**CHECKLIST PENANGANAN KERENTANAN & KEAMANAN WEB SERVER**

**DI {{nama oraganisasi}}**

**{{logo organisasi}}**

|  |  |
| --- | --- |
| No Dokumen | : 0.1 (Draft) |
| Revisi | : 00 |
| Tanggal Terbit | : |

|  |  |  |
| --- | --- | --- |
| Disusun  oleh : | Diketetahui  oleh: | Disetujui / Disahkan  oleh : |
|  |  |  |
| **NN**  NN | **NN**  NN | **NN**  NN |

**Riwayat Dokumen**

|  |  |  |
| --- | --- | --- |
| **Versi** | **Tanggal** | **Perubahan** |
| 0.1 (Draft) | 28/02/2023 | Rilis draft awal dengan hanya menyalin sepenuhnya konten dari **PEDOMAN TATA KELOLA KEAMANAN APLIKASI BERBASIS WEB - BSSN** |
| … | … | … |
|  |  |  |



**CHECKLIST PENANGANAN KERENTANAN BERBASIS OWASP**

# Tabel 5.1 Checklist Penanganan Kerentanan Berbasis OWASP

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Jenis Kerentanan** | **Checkbox** | **Aktivitas** |
| 1. | SQL Injection | * Done * Not Done * N/A | Membuat semua pernyataan SQL menggunakan placeholder. |
| * Done * Not Done * N/A | Saat membuat pernyataan SQL melalui concatenation maka gunakan aplikasi khusus yang ditawarkan oleh  mesin database untuk melakukan escaping dan memperbaiki literal pernyataan SQL dengan benar. |
| * Done * Not Done * N/A | Tidak menulis pernyataan SQL langsung di parameter yang akan dilewatkan ke aplikasi web. |
| * Done * Not Done * N/A | Membatasi informasi untuk ditampilkan dalam pesan kesalahan pada browser web. |
| * Done * Not Done * N/A | Memberikan hak minimum untuk akun basis data. |
| 2. | Injeksi perintah – perintah OS | * Done * Not Done * N/A | Menghindari penggunaan fungsi yang dapat memanggil perintah shell. |
| * Done * Not Done * N/A | Saat menggunakan fungsi yang dapat memanggil perintah shell, periksa semua variabel yang membentuk parameter shell dan pastikan untuk mengeksekusi hanya mereka  yang diberikan untuk dieksekusi. |
| 3. | Parameter Nama Jalur Tidak Dicari / Direktori Traversal yang Tidak Benar | * Done * Not Done * N/A | Tidak mencantumkan nama file yang disimpan di server web secara langsung menggunakan parameter eksternal. |
| Menggunakan direktori tetap untuk menangani nama file dan membatalkan nama direktori dalam nama file. |
| * Done * Not Done * N/A | Mengelola izin akses file dengan benar. |
| * Done * Not Done * N/A | Mengecek nama file |
| 4. | Manajemen Sesi yang tidak benar | * Done * Not Done * N/A | Membuat ID sesi yang sulit ditebak. |
| * Done * Not Done * N/A | Tidak menggunakan parameter URL untuk menyimpan ID sesi. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | * Done * Not Done * N/A | Mensetting atribut aman pada cookie ketika menggunakan HTTPS. |
| * Done * Not Done * N/A | Mulai sesi baru setelah login berhasil. |
| * Done * Not Done * N/A | Mengeluarkan rahasia setelah login dan autentikasi pengguna setiap kali pengguna bergerak di situs web. |
| * Done * Not Done * N/A | Menggunakan ID sesi acak |
| * Done * Not Done * N/A | Menetapkan tanggal kedaluwarsa cookie dengan hati-hati saat menyimpan id sesi dalam cookie. |
| 5. | Cross- SiteScripting | Tindakan agar Aplikasi Web tidak mengizinkan input teks HTML | * Done * Not Done * N/A | Melakukan Escaping untuk semua yang akan dikeluarkan ke halaman web. |
| * Done * Not Done * N/A | Saat mengeluarkan URL dalam HTML, diizinkan hanya yang memulai dengan pola tertentu, seperti "http: //" dan  "https: //". |
| * Done * Not Done * N/A | Tidak membuat konten tag <script> ... </script> secara dinamis. |
| * Done * Not Done * N/A | Tidak mengizinkan mengimpor stylesheet dari situs web yang tidak jelas. |
| * Done * Not Done * N/A | Mengecek nilai input |
| Tindakan untuk Aplikasi Web yang mengizinkan input teks  HTML | * Done * Not Done * N/A | Membuat pohon parse dari input teks HTML dan ekstrak hanya elemen yang tidak mengandung skrip. |
| * Done * Not Done * N/A | Hapus string skrip dalam input teks HTML. |
| Tindakan umum untuk semua aplikasi web | * Done * Not Done * N/A | Setting parameter rangkaian karakter dari header jenis konten HTTP. |
| * Done * Not Done * N/A | Setting atribut HttpOnly cookie dan nonaktifkan metode TRACE untuk mencegah pengungkapan informasi cookie. |
| 6. | CSRF(Cross-Site Request Forgery) | | * Done * Not Done * N/A | Akses halaman web, di mana operasi tertentu akan dijalankan, melalui metode POST rahasia memiliki halaman web sebelumnya menyisipkannya dalam file  tersembunyi yang disembunyikan, dan menjalankan operasi yang diminta hanya jika kebijakan ini benar. |
| * Done * Not Done * N/A | Meminta hak password sebelum menjalankan operasi yang diminta dan melanjutkannya hanya ketika password  tersebut benar. |
| * Done * Not Done * N/A | Memeriksa pengarah apakah URL yang diharapkan jika ya berlanjut hanya ketika URL benar |
| * Done * Not Done * N/A | Memberi tahu alamat email yang ditentukan sebelumnya secara otomatis ketika operasi penting telah dilakukan. |

