JCBD
JOURNAL OF COMPUTERS AND DIGITAL BUSINESS
E-ISSN : 2830 - 3121
Vol. 2, No. 3, September, 2023, pp. 112-119

Efektifitas Penerapan Algoritma Brute Force dan Penyalahgunaannya Dalam Sistem Berbasis Web

Sarah Aulia Rahmah
Program Studi Teknologi Rekayasa Perangkat Lunak, Politeknik Negeri Medan, Sumatra Utara, Indonesia.
sarahauliarahmah@students.polmed.ac.id *

* Email Koresponden

DOI : 10.56427/jcbd.v2n3.235

INFO ARTIKEL

Histori Artikel
Diterima : 20 September 2023
Ditinjau : 24 September 2023
Disetujui : 30 September 2023

Kata Kunci
Brute Force
Serangan Siber
Komputer
Keamanan Komputer
Algoritma

Keywords
Brute Force
Cyber Attack
Computer
Computer Security
Algorithm

ABSTRAK

Brute Force adalah teknik dalam industri keamanan komputer yang bergantung pada kecepatan dan ketelitian komputer untuk melakukan percobaan dan mencoba setiap kombinasi atau kata kunci yang mungkin sampai menemukan yang benar. *brute force* juga digunakan untuk melakukan serangan siber oleh para hacker. Tujuan penelitian adalah untuk memahami penggunaan *brute force* dapat menjadi sebuah alat yang efektif dan sekaligus penyalahgunaan yang dapat membahayakan sistem. Penelitian ini melakukan studi literatur tentang *brute force* dan studi kasus tentang keamanan komputer. Penelitian ini mencakup temuan kualitatif tentang seberapa efektif *brute force* sebagai alat pengujian keamanan sekaligus alat pencarian. Penemuan ini juga membahas seberapa baik metode *brute force* dapat menemukan kelemahan keamanan dan bagaimana melakukan strategi pencegahan.

Brute Force is a technique in the computer security industry that relies on a computer's speed and rigor to conduct experiments and try every possible combination or keyword to find the right one. brute force is also used to carry out cyber attacks by hackers. The aim of the research is to understand the use of brute force can be an effective tool and at the same time abuse that can harm the system. The study carried out a literature study on brute force and a case study on computer security. The study included qualitative findings about how effective brute Force is as a security test tool as well as a search tool. The findings also discussed how well brute-force methods can detect security weaknesses and how to implement preventive strategies.

1. Pendahuluan

Menurut buku ‘Web Hacking : Serangan dan Pertahanannya’ oleh Stuart McClure, Saumil Shah, dan Sheeraj Shah. Mengatakan bahwa pada Internet, beratus-ratus juta elektron mengarungi beribu-ribu mil panjang kabel setiap hari menuju ke dan dari tempat-tempat di sekeliling dunia dan luar dunia. Elektron-elektron ini membawa pesan-pesan tertulis, gambar-gambar visual, dan suara di anatara berjuta-juta komputer yang terhubung ke *World Wide Web*. [7]

Dalam industri keamanan komputer, *Brute Force* adalah teknik yang bergantung pada kecepatan dan ketelitian komputer untuk melakukan percobaan dan mencoba setiap kombinasi atau kata kunci yang mungkin untuk menemukan yang benar. *Brute Force* juga merupakan suatu metode yang digunakan baik dalam konteks keamanan komputer maupun dalam pemecahan masalah matematis atau algoritma.

Namun kegunaan *Brute Force* sendiri dapat menjadi masalah, *Brute Force Attack* adalah salah satu dari ribuan strategi hacker untuk meretas [6]. Namun, *Brute Force Attack* bukanlah virus melainkan jenis serangan siber yang dilakukan dengan mencoba setiap kombinasi kata sandi atau kunci enkripsi yang mungkin untuk mendapatkan akses yang tidak sah ke sistem, akun, atau data yang dilindungi.[1] Dengan teknik serangan *brute force* maka sistem keamanan sebuah website tersebut dapat diketahui dengan cara menggunakan percobaan terhadap semua kunci dan semua aktifitas yang dilakukan oleh pengguna HTTP juga dapat diketahui dan dengan teknik ini maka serangan *brute force* dapat di implementasikan oleh para *hacker* dengan lebih cepat.[7]

Objek penelitian kali ini akan mengeksplorasi mengenai penggunaan teknik *brute force* yang baik dan efektif serta penyalahgunaannya yang berbahaya pada situs *Web*. Dalam penelitian ini akan membahas implementasi teknik *brute force* yang baik dan efektif akan dipaparkan dengan penerapannya yang sederhana pada situs Web dan aplikasi dan penyalahgunaannya dalam konteks keamanan siber.

