**NAMA : IMAS PRADHIPTA BAGASKARA NIM : 16532674**

**KELAS : 4D PRODI : TEKNIK INFORMATIKA**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Topik Judul** | **Judul** | | **Latar Belakang** | | **Kajian Literatur** | | **Design Penelitian** | | **Hasil** | | **Kesimpulan** | |
| Website Security dan Vulnerability | Perancangan Replikasi Basis Data MYSQL dengan Mekanisme Pengamanan Menggunakan SSL Encryption | | Karena faktor pentingnya data dan informasi pada organisasi small medium business (SMB), maka diperlukan suatu replikasi basis data sehingga jika terjadi suatu keadaan force majure, organisasi tersebut tidak akan mengalami kehilangan data. Replikasi basis data ini melibatkan paling sedikit 2 sistem basis data yang terhubung dalam suatu jaringan komputer | | <https://media.neliti.com/media/publications/102982-ID-perancangan-replikasi-basis-data-mysql-d.pdf> | | informasi suatu organisasi. Di pengujian simulasi laboratorium ini akan ditempatkan 2 server basis data dan 1 buah komputer monitoring yang berguna untuk memantau dan menganalisa serta mengevaluasi pertukaran data antara 2 server basis data yang diujikan. | | Implementasi Replikasi Basis Data dengan MySQL Server | | Telah berhasil dilakukan replikasi basis data MySQL dengan dua buah server yaitu server master dan server slave, baik menggunakan mekanisme pengamanan SSL maupun tanpa pengamanan SSL.  Replikasi basis data MySQL dengan tanpa mekanisme pengamanan SSL memunculkan celah tersendiri yaitu hasil komunikasi paket datanya dapat di sadap dan pesan yang dikirimkan dalam bentuk pesan plain tidak tersantikan | |
| **Topik Judul** | **Judul** | **Latar Belakang** | | **Kajian Literatur** | | **Design Penelitian** | | **Hasil** | | **Kesimpulan** | |
| Website Security dan Vulnerability | Menangkal Serangan SQL Injection dengan Parameterized Query | Dalam penelitian ini diperkenalkan jenis penyerangan dengan cara sql injection secara server side scripting untuk kemudian diberikan solusi menghindarinya | | <https://researchgate.net/publication/318964950_Menangkal_Serangan_SQL_Injection_Dengan_Parameterized_Query/fulltext/5988650daca27266ada490d0/318964950_Menangkal_Serangan_SQL_Injection_Dengan_Parameterized_Query.pdf?origin=publication_detail> | | Memberikan pola serangan SQL Injection, Membangun rangkaian pemrograman yang berisikan metode parameterized query dengan php, Mengambil kesimpulan dari keseluruhan pengujian | | Menunjukan hasil dari query injection terhadap halaman autentikasi yang telah diberikan parameterized query. Pada tahapan ini membuktikan bahwa serangan melalui password dapat dicegah dengan baik | | Halaman autentikasi merupakan pintu pertama keamanan suatu data harus memiliki fasilitas pertahanan yang tinggi yang mampu mengikuti perkembangan teknologi dengan benar yang bertujuan mengikuti pola berpikir para penyerang yang semakin banyak karakteristik dan cara kerjanya nya.  Menentukan konsep pertahanan pada lapisan awal suatu layanan berbasis web perlu memperhatikan beberapa hal anatara lain : kenyamanan pengguna layanan dan pengaruhnya terhadap kecepatan proses. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Topik Judul** | **Judul** | **Latar Belakang** | **Kajian Literatur** | **Design Penelitian** | **Hasil** | **Kesimpulan** |
| Website Security dan Vulnerability | Analsis Vulnerability Web Based Application Menggunakan Nessus | Permintaan akses data dari client ke web server akan meningkat seiring dengan jumlah client yang terhubung. Dengan semakin meningkatnya jumlah client akan sebanding dengan tingkat ancaman, bahaya bahkan serangan ke web server yang akan menyebabkan terjadinya gangguan di web server. Menghindari kondisi semacam itu dapat dicegah dengan melakukan analisa berbagai kelemahan atau disebut dengan vulnerability pada web server sebelum web application dipublikasikan. | <http://download.portalgaruda.org/article.php?article=362790&val=8290&title=ANALISIS%20VULNERABILITY%20WEB%20BASED%20APPLICATION%20MENGGUNAKAN%20NESSUS> | Metode