|  |  |  |  |
| --- | --- | --- | --- |
| 7. | Http Header Injection | * Done * Not Done * N/A | Tidak mencetak header HTTP secara langsung tetapi melalui API HTTPheader yang disediakan oleh lingkungan  eksekusi atau bahasa pemrograman. |
| * Done * Not Done * N/A | Jika HTTP header API yang menawarkan netralisasi umpan tidak tersedia maka terapkan secara manual. |
| * Done * Not Done * N/A | Hapus semua karakter umpan baris yang muncul di input teks eksternal. |
| 8. | Mail Header Injection | * Done * Not Done * N/A | Gunakan nilai tetap untuk elemen header dan output semua external input ke badan email. |
| * Done * Not Done * N/A | Jika hal diatas tidak diterapkan, nilai tetap tidak dapat digunakan untuk header, gunakan API pengiriman email  yang ditawarkan oleh lingkungan atau bahasa eksekusi aplikasi web. |
| * Done * Not Done * N/A | Tidak mencantumkan alamat email dalam HTML. |
| * Done * Not Done * N/A | Hapus semua karakter umpan baris yang muncul di input teks eksternal. |
| 9 |  | * Done * Not Done * N/A | Ketika sebuah situs web memerlukan kontrol akses, terapkan mekanisme autentikasi yang mengharuskan pengguna memasukkan semacam informasi rahasia, seperti kata sandi. |
| * Done * Not Done * N/A | Terapkan otorisasi serta otentikasi untuk memastikan  bahwa pengguna login tidak dapat berpura-pura menjadi pengguna lain dan mengakses data mereka. |



**CHECKLIST PENGELOLAAN KEAMANAN WEB SERVER**

# Tabel 5.2 Checklist Pengelolaan Keamanan Web Server

|  |  |  |
| --- | --- | --- |
| **No** | **Checkbox** | **Aktivitas** |
| **1.** | **Perencanaan konfigurasi dan deployment Web Server** | |
| * Done * Not Done * N/A | Mengidentifikasi fungsi- fungsi dari Web server |
| * Done * Not Done * N/A | Mengidentifikasi kategori informasi yang akan disimpan, diproses, dan dikirim melalui Web server |
| * Done * Not Done * N/A | Mengidentifikasi kebutuhan keamanan informasi |
| * Done * Not Done * N/A | Mengidentifikasi bagaimana informasi dipublikasikan ke Web server |
| * Done * Not Done * N/A | Mengidentifikasi kebutuhan keamanan *host* lain yang terlibat (misalnya backend database atau Web server) |
| * Done * Not Done * N/A | Mengidentifikasi *host* yang ditunjuk untuk menjalankan Web server |
| * Done * Not Done * N/A | Mengidentifikasi layanan jaringan yang akan diberikan atau didukung oleh Web server |
| * Done * Not Done * N/A | Mengidentifikasi kebutuhan keamanan dari suatu layanan tambahan yang diberikan atau didukung oleh Web server |
| * Done * Not Done * N/A | Mengidentifikasi bagaimana Web server akan dikelola |
| * Done * Not Done * N/A | Mengidentifikasi para pengguna dan kategori para pengguna dari Web server dan tentukan priviledge dari setiap kategori pengguna |
| * Done * Not Done * N/A | Identifikasi metode otentikasi pengguna pada Web server dan bagaimana data otentikasi akan diproteksi |
| * Done * Not Done * N/A | Mengidentifikasi bagaimana akses ke sumber informasi akan diberlakukan |
| * Done * Not Done * N/A | Mengidentifikasi mekanisme keamanan fisik yang tepat |

