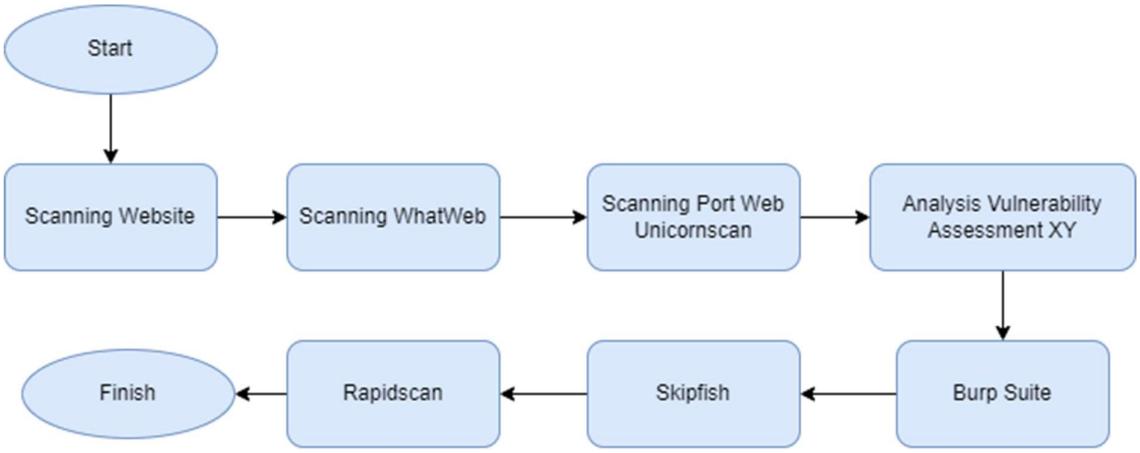
BAB III
METODE PENELITIAN

3.1. Licensing Research and Legality

Beberapa metode yang diperlukan dalam memenuhi penelitian mulai dari proses pemindaian website, menargetkan analisis penilaian kerentanan situs web dan juga melakukan penetrasi dalam upaya serangan brute force pada situs web menggunakan beberapa alat berbasis Linux seperti Burp Suite, Skipfish, Rapidscan sesuai dengan yang dijelaskan pada gambar 1 dibawah ini:



Gambar 3. 1 Alur Penelitian

3.2. Website Scanning

Tahapan ini merupakan langkah awal dalam melakukan penelitian, karena memerlukan informasi dasar tentang beberapa data situs web terkait, seperti alamat IP, port, dan komponen lain yang digunakan dalam struktur situs web. Langkah selanjutnya adalah melakukan pemindaian untuk mengidentifikasi potensi kerentanan keamanan pada situs web target menggunakan alat Whatweb dan Unicornscan. Pemindaian ini dapat dilakukan dalam dua cara berbeda, yaitu secara internal dan eksternal. Metode ini mampu mengatasi berbagai jenis komponen aplikasi dengan menggunakan metode statis dan dinamis, sehingga meningkatkan akurasi pemindaian. Namun, perlu diingat bahwa ada beberapa dampak negatif yang dapat mempengaruhi kinerja suatu aplikasi karena risiko pencurian dalam satu host yang sama [13].

Alat pemindaian kerentanan bertujuan untuk mengidentifikasi bagian-bagian sistem yang mungkin memiliki kerentanan terhadap ancaman keamanan, seperti kegagalan fungsi atau kesalahan konfigurasi [13]. Dalam mode eksternal, aplikasi mencoba bergantung pada titik akhir komponen yang berbeda. Oleh karena itu, pemindaian ini mungkin tidak mencapai tingkat akurasi yang diinginkan dan bahkan dapat meningkatkan beban pada sistem aplikasi [13]. Studi mendalam pemindaian situs web ini bertujuan untuk mengidentifikasi potensi kerentanan keamanan pada situs web yang sedang diteliti. Proses pemindaian situs web melibatkan penggunaan alat khusus yang secara otomatis menganalisis berbagai aspek dari situs web, termasuk konfigurasi server, sumber kode, kerentanan aplikasi web, dan pengaturan keamanan lainnya. Dengan melakukan pemindaian situs web, peneliti dapat mengumpulkan informasi tentang kemungkinan kerentanan yang mungkin ada di situs web Office XY. Ini mencakup pencarian celah keamanan seperti kerentanan terhadap serangan injeksi SQL, skrip lintas situs (XSS), kerentanan server, dan lain sebagainya.

Hasil pemindaian situs web akan memberikan gambaran tentang kerentanan yang ada dan membantu peneliti dalam mengidentifikasi area yang perlu perbaikan atau penguatan keamanannya. Tujuan dari studi pemindaian situs web yang mendalam ini adalah untuk membantu Office XY dalam meningkatkan keamanan situs web mereka dengan mengidentifikasi dan memperbaiki kerentanan yang terdeteksi. Dengan mengevaluasi kerentanan yang ada, langkah-langkah keamanan yang sesuai dapat diambil untuk mengurangi risiko serangan oleh pihak yang tidak berwenang serta melindungi data sensitif yang tersimpan di situs web tersebut.

3.2.1. Website Data Scanning using WhatWeb

Whatweb memiliki kemampuan untuk mengidentifikasi informasi yang terdapat pada situs web yang menjadi objek penelitian. Langkah-langkah dalam metode ini juga memungkinkan pemindaian respon HTTP yang diterima oleh situs web target, yang dapat digunakan untuk mengidentifikasi jenis server web yang digunakan dan struktur konten yang ada dalam aplikasi tersebut. Penggunaan Whatweb dalam pemindaian data situs web bertujuan untuk menganalisis berbagai aspek dari situs web Office XY, seperti teknologi

yang digunakan, potensi kerentanan yang mungkin ada, dan informasi yang relevan dengan aspek keamanan. Whatweb adalah alat yang digunakan untuk melakukan analisis otomatis terhadap situs web, dan dalam konteks penelitian ini, penggunaannya bertujuan untuk:

1. Identifikasi Teknologi yang Digunakan: Whatweb membantu mengidentifikasi teknologi yang digunakan dalam pengembangan situs web, seperti sistem manajemen konten (CMS), server web, bahasa pemrograman, database, dan lain sebagainya. Informasi ini penting karena dapat membantu pemahaman arsitektur situs web dan potensi kerentanan yang terkait dengan teknologi tersebut.
2. Pemindaian Kerentanan: Whatweb juga mampu mengidentifikasi potensi kerentanan yang ada pada situs web Office XY. Ini mencakup pencarian celah keamanan umum seperti serangan injeksi SQL, skrip lintas situs (XSS), pengungkapan file, akses direktori, dan lain sebagainya. Dengan mengidentifikasi kerentanan ini, peneliti dapat menyoroti area yang rentan dan memprioritaskan tindakan pengamanan yang diperlukan.
3. Pengumpulan Informasi: Whatweb dapat mengumpulkan informasi penting tentang situs web, seperti struktur halaman, direktori yang dapat diakses secara publik, alamat email yang terbuka, dan versi perangkat lunak yang digunakan. Informasi ini dapat memberikan wawasan tentang konfigurasi situs web dan mungkin memberikan petunjuk tentang kerentanan yang mungkin dapat dieksploitasi oleh pihak yang tidak sah.

