BAB II
TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

1. **Penelitian 1 – Renato Rojas, Ana Muedas, David Mauricio**

   Mengingat proyeksi yang menunjukkan peningkatan serangan terhadap sektor kesehatan dalam bidang keamanan informasi dan kurangnya penyebaran model kematangan keamanan yang memungkinkan organisasi untuk menilai status keamanan situs web mereka, serta kekurangan pemantauan pasca evaluasi pada model yang sudah ada, maka diperlukan usulan untuk mengembangkan model kematangan keamanan aplikasi web yang lebih mudah diterapkan, terutama berfokus pada sektor kesehatan. Model yang diusulkan akan didasarkan pada metodologi Kerangka Praktik Profesional Internasional dan akan mencakup kerentanan utama yang telah diterbitkan oleh Proyek Keamanan Aplikasi Web Terbuka untuk mengidentifikasi kelemahan dalam sistem web yang dievaluasi. Dengan demikian, perusahaan klien dapat mengidentifikasi dan memperkuat kelemahan yang ada. Selain itu, panduan akan disusun untuk membantu dalam memilih strategi yang dapat meningkatkan keamanan situs web dari berbagai sudut pandang. Hasil validasi menunjukkan bahwa dari 14 pengujian yang dilakukan, 5 di antaranya disetujui, menempatkan tingkat kematangan situs web pada level 3, yang mengindikasikan validasi terhadap struktur web, meskipun dengan beberapa kekurangan atau ketidakefisienan tertentu.

2. **Penelitian 2 – Sangeeta Nagpure, Sonal Kurkure**

   Seiring dengan meningkatnya penggunaan Internet yang semakin meluas, keamanan telah menjadi faktor yang sangat krusial dalam dunia online. Keamanan situs web saat ini memiliki peran yang sangat vital. Terdapat dua jenis pengujian kerentanan yang berbeda, yaitu Penilaian Kerentanan dan Pengujian Penetrasi. Kedua jenis pengujian ini memiliki kelebihan masing-masing dan seringkali digabungkan untuk mendapatkan analisis kerentanan yang lebih komprehensif. Pengujian Penetrasi dan Penilaian Kerentanan

menjalankan peran berbeda dalam konteks yang sama. Bagi setiap organisasi, penting untuk memiliki sistem keamanan yang efektif yang diuji melalui Penilaian Kerentanan dan Pengujian Penetrasi. Aplikasi web yang memiliki potensi kerentanan terhadap serangan seperti eksploitasi Sesi, Skrip Lintas Situs, injeksi SQL, Pemalsuan Permintaan Lintas Situs, Buffer over Flows, dan Kesalahan Konfigurasi Keamanan, dan lain sebagainya, ditemukan dalam Proyek Keamanan Aplikasi Web Terbuka Top 10. Baik uji penetrasi manual maupun otomatis dapat dilakukan, tergantung pada kerentanannya. Perbandingan antara kedua jenis pengujian tersebut kemudian diulas.

3. **Penelitian 3 – Muhamad Agreindra Helmiawan, Esa Firmansyah, Irfan Fadil, Yanyan Sofiyan, Fathoni Mahardika, Agun Guntara**

   Proyek Keamanan Aplikasi Web Terbuka 10, yang dikenal sebagai OWASP 10, adalah suatu kerangka pengujian keamanan aplikasi web yang berfokus pada aspek keamanan aplikasi web guna mengidentifikasi potensi kerentanan dalam sebuah situs web. Tujuan utama dari OWASP 10 adalah memeriksa dan memastikan tingkat keamanan suatu situs web dengan mengidentifikasi sepuluh jenis kerentanan situs web yang sangat berbahaya, termasuk injeksi, masalah otentikasi, serta paparan data sensitif, di antara lain. Artikel ini melaksanakan analisis dan uji coba keamanan situs web bersama dengan enam sub-domain, dengan maksud untuk mengevaluasi tingkat keamanan situs tersebut, menentukan apakah perlu peningkatan keamanan tambahan, dan memberikan rekomendasi yang sesuai. Temuan dari artikel ini menunjukkan bahwa tingkat keamanan situs web secara keseluruhan mencapai 80%, sementara sub-domain seperti teknik informatika web, sistem informasi, manajemen informatika, sistem akademik terintegrasi, penerimaan mahasiswa, dan e-learning memiliki tingkat keamanan yang bervariasi antara 60% hingga 80%. Hal ini menandakan bahwa situs web tersebut memiliki tingkat keamanan yang cukup baik secara umum, tetapi ada beberapa sub-domain yang memerlukan perbaikan lebih lanjut dalam hal keamanan. Dalam konteks evaluasi

keamanan situs web, penting untuk terus memantau dan meningkatkan keamanan guna mengurangi potensi risiko dari serangan siber. Evaluasi dan rekomendasi yang disampaikan dalam artikel ini dapat memberikan panduan yang berharga bagi pemilik situs web untuk mengidentifikasi dan mengatasi kerentanan serta memperkuat keamanan secara keseluruhan.