|  |  |  |  |
| --- | --- | --- | --- |
|  | * Done * Not Done * N/A | Mengidentifikasi mekanisme ketersediaan yang tepat | |
| * Done * Not Done * N/A | Pemilihan OS yang tepat untuk Web server | |
| * Done * Not Done * N/A | Mengidentifikasi penyingkapan kerentanan yang paling minimal | |
| * Done * Not Done * N/A | Kemampuan untuk membatasi aktifitas tingkat administratif atau root hanya untuk para pengguna yang sah | |
| * Done * Not Done * N/A | Kemampuan untuk mengontrol akses terhadap data pada server | |
| * Done * Not Done * N/A | Kemampuan untuk menonaktifkan layanan jaringan yang tidak diperlukan dalam perangkat lunak OS atau server | |
| * Done * Not Done * N/A | Kemampuan untuk mengontrol akses ke berbagai bentuk program yang dapat dieksekusi, seperti CGI script dan server plug-in | |
| * Done * Not Done * N/A | Kemampuan untuk merekam setiap aktifitas server untuk mendeteksi penyerangan dan usaha penyerangan | |
| * Done * Not Done * N/A | Ketersediaan kapabilitas firewall host-based | |
| * Done * Not Done * N/A | Ketersediaan staf yang berpengalaman untuk menginstal, mengkonfigurasi, dan memelihara OS | |
| * Done * Not Done * N/A | Pemilihan Platform yang tepat untuk Web Server   * General purpose OS * Trusted OS * Web server appliance * Pre-hardened OS and Web server * Virtualized Platform | |
| **2.** | **Patch dan upgrade OS** | | |
| * Done * Not Done * N/A | | Melakukan dan mendokumentasikan proses *patching* |
| * Done * Not Done * N/A | | Menjaga server agar tidak terhubung ke jaringan atau terisolasi yang membatasi koneksi sampai seluruh *patch* telah dipasang |
| * Done * Not Done * N/A | | Mengidentifikasi dan menginstalasi seluruh *patch* dan *upgrade* yang dibutuhkan ke OS |
| * Done * Not Done * N/A | | Mengidentifikasi dan menginstalasi seluruh *patch* dan *upgrade* yang dibutuhkan pada aplikasi dan layanan yang terkait dengan OS |

|  |  |  |
| --- | --- | --- |
|  | * Done * Not Done * N/A | Mengidentifikasi dan meminimalkan kerentanan yang tidak di-*patch* |
| **3.** | **Menonaktifkan layanan dan aplikasi yang tidak diperlukan** | |
| * Done * Not Done * N/A | Non-aktifkan atau hilangkan layanan dan aplikasi yang tidak diperlukan |
| **4.** | **Konfigurasikan otentikasi pengguna OS** | |
| * Done * Not Done * N/A | Hilangkan atau nonaktifkan akun default dan grup yang tidak dibutuhkan |
| * Done * Not Done * N/A | Non-aktifkan akun yang tidak interaktif |
| * Done * Not Done * N/A | Menciptakan grup-grup pengguna untuk komputer- komputer tertentu |
| * Done * Not Done * N/A | Menciptakan akun-akun pengguna untuk komputer- komputer tertentu |
| * Done * Not Done * N/A | Memeriksa kebijakan password organisasi dan atur akun password secara tepat (misal panjang, kompleksitas dan sebagainya) |
| * Done * Not Done * N/A | Mencegah penebakan password (misalnya memberikan jeda waktu antara percobaan login password, tolak login setelah sejumlah percobaan gagal yang telah ditentukan) |
| * Done * Not Done * N/A | Menginstalasi dan mengkonfigurasi mekanisme keamanan lain untuk memperkuat otentikasi |
| * Done * Not Done * N/A | Konfigurasi kontrol sumber daya secara tepat |
| * Done * Not Done * N/A | Menolak akses untuk membaca file-file dan direktori- direktori yang tidak diperlukan |
| * Done * Not Done * N/A | Menolak akses untuk menulis pada file-file dan direktori-direktori yang tidak diperlukan |
| * Done * Not Done * N/A | Membatasi priviledge dalam hal eksekusi dari tool sistem hanya pada administrator sistem |
| * Done * Not Done * N/A | Instalasi dan Konfigurasi control keamanan tambahan |
| * Done * Not Done * N/A | Memilih, menginstalasi, dan mengkonfigurasikan perangkat lunak tambahan untuk menyediakan kontrol-kontrol yang dibutuhkan yang tidak termasuk dalam OS |