Dengan menggunakan Whatweb untuk melakukan pemindaian data situs web, penelitian ini dapat memberikan pemahaman yang lebih komprehensif tentang kerentanan keamanan yang ada pada situs web Office XY di Jawa Timur. Hasil dari pemindaian ini dapat membantu Office XY dalam mengidentifikasi dan memperbaiki kerentanan yang ditemukan, serta meningkatkan keamanan situs web mereka secara keseluruhan. Whatweb berperan dalam mengumpulkan informasi yang relevan untuk menganalisis

kerentanan dan membantu mengidentifikasi celah keamanan pada situs web dengan memberikan wawasan tentang teknologi dan konfigurasi yang digunakan. Berikut adalah beberapa informasi khusus yang dapat dikumpulkan oleh Whatweb:

1. Jenis Server Web: Whatweb dapat mengenali jenis server web yang digunakan oleh situs web, seperti Apache, Nginx, atau Microsoft IIS. Informasi ini memiliki pentingnya karena setiap server web memiliki karakteristik dan potensi kerentanan yang berbeda.
2. Platform dan Teknologi: Whatweb mampu menghimpun informasi tentang platform dan teknologi yang digunakan dalam pengembangan situs web, seperti sistem manajemen konten (CMS) yang digunakan (seperti WordPress, Joomla, atau Drupal), bahasa pemrograman (contohnya PHP, Python, atau Ruby), atau penggunaan kerangka kerja (seperti Laravel, Django, atau Ruby on Rails).
3. Plugin dan Ekstensi: Whatweb dapat mengidentifikasi plugin dan ekstensi yang digunakan oleh situs web. Data ini memberikan petunjuk tentang fitur tambahan yang ada di situs web dan dapat memengaruhi potensi kerentanan yang mungkin ada.
4. File dan Direktori: Whatweb mampu mendeteksi file dan direktori yang terlihat atau dapat diakses secara publik di situs web. Hal ini mencakup file konfigurasi, file log, atau mungkin direktori yang berisi informasi yang bersifat sensitif.
5. Kerentanan Terkait: Whatweb juga dapat memberikan informasi tentang kerentanan yang terkait dengan teknologi yang digunakan dalam situs web. Sebagai contoh, jika Whatweb mendeteksi penggunaan versi perangkat lunak yang sudah usang dan rentan terhadap serangan yang telah diketahui, maka ini akan memberikan peringatan tentang potensi kerentanan tersebut.

Dengan mengumpulkan informasi ini, Whatweb berperan dalam membantu mengidentifikasi potensi kerentanan keamanan pada situs web.

Informasi tentang server web, platform, plugin, dan ekstensi yang digunakan dapat membantu dalam mengidentifikasi kerentanan yang spesifik terkait dengan teknologi tersebut. Jika ada kerentanan yang diketahui terkait dengan versi perangkat lunak atau konfigurasi yang digunakan, Whatweb dapat memberikan peringatan tentang potensi kerentanan tersebut. Informasi tentang file dan direktori yang terlihat atau dapat diakses juga membantu dalam mengidentifikasi kemungkinan celah keamanan akses. Tidak ada pencurian data atau informasi yang tidak sah yang terjadi dalam proses ini. Dengan demikian, Whatweb berperan dalam mengumpulkan informasi yang relevan untuk menganalisis kerentanan dan membantu mengidentifikasi celah keamanan pada situs web dengan memberikan wawasan tentang teknologi dan konfigurasi yang digunakan.

3.2.2. Scanning Website Ports using Unicornscan

Unicornscan merupakan alat pemindaian jaringan yang diciptakan untuk melaksanakan pemindaian dengan efisien dan cepat, memungkinkan pemindaian jaringan yang besar dalam waktu singkat. Alat ini mampu melakukan pemindaian port dan protokol situs web secara bersamaan, memungkinkan identifikasi layanan yang beroperasi pada port tertentu. Selain itu, Unicornscan juga mendukung jenis pemindaian seperti Ping, SYN, dan UDP. Keunggulan lainnya adalah kemampuannya untuk melakukan pemindaian yang tidak terdeteksi, sehingga memungkinkan pengecekan keamanan jaringan tanpa memicu deteksi oleh firewall. Pemindaian port melibatkan pengiriman paket ke port yang terbuka dan memeriksa tanggapan terhadap permintaan SYN, yang sering kali dianggap mencurigakan. Dalam proses pemindaian ini juga mempertimbangkan potensi serangan oleh penyerang, yang dapat memvariasikan port yang digunakan dalam upaya untuk menjalankan skrip. Dalam penelitian lain, Unicornscan digunakan sebagai alat untuk melakukan pemindaian port dalam rangka mengumpulkan data serangan. Penggunaan Unicornscan dalam pemindaian port situs web bertujuan untuk:

1. Identifikasi Port Terbuka: Dengan melakukan pemindaian port menggunakan Unicornscan, peneliti dapat mengidentifikasi port yang terbuka pada website Office XY. Informasi ini penting karena dapat memberikan wawasan tentang layanan atau aplikasi yang beroperasi di balik setiap port. Port yang terbuka tanpa alasan yang jelas dapat mengindikasikan konfigurasi yang kurang aman atau potensi kerentanan yang bisa dimanfaatkan oleh penyerang.
2. Pemindaian Kerentanan Port Terkait: Setelah mengidentifikasi port yang terbuka, peneliti dapat melanjutkan dengan melakukan pemindaian kerentanan yang berkaitan dengan port tersebut. Hal ini melibatkan penggunaan alat atau metode lain untuk menguji kerentanan keamanan atau aplikasi yang berjalan pada port tersebut. Contohnya, jika terdapat port HTTP (Port 80) yang terbuka, peneliti dapat menggunakan alat seperti Nikto atau OWASP ZAP untuk mencari kerentanan yang mungkin ada pada server web yang berjalan di port tersebut.
3. Pemahaman Infrastruktur Jaringan: Melalui pemindaian port, peneliti juga dapat memperoleh pemahaman tentang infrastruktur jaringan yang digunakan oleh website Office XY. Informasi mengenai port yang terbuka dan layanan yang berjalan di belakangnya dapat memberikan gambaran tentang arsitektur jaringan dan sistem yang digunakan. Hal ini dapat membantu peneliti dalam memahami potensi serangan yang dapat dilakukan terhadap infrastruktur tersebut dan memberikan rekomendasi keamanan yang sesuai.