2. Metodologi Penelitian

Penelitian ini dilakukan dengan mengintegrasikan dan menyusun data dari berbagai sumber literatur. Studi kasus dari literatur yang relevan dianalisis secara menyeluruh. Fokus utama artikel ini adalah mempelajari penggunaan teknik brute force, dengan penekanan khusus pada mengetahui seberapa efektif teknik tersebut digunakan dan potensi penyalahgunaannya dalam konteks situs web. Studi literatur dilakukan dengan mempelajari dan menyelidiki berbagai karya ilmiah yang berkaitan dengan topik tersebut. Buku, jurnal ilmiah, artikel, dan dokumen lainnya adalah sumber yang dipelajari. Setiap sumber diperiksa secara menyeluruh untuk mengumpulkan data penting tentang penggunaan brute force dalam keamanan situs web.

Tinjauan literatur lengkap digunakan sebagai dasar analisis artikel ini. Tinjauan ini mencakup pemahaman tentang bagaimana brute force dapat digunakan secara efektif dalam situasi tertentu. Selain itu, penyalahgunaan metode ini juga dianalisis dengan mengidentifikasi risiko yang mungkin dan konsekuensi negatifnya terhadap keamanan situs web. Dengan menggunakan metode ini, artikel ini bertujuan untuk memberikan pemahaman yang menyeluruh tentang penggunaan teknik brute force, baik dari segi manfaat maupun risiko yang terkait. Diharapkan bahwa penggabungan studi kasus dari literatur tertentu akan memungkinkan pemahaman yang lebih baik tentang cara dan konsekuensi penggunaan brute force pada situs web.

3. Hasil dan Pembahasan

Dalam mengamati data terkait brute force dalam konteks keamanan sistem berbasis web, kami melihat dua sisi yang berbeda. Pada satu sisi, algoritma brute force telah terbukti efektif dan maksimal ketika digunakan dengan tepat, seperti dalam *search engine* dan pencarian teks dalam aplikasi perangkat lunak kamus bahasa terjemahan. Sebaliknya, data yang diamati menunjukkan berbagai upaya untuk menyalahgunakan algoritma brute force, yang menimbulkan ancaman bagi keamanan siber. Penyerang membahayakan keamanan web dengan menggunakan berbagai kombinasi kata sandi dan teknik brute force untuk mendapatkan akses yang tidak sah ke akun pengguna dan sistem. Dengan demikian, penelitian ini menghasilkan kesimpulan dualitas dari penggunaan teknik *brute force*.

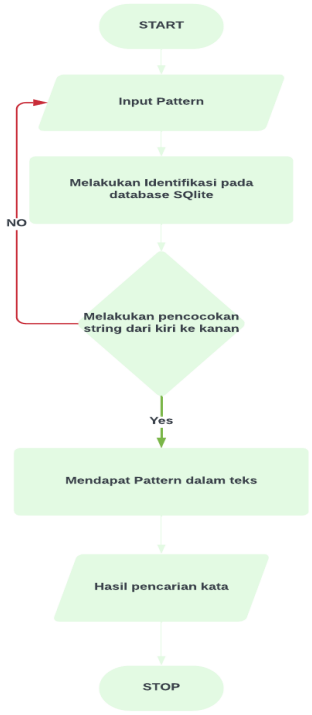
Dalam Algoritmanya, *Brute Force* adalah metode atau teknik pencarian yang digunakan untuk memecahkan masalah dengan mencoba semua solusi yang mungkin secara sistematis dan berurutan hingga menemukan solusi yang benar atau optimal. Metode ini digunakan dengan mencoba setiap kombinasi atau opsi yang mungkin tanpa memanfaatkan pengetahuan terperinci tentang pola atau struktur masalah.

