STRATEGI FORTIFIKASI WEB SERVER UNTUK MENGHADAPI SERANGAN DARI LUAR

Timothy Baptista Putra Tadu[1], Trifonio Angga Pramatya[2], Muhammad Rossi Pratama[3]
timothy2637@gmail.com[1], anggapramatya18@gmail.com[2], ociganteng81@gmail.com[3]
Universitas Teknologi Yogyakarta

ABSTRAK

Web server yang umunya dipakai pengguna, dapat terancam apabila pengguna tidak mengevaluasi secara menyeluruh keamanan dari web server yang diakses. Pada penelitian ini, kami melakukan analisis mengenai startegi fortifikasi yang dapat dilakukan, serta metode analisis terhadap kerentanan web server dari serangan luar. Dampak dari penyerangan terhadap cyber security yang diakses dapat memberikan imbas pada pengguna yang lain, jika hasil kerusakan cukup signifikan. Pengguna yang terkena dari dampak kerusakan tersebut, dapat menghadapi adanya kehilangan data, pencurian data pribadi atau manipulasi data pribadi.
Kata Kunci : Pemeliharaan web server, DVWA, Firewall.

ABSTRACT

Web servers that are generally used by users can be threatened if users do not thoroughly evaluate the security of the web servers they access. In this research, we conducted an analysis of possible fortification strategies, as well as methods of analyzing web server vulnerabilities from external attacks. The impact of an attack on accessed cyber security can have an impact on other users, if the resulting damage is significant. Users affected by this damage may face data loss, theft of personal data or manipulation of personal data.
Keywords: *Web server maintenance, DVWA, Firewall.*

PENDAHULUAN

Dengan berkembangnya system teknologi secara global, pencarian informasi semakin dimudahkan melalui beberapa klik pada handhone, atau beberapa ketikan pada Komputer. Salah satu sumber dari pencarian informasi dan hal – hal yang bersangkutan, dapat dilihat pada web server. Web server merupakan salah satu software (perangkat lunak) yang umumnya digunakan masyarakat dalam mencari dan mendapatkan suatu informasi.

Namun, dengan semakin maju teknologi dalam perbangannya, metode – metode dari cyber attack (penyerangan digital) menjadi semakin kreatif dan luas. Salah satu software yang umunya terdampak dari serangan tersebut yaitu web server. Dampak yang diterima pengguna yang terkena dampak serangan tersebut dapat dikatakan sangat besar untuk diterima. Sehingga perlu adanya metode dalam perlindungan web server yang diakses, hal tersebut dapat berupa penggunaan firewall, Analisa keamanan melalui penggunaan DVWA dan lainnya. Dalam penelitian ini kami menganalisis strategi yang dapat dilakukan untuk melindungi diri dari berbagai serangan cyber attack. Penelitian ini diharapkan dapat membantu dalam perlindungan diri terhadap ancaman – ancaman yang mungkin dapat diterima dalam dunia digital, terutama pada web server.

METODE PENELITIAN

Penelitian ini dilakukan dengan menganalisis sumber-sumber literatur yang ditemukan pada internet terkait metode pengamanan web server. Kami mencari referensi-referensi yang dapat membantu dalam proses strategi pengamanan atau fortifikasi web server. Sumber-sumber yang kami temukan meliputi tugas akhir, jurnal, dan artikel-artikel yang membahas solusi dari masalah keamanan web server.

Berdasarkan analisis kami, kami merekomendasikan strategi-strategi berikut untuk melindungi web server Anda dari serangan luar. Pertama, pastikan hosting Anda aman dengan memilih penyedia hosting yang memiliki lapisan keamanan ekstra dan konfigurasi keamanan yang memadai. Kedua, instal plugin keamanan yang relevan untuk platform web Anda dan gunakan secara aktif. Ketiga, rutin perbarui website Anda dengan versi terbaru sistem operasi, server web, dan aplikasi yang Anda gunakan untuk mendapatkan perbaikan keamanan terbaru. Selanjutnya, gunakan kombinasi username dan password yang kuat serta pertimbangkan penggunaan manajer kata sandi. Selalu backup data website Anda secara rutin dan gunakan perangkat lunak antivirus terbaik untuk memeriksa dan membersihkan file website dari malware dan virus. Aktifkan 2-Factor Authentication (2FA) untuk mengamankan akses ke akun admin dengan verifikasi tambahan. Atur waktu logout otomatis untuk menghindari akses tidak sah ke akun admin. Terakhir, gunakan layanan perlindungan DDoS untuk melindungi server Anda dari serangan DDoS.

Dengan menggabungkan strategi-strategi ini, Anda dapat meningkatkan keamanan web server Anda dan mengurangi risiko serangan luar yang dapat mengancam integritas dan keberlanjutan operasional website Anda.

HASIL DAN PEMBAHASAN

Sebelum mengenal metode – metode fortifikasi yang diperlukan, pengguna perlu mengenal berbabagai jenis serangan cyber attack terlebih dahulu. Terdapat berbagai jenis cyber attack yang dapat ditemukan dalam sejarah penyerangan web server. Dengan mengenal jenis – jenis serangan yang dapat diterima web server, pengguna dapat dengan cepat men-identifikasi dampak dari serangan tersebut serta metode yang dapat dilakukan untuk melindungi diri dari serangan tersebut. Berikut beberapa jenis serangan yang dapat ditemukan:

- DDos (Distributed Denial of Service)

  DDos merupakan salah satu metode yang digunakan penyerang terhadap suatu web server, dimana penyerang membanjiri target dengan jaringan lalu lintas yang tinggi. Sehingga menyebabkan lalulintas jaringan dan ketidaksediaan jaringan.
- Injeksi SQL (SQL Injection)

