Aplikasi N-Ary Tree Dalam Menganalisa Kerentanan Suatu Website

Muhammad Haidar Akita Tresnadi-13521025[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13521025@std.stei.itb.ac.id

***Abstract*—*Website* merupakan fasilitas internet yang mengandung halaman - halaman informasi berupa teks, gambar, video, audio dan bentuk- bentuk informasi lainnya yang bersifat terbuka sehingga bisa diakses oleh siapa pun. *Website* dapat diakses menggunakan koneksi internet dan *browser* seperti Mozilla Firefox, Google Chrome, Microsoft Edge dan tipe browser lainnya. Namun, *website – website* tersebut bisa saja memiliki kerentanan terhadap suatu serangan siber. Untuk menangani hal tersebut, penulis akan merancang *N-Ary tree* yang dapat merepresentasikan teknik – teknik yang digunakan oleh peretas setelah dilakukan analisis terhadap *website* tersebut.**

***Keywords—website*, web, situs, *N-Ary tree*, siber, peretas, analisis.**

I. PENDAHULUAN

Pada zaman yang serba digital ini, penyebaran informasi terjadi begitu cepat. Internet merupakan salah satu alat yang paling banyak digunakan untuk mendukung penyebaran informasi tersebut. Siapapun dapat mengakses informasi terbaru dari mana saja melalui *website* dengan menggunakan berbagai perangkat mulai dari smartphone, tablet, laptop hingga PC, hanya dengan menggunakan koneksi internet.

Situs web adalah salah satu platform paling populer untuk mencari informasi dan berbagai sarana komunikasi. Situs web pertama di dunia dibuat oleh Tim Berners-Lee pada akhir 1980-an sebagai bagian dari proyek World Wide Web (W3). *Website* ini resmi diluncurkan pada tanggal 6 Agustus 1991 dengan URL *http:/info.cern.ch.*

Tim Berners-Lee telah membuat *website* untuk memfasilitasi pertukaran informasi bagi para peneliti di tempat kerja. Baru pada tanggal 30 April 1993, situs web ini diumumkan secara publik dan dapat digunakan oleh semua individu, organisasi, dan bisnis secara gratis. Dari sana, situs tersebut berkembang pesat hingga seperti sekarang ini.

Saat ini banyak sekali aplikasi dan tutorial cara membuat situs web sendiri dari awal tanpa menulis kode apapun yang membuat proses pembuatan web menjadi lebih mudah dan jumlah halaman web di Indonesia semakin banyak. Penyebaran informasi yang cepat dan efisien adalah alasan utama mengapa web akan selalu menjadi sarana penting untuk mengumpulkan dan mengelola informasi. Untuk memudahkan menemukan informasi yang dicari pengunjung, halaman-halaman ini dikelompokkan bersama dalam satu menu yang dapat diakses dari halaman utama. Sebagian besar situs web telah menggunakan metode ini untuk lebih meningkatkan pengalaman pengunjung saat berkunjung. Namun, struktur dan tampilan halaman web tidak begitu rumit. Perhatian utama dari situs web adalah transmisi informasi. Di era modern ini, bisnis dapat menggunakan situs web sebagai platform pemasaran dengan menjangkau audiens yang lebih luas di internet. Misalnya seseorang telah memiliki toko atau kios sendiri, kini ia bisa membuka toko online agar calon pelanggan dapat dengan mudah membeli produk kapanpun dan dimanapun.

Tidak hanya sebagai tempat untuk mengupdate informasi produk terbaru bagi konsumen, website ini juga bisa menjadi tempat yang paling ideal untuk menggelar berbagai promosi menarik. Manfaat situs web juga digunakan untuk branding perusahaan. Kita dapat menyesuaikan situs web yang kita kelola dengan kebutuhan bisnis identitas yang sesuai dengan produk kita sendiri. Salah satu contohnya adalah menyertakan logo, identitas merek, dan lainnya.