|  |  |  |
| --- | --- | --- |
| **5.** | **Uji keamanan dari OS** | |
| * Done * Not Done * N/A | Mengidentifikasikan sistem identik yang terpisah |
| * Done * Not Done * N/A | Uji OS dilakukan setelah instalasi awal untuk menentukan kerentanan |
| * Done * Not Done * N/A | Uji OS secara berkala (missal triwulan) untuk menentukan kerentanan baru |
| **6.** | **Instalasi Web server secara aman** | |
| * Done * Not Done * N/A | Menginstalasi perangkat lunak Web server pada suatu host yang telah ditetapkan atau guest OS yang divirtualkan dan ditetapkan |
| * Done * Not Done * N/A | Mengaplikasikan suatu patches atau upgrade untuk memperbaiki kerentanan yang diketahui |
| * Done * Not Done * N/A | Membuat suatu phisical disc atau logical portion(terpisah dari OS dan aplikasi Web server) untuk konten Web |
| * Done * Not Done * N/A | Menghilangkan atau nonaktifkan seluruh layanan yang dipasang oleh aplikasi Web server namun tidak dibutuhkan (misal gopher, FTP, administrasi remote) |
| * Done * Not Done * N/A | Menghilangkan atau nonaktifkan seluruh akun login default yang tidak dibutuhkan yang dibuat pada saat instalasi Web server |
| * Done * Not Done * N/A | Menghilangkan seluruh dokumentasi manufaktur dari server |
| * Done * Not Done * N/A | Menghilangkan file contoh atau file uji apapun dari server, termasuk script dan kode yang dapat dijalankan |
| * Done * Not Done * N/A | Mengaplikasikan template keamanan yang sesuai atau hardening script ke server |
| * Done * Not Done * N/A | Mengkonfigurasikan kembali banner layanan HTTP (dan layanan lain yang dibutuhkan) untuk tidak melaporkan tipe dan versi dari Web server dan OS |
| **7.** | **Mengkonfigurasi OS dan Access Control Web server** | |
| * Done * Not Done * N/A | Mengkonfigurasikan proses Web server untuk dapat dijalankan oleh pengguna dengan priviledge yang dibatasi dengan ketat |
| * Done * Not Done * N/A | Mengkonfigurasikan Web server sedemikian hingga file konten Web dapat dibaca namun tidak dapat ditulis oleh proses layanan |

|  |  |  |
| --- | --- | --- |
|  | * Done * Not Done * N/A | Mengkonfigurasikan Web server sedemikian hingga proses layanan tidak dapat menulis ke direktori dimana konten Web disimpan |
| * Done * Not Done * N/A | Mengkonfigurasikan Web server sedemikian rupa hingga hanya proses yang berhak untuk administrasi Web server yang dapat menulis file konten Web |
| * Done * Not Done * N/A | Mengkonfigurasikan OS host sedemikian hingga Web server dapat menulis file log namun tidak dapat membacanya |
| * Done * Not Done * N/A | Mengkonfigurasikan host OS sehingga file temporer yang dibuat oleh aplikasi Web server terbatas untuk subdirektori yang khusus dan dilindungi dengan baik. |
| * Done * Not Done * N/A | Mengkonfigurasikan host OS sehingga akses untuk file temporer manapun yang dibuat oleh aplikasi Web server terbatas untuk proses layanan yang telah membuat file. |
| * Done * Not Done * N/A | Menginstalasikan konten Web pada suatu hard drive atau logical partition yang berbeda dari OS dan aplikasi Web server |
| * Done * Not Done * N/A | Jika upload ke Web server diperbolehkan, konfigurasikan sedemikian hingga ada suatu batasan tentang jumlah ruang hard drive yang ditetapkan untuk tujuan ini; upload sebaiknya ditempatkan dalam partisi yang terpisah |
| * Done * Not Done * N/A | Pastikan bahwa file log tersimpan dalam suatu lokasi yang diukur secara tepat; file log sebaiknya ditempatkan pada suatu partisi terpisah |
| * Done * Not Done * N/A | Konfigurasi jumlah maksimum proses Web server dan/atau koneksi jaringan yang sebaiknya diperbolehkan oleh Web server |
| * Done * Not Done * N/A | Pastikan bahwa guest OS virtual apapun mengikuti checklist ini |
| * Done * Not Done * N/A | Pastikan bahwa para pengguna dan administrator dapat mengubah password |
| * Done * Not Done * N/A | Non-aktifkan para pengguna setelah tidak-aktif untuk periode tertentu |
| * Done * Not Done * N/A | Pastikan para pengguna dan administrator yang memiliki ID yang unik |
| **8.** | **Mengkonfigurasikan suatu direktori konten web yang aman** | |
| * Done * Not Done * N/A | Tetapkan suatu hard drive atau logical partition tunggal untuk konten Web dan bangun subdirektori terkait khusus untuk file konten Web server, termasuk grafik namun tidak termasuk script dan program lain |
| * Done * Not Done * N/A | Tentukan suatu direktori tunggal khusus untuk seluruh script atau program program eksternal yang dijalankan sebagai bagian dari konten Web server (missal CGI, ASP) |