  Injeksi SQL merupakan metode dimana penyerang menyisipkan suatu perintah SQL yang berbahaya terhadap basis data milik web server. Sehingga menyebabkan manipulasi, pencurian, atau dapat menghapus data – data yang terdapat di dalamnya.
- XSS (Cross Side Scripting)

  XSS bekerja dengan mengirimkan suatu script berbahaya terhadap halaman web yang diakses pengguna. Script tersebut akan mencuri informasi – informasi pribadi yang diinputkan pengguna, dalam halaman web yang dibuka seperti informasi sign up (pendaftaran) dan lain – lain.
- Brute Force

  Brute Force melibatkan upaya penyerang untuk menebak atau menerobos kata sandi dengan mencoba semua kemungkinan kombinasi secara sistematis. Penyerang menggunakan program otomatis atau skrip untuk mencoba password yang berbeda dengan harapan menemukan kombinasi yang benar.
- CSRF (Cross-Site Request Forgery)

  CSRF terjadi ketika penyerang memanfaatkan kepercayaan yang diberikan oleh web server kepada pengguna dengan mengirimkan permintaan yang tidak diinginkan atau berbahaya dari sumber yang sah. Jika pengguna yang terpengaruh mengklik tautan atau menjalankan aksi yang diminta, tindakan tersebut dapat dilakukan atas nama pengguna tanpa sepengetahuannya.

- Phishing

  Phishing melibatkan penipuan dengan menyamar sebagai entitas terpercaya untuk mencuri informasi sensitif dari pengguna, seperti kata sandi, nomor kartu kredit, atau data pribadi lainnya. Penyerang menggunakan email, pesan teks, atau situs web palsu untuk menipu pengguna agar mengungkapkan informasi mereka.
- SSRF (Server Side Request Forgery)

  SSRF terjadi ketika penyerang memanipulasi aplikasi web untuk melakukan permintaan ke sumber daya internal atau eksternal yang tidak seharusnya dapat diakses. Penyerang dapat menggunakan serangan ini untuk mendapatkan akses ke sistem yang sensitif atau melakukan serangan lain yang mengancam keamanan.

Ini hanyalah beberapa contoh serangan yang dapat diterima oleh web server. Penting bagi pengguna untuk memahami jenis-jenis serangan ini dan mengambil langkah-langkah yang tepat untuk mencegah serangan tersebut melalui implementasi lapisan keamanan yang tepat dan pembaruan yang teratur.

Strategi Fortifikasi

Terdapat banyak strategi fortifikasi keamanan web server, yang dapat digunakan pengguna agar dapat mencegah serangan – serangan yang dapat merugikan diri sendiri dan orang lain. Hal tersebut dapat berupa men-install plugin keamanan, penggunaan perlindungan DDoS (Distributed Denial of Service), penggunaan firewall, penerapan 2FA (2-Factor Autentification), pemeliharaan keamanan secara berkala dan masih banyak lagi.

Salah satu metode yang dapat membantu dalam strategi tersebut adalah dengan menggunakan platform DVWA (Damn Vulnerable Web Aplication). DVWA merupakan sebuah aplikasi web yang dirancang rentan terhadap berbagai jenis cyber attack seperti yang disebutkan sebelumnya. Pada platform DVWA pengguna dapat men-simulasikan suatu penyerangan dengan menjadi pelaku dari cyber attack, dan meneliti secara detail cara atau metode untuk menghindari atau menghadapi serangan – serangan tersebut.

Pengguna juga dapat menggunakan Firewall, yang mana dapat membantu dalam proses perlindungan suatu web server. Firewall merupakan suatu sistem keamanan yang umunya bertugas mengontrol lalu lintas data yang masuk dan keluar dari jaringan. Aplikasi Firewall dapat berupa perangkat keras, seperti Cisco Firepower, Fortinet FortiGate Next-Generation Firewall dan lainnya, serta dapat berupa software (Perangkat Lunak), seperti pfSense, Windows Firewall, dan lainnya. Firewall juga dapat mencatat aktivitas jaringan yang berjalan, dengan begitu pengguna dapat lebih termudahkan dalam meneliti keamanan suatu web server.

KESIMPULAN

Secara keseluruhan, penelitian ini memberikan strategi – strategi yang dapat dapat membantu dalam pembangunan keamanan suatu web server, serta pengenalan berbagai jenis serangan yang mungkin dapat dihadapi dalam penggunaan web server.

DAFTAR PUSTAKA

Jeffrey, J. (2017). Petunjuk Penulis Jurnal ESDM. 1(1), 1-4.https://id.scribd.com/document/354570984/Petunjuk-Penulis-Jurnal-ESDM

Ade, P. Armadani., Dicky, N., Khairi, I. (2022). Analisis Keamanan untuk Mengetahui Vulnerability pada DVWA Lab Esting Menggunakan Penetration Testing Standart OWASP. 21(2). 1-2. https://www.researchgate.net/publication/364750066_Analisis_Keamanan_Untuk_Mengetahui_Vulnerability_Pada_DVWA_Lab_esting_Menggunakan_Penetration_Testing_Standart_OWASP

Budi, Eko., Dwi Wira., dan Ardian Infantono. (2021). Strategi Penguatan Cyber Security Guna

Mewujudkan Keamanan Nasional di Era Society 5.0. Yogyakarta. Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia, Akademi Angkatan Udara.

Rizqi, Muhamad Fahrizal,. Rohmat Tulloh,. Nazel Djibran,. (2023). Implementasi Web Application Firewall untuk Melindungi Aplikasi Web dari Serangan Malware. Program Studi Teknik Informatika Universitas Pamulang. Pamulang.

Muzakir, Ari. (2013). PERANCANGAN DAN UJICOBA SISTEM KEAMANAN WEB SERVICE DENGAN METODE WS-SECURITY. Neliti.