Dibalik banyaknya manfaat dari situs web yang bisa kita peroleh, para pemilik situs ini seringkali dihantui oleh pihak-pihak yang tidak bertanggung jawab seperti *hacker*, *cracker*, dan penjahat-penjahat siber lainnya. Seorang hacker adalah seseorang yang memiliki kemampuan untuk membobol sistem keamanan komputer atau jaringan komputer yang dilengkapi dengan keterampilan pemrograman yang terampil. Tujuannya pun beragam, mulai dari menguji sistem keamanan hingga melakukan kejahatan. Merupakan tindakan kriminal yang dilakukan oleh hacker untuk merugikan pihak tertentu. Contohnya termasuk pencurian data pribadi dari situs web toko online.

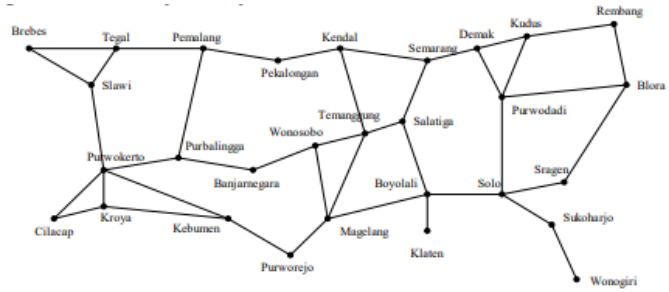
Maka dari itu, penulis akan memberikan rancangan N-Ary tree untuk mempermudah dalam proses evaluasi keamanan sistem suatu *website*.

II. LANDASAN TEORI

2.1 Graf

Graf terdiri dari struktur non-linear. Graf adalah kumpulan titik-titik yang tidak terhubung atau dihubungkan oleh garis. Tidak masalah ukuran titik-titik yang digambar atau panjang garis yang menghubungkan titik-titik tersebut. Titik-titik dalam graf disebut simpul, simpul, simpul, atau titik, dan himpunan titik disebut simpul (simpul atau titik). Garis yang menghubungkan simpul-simpul disebut sisi, dan himpunan garis

dalam grafik disebut sisi. Himpunan V (Vertex) memiliki elemen yang disebut vertex (atau titik atau node atau titik), Himpunan E (Edge) adalah pasangan vertex yang tidak terurut, elemennya disebut segmen (edge atau edge). G(V, E) Dimana G merupakan graf dan V adalah simpul atau simpul, atau simpul atau titik serta E merupakan *Arc* atau *Edge*, atau busur.



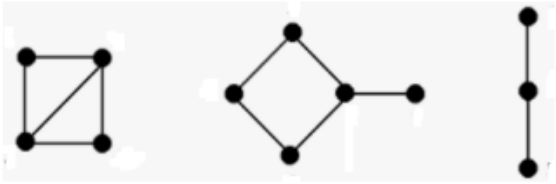
Gambar 2.1 Representasi graf jalan yang menghubungkan kota-kota di Provinsi Jawa Tengah.
(Sumber:https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Graf-2020-Bagian1.pdf)

2.2 Jenis Jenis Graf

Berdasarkan ada tidaknya gelang atau sisi ganda pada suatu graf, maka graf digolongkan menjadi dua jenis:

1. Graf sederhana (simple graph).

Graf yang tidak mengandung gelang maupun sisi ganda dinamakan graf sederhana.

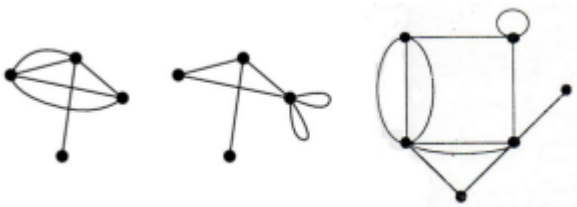


Gambar 2.2.1 Contoh graf sederhana (Sumber:https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Graf-2020-Bagian1.pdf)

2. Graf tak-sederhana (unsimple-graph).

Graf yang mengandung sisi ganda atau gelang dinamakan graf taksederhana (unsimple graph).