Dengan menggunakan Unicornscan untuk melakukan pemindaian port pada situs web, penelitian ini dapat melakukan analisis kerentanan dengan memeriksa port yang terbuka pada website Office XY. Hasil pemindaian port membantu dalam mengidentifikasi potensi kerentanan, menguji layanan keamanan yang berjalan pada port tersebut, dan memberikan pemahaman yang lebih mendalam tentang infrastruktur jaringan yang digunakan. Semua hal ini

akan berkontribusi pada upaya meningkatkan keamanan situs web dan melindungi data yang disimpan di dalamnya. Alat ini berperan dalam mengidentifikasi celah keamanan dengan mengumpulkan informasi spesifik mengenai port yang terbuka dan layanan yang berjalan pada port tersebut. Berikut adalah beberapa informasi spesifik yang dapat dikumpulkan dengan menggunakan Unicornscan:

1. Port Terbuka: Unicornscan dapat mengidentifikasi port yang terbuka pada sistem atau jaringan. Informasi ini membantu untuk mengetahui layanan atau protokol yang mungkin berjalan pada port tersebut, seperti port HTTP (80), port HTTPS (443), atau port SSH (22).
2. Spanduk Layanan dan Versi: Unicornscan juga dapat mengumpulkan informasi tentang spanduk dan versi layanan yang beroperasi pada port terbuka. Informasi ini memberikan petunjuk mengenai jenis layanan yang berjalan dan versi perangkat lunak yang digunakan. Versi perangkat lunak yang sudah usang atau rentan dapat mengungkap potensi kerentanan yang bisa dieksploitasi oleh penyerang.
3. Protokol Jaringan: Unicornscan dapat mengidentifikasi protokol jaringan yang digunakan pada port terbuka, seperti TCP (Transmission Control Protocol) atau UDP (User Datagram Protocol). Ini membantu dalam menentukan jenis layanan yang berjalan dan metode yang tepat untuk melakukan analisis lebih lanjut.
4. Respons Layanan: Unicornscan dapat menganalisis respons yang diberikan oleh layanan pada port terbuka. Respons ini memberikan tambahan informasi mengenai layanan yang sedang berjalan, struktur protokol yang digunakan, atau potensi celah keamanan yang terkait.

Dengan mengumpulkan informasi ini, Unicornscan berperan dalam mengidentifikasi celah keamanan dengan mengeksplorasi port terbuka dan

layanan yang berjalan di dalamnya. Informasi tentang port terbuka, spanduk dan versi layanan, serta protokol jaringan membantu dalam mengidentifikasi jenis layanan yang mungkin rentan atau perlu diperiksa lebih lanjut. Jika versi perangkat lunak yang sudah usang atau rentan terdeteksi, ini memberikan petunjuk tentang potensi kerentanan yang ada dan perlu diperbaiki. Selain itu, respons layanan memberikan pemahaman yang lebih mendalam tentang protokol yang digunakan dan membantu dalam melakukan analisis lanjutan terhadap layanan yang beroperasi pada port tersebut. Dengan demikian, Unicornscan berperan dalam mengumpulkan informasi tentang port terbuka, layanan yang berjalan, dan respons layanan untuk mengidentifikasi celah keamanan dan memberikan wawasan tentang potensi kerentanan pada sistem atau jaringan yang sedang dianalisis.

3.3. Vulnerability Assessment Analysis Website

Pada tahap analisis, penilaian kerentanan website ini merupakan bagian dari proses identifikasi dan klasifikasi celah keamanan berdasarkan tingkat kematangan penerapan kontrol pada sebuah website [8]. Perlunya mempertimbangkan suatu risiko dalam melakukan penilaian kerentanan dalam suatu desain pemodelan ancaman yang memungkinkan seseorang menemukan masalah dalam pengujian aplikasi [14]. Proses investigasi melibatkan perolehan informasi dan mengidentifikasi situs web yang dinilai berdasarkan analisis. Hal ini dapat dijadikan skor dalam memperbarui peningkatan keamanan situs webnya untuk kedua tujuan. Cara ini dimaksudkan untuk mengetahui tingkat kerentanan situs. Ada berbagai alat untuk memindai kerentanan melalui upaya sniffing yang ditujukan untuk Aktivitas yang termasuk dalam kategori ini termasuk mengumpulkan informasi. Aktivitas yang terlibat dalam konteks ini termasuk upaya untuk menembus jaringan nirkabel, memecahkan kata sandi, menggunakan alat forensik untuk menyelidiki insiden keamanan, melakukan spoofing hingga memanipulasi informasi, dan membahayakan perangkat elektronik [14]. Proses ini melibatkan penggunaan alat khusus yaitu Burp Suite, Skipfish, dan Rapidscan. Tahap analisis penilaian kerentanan situs web mencakup pembuatan situs web, yang melibatkan berbagai kerentanan seperti injeksi SQL. Selama fase analisis penilaian kerentanan situs

web, kerentanan seperti otentikasi tidak aman dan manajemen sesi, pembuatan skrip lintas situs (XSS), pengaturan keamanan yang salah dikonfigurasi, referensi objek langsung yang tidak aman, dan paparan data sensitif diidentifikasi. Teknik pemindaian dasar juga digunakan dalam fase ini [15].

SQL injection merupakan suatu teknik yang menggabungkan injeksi kode dengan menambahkan beberapa virus yang dapat merusak struktur database yang terdapat pada website. Tidak hanya itu, teknik ini akan menyerang dinding lapisan firewall pada jaringan yang tidak mempunyai pertahanan serangan [16]. Penyerang akan menghindari otentikasi dan otorisasi untuk mengambil informasi penting. Dalam beberapa kasus, teknik SQL injection seringkali menimbulkan berbagai persepsi bahwa kebocoran data yang berlebihan akan menjadi kekhawatiran bagi administrator untuk lebih bisa menangani kondisi tersebut dengan serius, SQL injection menggunakan metode POST dalam rangka menyimpan data [17], [18]. Script coding injection pada teknik ini mempunyai beberapa query untuk mengambil data yang dilakukan oleh penyerang, yaitu dengan menulis "SELECT Column1, Column2 FROM Table1 WHERE Column3=4", dengan menambahkan beberapa query lain seperti "UNION" atau ">=12" [19]. Otentikasi rusak merupakan kerentanan umum terkait implementasi dan teknis otentikasi pada aplikasi, hal ini dapat membuat penyerang melakukan peniruan identitas secara permanen atau sementara. Manajemen sesi yang salah dikonfigurasi menyebabkan kegagalan otentikasi. Setelah proses otentikasi selesai, komunikasi data untuk pengguna tertentu menjadi mungkin [20]. Perlunya upaya penyimpanan data rahasia dan perlunya perlindungan komponen paparan data sensitif [17].