Dari pengertian tersebut, dapat di pahami bahwa *brute force* merupakan metode pencarian yang sistematis, meng-*output*-kan cakupan semua kemungkinan, dan kecocokan solusi.

a. Penerapanya yang Efektif

Pada dasarnya, implementasi *brute force* sering kita jumpai, salah satunya adalah pada mesin *Search Engine*. *Brute Force* termasuk dalam kategori *String Matching*, yang merupakan algoritma yang digunakan

untuk mencocokan teks dengan teks lain, juga dikenal sebagai "*search text*" [2]. Sebagian besar, implementasinya di situs web terletak pada bagian *search engine*.



Gambar 1. *Flowchart Brute Force*

Dalam algoritma *Brute Force*, pengguna memasukkan *pattern* yang ingin dicari, dan sistem membaca pattern pada *database* Kamusku dan melakukan pencocokan *pattern* dari kiri ke kanan. Setelah melakukan pencocokan *pattern*, sistem melakukan *looping* pencocokan *string* dan menampilkan data yang sesuai dengan *pattern* yang dicari [2]. Saat mencocokkan *string*, algoritme *Brute Force* melakukan hal-hal berikut secara sistematis:

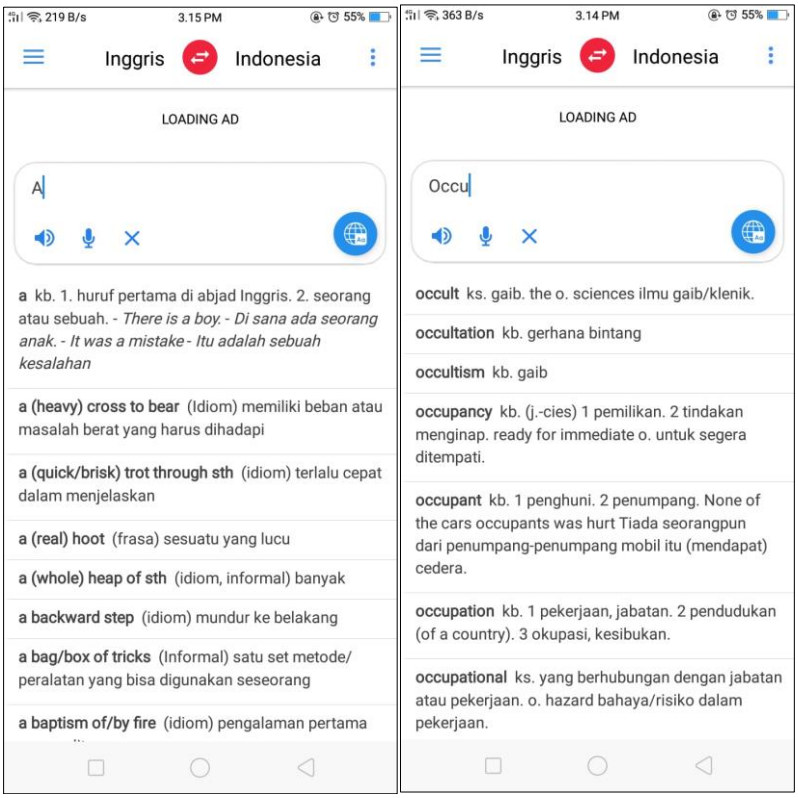
1. Algoritme ini mulai mencocokkan pola pada awal teks [2].
2. Algoritme ini akan mencocokkan karakter per pola dengan karakter di teks yang bersesuaian dari kiri ke kanan, sampai salah satu kondisi berikut dipenuhi:

a. Karakter dalam pola dan teks yang dibandingkan tidak cocok.
b. Algoritma akan melaporkan penemuan ketika semua karakter dalam pola cocok [2].

3. Setelah itu, algoritma terus mengubah pola satu ke kanan dan mengulangi langkah kedua sampai pola tiba di ujung teks [2].