Gambar 2.2.2 Contoh graf tidak sederhana



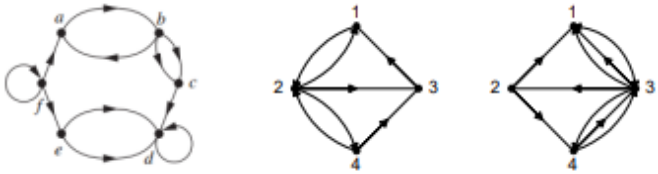
(Sumber:https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Graf-2020-Bagian1.pdf)

Berdasarkan orientasi arah pada sisi, graf dibedakan atas dua jenis:

1. Graf tak-berarah (undirected graph) Graf yang sisinya tidak mempunyai orientasi arah disebut graf tak-berarah.

Gambar 2.2.3 Contoh graf tak berarah (Sumber:https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Graf-2020-Bagian1.pdf)

2. Graf berarah (directed graph atau digraph) Graf yang setiap sisinya diberikan orientasi arah disebut sebagai graf berarah.

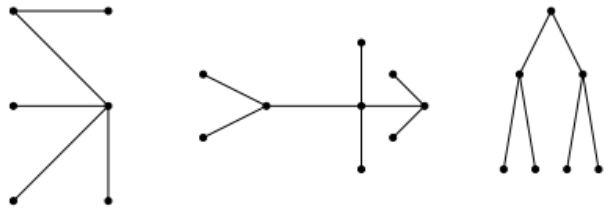


Gambar 2.2.4 Contoh graf berarah (Sumber:https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Graf-2020-Bagian1.pdf)

2.3 Pohon

Pohon adalah graf tak-berarah terhubung yang tidak mengandung sirkuit. Pohon memiliki Sifat-sifat (properti) pohon sebagai berikut Teorema. Misalkan G = (V, E) adalah graf tak-berarah sederhana dan jumlah simpulnya n. Maka, semua pernyataan di bawah ini adalah ekivalen:

1. G adalah pohon.
2. Setiap pasang simpul di dalam G terhubung dengan lintasan tunggal.
3. G terhubung dan memiliki m = n – 1 buah sisi.
4. G tidak mengandung sirkuit dan memiliki m = n – 1 buah sisi.
5. G tidak mengandung sirkuit dan penambahan satu sisi pada graf akan membuat hanya satu sirkuit.
6. G terhubung dan semua sisinya adalah jembatan.



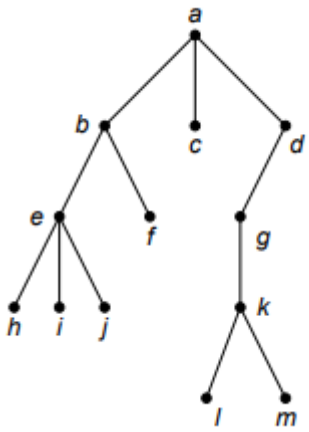
Gambar 2.3 Contoh Pohon
(Sumber:https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Pohon-2020-Bag1.pdf)

2.4 Pohon berakar (rooted tree)

Pohon yang satu buah simpulnya diperlakukan sebagai akar dan sisi-sisinya diberi arah sehingga menjadi graf berarah dinamakan pohon berakar (rooted tree). Berikut merupakan beberapa terminologi pada pohon berakar :

1. Anak (child atau children)
   Anak adalah simpul yang memiliki orang tua
2. Orangtua (parent)
   Orangtua adalah simpul yang memiliki anak

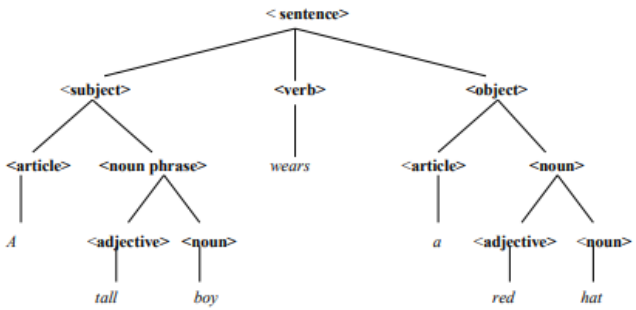
3. Lintasan (path)
   Lintasan adalah simpul yang harus dilalui untuk mencapai suatu simpul tujuan.
4. Saudara kandung (sibling)
   Saudara kandung adalah simpul yang memiliki parent yang sama.
5. Upapohon (subtree).
6. Derajat (degree)
   Derajat sebuah simpul adalah jumlah upapohon (atau jumlah anak) pada simpul tersebut.
7. Daun (leaf)
   Simpul yang berderajat nol (atau tidak mempunyai anak) disebut daun.
8. Simpul Dalam (internal nodes)
   Simpul yang mempunyai anak disebut simpul dalam.
9. Aras (level) atau Tingkat.
10. Tinggi (height) atau Kedalaman (depth)
    Aras maksimum dari suatu pohon disebut tinggi atau kedalaman pohon tersebut.