yang digunakan dalam analisa vulnerability ini dengan cara menscan web application yang telah di unggah di web server kemudian di scan menggunakan vulnerability scanner yakni Nessus. Adapun bagan dari topologi jaringan bisa dilihat pada gambar 2 di bawah ini. Topologi yang digunakan sedapat mungkin disesuaikan dengan kenyataan saat web application di publikasikan di sebuah web hosting. | Hasil dari analisa vulnerability terhadap web application dapat diketahui beberapa kelemahan- kelemahan yang bisa menjadi pintu masuk bagi attacker untuk menguasai web application. Hasil yang ditunjukkan Nessus Scanner dapat diketahui terdapat 95 jenis kelemahan terdiri dari berbagai kategori yakni critical, high, mediun dan info. Pada gambar 4 di bawah ini ditunjukkan hasil dari Nessus Scanner. | Web application yang di evaluasi menggunakan Nessus Scannerterdapat beberapa celah bagi attacker untuk bisa menguasi web application yang telah dibuat oleh administrator. Terdapat 95 macam kelemahan dengan 4 kategori yakni critical, high, medium dan info.  Dengan menggunakan Nessus Scanner, sebuah web application bisa di evaluasi mengenai kelemahan-kelemahan yang terjadi sebelum sebuah web application tersebut di upload pada sebuah web server. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Topik Judul** | **Judul** | **Latar Belakang** | **Kajian Literatur** | **Design Penelitian** | **Hasil** | **Kesimpulan** |
| Website Security dan Vulnerability | Konsep Solusi Keamanan Web pada Pemrograman PHP | Keamanan Web menjadi lebih lagi dibutuhkan dengan adanya kasus-kasus pencurian melalui Web, penipuan, perusakan, virus, worm, dan lain-lain. pengembangan Web akan digunakan untuk aplikasi-aplikasi yang rentan atau kritis, maka kemanan yang baik akan menghindarkan kerugian yang mungkin didapat yang jumlahnya mungkin bisa sangat besar, baik secara material maupun nonmaterial. | <http://jurnal.stmik-mi.ac.id/index.php/jcb/article/download/23/23> | Sebagai konsekuensi kepraktisan dan kemudahannya, instalasi default PHP banyak memiliki kelemahan keamanan. Variabel global di PHP dapat berasal dari masukan pengunjung Web (dari GET/POST/Cookie), sehingga bila programernya ceroboh tidak melakukan inisialisasi tiap variabel sebelum pemakaian, seorang penyerang dapat memasukkan nilai-nilai awal variabel ke dalam skrip untuk mengubah kelakuannya. Sebelum PHP 3.0.18 terdapat bug pada file upload yang banyak dieksploitasi untuk menembus banyak situs PHP. | Interpreter PHP mempunyai kemampuan untuk mengakses hampir semua host-file system, network interfaces, IPC, dan lain-lain. Konsekwensinya PHP potensial mendapat serangan dari attacker. Untuk meminimalkan serangan programmer harus menyadari dan mengetahui hal-hal yang tidak diharapkan (merusak) saat program dijalankan, yaitu pengetahuan kelemahan suatu sistem dan modus serangan secara umum yang diarahkan untuk mengganggu keamanan program tersebut. Lubang keamanan yang paling umum di dalam skrip PHP dan tak terkecuali pada aplikasi web yang manapun, adalah berkaitan dengan User Input. | Teknologi Web server merupa-kan inti setiap desain aplikasi Web. Tanpa memberi perhatian khusus pada keamanannya, konfigurasi defaultnya justru akan menjadi sejumlah jalan penyerangan bagi para penyerang. Konfigurasi default biasa-nya memberikan berbagai kemudahan dan fitur tambahan, namun tidak selalu diperlukan. Untuk itu perlu diperhatikan sekali lubang keamanannya. |
| **Topik Judul** | **Judul** | **Latar Belakang** | **Kajian Literatur** | **Design Penelitian** | **Hasil** | **Kesimpulan** |
