobaan awal

Pada saat hasil ini, jika hasil yang didapatkan negatif untuk SQL Injection pada website tersebut, peneliti akan mencoba melakukan percobaan ulang sekali lagi untuk memastikan bahwa kerentanan terhadap SQL Injection benar-benar tidak dapat ditemukan.

I. Memanipulasi data

Pada saat ini, jika hasil yang didapatkan positif, peneliti akan mencoba memanipulasi data sebagai percobaan saja, namun tidak mempublikasikan kerentanan website tersebut karena hal ini ditakutkan akan merusak website itu sendiri. Namun, jika hal ini terjadi pada website uji coba, peneliti akan mencoba memanipulasi data untuk membuktikan bahwa website yang telah dikonfigurasi tersebut dapat dibobol melalui SQL injection.

J. Analisa

Peneliti akan menganalisis hasil yang diperoleh dari serangan untuk menentukan langkah selanjutnya atau mengevaluasi efektivitas serangan tersebut. Pada titik ini, penyerang dapat menghentikan serangan atau memulai kembali jika diperlukan.

3. Hasil dan Pembahasan

Pada penelitian ini keamanan website akan diuji menggunakan aplikasi Acunetix Web Vulnerability Scanner dan tools SQLMap, pengujian ini dilakukan untuk menemukan beberapa kelemahan pada setiap website.

3.1. Hasil Pengujian pada Setiap Website menggunakan Aplikasi Accunetix Web Vulnerability Scanner

Pada hasil scanning menggunakan aplikasi acunetix web vulnerability scanner terdapat berbagai tingkat ancaman dan jenis serangan. Persentasi hasil kerentanan yang ditemnukan pada scanning menggunakan aplikasi acunetix web Vulnerability Scanner dapat dilihat pada Tabel I.

Tabel 1. Persentase pada setiap website

Percobaan	Total indeks	Total Lokasi	Persentase
Website ke 1	26	456	5,7%
Website ke 2	24	487	4,9%
Website ke 3	27	164	16,5%
Website ke 4	1	1	100%

Pada hasil scanning ke website pertama terdapat 26 total indeks dari 456 total lokasi yang di scanning menggunakan aplikasi acunetix web vulnerability scanner tersebut. Pada hasil tersebut memiliki kerentanan website sekitar 5.7% atau akurasi keamanan website pertama yaitu 94.3%. Potensi kelemahan website tersebut tergantung berdasarkan jenis kelemahan yang didapatkan pada aplikasi acunetix web vulnerability scanner tersebut.

Pada hasil scanning website kedua terdapat 24 total indeks dari 487 total lokasi yang di scanning menggunakan aplikasi acunetix web vulnerability scanner tersebut. Pada hasil tersebut memiliki kerentanan website tersebut sekitar 4.9%. atau tingkat keamanan website kedua yaitu 95.1%. potensi kelemahan website tersebut tergantung berdasarkan jenis kelemahan yang ditemukan pada aplikasi acunetix web vulnerability scanner tersebut.

Pada hasil scanning website ketiga terdapat 27 total indeks dari 164 total lokasi yang di scanning menggunakan aplikasi acunetix web vulnerability scanner tersebut. Pada hasil tersebut memiliki kerentanan website sekitar 16.5% atau tingkat akurasi keamanan website ketiga yaitu 83.5%. Potensi kelemahan website tersebut tergantung berdasarkan jenis kelemahan yang ditemukan pada aplikasi acunetix web vulnerability scanner.

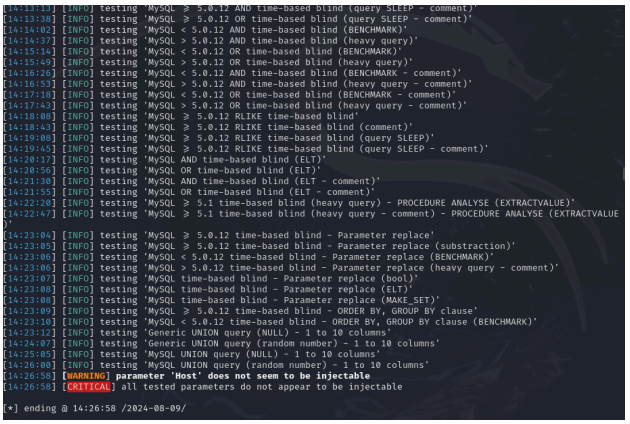
Pada hasil scanning website keempat terdapat 1 total indeks dari 1 total lokasi yang di scanning menggunakan aplikasi acunetix web vulnerability scanner tersebut. Pada hasil tersebut memiliki kerentanan website sekitar 100% atau tingkat akurasi keamanan website keempat yaitu 0%. Pada website keempat peneliti menyimpulkan website keempat telah menerapkan beberapa lapisan keamanan untuk melindungi data website tersebut, sehingga pada pengujian scanning menggunakan aplikasi acunetix web vulnerability scanner tidak dapat melakukan secara maksimal atau secara menyeluruh.