Gambar 2.4 Contoh Pohon Berakar
(Sumber: https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2021-2022/Pohon-2021-Bag2.pdf)

2.5 Pohon N-Ary

Pohon berakar yang setiap simpul cabangnya mempunyai paling banyak n buah anak.



Gambar 2.5 Contoh Pohon N-Ary.
(Sumber:https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2021-2022/Pohon-2021-Bag2.pdf)

2.6 *Website*

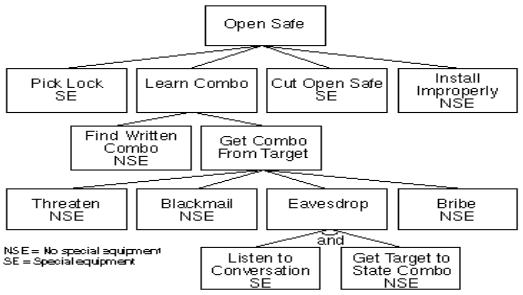
Sebuah *website* tersusun dari komponen dan elemen dengan fungsinya masing-masing, lalu terkumpul dan saling berkaitan. Berikut merupakan bagian-bagian umum dari *website* :

1. *Header*
   bagian atas halaman web, biasanya berisi logo situs sekaligus menu utama. Header biasanya merupakan bagian permanen dari halaman web tempat konten utama dapat bergulir ke bawah. Header berisi informasi penting untuk navigasi situs.
2. Menu
   sering ditempatkan di tempat yang mudah diakses di situs web, memudahkan pengguna menavigasi situs. Menu utama biasanya ditemukan di header atau di panel yang dapat dilipat (terutama dalam tampilan situs seluler) dan digunakan untuk menavigasi halaman situs web.
3. *Body*
   Area *body website* adalah area *website* yang paling banyak memuat konten. Ada beberapa jenis konten. Beberapa halaman akan berisi konten tertentu. Beranda bergambar berisi contoh jenis konten ini seperti yang muncul di beranda.
4. *Posts and "feed" content*
   Cara mudah untuk membuat pengunjung situs web berinteraksi dengan konten konten yang disediakan adalah dengan menyediakan konten *"feed"*. konten Ini, seperti pameran produk yang direkomendasikan atau, salah satu contohnya adalah, memposting blog terbaru, yang dimaksudkan untuk melibatkan pengunjung dan membuat mereka bisa saling berinteraksi.
5. *Footer*
   Biasanya terdiri dari informasi hak cipta, kepemilikan, link tambahan, sumber daya, sponsor dan kredit sebuah website.

2.7 *Attack Tree*

Pohon serangan memungkinkan ancaman terhadap keamanan system yang dimodelkan secara ringkas dalam format grafis sehingga mudah dipahami. Efektivitas keamanan siber, keamanan jaringan, keamanan sistem perbankan, instalasi, dan keamanan personel semuanya dapat dimodelkan menggunakan pohon serangan. Dengan meningkatnya risiko serangan teroris terhadap keamanan dalam negeri, serangan peretasan pada sistem komputer, dan penipuan berbasis komputer pada sistem perbankan, analisis pohon serangan merupakan alat yang sangat berharga bagi perancang sistem dan petugas keamanan.

Analisis pohon serangan menyediakan metode untuk memodelkan ancaman terhadap sistem dengan cara grafis yang mudah dipahami. Jika kita memahami cara-cara di mana suatu sistem dapat diserang, kita dapat mengembangkan tindakan pencegahan untuk mencegah serangan tersebut mencapai tujuannya.