|  |  |  |
| --- | --- | --- |
|  | * Done * Not Done * N/A | Non aktifkan eksekusi script yang tidak secara khusus dibawah kontrol akun administratif. Tindakan ini dicapai dengan pembuatan dan pengontrolan akses ke suatu direktori terpisah yang dimaksudkan untuk memuat script yang berhak Non aktifkan penggunaan hard atau symbolic link (misal, shortcut untuk Windows) |
| * Done * Not Done * N/A | Identifikasikan folder dan file mana dalam dokumen Web server yang harus dibatasi dan mana yang sebaiknya dapat diakses (dan oleh siapa) |
| * Done * Not Done * N/A | Cek kebijakan password dari organisasi dan atur akun password secara tepat misal, panjang, kompleksitas) |
| * Done * Not Done * N/A | Menggunakan file robots.txt, jika sesuai |
| * Done * Not Done * N/A | Konfigurasikan perlindungan anti spambot, jika ada (misal, CAPTCHA, nofollow, atau keyword filtering) |
| * Done * Not Done * N/A | Pastikan tidak ada tipe-tipe informasi berikut ini yang terdapat pada atau melalui suatu Web server |
| * Done * Not Done * N/A | Rekaman (Record) yang diklasifikasikan |
| * Done * Not Done * N/A | Aturan dan prosedur personil lingkup internal |
| * Done * Not Done * N/A | Informasi sensitif atau berklasifikasi |
| * Done * Not Done * N/A | Informasi pribadi tentang personil suatu organisasi |
| * Done * Not Done * N/A | Nomor telepon, alamat email, atau daftar umum staf kecuali jika diperlukan untuk memenuhi persyaratan yang bersifat organisasi |
| * Done * Not Done * N/A | Jadwal pimpinan organisasi atau lokasi tepat mereka (apakah ada atau tidak di lokasi kantor) |
| * Done * Not Done * N/A | Informasi komposisi, persiapan atau penggunaan dari materi berbahaya. |
| * Done * Not Done * N/A | Informasi sensitif yang berkaitan dengan keamanan negara |
| * Done * Not Done * N/A | Catatan investigasi |

|  |  |  |
| --- | --- | --- |
|  | * Done * Not Done * N/A | Catatan keuangan (diluar yang telah tersedia secara publik) |
| * Done * Not Done * N/A | Catatan medis |
| * Done * Not Done * N/A | Prosedur keamanan fisik dan informasi organisasi |
| * Done * Not Done * N/A | Informasi tentang jaringan organisasi dan infrastruktur sistem informasi |
| * Done * Not Done * N/A | Informasi yang mengkhususkan atau mengimplikasikan kerentanan keamanan fisik |
| * Done * Not Done * N/A | Rencana, peta, diagram, foto udara, dan rencana arsitektural organisasi gedung, properti, atau instalasi gedung |
| * Done * Not Done * N/A | Materi hak cipta tanpa ijin tertulis dari pemilik |
| * Done * Not Done * N/A | Kebijakan privasi atau keamanan yang menunjukkan tipe adanya tindakan keamanan hingga tingkat yang mungkin berguna bagi penyerang |
| **9.** | **Menetapkan suatu kebijakan formal dan proses terdokumentasi dalam lingkup organisasi (organizational-wide documented) mengenai konten web yang ditampilkan** | |
| * Done * Not Done * N/A | Informasi teridentifikasi yang sebaiknya dipublikasikan pada Web |
| * Done * Not Done * N/A | Sasaran audiens teridentifikasi |
| * Done * Not Done * N/A | Identifikasi efek negatif yang mungkin muncul akibat publikasi informasi |
| * Done * Not Done * N/A | Penanggung jawab yang jelas untuk pembuatan, publikasi, dan pemeliharaan informasi khusus. |
| * Done * Not Done * N/A | Menyediakan pedoman dalam hal gaya dan bentuk yang sesuai untuk publikasi Web |
| * Done * Not Done * N/A | Menyediakan tinjauan ulang yang sesuai terhadap informasi dalam hal sensifitas dan distribusi/kontrol peluncuran (termasuk sensifitas informasi dalam  suatu kumpulan) |
| * Done * Not Done * N/A | Menentukan kontrol akses dan keamanan yang sesuai |