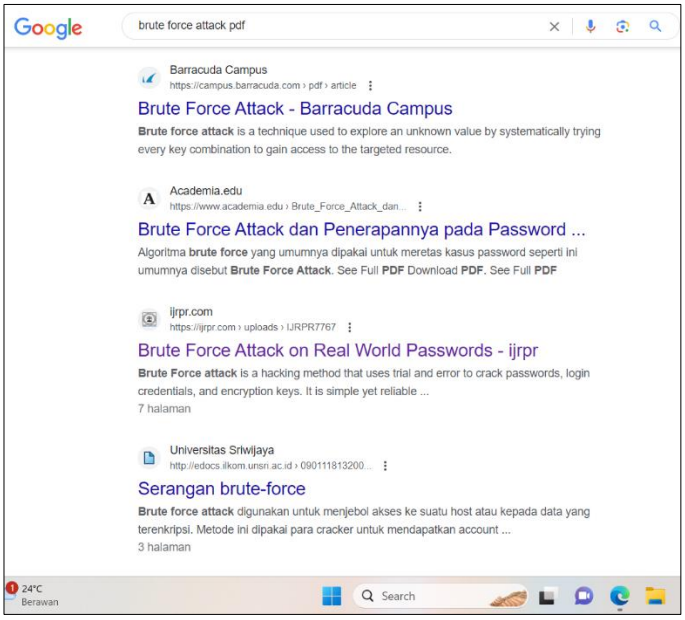
Sebagai contoh sederhana, algoritma *brute force* juga digunakan dalam aplikasi perangkat lunak seperti kamus terjemahan bahasa, seperti Kamusku, yang menerjemahkan antara bahasa Inggris dan bahasa Indonesia.

Algoritma *Brute Force* paling optimal diterapkan pada aplikasi ini. Algoritma ini beroperasi dari kiri ke kanan, atau dari kiri ke . Jika salah satu huruf dalam pola yang ingin dicocokkan tidak sesuai dengan salah satu huruf dalam teks, maka pencarian akan diulang dan dimulai pada huruf berikutnya dalam teks.

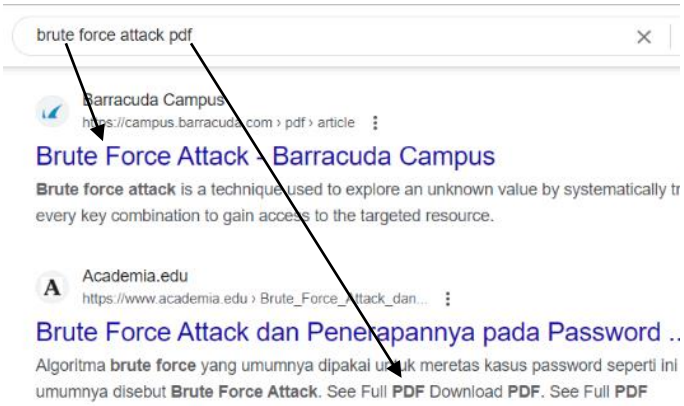


Gambar 2. Tampilan saat melakukan pencarian kata pada aplikasi Kamusku

Pada alat *search engine* seperti *Google*, *Brute Force* di implementasikan menggunakan ‘kata kunci’ yang mana mencocokan kata didalam artikel yang sama dengan *pattern* pada kolom *search*. Dapat di lihat pada beberapa kata yang di ***bold*** untuk menunjukan kecocokan *string* tersebut.



Gambar 3. Penerapan *Brute Force* pada *Search Engine*



Gambar 4. Kecocokan kata kunci

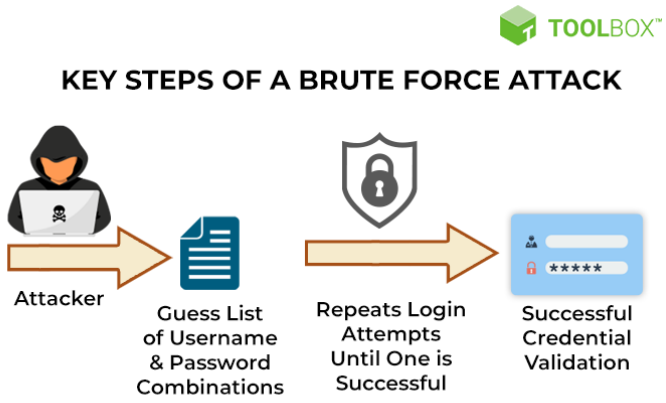
Kelebihan Algoritma *Brute Force* [2]:
1. Ini sederhana dan mudah dipahami,
2. Dapat digunakan untuk memecahkan hampir semua masalah.
3. Menghasilkan algoritma yang layak untuk masalah penting seperti pencarian, pengurutan pencocokan string, dan perkalian matriks.