Gambar 2.7 Contoh attack tree
(Sumber:https://www.schneier.com/academic/archives/1999/12/attack_trees.html)

III. HASIL PENELITIAN

3.1 Data yang Diperlukan

Dalam melakukan analisis keamanan situs web, diperlukan pemahaman yang mendalam mengenai perkiraan cara kerja dari situs web tersebut. Setelah mengetahui infrastruktur situs web secara keseluruhan, perancang pohon penyerangan juga perlu mengetahui berbagai macam jenis serangan yang mungkin dilakukan, dampak yang bisa ditimbulkan dari serangan siber tersebut , dan tindak pencegahan yang dapat dilakukan sehingga kasus kebocoran data penting dapat diminimalisir. Untuk merancang itu semua, diperlukan suatu media yang dapat digunakan untuk memetakan serangan – serangan yang mungkin dilakukan. Dalam jurnal ini, penulis menggunakan metode representasi pemetaaan serangan dengan pendekatan *attack tree*. Pembuatan *attack tree* memerlukan pendefinisian root dan simpul sehingga diperlukan informasi atau data yang bisas dijadikan acuan. Berikut adalah data-data yang diperlukan dalam melakukan perancangan *attack tree* dari fitur serta struktur suatu *website*.

1. Menentukan *Root*

Analisis pertama yang paling mudah dilakukan oleh seorang pemilik web tersebut adalah melakukan pengecekan mengenai data-data apa saja yang sekiranya penting atau memiliki tingkat kerahasiaan yang tinggi di dalam website tersebut. Data yang dianggap penting tersebut akan dijadikan root dalam tree yang akan dirancang nanti.

2. Menentukan Anak Pertama

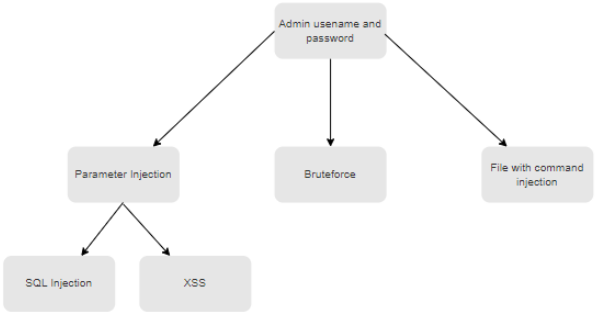
Setelah mengetahui data yang ingin dilindungi, hal selanjutnya yang dapat dilakukan adalah menganalisa seluruh fitur yang disediakan oleh website tersebut. Contoh dari fitur fitur tersebut seperti fitur pencarian, fitur register, fitur login, fitur komentar, fitur notifikasi dan seluruh fitur – fitur yang disediakan oleh website tersebut. Dengan adanya analisa seluruh fitur ini, kita dapat mengetahui kerentanan apa saja yang bisa dimanfaatkan oleh seorang peretas atau penjahat siber dalam mengakses data rahasia tersebut. Anak- anak pertama dari *root* atau akar adalah tipe fitur-fitur yang sekiranya dapat diekploitasi., sebagai contohnya adalah fitur pencarian. Pada fitur pencarian, pengguna biasa hanya akan memanfaatkannya fitur tersebut secara normal. Namun, sebenarnya fitur tersebut dapat dimanfaatkan untuk melakukan teknik SQL *injection* Untuk melakukan perintah SQL terhadap database sehingga penyerang tersebut bisa mengetahui *username* dan *password* akun yang bukan miliknya.

3. Menentukan Upapohon Berikutnya

Setelah anak pertama berhasil ditentukan, upapohon lainnya dapat dibentuk dengan pendekatan yang kurang lebih sama dengan pendekatan kedua, bisa seperti teknik-teknik penyerangan yang dapat dikombinasikan (SQL *injection* dengan *bruteforce*), bisa juga dikategorikan berdasarkan tipe penyerangan yang hampir mirip (SQL *injection* dengan XSS), dan masih banyak lagi.