Kontrol akses yang rusak adalah teknik yang dilakukan oleh beberapa penyerang dalam memanipulasi jalur yang tidak sah, sehingga dapat mengakses fungsionalitas data yang telah dilindungi. Kesalahan konfigurasi keamanan adalah kerentanan yang dimiliki alat OWASP, yang mengacu pada penggunaan konfigurasi sistem serangan. Serangan Cross-Site Scripting (XSS) dikategorikan sebagai kerentanan yang dapat dieksploitasi melalui skrip crossweb, yang melibatkan penyuntikan data tidak aman ke halaman web dengan tujuan mengeksekusi kode berbahaya [17], [21], [22] [24]. Sehingga terdapat hubungan

teknologi dalam pembuatan konten website dengan mengeksekusi kode di browser [25]. XSS akan berfungsi ketika website memberikan input yang tidak valid, karena dapat memungkinkan penyerang melakukan pembajakan [15], [18], [26]. XSS akan memberikan beberapa peringatan dengan menggunakan kode “string” berbentuk “alert (1)” untuk dikirimkan ke HTTP, sehingga XSS dapat memberikan observasi dalam proses pengujian penetrasi untuk menggunakan payload “<script> alert (1); < /script> atau onerror = “alert (1);" [23]. Payload akan mengidentifikasi jika ditemukan kata kunci yang tergolong rentan terhadap ancaman penyerang, sehingga akan ada tindakan URL yang disisipkan kode yang telah disuntikkan sebelumnya [24] Terdapat parameter yang terletak pada halaman HTML, dimana parameter tersebut akan menjalankan kode pada saat serangan.

Deserialisasi yang tidak aman sering digunakan untuk mengirimkan sejumlah data melalui jaringan dengan tujuan melindungi data tersebut. Hal ini memerlukan kode deserialisasi untuk dieksekusi sehingga penyerang tidak dapat memanipulasi data dengan cara yang berbahaya [19]. CSP (Content Security Policy) adalah komponen analisis kerentanan yang mampu mengolah skrip untuk mengeksploitasi situs web. Untuk melakukan hal ini, diperlukan mesin rendering seperti Firefox atau browser web lainnya agar dapat memanggil fungsi onload, yang bertujuan untuk mengumpulkan nilai hash dari skrip yang dihasilkan setelah mengakses halaman dan mengirimkannya ke pihak ketiga. Komponen ini bertanggung jawab untuk membuat header CSP yang dapat mengumpulkan banyak laporan dari sebuah situs web. Jika suatu situs web belum memiliki header CSP, maka akan disesuaikan dengan database CSP yang ada. Ada beberapa kegunaan CSP yang berdasarkan kode JavaScript dengan proses penghapusan skrip yang terdapat dalam database CSP. Jika suatu situs web tidak menggunakan kode JavaScript, maka situs web tersebut dianggap tidak aman [12]. CSRF (Cross-Site Request Forgery) merupakan salah satu komponen dari 10 analisis kerentanan teratas yang berguna dalam melakukan permintaan penipuan yang memungkinkan penyerang memodifikasi database sehingga pemilik situs web tidak dapat membedakan server berdasarkan permintaan yang sah atau tidak valid [28], [29]. Tujuan dari penggunaan metode ini dalam pembelajaran adalah sebagai berikut:

1. Mengidentifikasi Kerentanan: Tujuan utama metode ini adalah untuk mengidentifikasi potensi kerentanan yang mungkin ada di situs web Office XY. Melalui analisis kerentanan, peneliti dapat menemukan celah keamanan, konfigurasi yang rentan, atau ketidakpatuhan terhadap praktik keamanan yang baik yang dapat dimanfaatkan oleh penyerang. Dengan mengidentifikasi kerentanan, langkah-langkah perlindungan yang sesuai dapat diambil untuk memperbaiki dan melindungi situs web.
2. Mengukur Risiko: Analisis Penilaian Kerentanan Situs web membantu dalam mengevaluasi risiko yang terkait dengan kerentanan yang ditemukan. Peneliti dapat mengkategorikan kerentanan berdasarkan tingkat keparahan, probabilitas eksploitasi, dan dampak potensial. Dengan demikian, peneliti dapat memprioritaskan tindakan keamanan berdasarkan risiko yang ditimbulkan oleh masing-masing kerentanan.
3. Memberikan Rekomendasi Keamanan: Setelah mengidentifikasi kerentanan dan mengukur risiko, tujuan dari Analisis Penilaian Kerentanan Situs web adalah memberikan rekomendasi keamanan yang sesuai. Rekomendasi ini dapat mencakup langkah-langkah untuk memperbaiki kerentanan, menerapkan praktik keamanan yang lebih baik, mengonfigurasi sistem atau aplikasi secara berulang, atau menggunakan solusi keamanan tambahan. Rekomendasi ini membantu Office XY dalam meningkatkan keamanan situs web mereka dan melindungi data yang disimpan di dalamnya.
4. Memberikan Laporan Hasil: Hasil Analisis Penilaian Kerentanan Situs web disampaikan dalam bentuk laporan. Laporan ini berisi ringkasan temuan kerentanan, tingkat risiko, dan rekomendasi keamanan. Laporan ini dapat digunakan sebagai dasar untuk berkomunikasi tentang temuan dan rekomendasi kepada pihak yang berkepentingan, seperti pengelola situs web, tim keamanan, atau manajemen organisasi.

Dengan demikian, metode ini bertujuan untuk mengidentifikasi, mengukur risiko, memberikan rekomendasi keamanan, dan menyajikan laporan hasil analisis

kerentanan situs web untuk meningkatkan keamanan situs web Office XY serta melindungi data yang ada di dalamnya.

3.3.1. Burp Suite

Burp Suite didirikan pada tahun 2004 sebagai alat pengujian keamanan yang digunakan untuk menguji aplikasi web. Alat pengujian keamanan aplikasi web telah menjadi pilihan untuk pendeteksian bug yang berkembang dalam API dan aplikasi seluler. Untuk menguji keamanan aplikasi dengan efektif, seseorang harus memiliki pemahaman tentang berbagai kerentanan yang mungkin ada dalam aplikasi tersebut [38]. Jenis penelitian juga menjelaskan Burp Suite sebagai alat proxy web yang dibahas dalam makalah. Alat ini berfungsi untuk menangkap dan mengubah lalu lintas HTTP antara browser web dan server web. Burp Suite sangat berguna untuk pengujian keamanan dan pemindaian kerentanan dalam aplikasi web [32]. Selain itu, Burp Suite dipilih karena merupakan alat keamanan sumber terbuka yang digunakan untuk melakukan dan menguji fitur keamanan aplikasi web [33].