Kelemahan Algoritma *Brute Force* [2]:
1. Jarang menghasilkan algoritma yang mangkus atau efektif.
2. Sangat lambat, hingga tidak dapat diterima.
3. Metode pemecahan masalah lainnya yang tidak kreatif.

b. Penyalahgunaannya

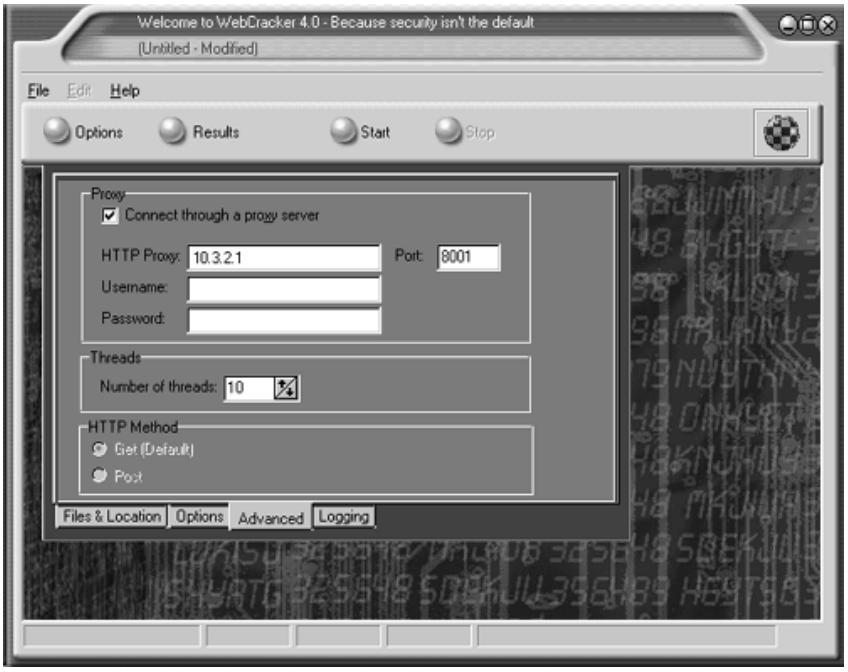
Brute Force dapat berubah menjadi sebuah serangan siber yang di sebut sebagai *Brute Force Attack* [6]. Tujuan dari serangan *Brute Force* adalah untuk mendapatkan akses ke otoritas "Administrator" pada sistem target. Otoritas administrator dapat melihat semua pengaturan khusus pada komputer dan memiliki akses penuh terhadap file yang diinginkannya. Penyerang harus berhasil melakukan serangan *brute force* untuk mendapatkan akses jarak jauh ke komputer target [1].

Akses jarak jauh dapat memungkinkan banyak aktivitas selain hanya berkomunikasi dengan penyerang. Ini dapat mengaktifkan transmisi dengan berbagi file atau folder. Dengan memberikan akses kepada penyerang, ia dapat mengontrol alat-alat seperti kamera, mouse atau keyboard. Jika Administrator dilindungi oleh kata sandi, kata sandi ini harus dibobol dengan serangan *Brute force*. Untuk tujuan ini, disiapkan "Daftar Lulus" yang berisi angka, huruf, dan karakter khusus yang telah disiapkan sebelumnya. Upaya dilakukan untuk mengakses kata sandi, dan setelah kata sandi yang benar ditemukan, serangan Brute force berhenti.[1]