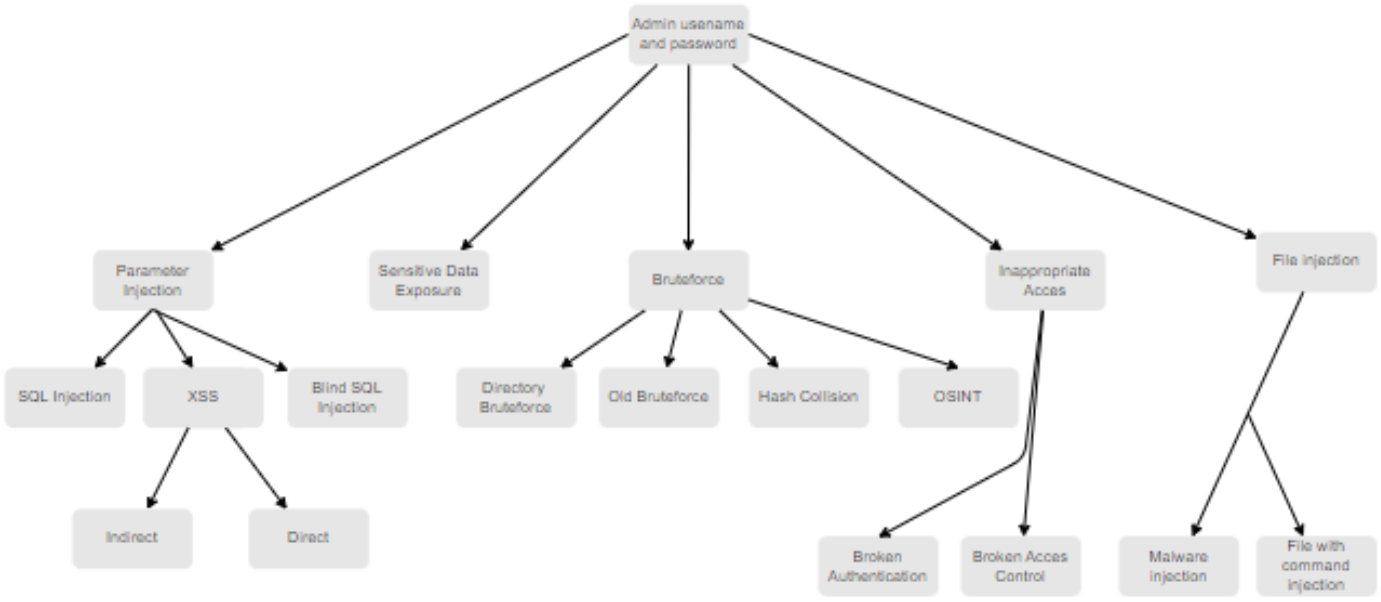
3.2 Perancangan *Attack Tree*

Setelah data yang dibutuhkan sudah lengkap, kita bisa langsung menggambarkan rancangan tersebut dalam bentuk *attack tree*. Berikut adalah contoh gambar sederhana dari attack tree :



Gambar 3.1 Contoh attack tree sederhana untuk analisa kerentanan situs web

Pada rancangan gambar attack tree sederhana tersebut, penulis mengambil contoh kasus yang umum terjadi. Situs web yang akan dianalisa oleh penulis merupakan situs web yang menampilkan sekumpulan data resep masakan yang diunggah oleh pengguna atau *user* yang telah melakukan registrasi akun di sana. Data penting yang dijadikan *root* adalah *username* dan *password* administrator dari suatu situs web. *Username* dan *password* akun milik administrator merupakan informasi dengan tingkat kerahasiaan yang tinggi dikarenakan kekuasaan dan *privilege* tinggi dari akun tersebut. Akun administrator dapat melakukan hal-hal seperti pengaturan ulang situs web, pengaksesan seluruh akun yang terdaftar di situs tersebut, dan memiliki kontrol penuh terhadap semua aset yang ada di situs terkait. Jika seseorang yang tidak bertanggung jawab dan memiliki niat jahat memiliki akses terhadap akun administrator maka pihak pemilik situs web tersebut kemungkinan besar akan mendapatkan kerugian dengan tingkatan sesuai dengan aset yang ada di dalam situs web tersebut. Setelah ditentukan data yang penting untuk dijadikan *root*, penulis menjadikan *parameter injection*, *bruteforce*, dan *file with command injection* sebagai *child* pertama dari *attack tree*. Pada perancangan ini, situs yang dianalisa oleh penulis memilki fitur kolom pencarian untuk mencari nama - nama resep makanan yang telah diunggah oleh pengguna situs web. Fitur yang menerima parameter berupa id suatu resep lalu mengambilnya dari *database* situs web terkait memiliki potensi kerentanan terhadap *parameter injection*. *Parameter injection* ini, dapat dilakukan dengan dua jenis serangan yaitu *SQL injection* dan XSS (Cross Site Scripting), sehingga parameter *injection* memiliki dua *child*. Dari analisa di atas, akhirnya penulis menjadikan *parameter injection* sebagai *child* atau anak pertama dari *root*. Saudara kandung dari *parameter injection* adalah