| Website Security dan Vulnerability | Membangun System Keamanan ARP Spoofing Memanfaatkan ARPWATCH dan Addons Firefox | Dalam mencegah ancaman terhadap kriminalitas yang di lakukan di dalam jaringan internet (dunia maya) banyak tool yang dapat digunakan untuk melindungi sistem yang dibangun. Terdapat banyak tool dan IDS (Intrusion Detection System) yang dapat di download karena bersifat free, prabayar serta open source. Arpwatch adalah salah satu tool yang dapat mendeteksi serangan arp spoofing serta melihat anomali paket data yang berjalan di dalam jaringan dan dapat membari laporan kepada user melalui email. Addons firefox dimanfatkan untuk mendeteksi serta memblok serangan arp spoofing dari user. | <https://media.neliti.com/media/publications/236162-membangun-sistem-keamanan-arp-spoofing-m-979186ed.pdf> | ARP Spoofing merupakan cara untuk memanipulasi pemetaan ARP Cache. ARP Spoofing akan membuat paket ARP Reply palsu dan dikirimkan secara terus-menerus. ARP Spoofing juga biasanya diikuti dengen serangan untuk menangkap atau mengambil alih komunikasi yang tidak terenkripsi atau tidak memiliki digital signature. Kemudian dilakukan analisa terhadap simulasi program ARP Spoofing yang dibuat, dan diharpkan dapat memberi solusi dengan mengimplementasikan VLAN dan Bandwidth Management dalam jaringan lokal agar komunikasi yang terjadi tidak dapat disadap atau diambil alih oleh attacker. | Pengujian sistem dapat dilakukan dalam jaringan menggunakan aplikasi servicearpwatch fillter yang dibuat untuk mendeteksi serangan serta melakukan actiondrop dalam jaringan.  Dalam mendeteksi serangan arp spoofing, user menginstall apliasi addons firefox untuk mendeteksi serangan arp spoofing serta melindungi dirinya dari dalam jaringan. Dapat dilihat pada aplikasi addons firefox yang belum menampilkan serangan arp spoofing. | Aplikasi atau script service arpwatch fillter dipasangkan pada komputer server yang akan mendeteksi adanya serangan ARP Spoofing di dalam jaringan.  Aplikasi addons firefox akan menampilkan warning pada device user dan user dapat melakukan blok terhadap attacker sehingga Mikrotik dengan langsung akan melakukan action blok terhadap alamat mac attacker.  Tabel uji coba arp spoofing pada komputer user dalam percobaan satu, dua dan tiga dapat mendeteksi adanya serangan arp spoofing dan dapat melakukan action blok secara langsung ke Mikrotik, dengan persentase 83% sehingga dari sisi keamanan di dalam jaringan tersebut aman dikarenakan terhindar dari Attacker. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Topik Judul** | **Judul** | **Latar Belakang** | **Kajian Literatur** | **Design Penelitian** | **Hasil** | **Kesimpulan** |
| Website Security dan Vulnerability | Pengembangan Pencegahan Serangan Distributed Denial of Services (DDOS) pada Sumber Daya Jaringan Dengan Integrasi Network Behavior Analysis dan Client Puzzle. | Serangan DDoS dapat mengakibatkan ketidakmampuan server untuk melayani service request yang sah, dimana serangan ini memanfaatkan sejumlah besar komputer untuk menjalankan serangan DoS kepada server, web service, atau sumber daya jaringan lain. Mengingat resiko besar yang diakibatkan serangan DDoS ini, banyak peneliti yang terdorong untuk merancang mekanisme pengamanan sumber daya jaringan. | <http://juti.if.its.ac.id/index.php/juti/article/viewFile/388/277> | Secara umum, paket data yang beredar di jaringan menggunakan protokol TCP / IP untuk transmisinya. Paket ini sendiri tidak berbahaya, tetapi jika ada terlalu banyak paket yang abnormal, maka perangkat jaringan atau server akan mengalami kelebihan beban/overload. Kondisi ini dapat dengan cepat mengkonsumsi sumber daya sistem. Kasus lain adalah jika paket serangan memanfaatkan celah keamanan pada protokol tertentu (misalnya request layanan yang tidak lengkap atau penyalahgunaan formasi protokol). Tindakan ini juga dapat menyebabkan kegagalan perangkat jaringan atau server. | Dari hasil percobaan, terbukti metode ini dapat mendeteksi serangan DDoS sekaligus menjamin bahwa service request yang sah mendapat pelayanan yang seharusnya sehingga server dapat melayani service request dengan baik. | Berdasarkan hasil analisa uji coba, tingkat presisi sistem untuk mendeteksi serangan DDoS sangat baik, mencapai tingkat 86.67% yang berarti sistem dapat mendeteksi dengan tepat web service yang diserang, namun mekanisme ini juga memiliki tingkat sensitifitas yang tinggi, yaitu 90.09% yang mendeskripsikan bahwa kemampuan sistem untuk mendeteksi serangan DDoS sangat tergantung pada parameter/tresholding yang ditentukan (dalam hal ini adalah tingkat kepadatan jaringan maksimal untuk identifikasi serangan DDoS). |