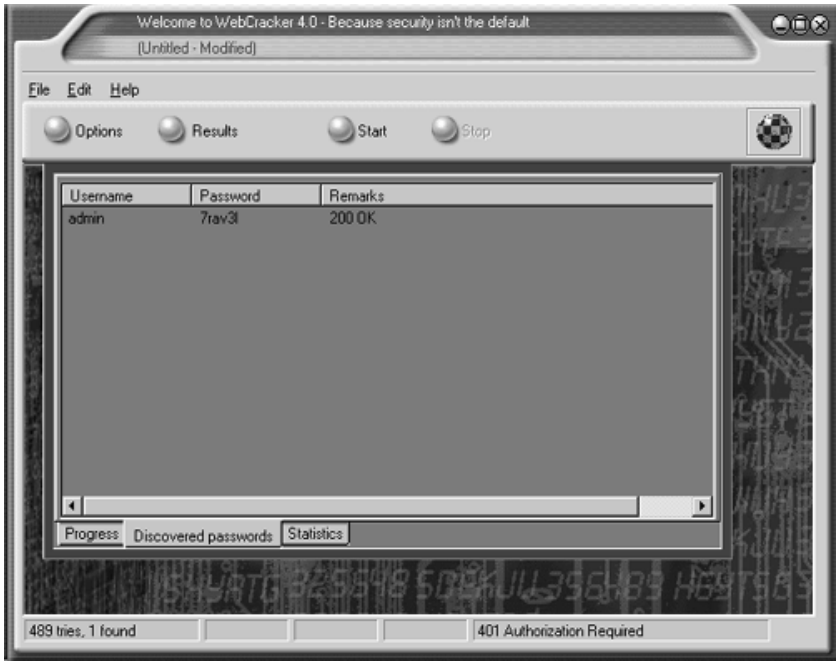


Gambar 5. Cara kerja Brute Force Attack

Teknik *Bruce Force Attack* sering di terapkan oleh para *hacker* pada HTTP *Authentication.* Menurut buku '*Web Hacking* : Serangan dan Pertahanan*'* oleh Stuart McClure, Saumil Shah, dan Sheeraj Shah. Dari semua layer aplikasi otentikasi protokol, barangkali otentikasi HTTP merupakan yang paling mudah di-crack dengan menggunakan teknik *Brute Force*.[7] Pada dasarnya, cara kerja *Brute Force Attack* adalah mencoba-coba sebanyak mungkin kombinasi password untuk bisa meretas akun, atau komputer hingga akhirnya menemukan kombinasi yang benar. Berikut adalah *tools* untuk *Brute Forcing* HTTP yang sangat terkenal amtara lain, *WebCracker* 4.0. [6] *WebCracker* terkonfigurasi untuk menjalankan serangan *brute force* dengan cara mem-*brute force* web server yang berjalan. Saat *WebCracker* di jalankan, ia akan menampilkan daftar hubungan dan *username* serta *password* yang sedang di coba-coba. Ketika menemukan kombinasi yang benar, *WebCracker* berhenti dan menampilkan hasilnya pada Gambar 5.[7]



Gambar 6. WebCracker 4.0



Gambar 7. WebCracker berhasil mengcrack sebuah account

Ada pun cara memperkuat situs web HTTP agar tidak mudah di retas oleh tools *brute force attack* antara lain :

a. Menonaktifkan Proxy Balik: Proxy balik adalah server perantara yang menghubungkan pengguna akhir dengan server aplikasi. Meskipun reverse proxy dapat meningkatkan kinerja dan keamanan, jika dikonfigurasi dengan salah, mereka dapat memungkinkan penyerang melakukan serangan brute force. Pastikan konfigurasi reverse proxy dikonfigurasi dengan benar dan memungkinkan hanya koneksi yang sah, serta secara teratur memeriksa dan memantau log aktivitas reverse proxy [7].

b. Meningkatkan Otentikasi Password HTTP: Ini adalah langkah penting untuk melindungi diri dari serangan brute force, terutama pada layanan yang berbasis web. Ini mencakup menjamin bahwa kata sandi yang digunakan pengguna cukup rumit. Untuk melindungi password, gunakan kombinasi huruf besar dan kecil, angka, dan simbol. Jangan lupa untuk selalu membaharui password Anda [7].

c. Menonaktifkan *Browsing Directory*: Fitur ini memungkinkan pengguna melihat daftar file dan direktori yang ada di server web, tetapi menonaktifkannya dapat mencegah penyerang mendapatkan informasi tentang struktur direktori. Konfigurasikan server web Anda untuk menonaktifkan *directory browsing*. Ini dapat dicapai dengan mengubah file .**htaccess** pada server Apache atau dengan menggunakan pengaturan server web yang sesuai lainnya [7].