Gambar 3.2 Contoh attack tree untuk analisa kerentanan situs web

bruteforce dan *file with command injection*. Pada situs web yang dianalisa oleh penulis, terdapat fitur *login* yang bisa diserang menggunakan teknik *bruteforce*. *Bruteforce* adalah teknik dimana seorang penyerang siber melakukan percobaan untuk menebak kombinasi *username* maupun *password* dari suatu akun dengan cara mencoba seluruh kombinasi angka dan karakter yang ada. Fitur lain yang ditemukan pada situs web ini adalah fitur mengunggah file yang berupa resep dari suatu makanan. Fitur ini memiliki potensi kerentanan terhadap *file with command injection* yakni berupa serangan dengan memasukkan kode file yang berbahaya di dalam file yang akan diunggah. Kode yang disisipkan dalam file bisa bermacam macam tergantung niat dari penyerang itu sendiri. Penyerangan ini bahkan dapat mengakibatkan server dari situs web tersebut dimatikan dan dikontrol sesuka hati. Setelah diagram *attack tree* dibuat, kita dapat melakukan kembali analisis berdasarkan rangkaian kemungkinan serangan dari representasi setiap simpul. Analisa solusi dilakukan tiap simpul demi simpul sehingga dapat dipastikan tidak ada yang terlewat.

Pada gambar *attack tree* 3.2, skenario yang diberikan pada kasus tersebut lebih kompleks dibandingkan dengan skenario pada *attack tree* pertama. Jika dilakukan perbandingan antara skenario satu dengan skenario dua, implementasi *attack tree* di skenario ke dua lebih terasa dampaknya dibandingkan dengan skenario pertama. Hal ini disebabkan oleh perbedaan jumlah Upapohon, *child*, saudara kandung, orang tua dan bagian – bagian pohon lainnya. Pada kasus yang kedua ini, *attack tree* akan membuat analisa kita semakin matang dan sistematis sehingga meminimalisir kesalahan yang tidak perlu. *Attack tree* juga mempermudah kita dalam mengeliminasi analisa yang telah kita lakukan sehingga menjadi lebih rapi dan mudah diorganisir. Dengan attack tree, kerjasama dalam tim pun dapat dipermudah. Hal ini bisa terjadi karena pembagian tugas untuk melakukan pengujian kerentana situs web sebagai tim dapat dibagi dengan baik. Efektifitas waktu yang dihasilkan dengan pembagian tugas ini pun bisa dimanfaatkan untuk menganalisa kasus dari tiap simpul semakin dalam sehingga kemungkinan terjadinya kebocoran data pun semakin kecil. Representasi *attack tree* ini juga dapat mempermudah pemilik situs web yang awam untuk mengetahui kerentanan apa saja yang bisa terjadi pada website yang dikelolanya.

Pada contoh kasus nyata, penerapan *attack tree* ini dapat ditambahkan nilai *cost* atau biaya, nilai prioritas, dan perkiraan frekuensi dari jumlah penyerangan setiap simpulnya. Hal ini dilakukan agar dari semua simpul yang ada dapat dilakukan analisa tiap simpulnya sehingga ditentukan prioritas yang sesuai dengan kebutuhan perusahaan atau lembaga terkait saat itu. Salah satu contohnya adalah ketika terdapat perusahaan A yang ingin melakukan evaluasi terhadap keamanan serta kerentanan dari situs web yang dimiliki perusahaan tersebut, maka perusahaan A akan mencoba membuat *attack tree* yang sesuai dengan situs web yang dimilikinya. Selanjutnya, *attack tree* tersebut akan diberi bobot setiap simpulnya agar prioritasnya dapat ditentukan. Pemilihan prioritas ini bersifat dinamis dan bergantung pada kondisi perusahaan A saat ini sehingga alokasi waktu dan akomodasi yang diberikan oleh perusahaan A merupakan keputusan yang paling tepat untuk diambil saat itu. Jika bobot prioritas ini tidak dibuat, maka perusahaan A akan kesulitan dalam memilih evaluasi kerentanan situs web mana yang terbaik untuk diambil. Penerapan *attack tree* ini pada akhirnya sesuai dengan kebutuhan perancang. Jika diagram ini memang hanya diperlukan untuk mengetahui tipe – tipe serangan yang mungkin terjadi pada suatu situs web, maka tanpa bobot pun tidak masalah. Namun, jika diperlukan pemilihan analisa berdasarkan skala prioritas tertentu, maka penulis menyarankan untuk membuat attack tree dengan parameter bobot yang sesuai.