Dalam penelitian ini, Burp Suite digunakan untuk menangkap aliran data dengan mengaturnya sebagai proxy pendengar yang bertindak sebagai server proxy HTTP lokal. Pendengar proksi ini akan mengintersep semua permintaan pada port 8080 di antarmuka loopback. Dengan mengkonfigurasi browser web pada sistem penyerang sebagai server proxy, paket data akan dialihkan melalui Burp Suite. Dalam sistem penyerang yang menggunakan Burp Suite, parameter intersepsi diaktifkan, dan antarmuka ini memungkinkan akses ke semua data yang mengalir dari klien ke server ThinkSpeak selama periode waktu tertentu. Burp Suite adalah salah satu alat penting dalam pengujian penetrasi dan analisis keamanan aplikasi web. Alat ini memiliki berbagai fitur yang sangat berguna dalam mengidentifikasi kerentanan keamanan dan menguji ketahanan aplikasi web. Berikut adalah penjelasan mengenai fungsi Burp Suite:

1. Pemindaian Kerentanan: Burp Suite memungkinkan pemindaian otomatis terhadap aplikasi web dengan mengirim serangkaian serangan ke target yang ditentukan. Alat ini mencoba berbagai jenis serangan seperti injeksi

SQL, XSS, CSRF, dan lainnya untuk mengidentifikasi kerentanan yang mungkin ada.

2. Proxy Pendengar: Burp Suite berperan sebagai proxy pengamat yang memantau dan memodifikasi permintaan dan tanggapan yang dikirim antara browser dan server web. Ini memungkinkan deteksi dan manipulasi potensial seperti injeksi, overflows buffer, dan perubahan parameter
3. Pengindeksan dan Pemetaan Situs Web: Burp Suite dapat melakukan pengindeksan (spidering) dan pemetaan otomatis terhadap situs web untuk mengidentifikasi semua bagian dan fungsi aplikasi web. Ini membantu memastikan bahwa tidak ada area yang terlupakan atau rentan yang tersembunyi dari serangan
4. Analisis Kerentanan Manual: Selain fitur otomatisnya, Burp Suite juga menyediakan alat untuk melakukan analisis kerentanan secara manual. Ini memungkinkan analisis mendalam hingga kerentanan yang kompleks atau tidak dapat dideteksi secara otomatis.

Informasi yang Dikumpulkan oleh Burp Suite adalah sebagai berikut:

1. Permintaan dan Respons: Burp Suite mencatat setiap permintaan dan respons yang dikirim antara browser dan server web. Informasi ini termasuk URL, parameter, header, cookie, serta konten dan sumber kode halaman web. ini membantu dalam menganalisis interaksi antara aplikasi web dan pengguna serta mengidentifikasi potensi kerentanan.
2. Kerentanan Terkait Versi Perangkat Lunak: Burp Suite dapat mengidentifikasi versi perangkat lunak dan kerentanan terkait dengan versi tersebut. Informasi ini membantu dalam memperkirakan tingkat kerentanan berdasarkan versi perangkat lunak yang digunakan pada server web.

Kontribusi Burp Suite dalam mengidentifikasi Hole Security adalah sebagai berikut:

1. Kerentanan pemindaian otomatis : Burp Suite membantu mengidentifikasi kerentanan umum pada aplikasi web dengan melakukan pemindaian

otomatis. alat ini mengirimkan serangkaian serangan terhadap target dan menganalisis respons untuk mencari indikasi kerentanan seperti injeksi celah, kerentanan XSS, dan sebagainya.

2. Intercepting Proxy: Fitur proxy Burp Suite memungkinkan pengguna Untuk memantau dan mengubah permintaan dan tanggapan yang dikirim antara browser dan server web. ini membantu mengidentifikasi kemungkinan kerentanan yang terlewatkan dalam pemindaian otomatis, serta kemungkinan menguji serangan yang lebih mendalam.
3. Analisis Kerentanan Manual: Burp Suite menyediakan alat yang ampuh untuk melakukan analisis kerentanan secara manual. Pengguna yang mungkin ini Untuk menjelajahi dan mengaudit aplikasi web secara mendalam, mencari kerentanan yang kompleks atau Tidak terdeteksi secara otomatis.

Secara keseluruhan, Burp Suite adalah alat yang sangat berguna dalam mengidentifikasi lubang keamanan aplikasi web. Dengan fitur pemindaian kerentanan otomatis, pencegatan proxy, dan kemampuan analisis manual, Burp Suite membantu dalam mengidentifikasi kerentanan yang ada, memantau interaksi antara aplikasi web dan pengguna, serta memberikan informasi yang diperlukan untuk memperbaiki lubang keamanan yang terdeteksi.

3.3.2. Skipfish

Skipfish merupakan alat pemindaian aplikasi web open source dengan struktur pemrograman C, tujuan alat ini mirip dengan penggunaan nmap dan nessus, namun skipfish memungkinkan pengembangan web untuk dapat melakukan pengintaian. Skipfish dirancang untuk menemukan kerentanan sebelum peretas melakukan proses eksploitasi. Alat ini dapat mendefinisikan kode dalam situs web terhadap serangan injeksi XSS, SQL dan XML [41]. Studi sebelumnya dalam penggunaan alat skipfish menunjukkan bahwa Skipfish adalah alat pemindai aplikasi web sumber terbuka yang digunakan untuk menemukan kerentanan dalam aplikasi web sebelum peretas dapat mengeksploitasinya. Ini mirip dengan pemindai lubang keamanan web lainnya seperti Nmap dan Nessus. Skipfish dapat digunakan untuk memindai aplikasi

web atau situs untuk kemungkinan masalah keamanan yang mungkin ada. Itu dapat beroperasi di berbagai sistem operasi seperti Linux, BSD, MAC, dan Windows. Skipfish dapat digunakan untuk menentukan apakah kode di situs web rentan terhadap serangan umum seperti serangan skrip lintas situs (XSS), SQL, dan injeksi XML. Laporan akhir yang dihasilkan oleh alat ini dimaksudkan untuk berfungsi sebagai dasar penilaian keamanan aplikasi web [34].