3.2. Potensi Kerentanan SQL Injection

Pada tahap ini untuk menguji kelemahan website pada jenis serangan SQL Injection menggunakan Tools SQLMap. Fungsi SQLMap adalah alat penetrasi sumber terbuka yang digunakan untuk mendeteksi dan mengeksploitasi kelemahan injeksi SQL (SQLi) pada aplikasi web.

A. Pengujian SQLMap pada website pertama

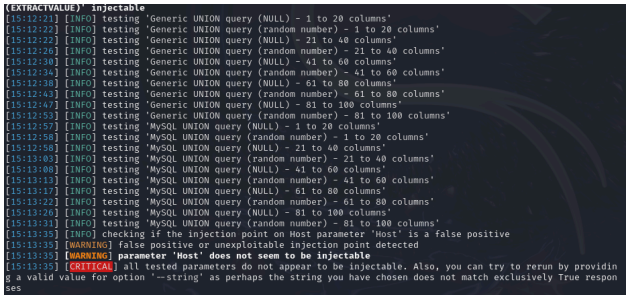
Pengujian ini dilakukan untuk mendapatkan hasil kerentanan website terhadap serangan SQL Injection. Pada gambar 4 yang telah diuji beberapa kali percobaan menggunakan scanning tools SQLMap dapat disimpulkan bahwa setelah mencoba berbagai teknik, SQLmap tidak berhasil menemukan kerentanan SQL Injection pada parameter yang diuji pada website pertama. Ini adalah hasil yang baik, karena menunjukkan bahwa setidaknya pada bagian yang diuji, aplikasi web tersebut telah terlindungi dari jenis serangan ini. Pada proses scanning menggunakan tools SQLMap ini membutuhkan waktu kurang lebih 2 jam untuk mendapatkan hasil scanning secara menyeluruh, namun hasil scanning SQLMap menunjukkan tidak ada potensi kerentanan terhadap website tersebut. Hal ini menunjukkan bahwa keamanan website tersebut dapat dikatakan sangat baik terhadap serangan SQL Injection, namun kerentanan pada keamanan lainnya harus diperbaiki untuk memaksimalkan keamanan website dapat terjaga.



Gambar 4. Hasil Scanning Menggunakan Tools SQLMap Pada Website Pertama

B. Pengujian SQLMap pada Website kedua

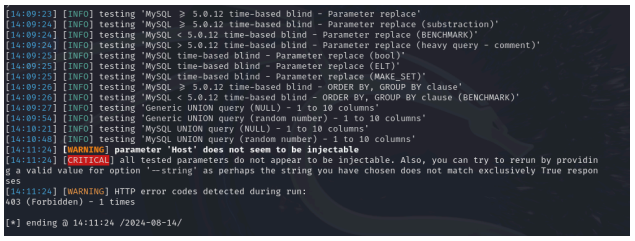
Pengujian ini dilakukan untuk mendapatkan hasil kerentanan website terhadap serangan SQL Injection. Dari hasil pengujian yang dilakukan beberapa kali seperti yang ditunjukkan pada Gambar 5, dapat disimpulkan bahwa SQLmap tidak berhasil menemukan kerentanan SQL Injection pada parameter yang diuji di website kedua, meskipun berbagai teknik telah dicoba. Ini merupakan hasil yang positif, karena menunjukkan bahwa bagian yang diuji pada aplikasi web tersebut terlindungi dari serangan jenis ini. Namun, untuk memastikan keamanan website tetap terjaga, pemilik website disarankan untuk melakukan pengecekan keamanan secara berkala. Langkah ini penting untuk mencegah kemungkinan serangan malware, terutama di era teknologi yang semakin maju ini.



Gambar 5. Hasill Scanning Menggunakan Tools SQLMap pada Website kedua

C. Pengujian SQLMap pada Website Ketiga

Pengujian ini dilakukan untuk mendapatkan hasil kerentanan website terhadap serangan SQL Injection. Dari hasil pengujian yang dilakukan beberapa kali seperti yang ditunjukkan pada Gambar 6, dapat disimpulkan bahwa SQLmap tidak berhasil menemukan kerentanan SQL Injection pada parameter yang diuji di website ketiga, meskipun berbagai teknik telah dicoba. Ini merupakan hasil yang positif, karena menunjukkan bahwa bagian yang diuji pada aplikasi web tersebut terlindungi dari serangan jenis ini. Namun, pada celah kerentanan lainnya patut diwaspadai dikarenakan dari hasil scanning pada website ini menunjukkan tingkat kerentanan tinggi.