IV. KESIMPULAN

Dalam menganalisa kerentanan suatu website, dapat dilakukan dengan representasi N-ary tree berupa *attack tree*. Meskipun attack tree ini belum bisa dikatakan sebagai representasi terbaik untuk menganalisa sistem keamanan dari *website* publik, attack tree dapat mempermudah mengorganisir dan menyusun serangan – serangan yang memiliki potensi untuk membocorkan data penting dari situs web tersebut. *Attack tree* ini juga dapat meminimalisir kesalahan – kesalahan akibat *human error* ketika melakukan analisis system keamanan dikarenakan *attack tree* ini bersifat sistematis dan efektif. Penggunaan *attack tree* di industri juga dapat mempermudah penentuan evaluasi keamanan sistem web yang ingin diprioritasikan terlebih dahulu sehingga keputusan yang akan diambil nantinya semakin matang.

V. SARAN

Saran yang ingin disampaikan penulis adalah rancang *attack tree* sesuai kebutuhan. Jika hanya membutuhkan segala jenis serangan yang mungkin terjadi pada situs web, maka tidak memberikan bobot pada setiap simpul tidak masalah. Namun jika diperlukan skala prioritas analisa yang ingin dilakukan, maka disarankan untuk memberikan bobot sesuai parameter yang diinginkan.

VI. UCAPAN TERIMA KASIH

Puji dan syukur penulis panjatkan kepada Allah SWT, atas berkat, rahmat, karunia serta nikmatnya makalah ini dapat diselesaikan dengan baik dan tepat waktu. Penulis juga ingin mengucapkan terima kasih kepada Dr. Ir. Rinaldi Munir, M.T. selaku Dosen Mata Kuliah IF2120 Matematika Diskrit Kelas 03 yang telah sabar, merelakan tenaga dan pikiran dalam membimbing serta mencurahkan segala ilmunya dengan segenap hati kepada penulis.

REFERENCES

[1] R. Munir. Graf (Bagian 1): "Bahan Kuliah IF2120 Matematika Diskrit." Bandung, Indonesia, 2022. Diakses pada 11 Desember 2022.
[2] R. Munir. Pohon (Bagian 1): "Bahan Kuliah IF2120 Matematika Diskrit." Bandung, Indonesia, 2022. Diakses pada 11 Desember 2022.
[3] R. Munir. Pohon (Bagian 2): "Bahan Kuliah IF2120 Matematika Diskrit." Bandung, Indonesia, 2022. Diakses pada 11 Desember 2022.
[4] Redaksi, T. (2022, June 18). 7 pengertian website Menurut Ahli, Lengkap Jenis & Fungsinya. CNBC Indonesia. Retrieved December 11, 2022, from https://www.cnbcindonesia.com/tech/20220618152119-37-348229/7-pengertian-website-menurut-ahli-lengkap-jenis
[5] *13 parts of a website you should know about*. DigiWorks. (2015, October 22). Retrieved December 11, 2022,from https://www.digiworks.co.za/13-parts-of-a-website-you-should-know-about/
[6] *Attack tree modeling in Attacktree*. Isograph. (n.d.). Retrieved December 11, 2022, from https://www.isograph.com/software/attacktree/creating-an-attack-tree/
[7] Beccaro, M. (2018). Attack Trees - Methodology and Application in Red Teaming Operations. hackinthebox. Diakses pada 11 Desember 2022.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 12 Desember 2022

Muhammad Haidar Akita Tresnadi
NIM: 13521025