Skipfish adalah pengujian pemindaian alat - struktur keamanan terfokus dan aplikasi web konten. alat ini digunakan Untuk mengevaluasi keamanan dan mengidentifikasi kerentanan terkait dengan konfigurasi, pengaturan, dan struktur aplikasi web. Tujuan penggunaan Skipfish dalam penelitian ini adalah untuk melakukan scan pada website AB Office dan XY Office. Alat ini digunakan untuk menganalisis struktur aplikasi web, mencari kerentanan terkait konfigurasi yang aman, dan mengidentifikasi kemungkinan celah keamanan yang ada. Tujuan Terakhir adalah Untuk memberikan rekomendasi perbaikan yang diperlukan Untuk meningkatkan keamanan aplikasi web. Skipfish adalah alat pemindaian keamanan yang digunakan untuk menguji keamanan aplikasi web dan mengidentifikasi lubang keamanan. Berikut penjelasan tentang Fungsi Skipfish yaitu Memindai Struktur dan Konten: Skipfish melakukan pemindaian struktur dan konten aplikasi web secara menyeluruh Untuk mengidentifikasi kerentanan dan celah keamanan. Alat ini mencoba memetakan seluruh struktur halaman web, termasuk URL, parameter, dan fitur lainnya, untuk mencari potensi kerentanan. Kemudian Informasi yang Dikumpulkan oleh Skipfish adalah:

1. Struktur Aplikasi Web: Skipfish mengumpulkan informasi tentang struktur Aplikasi web medium yang dianalisis. Ini termasuk URL, parameter, dan halaman hierarki. Informasi ini berguna Untuk pemetaan dan pemahaman lebih lanjut tentang aplikasi web medium yang dianalisis.
2. Konfigurasi Terkait Kerentanan : Skipfish mencoba mengidentifikasi kerentanan terkait dengan konfigurasi yang aman. Misalnya, alat ini dapat

mendeteksi jika pengaturan akses file atau konfigurasi server tidak memadai dan dapat menyebabkan kerentanan keamanan.

Kontribusi Skipfish dalam mengidentifikasi Keamanan Lubang :

1. Kerentanan pemindaian terstruktur: Skipfish melakukan pemindaian terstruktur pada aplikasi web untuk mengidentifikasi kemungkinan celah keamanan yang ada. Dengan aplikasi web struktur peta secara menyeluruh, alat ini dapat menemukan kerentanan terkait dengan konfigurasi, pengaturan, atau implementasi yang tidak aman.
2. Deteksi kerentanan Konfigurasi : Skipfish dapat mengidentifikasi kerentanan terkait dengan konfigurasi yang aman. alat ini dapat mengungkapkan pengaturan server yang tidak aman, izin file yang salah, atau konfigurasi lain yang dapat menunjukkan kerentanan dalam aplikasi web.

Dengan fokus pada pemindaian struktur dan konten aplikasi web, Skipfish berkontribusi dalam mengidentifikasi lubang keamanan dengan mencari kerentanan terkait dengan konfigurasi, pengaturan, dan implementasi yang tidak aman. alat ini membantu menyelesaikan pemindaian kerentanan secara menyeluruh dalam upaya meningkatkan keamanan aplikasi web.

3.3.3. RapidScan

Rapidscan adalah alat pengujian multiscanner yang menampilkan pemindaian gabungan dari beberapa alat pemindaian situs web. Rapidscan adalah alat pemindaian keamanan yang digunakan secara otomatis untuk mengidentifikasi kerentanan dalam aplikasi web. Alat ini dapat melakukan pemindaian terhadap aplikasi web dan mencari kerentanan yang sering terjadi. Tujuan penggunaan Rapidscan dalam mempelajari hal ini adalah untuk melakukan scan kerentanan pada website AB Office dan XY Office. tool ini digunakan untuk mencari kerentanan umum seperti SQL injection, XSS, LFI, dan lain-lain. Tujuan Terakhir adalah Untuk mengidentifikasi kerentanan dan memberikan rekomendasi perbaikan yang diperlukan Untuk meningkatkan keamanan aplikasi web. mohon secara keseluruhan, fungsi dari masing-masing tools (Burp Suite, Skipfish, dan Rapidscan) dalam penelitian ini adalah Untuk

melakukan pemindaian kerentanan, mengidentifikasi celah keamanan yang ada, dan memberikan rekomendasi perbaikan yang diperlukan Untuk meningkatkan keamanan aplikasi web AB Office dan XY Office di Jawa Timur. Rapidscan adalah alat pemindaian keamanan otomatis yang digunakan untuk mengidentifikasi lubang keamanan aplikasi web. Berikut penjelasan mengenai Fungsi Rapidscan:

1. Kerentanan pemindaian Otomatis: Rapidscan melakukan pemindaian otomatis ke aplikasi web dengan mencoba berbagai jenis serangan umum dan skenario yang digunakan oleh penyerang. alat ini mencari kerentanan umum yang terjadi seperti injeksi SQL, kerentanan XSS, LFI (Local File Inclusion), RFI (Remote File Inclusion), dan sebagainya.
2. Analisa Keamanan Konfigurasi: Rapidscan juga menganalisa keamanan konfigurasi pada web server untuk mencari celah yang mungkin dimanfaatkan oleh penyerang. alat ini mencoba mendeteksi konfigurasi yang rentan seperti izin file yang tidak tepat, pengaturan server tidak aman, atau parameter yang tidak dilindungi.

Berikut ini adalah Informasi yang Dikumpulkan oleh Rapidscan :

1. Kerentanan Mengenai Input Pengguna: Rapidscan mengidentifikasi kerentanan terkait dengan input pengguna seperti injeksi SQL, XSS, dan sejenisnya. Alat ini mencoba memanfaatkan celah keamanan yang mungkin terjadi ketika input pengguna tidak diproses dengan benar oleh aplikasi web.
2. Keamanan Konfigurasi: Rapidscan juga mencoba mengidentifikasi kerentanan terkait keamanan konfigurasi pada server web. Informasi yang dikumpulkan meliputi versi perangkat lunak yang rentan, pengaturan server tidak aman, atau kemungkinan konfigurasi lain yang menunjukkan kerentanan dalam aplikasi web.

Kontribusi Rapidscan dalam mengidentifikasi Lubang Keamanan adalah sebagai berikut:

1. Pemindaian Otomatis: Rapidscan membantu mengidentifikasi lubang keamanan aplikasi web dengan melakukan pemindaian otomatis. alat ini mencoba skenario dan serangan yang biasa dieksploitasi oleh penyerang. Dengan melakukan pemindaian otomatis, Rapidscan dapat mengungkapkan kemungkinan kerentanan yang terlewat atau Tidak terdeteksi dengan pengujian manual.
2. Pengidentifikasi Kerentanan Input Pengguna: Rapidscan fokus pada kerentanan terkait dengan input pengguna. Dengan metode pengujian aplikasi web merespons dan memproses masukan pengguna, alat ini membantu mengidentifikasi celah keamanan yang mungkin dieksploitasi oleh penyerang.