4. **Penelitian 4 – Jung-Sik Cho, Sang-Soo Yeo, Sung Kwon Kim**

   Sistem Identifikasi Frekuensi Radio (RFID) adalah suatu sistem pengenalan otomatis tanpa kontak yang menggunakan tag RFID yang kecil dan memiliki biaya yang terjangkau. Sistem ini memungkinkan pengidentifikasian informasi dari tag melalui komunikasi frekuensi radio, dengan menempelkan tag RFID pada objek, baik yang hidup maupun mati. Karena sistem RFID memiliki keunggulan dalam mengenali informasi dari sejumlah besar objek secara bersamaan, maka sistem ini diharapkan dapat menggantikan penggunaan kode batang. Salah satu masalah utama yang muncul dalam penggunaan sistem RFID adalah potensi akses oleh pihak yang tidak sah terhadap informasi yang terdapat pada tag, sehingga menciptakan permasalahan seputar privasi dan pemalsuan. Dalam tulisan ini, disajikan suatu protokol otentikasi timbal balik yang menggunakan hash sebagai solusi. Protokol yang diajukan ini dirancang untuk mengirimkan nomor acak yang dihasilkan oleh tag ke server back-end tanpa mengungkapkan nomor acak tersebut. Selain itu, nomor acak tersebut digantikan dengan nilai rahasia yang akan digunakan dalam pesan respons. Karakteristik dari protokol yang diajukan memungkinkan pembuatan pesan respons yang berbeda secara tetap tanpa terpengaruh oleh permintaan yang tidak sengaja atau tidak bermakna yang dapat dihasilkan oleh pihak yang tidak sah, sementara nilai rahasianya tidak dikirimkan secara langsung. Protokol yang diusulkan juga mempersulit upaya penyerang untuk melakukan serangan brute force yang berhasil terhadap pendekatan yang digunakan.

5. **Penelitian 5 – R. Seri Devi, M. Mohan Kumar**

   Di era digital, segala hal saling terhubung melalui jaringan, dan ketika berbagai layanan disediakan oleh aplikasi web, orang menjadi rentan terhadap serangan peretasan. Menurut laporan tentang ancaman keamanan internet pada tahun 2019 yang disusun oleh Symantec, rata-rata terdapat 4.800 situs web yang memiliki potensi rentan terhadap serangan pencurian informasi digital, yang dikenal sebagai "form jacking." Tujuan utama dari makalah ini adalah untuk mengidentifikasi kerentanan dan kelemahan dalam jaringan dan aplikasi web dengan menggunakan pengujian penetrasi, dengan tujuan melindungi lembaga dari ancaman di dunia maya. Ada banyak metode pemindaian yang telah diusulkan oleh berbagai penulis untuk mengungkap kerentanannya. Namun, dalam penelitian kami, analisis dan penilaian kerentanan dilakukan menggunakan alat-alat seperti Nikto, alat proxy serangan Zed OWASP, Netcraft, Sparta, dan network mapper (Nmap) yang diuji melalui platform Kali Linux dan mesin pencari. Alat-alat seperti ZAP dan Nikto telah diuji pada sepuluh domain berbeda untuk mengidentifikasi kerentanannya. Dari hasil analisis yang dilakukan, terungkap bahwa alat ZAP berhasil mendeteksi serangan dengan tingkat risiko rendah. Dalam perbandingan antara alat Nikto dan ZAP, alat Nikto mampu mengidentifikasi lebih banyak kerentanannya dibandingkan dengan ZAP.