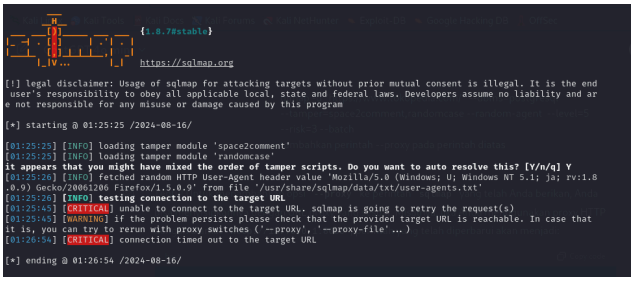


Gambar 6. Hasill Scanning Menggunakan Tools SQLMap pada Website ketiga

D. Pengujian SQLMap pada Website Keempat

Pengujian ini dilakukan untuk mendapatkan hasil kerentanan website terhadap serangan SQL Injection. Pada gambar 7 dapat disimpulkan SQLMap gagal melakukan pengujian SQL Injection karena firewall atau sistem keamanan pada target memungkinkan memblokir permintaan dari SQLMap. SQLMap menyarankan menggunakan opsi –proxy yang dapat melewati beberapa bentuk pembatasan jaringan. Namun untuk menggunakan –proxy, SQLMap membutuhkan port proxy dari website itu sendiri, dikarenakan peneliti tidak

mendapatkan port proxy pada website tersebut, maka pengujian SQL Injection tidak dapat dilanjutkan untuk mendapatkan informasi lebih lanjut.



Gambar 7. Hasill Scanning Menggunakan Tools SQLMap pada Website ketiga

4. Kesimpulan

Pada penelitian ini dapat disimpulkan setelah melakukan Analisis Kerentanan dan Kelemahan Keamanan *Content Delivery Network* (CDN) Terhadap Serangan SQL Injection Menggunakan Metode *Vulnerability Assesment* (VA) menunjukkan bahwa keempat website yang diuji memiliki tingkat keamanan yang beragam diantaranya 94.3%, 95.1%, 83.5% dan 100%%. Pada pengujian keempat, keamanan website tidak dapat mendapatkan angka akurasi yang tepat dikarenakan website tersebut mungkin saja sudah menerapkan beberapa lapisan keamanan. Pengujian keamanan CDN (Content Delivery Network) pada website bertujuan untuk menguji pada sistem keamanan CDN tersebut. Namun berdasarkan hasil penelitian, CDN memiliki sistem keamanan khusus terhadap website yang telah diimplementasikan WAF (Web Application Firewall) yang berfungsi untuk melindungi dari berbagai jenis serangan website tersebut. Hal ini peneliti dapat menyimpulkan bahwa keamanan website bergantung pada keamanan website itu sendiri, begitu juga dengan persentase keamanan website tersebut.

REFERENSI

[1] D. Laksmiati, "IMPLEMENTASI CONTENT DELIVERY NETWORK (CDN) UNTUK OPTIMASI KECEPATAN AKSES WEBSITE," vol. 5, 2020.
[2] D. E. Jayanti, R. Umar, and I. Riadi, "Implementation of Cloudflare Hosting for Access Speed on Trading Websites," SISFOTENIKA, vol. 10, no. 2, p. 227, Jun. 2020, doi: 10.30700/jst.v10i2.962.
[3] Y. Trimarsiah and M. Arafat, "ANALISIS DAN PERANCANGAN WEBSITE SEBAGAI SARANA INFORMASI PADA LEMBAGA BAHASA KEWIRAUSAHAAN DAN KOMPUTER AKMI BATURAJA".
[4] D. Laksmiati, "PENGUJIAN OPTIMASI PERFORMA WEBSITE MENGGUNAKAN CLOUDFLARE DENGAN METODE STRESS TEST," Akrab Juara J. Ilmu-Ilmu Sos., vol. 7, no. 3, p. 261, Aug. 2022, doi: 10.58487/akrabjuara.v7i3.1903.
[5] S. Arifin and Y. Krisnadita, "APLIKASI PLUGIN TRANSFER DOMAIN DI PT BEON INTERMEDIA," J. Teknol. Inf., pp. 1–84, Mar. 2017, doi: 10.36382/jti-tki.v8i1.252.
[6] M. I. Kurniansyah and S. Sinurat, "Sistem Pendukung Keputusan Pemilihan Server Hosting dan Domain Terbaik Untuk WEB Server Menerapkan Metode VIKOR," vol. 2, 2020.
[7] R. Farismana and D. Pramadhana, "VULNERABILITY ASSESSMENT UNTUK ANALISIS TINGKAT KEAMANAN PADA SISTEM INFORMASI REPOSITORI KARYA ILMIAH POLITEKNIK XYZ," vol. 3, 2023.
[8] A. S. Fitrani, M. A. Rosid, and S. Aji, "STUDI ANALISA SERANGAN SQL INJECTION," 2022.
[9] F. Al Fajar, "ANALISIS KEAMANAN APLIKASI WEB PRODI TEKNIK INFORMATIKA UIKA MENGGUNAKAN ACUNETIX WEB VULNERABILITY," INOVA-TIF, vol. 3, no. 2, p. 110, Dec. 2020, doi: 10.32832/inova-tif.v3i2.4127.
[10] F.- Sonata, "Pemanfaatan UML (Unified Modeling Language) Dalam Perancangan Sistem Informasi E-Commerce Jenis Customer-To-Customer," J. Komunika J. Komun. Media Dan Inform., vol. 8, no. 1, p. 22, Jun. 2019, doi: 10.31504/komunika.v8i1.1832.