|  |  |  |
| --- | --- | --- |
|  | * Done * Not Done * N/A | Menyediakan pedoman tentang informasi yang dimuat dalam source code dari konten Web |
| **10.** | **Mengelola privasi pengguna Web** | |
| * Done * Not Done * N/A | Kelola suatu kebijakan privasi yang dipublikasikan |
| * Done * Not Done * N/A | Lakukan larangan pengumpulan data identifikasi secara pribadi tanpa ijin eksplisit dari pengguna dan hanya kumpulkan data yang diperlukan |
| * Done * Not Done * N/A | Lakukan larangan penggunaan cookies yang “menetap ” |
| * Done * Not Done * N/A | Gunakan session cookie hanya jika diidentifikasikan secara jelas dalam kebijakan privasi yang dipublikasikan |
| * Done * Not Done * N/A | Kurangi serangan tidak langsung pada konten |
| * Done * Not Done * N/A | Pastikan para pengguna situs waspada terhadap bahaya serangan phishing dan pharming dan bagaimana menghindarinya |
| * Done * Not Done * N/A | Validasi komunikasi resmi dengan membuat emails yang khas (personilized email) dan menyediakan informasi identifikasi yang unik (tetapi tidak rahasia) yang sebaiknya hanya organisasi dan pengguna yang tahu |
| * Done * Not Done * N/A | Gunakanan signature pada email jika sesuai |
| * Done * Not Done * N/A | Jalankan validasi konten dalam aplikasi Web untuk menghindari serangan phishing yang lebih rumit (misal serangan berbasis scripting antar-situs) |
| * Done * Not Done * N/A | Buatlah konten Web (personalize) untuk mengidentifikasi situs Web yang sah |
| * Done * Not Done * N/A | Gunakan otentikasi berbasis token atau otentikasi mutual jika dapat diaplikasikan |
| * Done * Not Done * N/A | Sarankan penggunaan Web browser atau browser toolbars dengan perlindungan terhadap phishing/pharming |
| * Done * Not Done * N/A | Gunakan versi terkini dari software DNS dengan patch keamanan versi terakhir |
| * Done * Not Done * N/A | Instalasi mekanisme perlindungan DNS server-side |

|  |  |  |
| --- | --- | --- |
|  | * Done * Not Done * N/A | Monitor domain organisasi dan domain yang serupa |
| * Done * Not Done * N/A | Sederhanakan struktur nama domain organisasi |
| * Done * Not Done * N/A | Gunakan koneksi yang aman untuk login |
| * Done * Not Done * N/A | Jika perlu, ikutsertakan suatu vendor untuk menyediakan tindakan anti-phishing/ anti-pharming yang lebih kuat |
| * Done * Not Done * N/A | Pertimbangkan resiko dan keuntungan active contentclient-side |
| * Done * Not Done * N/A | Jangan ambil tindakan tanpa pernyataan ijin dari pengguna |
| * Done * Not Done * N/A | Jika mungkin, gunakan hanya active content yang diadopsi secara luas seperti JavaScript, PDF, dan Flash |
| * Done * Not Done * N/A | Jika mungkin, sediakan beberapa alternatif (misal, HTML yang disediakan bersama PDF) |
| **11.** | **Kelola keamanan active content server-side** | |
| * Done * Not Done * N/A | Hanya kode yang sederhana, mudahuntuk dimengerti yang sebaiknya digunakan |
| * Done * Not Done * N/A | Batasi atau tidak ada pembacaan atau penulisan kepada file sistem yang sebaiknya diijinkan |
| * Done * Not Done * N/A | Batasi atau tidak ada interaksi dengan program- program lain (misal, sendmail) yang semestinya diijinkan |
| * Done * Not Done * N/A | Sebaiknya tidak ada persyaratan untuk menjalankan dengan suid privileges pada UNIX atau Linux |
| * Done * Not Done * N/A | Nama path yang jelas sebaiknya digunakan (yaitu tidak bergantung pada variablel path) |
| * Done * Not Done * N/A | Tidak ada direktori yang memiliki ijin untuk menulis dan eksekusi |
| * Done * Not Done * N/A | Seluruh file yang dapat dijalankan ditempatkan dalam suatu folder yang telah ditetapkan |
| * Done * Not Done * N/A | SSL di non-aktifkan atau fungsi eksekusi di nonaktifkan |