2.2. Licensing Research and Legality

Penelitian ini mencakup tahapan analisis situs web yang dilakukan peneliti setelah mendapatkan izin dari pemilik situs web yang diselidiki, yaitu Layanan AB & XY. Izin tersebut diperoleh melalui surat yang telah disetujui oleh pemilik situs web. Perizinan sebelum melakukan analisis situs web merupakan langkah penting dalam penelitian ini untuk memastikan kepatuhan terhadap etika penelitian dan privasi data yang terkait dengan situs web yang diselidiki. Dalam penelitian ini, peneliti menghormati hak privasi dan kepentingan pemilik situs web. Permohonan izin telah diajukan ke Layanan AB & XY untuk melakukan analisis pada situs web

mereka. Surat tersebut menjelaskan tujuan, metode, dan cakupan penelitian yang akan dilakukan. Selain itu, surat tersebut juga berisi informasi tentang keamanan data dan privasi yang harus dijaga selama proses analisis. Proses perizinan ini sangat penting untuk menjaga kepercayaan antara peneliti dan pemilik situs web. Peneliti menjelaskan tujuan penelitian dengan jelas, yaitu untuk mengidentifikasi potensi kerentanan keamanan pada situs web Layanan AB & XY. Selain itu, peneliti juga menegaskan bahwa semua data yang diperoleh selama analisis akan dijaga kerahasiaannya dan hanya digunakan untuk penelitian yang obyektif.

Pemilik situs web, dalam hal ini Layanan AB & XY, melakukan evaluasi yang cermat terhadap permohonan izin tersebut. Mereka menilai minat penelitian, metode yang akan digunakan, dan langkah-langkah yang diambil untuk melindungi keamanan data mereka. Setelah pertimbangan yang matang, pemilik situs web memberikan persetujuan tertulis melalui surat yang telah disetujui sebagai tanda persetujuan untuk melanjutkan proses analisis. Dalam konteks penelitian ini, izin ini sebelum analisis situs web memiliki makna yang sangat penting. Ini menunjukkan bahwa peneliti berkomitmen untuk menjaga integritas penelitian dan melibatkan pemilik situs web dalam prosesnya. Dengan mendapatkan izin sebelum melakukan analisis, peneliti menunjukkan sikap profesionalisme dan etika penelitian yang tinggi. Selain itu, izin sebelum analisis situs web juga melibatkan aspek hukum dan kepatuhan terhadap peraturan yang berlaku. Peneliti harus mematuhi konstitusi privasi data dan peraturan penggunaan situs web yang sah. Dalam hal ini, surat izin yang telah disetujui oleh pemilik situs web merupakan bukti bahwa penelitian ini dilakukan dengan mematuhi peraturan yang berlaku. Secara keseluruhan, perizinan sebelum melakukan analisis situs web Layanan AB & XY melalui surat yang telah disetujui oleh pemilik situs web memiliki arti penting dalam menjaga kepercayaan, integritas, dan kepatuhan terhadap aturan yang berlaku dalam penelitian ini. Langkah ini juga mencerminkan sikap profesionalisme dan etika penelitian yang tinggi dari peneliti. Dengan adanya perizinan ini, penelitian ini dapat dilakukan dengan memperhatikan aspek privasi data, keamanan, dan kepentingan pemilik situs web yang diselidiki.

2.3. Website Scanning

Web scanning, juga dikenal sebagai pemindaian web, adalah proses sistematis untuk mengidentifikasi dan menganalisis potensi kerentanan serta kelemahan keamanan pada sebuah situs web. Tujuan utama dari web scanning adalah untuk meningkatkan keamanan suatu situs web dengan mengidentifikasi potensi titik rentan yang dapat dimanfaatkan oleh pihak tidak berwenang atau penyerang. Dalam proses ini, berbagai alat dan teknik digunakan untuk memeriksa berbagai aspek dari situs web, termasuk konfigurasi server, kode sumber, dan pengaturan keamanan lainnya. Informasi yang diperoleh dari pemindaian ini mencakup potensi kerentanan seperti injeksi SQL, Cross-Site Scripting (XSS), dan berbagai masalah keamanan lainnya. Tim keamanan komputer atau profesional keamanan siber melakukan web scanning secara berkala untuk memastikan bahwa situs web tetap aman dan terlindungi dari ancaman keamanan potensial. Dengan melakukan web scanning secara teratur, risiko serangan atau eksploitasi terhadap situs web dapat diminimalkan, memastikan keamanan data sensitif dan integritas sistem. Tujuan dari web scanning adalah untuk meningkatkan keamanan situs web dengan mengidentifikasi dan memperbaiki kerentanan sebelum penyerang dapat mengeksploitasinya. Beberapa aspek yang dapat diidentifikasi melalui web scanning meliputi:

1. Kerentanan Aplikasi Web

   Pemindaian dapat mengidentifikasi kerentanan seperti injeksi SQL, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), dan lain sebagainya yang dapat dimanfaatkan oleh penyerang untuk meretas atau merusak situs web.
2. Konfigurasi Server

   Pemindaian dapat memeriksa konfigurasi server web dan mengidentifikasi masalah seperti akses yang tidak aman, izin file yang salah, atau pengaturan server yang berpotensi membuka celah keamanan.
3. Pengaturan Keamanan

Penilaian ini dapat mengungkapkan masalah dalam pengaturan keamanan, termasuk izin akses, pengelolaan kata sandi yang buruk, atau penggunaan protokol yang tidak aman.