4. Kesimpulan

Brute Force adalah metode atau teknik pencarian dalam algoritmanya yang digunakan untuk memecahkan masalah dengan mencoba semua solusi yang mungkin secara sistematis dan berurutan hingga menemukan solusi yang benar atau optimal. Pada penerapan optimal *Brute Force* pada algoritma proses pencarian kata di aplikasi terjemahan Kamusku dan *search engine* dan situs-situs *web* seperti *Google* dengan cara mencocokkan kata yang dimasukkan dengan data yang ada didalam database dimulai dari kiri dan bergeser terus ke kanan hingga kata yang di masukkan cocok dengan kata yang dicari. Merupakan bukti dari penerapan Brute Force pada tahap yang sederhana.

Juga, penyalahgunaan *Brute Force* dalam konteks keamanan siber yang berbahaya pada situs Web. Serangan *brute force* dikenal sebagai perangkat lunak yang dirancang untuk memecahkan kata sandi dan kata sandi yang disimpan di sistem target. Dengan serangan *brute force* memungkinkan diperolehnya seluruh informasi pada komputer target dan mengubah informasi yang diinginkan. Sangat sulit untuk menentukan siapa yang melakukan serangan tersebut karena penyerang jarang meninggalkan jejak.
Cara memperkuat situs *web* HTTP dari serangan *Brute Force Attack* adalah, menonaktifkan proxy balik, meningkatkan otentikasi password HTTP, dan menonaktifkan *browsing.*
Hasil penelitian ini di harapkan berkontribusi untuk menambah wawasan orang-orang mengenai dualitas *Brute Force* dan menjadi acuan pengembangan *anti-cyber attack*.

Referensi

[1] Kara I, “Detection, Technical Analysis of Brute Force Attack”, In *Sakarya University Journal of Computer and Information Sciences*, 2019.
[2] Irawan C, Pratama M, “Perbandingan Algoritma Boyer-Moore dan Brute Force pada Pencarian Kamus Besar Bahasa Indonesia Berbasis Android.”, in *BIOS : Jurnal Teknologi Informasi dan Rekayasa Komputer*, 2021.
[3] Rahmawati Y, Adi Pribadi I, Heningtyas Y, “Penerapan Algoritma Brute Force Pada Menu Search Website “Calonku” Dalam Rangka Pemilu Berbasis Web”, In Jurnal Pepadun, 2021.
[4] Sugiharto S, “Implementasi Algoritma Brute Force Dalam Pencarian Kebudayaan Di Indonesia Berbasis Mobile Application”, In Buffer Informatika, 2018.
[5] Santoso B, Sundawa F, Azhari M, “Implementasi Algoritma Brute Force Sebagai Mesin Pencari (Search Engine) Berbasis Web Pada Database”, In Jurnal Sisfotek Global, 2016.
[6] Pratita H., “Analisa Brute Force Attack menggunakan Scanning Aplikasi pada HTTP Attack”, 2016.
[7] S. McClure, et al., “Bab 9: Cyber Graffiti”, in Web Hacking : Serangan & Pertahanannya, Yogyakarta, ANDI Yogyakarta, 2003.
[8] Saputra K, et al., “Implementasi Algoritma Brute Force Dalam Pencocokan String Pada Aplikasi Pencarian Musik”, in Jurnal Informatika Upgris, 2021.

[9] Samah K, et al., “Brute force algorithm implementation for traveljoy travelling recommendation system”, in Indonesian Journal of Electrical Engineering and Computer Science, 2019.
[10] Mukaromah I, et al., “Analisis Pencocokan String Menggunakan Algoritma Brute Force”, in Jurnal Teknik Informatika dan Sistem Informasi (JURTISI), 2021.