Secara keseluruhan, peran Rapidscan dalam mengidentifikasi lubang keamanan aplikasi web, melakukan pemindaian otomatis dan menganalisis keamanan konfigurasi. alat ini membantu meningkatkan keamanan aplikasi web dengan mengungkapkan kemungkinan kerentanan yang ada dan kemungkinan tindakan perbaikan yang tepat dapat dilakukan. Burp Suite, Skipfish, dan Rapidscan adalah alat yang digunakan dalam penelitian untuk mengevaluasi keamanan situs web. Berikut perbandingan dan evaluasi terhadap ketiga alat tersebut:

1. Burp Suite:
    a. Kelebihan: Burp Suite adalah alat yang sangat kuat dan komprehensif untuk menguji keamanan aplikasi web. Ia menyediakan berbagai fitur yang mencakup pemindaian otomatis, pengujian manual, perekaman dan pemutaran ulang HTTP, analisis kerentanan, dan permintaan manipulasi. Burp Suite juga mendukung integrasi dengan alat lain dan memiliki komunitas aktif.
    b. Keterbatasan: Meskipun Burp Suite memiliki banyak fitur, penggunaannya mungkin memerlukan pemahaman mendalam tentang keamanan web. alat ini cenderung rumit bagi pengguna yang belum berpengalaman dalam menguji keamanan. Selain itu,

versi lengkap Burp Suite adalah produk berbayar, meskipun ada juga versi gratis dengan fitur terbatas.

2. Skipfish:
    a. Kelebihan: Skipfish adalah alat yang ringan dan cepat untuk menguji keamanan web. Dia memiliki kemampuan untuk mengidentifikasi kerentanan umum seperti injeksi SQL, skrip lintas situs (XSS), dan direktori terbuka. Skipfish dapat berjalan dengan mudah dan memberikan laporan terstruktur tentang kerentanan yang ditemukan.
    b. Keterbatasan: Skipfish Kemungkinan Tidak komprehensif seperti Burp Suite di dalam fitur materi dan pengujian kelengkapan level. alat ini cenderung berfokus pada kerentanan yang umum dan mungkin terjadi. Tidak ada deteksi kerentanan yang lebih spesifik atau baru. Skipfish Lagi juga tidak aktif dikembangkan oleh pengembang, jadi Kemungkinan Tidak mendapatkan update terbaru.
3. Rapidscan:
    a. Kelebihan: Rapidscan merupakan tools yang terdiri dari beberapa sub-tool seperti Fierce Bruter Subdomain, SSLyze, NMAP, dan Wafw00f, yang digunakan untuk menguji keamanan website dari berbagai aspek. alat ini mencakup pemindaian subdomain, analisis SSL, pemindaian port, dan deteksi firewall web. Rapidscan memberikan hasil yang komprehensif dalam alat One Suite.
    b. Keterbatasan: Rapidscan Kemungkinan Tidak ada pengujian kedalaman level sendiri dan kelengkapan fitur yang sama seperti Burp Suite. Selain itu kemampuan pengujian Rapidscan Kemungkinan terbatas pada kerentanan dan komponen yang sudah diketahui, dan mungkin Tidak efektif dalam mendeteksi lebih banyak kerentanan spesifik atau baru.

3.4. Website Testing Brute Froce Attack

Pada langkah ini perlu dilakukan percobaan praktik sebagai bentuk dan upaya peneliti dalam memberikan hasil yang nyata. Peneliti akan melakukan percobaan percobaan dengan serangan brute force pada website Layanan XY. Nantinya akan diketahui website mana di antara keduanya yang tergolong memiliki struktur pembuatan keamanan website dengan integritas lebih tinggi. Ada beberapa cara atau kemungkinan yang bisa dilakukan dalam melakukan serangan yaitu dengan 2 cara seperti serangan aktif dan pasif. Upaya serangan aktif dapat dilakukan dengan menguji alat dengan merusak informasi, memalsukan pesan, dan menolak layanan. Begitu pula dengan serangan pasif, dimana serangan ini dilakukan dalam bentuk manipulasi informasi dari objek yang menjadi sasaran tanpa persetujuan administrator [4]. Serangan brute force masuk dalam kategori phishing dengan pengujian penetrasi yang memungkinkan penyerang memanipulasi email, namun beberapa penelitian menunjukkan bahwa serangan tersebut tidak memberikan akurasi yang sebenarnya, sehingga pengaruhnya kecil dalam kehidupan nyata [35]. Serangan brute force dapat dicegah menggunakan serangkaian algoritma dengan pengalihan vendor dan upaya kata sandi yang sering diubah. Solusi lainnya adalah disarankan untuk mengunci akun dengan batasan waktu. Pengujian penetrasi juga perlu mempunyai pemahaman bahwa perlu adanya pengumpulan informasi secara detail, pengujian akan memetakan informasi dari alamat IP dan membuka jaringan port website.

Pengujian penetrasi ini dilakukan dalam berbagai percobaan dalam menganalisis celah-celah yang terhubung dalam suatu sistem ke dalam jaringan. Studi sebelumnya [36] dengan hasil Makalah ini mengusulkan sistem deteksi intrusi berbasis pembelajaran mendalam untuk mendeteksi serangan brute force pada jaringan MQTT-IoT. Sistem yang diusulkan menggunakan kumpulan data terbaru, kumpulan data MQTT-IoTIDS2020, untuk melatih model pembelajaran mendalam dengan jumlah instance yang banyak dan menggunakan fitur berbasis aliran. Model klasifikasi sangat akurat dalam mendeteksi serangan tersebut dengan akurasi lebih dari 99% dalam membedakan antara serangan normal dan brute force. Sistem yang diusulkan dapat digunakan oleh administrator jaringan IoT untuk mendeteksi dan

mencegah serangan brute force pada jaringan mereka, yang dapat menyebabkan kerusakan parah pada jaringan IoT. Makalah ini juga menyediakan dua set fitur, fitur Bi-flow dan fitur Uni-flow, yang dapat digunakan oleh peneliti dan praktisi di bidang keamanan IoT untuk mengembangkan sistem deteksi intrusi untuk jenis serangan lainnya.

Serangan brute force adalah serangan yang dilakukan dengan mencoba segala kemungkinan kombinasi kata sandi secara berulang-ulang hingga menemukan kata sandi yang benar. Tujuan utama dari penggunaan metode ini dalam pembelajaran adalah sebagai berikut:

1. Uji Kekuatan Kata Sandi: Metode ini bertujuan untuk menguji kekuatan kata sandi yang digunakan pada situs web Office XY. Dengan melakukan serangan brute force, peneliti dapat memeriksa password apa yang digunakan memiliki kompleksitas yang cukup tinggi atau mudah ditebak. Jika kata sandi lemah ditemukan, hal ini dapat menunjukkan adanya kelemahan keamanan yang perlu diperbaiki.
2. Identifikasi Potensi Serangan: Dengan melakukan serangan brute force, peneliti dapat mengidentifikasi potensi serangan pada website. Jika serangan brute force berhasil, ini menandakan bahwa situs web tersebut memiliki mekanisme yang memadai untuk melindungi pengguna akun dari serangan upaya kata sandi berulang kali. Peneliti dapat menggunakan hasil ini untuk memberikan rekomendasi pengamanan yang sesuai, misalnya menerapkan kebijakan kata sandi yang lebih kuat atau mengaktifkan perlindungan fitur terhadap serangan brute force.
3. Menyadari Risiko Keamanan: Dengan melihat seberapa rentan situs web terhadap serangan brute force, peneliti dapat meningkatkan kesadaran tentang kemungkinan risiko keamanan yang dihadapi oleh situs web Office XY. Serangan brute force dapat digunakan oleh penyerang untuk mendapatkan akses yang tidak sah bagi pengguna akun atau area terlarang lainnya di situs web. Dengan mengetahui potensi risiko berikut adalah langkah-langkah pengamanan tepat yang dapat dilakukan untuk melindungi website dan data-data yang terkandung di dalamnya.