|  |  |  |
| --- | --- | --- |
|  | * Done * Not Done * N/A | Seluruh input pengguna di validasi |
| * Done * Not Done * N/A | Kode pembangkit konten Web harus di scan atau di audit |
| * Done * Not Done * N/A | Halaman yang dibuat secara dinamis tidak menghasilkan meta characters yang berbahaya |
| * Done * Not Done * N/A | Pengkodean himpunan karakter harus diatur dengan jelas dalam setiap halaman |
| * Done * Not Done * N/A | Data pengguna harus di scan untuk menjamin hanya mengandung input yang diharapkan, (misal a- z, A\_Z, 0-9); care should be taken dengan karakter khusus atau HTML tags |
| * Done * Not Done * N/A | Cookies harus diperiksa dalam hal karakter khusus apapun |
| * Done * Not Done * N/A | Mekanisme enkripsi harus digunakan untuk mengenkripsi password yang dimasukkan melalui bentuk script |
| * Done * Not Done * N/A | Untuk aplikasi Web yang dibatasi oleh nama pengguna dan password, tidak ada halaman Web dalam aplikasi yang semestinya dapat di akses tanpa mengeksekusi proses login yang sesuai |
| * Done * Not Done * N/A | Seluruh script contoh dihilangkan |
| * Done * Not Done * N/A | Tidak ada script pihak ketiga atau kode yang dapat di eksekusi yang digunakan tanpa memverifikasi source code |
| **12.** | **Melindungi terhadap serangan brute force** | |
| * Done * Not Done * N/A | Gunakan otentikasi yang kuat jika memungkinkan |
| * Done * Not Done * N/A | Gunakan delay setelah usaha login yang gagal |
| * Done * Not Done * N/A | Lock-out suatu akun setelah satu set usaha login yang gagal |
| * Done * Not Done * N/A | Berlakukan suatu kebijakan password |
| * Done * Not Done * N/A | Blacklist IP address atau domain yang diketahui untuk usaha serangan brute force |
| * Done * Not Done * N/A | Gunakan software pengawasan log untuk mendeteksi serangan brute force |

|  |  |  |
| --- | --- | --- |
|  | * Done * Not Done * N/A | Konfigurasikan teknologi otentikasi dan enkripsi Web |
| * Done * Not Done * N/A | Untuk sumber daya Web yang memerlukan proteksi minimal dan terdiri dari peserta yang sedikit dan jelas, konfigurasikan otentikasi yang berdasarkan alamat |
| * Done * Not Done * N/A | Untuk sumber daya Web yang memerlukan perlindungan tambahan akan tetapi terdiri dari peserta yang sedikit dan jelas, konfigurasikan otentikasi berdasarkan alamat sebagai garis pertahanan kedua |
| * Done * Not Done * N/A | Untuk sumber daya Web yang memerlukan perlindungan minimal tetapi tidak terdiri atas peserta yang didefinisikan dengan jelas, konfigurasikan otentikasi dasar atau digest (lebih baik) |
| * Done * Not Done * N/A | Untuk sumber daya Web yang memerlukan perlindungan dari malicious bots, konfigurasikan otentikasi dasar atau digest (lebih baik) atau implementasikan teknik-teknik mitigasi |
| * Done * Not Done * N/A | Untuk sumber daya Web yang memerlukan perlindungan maksimal, konfigurasikan SSL/TLS dengan cipher suite yang kuat |
| * Done * Not Done * N/A | Konfigurasikan SSL/TLS |
| **13.** | **Memastikan implementasi SSL/TLS telah dilakukan patch sepenuhnya** | |
| * Done * Not Done * N/A | Gunakan suatu issued certificate pihak ketiga untuk otentikasi server (kecuali seluruh sistem yang menggunakan server di atur secara organisasi dapat digunakan self-signed certificate. |
| * Done * Not Done * N/A | Untuk konfigurasi yang membutuhkan otentikasi klien tingkat menengah, konfigurasikan server untuk membutuhkan nama pengguna dan password  melalui SSL/TLS |
| * Done * Not Done * N/A | Untuk konfigurasi yang membutuhkan otentikasi klien tingkat tinggi, konfigurasikan server untuk membutuhkan sertifikat klien melalui SSL/TLS |
| * Done * Not Done * N/A | Pastikan cipher suit yang lemah dinonaktifkan sesuai dengan ketentuan yang berlaku. |
| * Done * Not Done * N/A | Konfigurasikan pengecek keutuhan file untuk mengawasi sertifikat Web server |
| * Done * Not Done * N/A | Jika hanya SSL/TLS yang digunakan dalam Web server, pastikan akses melalui port TCP daripada 443 di nonaktifkan |
| * Done * Not Done * N/A | Jika sebagian besar lalu lintas pada Web server akan melalui SSL/TLS yang terenkripsi, pastikan bahwa mekanisme logging dan deteksi yang sesuai digunakan dalam  Web server (karena pengawasan jaringan tidak efektif menghadapi sesi SSL/TLS) |
| **14.** | **Melakukan penilaian terhadap konfigurasi firewall** | |
| * Done * Not Done * N/A | Web server dilindungi oleh suatu firewall |