| **Topik Judul** | **Judul** | **Latar Belakang** | **Kajian Literatur** | **Design Penelitian** | **Hasil** | **Kesimpulan** |
| Website Security dan Vulnerability | Melindungi Aplikasi dari Serangan CrossSite Scripting (XSS) Dengan Metode Metacharacter | CrossSite Scripting merupakan jenis serangan injection terhadap situs dengan mengandalkan kelemahan dari target atau pengguna internet. Penyerang akan memanfaatkan kelemahan pengguna melalui ajakan atau bujukan untuk mengikuti arahan menuju suatu kondisi tertentu yang telah dimuati oleh usaha untuk pencurian data, kerahasiaan atau perintah tertentu melalui code scripting oleh penyerang. | <http://teknosi.fti.unand.ac.id/index.php/teknosi/article/download/170/85> | Menangkal Serangan SQL Injection Dengan Parameterized Query merupakan jurnal yang membahas tentang metode menangkal serangan terhadap situs secara injection melalui halaman login yang di berikan logika SQL, dengan tujuan dimana query yang diberikan akan dianggap selalu bernilai benar. Tujuan utama dari SQL Injection adalah memasuki database melalui user dan password yang telah diambil alih oleh penyusup untuk dikuasai Rancang Bangun Add-ons Deteksi Cross Site Scripting Pada Peramban Mozilla Firefox merupakan jurnal yang membahas secara khusus serangan Cross-Site pada browser. | Hasil Eksperimen membuktikan bahwa metode metacharacter terbukti mampu menutup masuknya serangan Cros Site Scripting terhadap sebuah situs. | Metode metacharacter mudah untuk diimplementasikan dan efekti dalam hasil yang dicapai.  Menentukan konsep keamanan pada lapisan awal suatu layanan berbasis web perlu memperhatikan beberapa hal antar lain: kenyamanan pengguna layanan dan pengaruhnya terhadap kecepatan proses |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Topik Judul** | **Judul** | **Latar Belakang** | **Kajian Literatur** | **Design Penelitian** | **Hasil** | **Kesimpulan** |
| Website Security dan Vulnerability | Keamanan Aplikasi Web Melalui Penerapan Cross Site Request Forgery(CSRF) | Aplikasi web merupakan platform perangkat lunak terbaru yang dominan pada saat ini, dikembangkan setiap harinya demi memudahkan kinerja manusia dalam menyelesaikan pekerjaan. Serangan cross site request forgery(CSRF) merupakan ancaman aplikasi web yang ditunjukkan untuk mencuri informasi pengguna aplikasi web. | <https://www.syekhnurjati.ac.id/jurnal/index.php/itej/article/download/1517/1035> | Dalam proyek ini, penulis memberitahukan bahwa kita bisa mengembangkan sebuah alat open source SASERIDE yang mana merupakan alat semi otomatis dan pengembangan kode program SERIDE yang telah ada.(Ramarao, 2009, p. 82) Dari penelitian yang telah dilakukan tersebut di atas disimpulkan bahwa penggunaan token dalam mengamankan aplikasi web merupakan pilihan yang tepat untuk mengatasi serangan cross site request forgery dimana token akan di enkripsi terlebih dahulu agar penyerang tidak dapat mengira apa isi token tersebut. | Mengetahui penggunaan metode enkripsi keamanan aplikasi web melalui teknik cross site request forgery(csrf) protection, Merancang kunci enkripsi token keamanan aplikasi web melalui teknik cross site request forgery(csrf) protection, Mengimplementasi keamanan aplikasi web melalui teknik cross site request forgery(csrf) protection, Mengevaluasi keamanan aplikasi web melalui teknik cross site request forgery(csrf) protection. | Pada penrancangan kunci enkripsi diperlukan kunci yang tidak mudah ditebak, tidak sering dipakai, dan tidak pendek sehingga, kunci tidak mudah ditebak atau lolos ke tangan orang yang memiliki niat jahat pada aplikasi web. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Topik Judul** | **Judul** | **Latar Belakang** | **Kajian Literatur** | **Design Penelitian** | **Hasil** | **Kesimpulan** |