Dalam konteks penelitian ini, penggunaan metode Brute Force Attack Website Testing bertujuan untuk mengidentifikasi kerentanan keamanan terkait dengan password yang digunakan pada website Office XY. Hasil pengujian ini dapat membantu dalam mengidentifikasi kelemahan keamanan, memberikan rekomendasi untuk meningkatkan kompleksitas kata sandi dan menerapkan langkah-langkah penambahan keamanan untuk melindungi situs web dari serangan brute force. Pengujian Brute Force Attack merupakan salah satu metode pengujian keamanan yang digunakan untuk menguji kekuatan kata sandi (password) pada suatu sistem atau aplikasi. Brute Force Attack melibatkan teknik pengujian yang diulang-ulang dengan mencoba semua kombinasi yang mungkin dari kata sandi hingga menemukan yang tepat. Berikut penjelasan mengenai Fungsi Pengujian Brute Force Attack:

1. Uji Kelemahan Kata Sandi: Metode ini digunakan Untuk menguji kelemahan sistem keamanan kata sandi yang berkaitan dengan mencoba berbagai kombinasi kata sandi secara berulang-ulang. Tujuannya untuk mengetahui seberapa mudah atau sulitnya sistem atau aplikasi yang dapat diakses menggunakan teknik serangan Brute Force.
2. Evaluasi Kekuatan Kata Sandi: Dengan mencoba berbagai kombinasi kata sandi, Pengujian Brute Force Attack dapat membantu mengevaluasi kekuatan kata sandi yang digunakan dalam sistem. Jika sistem mudah ditembus dengan serangan Brute Force, maka password kemungkinan rentan dan harus diperkuat.

Informasi yang Dikumpulkan dengan Menguji Brute Force Attack adalah sebagai berikut :

1. Tes Kata Sandi: Menguji Serangan Brute Force mencoba berbagai kombinasi kata sandi Untuk mencari tahu kata sandi yang benar. Alat atau skrip yang digunakan akan mengulangi serangkaian pengujian kata sandi hingga ditemukan valid.
2. Waktu yang Dibutuhkan: Informasi yang dikumpulkan adalah waktu yang diperlukan untuk mencoba setiap kombinasi kata sandi. ini dapat

memberikan indikasi betapa mudah atau sulitnya menebak kata sandi yang benar.

Kontribusi Pengujian Brute Force Attack dalam mengidentifikasi Keamanan Lubang adalah sebagai berikut :

1. Mengidentifikasi Kata Sandi yang Lemah: Dengan melakukan serangan Brute Force, metode ini dapat mengidentifikasi kata sandi yang lemah atau rentan. Jika sistem atau aplikasi memungkinkan kata sandi mudah ditebak atau tidak kuat, serangan Brute Force Dalam konteks studi ini, penggunaan metode Brute Force Attack Pengujian Situs Web bertujuan untuk mengidentifikasi kerentanan keamanan terkait dengan kata sandi yang digunakan pada situs web Office XY. Hasil pengujian ini dapat membantu dalam mengidentifikasi kelemahan keamanan, memberikan rekomendasi untuk meningkatkan kompleksitas kata sandi dan menerapkan langkah-langkah penambahan keamanan untuk melindungi situs web dari serangan brute force. Pengujian Brute Force Attack merupakan salah satu metode pengujian keamanan yang digunakan untuk menguji kekuatan kata sandi (password) pada suatu sistem atau aplikasi. Brute Force Attack melibatkan teknik pengujian yang diulang-ulang dengan mencoba semua kombinasi yang mungkin dari kata sandi hingga menemukan yang tepat.

Berikut penjelasan tentang Fungsi Pengujian Brute Force Attack:

1. Menguji Kelemahan Kata Sandi: Metode ini digunakan Untuk menguji kelemahan kata sandi keamanan sistem yang berkaitan dengan mencoba berbagai kombinasi kata sandi secara berulang-ulang. Tujuannya untuk mengetahui seberapa mudah atau sulitnya sistem atau aplikasi yang dapat diakses menggunakan teknik serangan Brute Force.
2. Evaluasi Kekuatan Kata Sandi: Dengan mencoba berbagai kombinasi kata sandi, Pengujian Brute Force Attack dapat membantu mengevaluasi kekuatan kata sandi yang digunakan dalam sistem. Jika sistem mudah ditembus dengan serangan Brute Force, maka password kemungkinan rentan dan harus diperkuat.

Informasi yang Dikumpulkan dengan Menguji Brute Force Attack adalah sebagai berikut:

1. Tes Kata Sandi: Menguji Serangan Brute Force mencoba berbagai kombinasi kata sandi Untuk mencari tahu kata sandi yang benar. Alat atau skrip yang digunakan akan mengulangi serangkaian pengujian kata sandi hingga ditemukan valid.
2. Waktu yang Dibutuhkan: Informasi yang dikumpulkan adalah waktu yang diperlukan untuk mencoba setiap kombinasi kata sandi. ini dapat memberikan indikasi betapa mudah atau sulitnya menebak kata sandi yang benar.

Kontribusi Pengujian Brute Force Attack dalam mengidentifikasi Keamanan Lubang adalah sebagai berikut:

1. Mengidentifikasi Kata Sandi yang Lemah: Dengan melakukan serangan Brute Force, metode ini dapat mengidentifikasi kata sandi yang lemah atau rentan. Jika sistem atau aplikasi memungkinkan kata sandi mudah ditebak atau tidak kuat, serangan Brute Force dapat dengan mudah berhasil. Hal ini memberikan instruksi bahwa sistem perlu memperkuat kebijakan kata sandi atau menerapkan penambahan mekanisme perlindungan.
2. Meningkatkan Kesadaran Keamanan: Melalui Pengujian Brute Force Attack, organisasi atau pengembang dapat menyadari pentingnya penggunaan kata sandi yang kuat dan kebijakan keamanan yang tepat. Serangan Brute Force seringkali menjadi metode paling sederhana dan efektif bagi penyerang untuk mendapatkan akses yang tidak valid. Dengan menguji kekuatan kata sandi, mereka dapat meningkatkan keamanan kebijakan dan kesadaran akan pentingnya perlindungan kata sandi yang kuat.