4. Pemindaian Port

   Pemindaian dapat memeriksa port yang terbuka pada server web dan menentukan apakah ada layanan yang berjalan dan dapat diakses dari luar.

5. Pencarian Informasi

   Web scanning juga dapat mencari informasi yang tersedia publik tentang situs web, seperti direktori terbuka atau informasi kontak yang tidak diinginkan.

6. Pengumpulan Data

   Pemindaian dapat digunakan untuk mengumpulkan data tentang struktur situs web, seperti peta situs atau informasi tentang file dan direktori yang ada.

Web scanning biasanya dilakukan oleh profesional keamanan komputer atau tim keamanan siber untuk mengidentifikasi dan mengatasi kerentanan sebelum penyerang dapat memanfaatkannya. Pemindaian secara berkala dan pemantauan keamanan yang terus-menerus merupakan praktik yang penting dalam menjaga situs web tetap aman dan melindungi data sensitif yang disimpan di dalamnya.

2.4. Vulnerability Assessment Analysis Website

Vulnerability Assessment Analysis Website adalah proses evaluasi dan analisis terhadap situs web dengan tujuan mengidentifikasi dan mengukur potensi kerentanan keamanan yang ada di dalamnya. Dalam konteks ini, "vulnerability" merujuk kepada potensi kelemahan atau celah yang dapat dimanfaatkan oleh penyerang untuk meretas, merusak, atau mengakses informasi yang tidak seharusnya mereka akses. Proses ini melibatkan penggunaan alat dan metode khusus untuk memeriksa berbagai aspek situs web, termasuk konfigurasi server, sumber kode, pengaturan keamanan, dan komponen aplikasi. Hasil dari Vulnerability Assessment Analysis Website dapat mencakup identifikasi

kerentanan seperti injeksi SQL, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), dan berbagai kerentanan keamanan lainnya.

Setelah identifikasi kerentanan, langkah selanjutnya adalah menganalisis tingkat risiko yang terkait dengan setiap kerentanan yang ditemukan. Ini membantu pemilik situs web atau tim keamanan untuk memprioritaskan perbaikan dan tindakan yang harus diambil untuk mengatasi kerentanan tersebut. Vulnerability Assessment Analysis Website adalah salah satu aspek penting dalam menjaga keamanan situs web, terutama di lingkungan internet yang penuh dengan ancaman cyber. Dengan melakukan evaluasi yang teratur dan memperbaiki kerentanan yang ada, situs web dapat lebih terlindungi dari serangan cyber dan risiko potensial yang dapat merugikan integritas data serta reputasi online.

2.5. Website Testing Brute Froce Attack

Website Testing Brute Force Attack adalah salah satu metode pengujian keamanan situs web yang melibatkan upaya untuk mengidentifikasi potensi kerentanan terhadap serangan brute force. Serangan brute force adalah taktik di mana penyerang mencoba secara berulang-ulang untuk menebak kombinasi username dan password yang benar untuk mengakses akun atau sistem yang dilindungi oleh kata sandi. Dalam konteks pengujian keamanan situs web, tindakan ini biasanya dilakukan oleh profesional keamanan atau etis hacker dengan izin dari pemilik situs web untuk menilai sejauh mana situs web tahan terhadap serangan brute force. Selama Website Testing Brute Force Attack, pengujian dilakukan dengan mencoba berbagai kombinasi kata sandi yang mungkin, biasanya dengan menggunakan alat otomatis. Tujuannya adalah untuk menguji apakah situs web memiliki mekanisme perlindungan yang memadai terhadap serangan brute force, seperti penguncian akun setelah beberapa percobaan gagal atau memerlukan verifikasi captcha setelah beberapa upaya login yang salah.

Hasil dari pengujian ini memberikan pemilik situs web pemahaman tentang seberapa kuat perlindungan mereka terhadap serangan brute force. Jika ada kerentanan atau kelemahan yang ditemukan, pemilik situs web dapat mengambil tindakan perbaikan untuk meningkatkan keamanan dan mencegah serangan brute

force yang berhasil. Penting untuk dicatat bahwa Website Testing Brute Force Attack harus dilakukan dengan izin dan persetujuan dari pemilik situs web, dan biasanya dilakukan sebagai bagian dari pengujian keamanan komprehensif untuk memastikan bahwa situs web terseut tahan terhadap berbagai jenis serangan cyber.