| Website Security dan Vulnerability | Analisis Perbandingan Penetration Testing Tool Untuk Aplikasi Web | Dalam upaya untuk memecahkan masalah keamanan dan mematuhi peraturan keamanan yang berlaku, pakar keamanan telah mengembangkan berbagai metode jaminan keamanan yang mencakup bukti kebenaran desain berlapis, lingkungan rekayasa perangkat lunak dan uji penetrasi. | <http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/download/73/37/> | Proses ini melibatkan analisis aktif sistem untuk setiap potensi kerentanan, termasuk konfigurasi sistem yang buruk atau tidak tepat, kelemahan hardware dan software, dan kelemahan operasional dalam proses atau penanggulangan teknis. Beberapa tool yang digunakan dalam uji penetrasi ini adalah w3af , wapiti, dan arachni dari setiap tool ini mempunyai kelebihan dan kekurangan dalam melakukan uji penetrasi yang memungkinkan tool tersebut apakah dapat mendeteksi semua kerentanan pada web aplikasi yang di uji. | Hasil analisis yang didapat dengan menggunakan tool w3af, wapiti, dan arachni setelah melakukan 5 kali percobaan memberikan hasil tool arachni yang mendapatkan kerentanan pada identifikasi tersebut lebih banyak dari tool w3af dan wapiti. | Identifikasi yang dilakukan dengan menggunakan tools w3af ,wapiti, dan arachni dapat dibandingkan dengan menggunakan 5 kali percobaan agar setiap aplikasi web yang di identifikasi dapat hasil yang berbeda. |
| **Topik Judul** | **Judul** | **Latar Belakang** | **Kajian Literatur** | **Design Penelitian** | **Hasil** | **Kesimpulan** |
| Website Security dan Vulnerability | Uji Kelayakan Implementasi SSH sebagai Pengaman FTP Server dengan Penetration Testing | Beberapa penelitian yang berkaitan dengan penetration testing dan FTP Server telah dilakukan diantaranya penelitian yang membahas analisa keamanan FileZilla Server sebagai salah satu server FTP berbasis Open Source. Selain itu, penelitian yang membahas tentang bentuk-bentuk penetration testing yang dilakukan pada jaringan komputer yang memiliki mekanisme protokol kemananan tinggi. | <https://jurnal.uns.ac.id/itsmart/article/download/620/572> | Pengujian dilakukan pada sistem yang dibangun sebagai objek penelitian dimana sistem tersebut terisolasi sehingga tidak memerlukan manajemen user secara mendetail. Sistem dibangun di Lab Komputer Jurusan Informatika UNS. Pengujian akan berfokus pada fungsi SSH dalam mengamankan transmisi FTP namun tidak mengikutsertakan teknik enkripsi yang digunakan pada SSH kedalam topik penelitian. Metode yang digunakan adalah white-box testing dimana pengujian dilakukan dari dalam jaringan dengan tanpa melakukan pengumpulan informasi terlebih dahulu. | Hasil penelitian menunjukkan bahwa implementasi SSH secara standar tidak cukup efektif untuk mengamankan FTP. Sebab SSH hanya mampu melindungi transmisi FTP dari penyadapan data. SSH terbukti rentan terhadap serangan brute force dan fitur keamanannya tidak berpengaruh pada pengaksesan backdoor yang telah dipasang pada FTP. SSH memerlukan konfigurasi khusus dan piranti pendukung lain untuk mengoptimalkan fungsi keamanannya. | Hasil penelitian ini membuktikan bahwa implementasi SSH secara standart tidak cukup efektif dalam mengamankan transmisi FTP. SSH secara standar terbukti hanya dapat melindungi transmisi FTP dari penyadapan pada fase sniffing. Teori tentang kelemahan SSH pada brute force rootlogin terbukti benar dengan hasil yang didapat pada fase brute force dengan Hydra. Password dari root dapat ditemukan dalam waktu kurang dari 2 menit walaupun estimasi total waktu yang dibutuhkan untuk mencoba semua kemungkinan password berjumlah 1707 jam dan 40 menit. |