|  |  |  |
| --- | --- | --- |
|  | * Done * Not Done * N/A | Web server, jika berhadapan dengan ancaman yang lebih tinggi atau jika lebih rentan, dilindungi oleh suatu firewall layer aplikasi |
| * Done * Not Done * N/A | Firewall mengendalikan semua lalu lintas antara Internet dan Web server |
| * Done * Not Done * N/A | Firewall memblokir semua inbound traffic ke Web server kecuali TCP ports 80 (HTTP) dan/atau 443 (HTTP), jika dibutuhkan |
| * Done * Not Done * N/A | Firewall memblokir (dalam hubungannya dengan IDPS) alamat IP atau subnet yang dilaporkan IDPS sedang menyerang jaringan organisasi |
| * Done * Not Done * N/A | Firewall memberitahukan jaringan atau administrator Web server mengenai kegiatan yang mencurigakan melalui suatu cara yang sesuai |
| * Done * Not Done * N/A | Firewall menyediakan penyaring konten (firewall layer aplikasi) |
| * Done * Not Done * N/A | Firewall dikonfigurasi untuk melindungi dari serangan DoS |
| * Done * Not Done * N/A | Firewall mendeteksi permintaan URL yang salah format atau serangan terhadap permintaan URL yang dikenal |
| * Done * Not Done * N/A | Firewall me-log kejadian kritis |
| * Done * Not Done * N/A | Firewall dan OS firewall dipatch hingga tingkat aman yang paling mutakhir atau yang paling tinggi |
| **15.** | **Melakukan evaluasi terhadap deteksi intrusi dan sistem pencegahan** | |
| * Done * Not Done * N/A | IDPS berbasis host digunakan untuk Web server yang beroperasi terutama menggunakan SSL/TLS |
| * Done * Not Done * N/A | IDPS dikonfigurasikan untuk memonitor lalu intas jaringan dari dan ke Web server setelah firewall |
| * Done * Not Done * N/A | IDPS dibentuk untuk memonitor perubahan atas file kritis pada Web server (IDPS berbasis host atau pengecek integritas file) |
| * Done * Not Done * N/A | IDPS memblokir (dalam hubungannya dengan firewall) alamat IP atau subnet yang menyerang jaringan organisasi |
| * Done * Not Done * N/A | IDPS memberitahu para administrator IDPS atau administrator Web server mengenai serangan melalui cara yang sesuai |
| * Done * Not Done * N/A | IDPS dikonfigurasikan untuk memaksimalkan deteksi dengan suatu tingkat penerimaan dari kesalahan yang positif |

|  |  |  |
| --- | --- | --- |
|  | * Done * Not Done * N/A | IDPS dikonfigurasikan untuk me-log kejadian |
| * Done * Not Done * N/A | IDPS di-update dengan tanda serangan baru secara berkala (misal berdasarkan harian) |
| * Done * Not Done * N/A | IDPS berbasis host dikonfigurasikan untuk memonitor sumber daya sistem yang ada pada Web server host |
| **16.** | **Melakukan penilaian terhadap switch jaringan** | |
| * Done * Not Done * N/A | Switch jaringan digunakan untuk memproteksi jaringan dari penyadap jaringan |
| * Done * Not Done * N/A | Switch jaringan dikonfigurasikan pada model keamanan yang tinggi untuk mengalahkan ARP spoofing dan serangan-serangan ARP poisoning |
| * Done * Not Done * N/A | Switch jaringan dikonfigurasikan untuk mengirimkan semua lalu lintas pada segmen jaringan ke IDPS berbasis jaringan |
| * Done * Not Done * N/A | Lakukan evaluasi terhadap load balancer |
| * Done * Not Done * N/A | Load balancer digunakan untuk meningkatkan ketersediaan Web server |
| * Done * Not Done * N/A | Load balancer diperbesar dengan Web cache, jika dapat diaplikasikan |
| * Done * Not Done * N/A | Lakukan evaluasi terhadap reverse proxy |
| * Done * Not Done * N/A | Reverse proxy digunakan sebagai suatu gerbang pengamanan untuk meningkatkan ketersediaan Web server |
| * Done * Not Done * N/A | Reverse proxy diperbesar dengan penambahan |
| * Done * Not Done * N/A | Kecepatan enkripsi, otentikasi pengguna, dan kemampuan penyaring konten, jika dapat diaplikasikan |
| **17.** | **Melakukan Logging** | |
| * Done * Not Done * N/A | Gunakan format log kombinasi untuk menyimpan Log Transfer atau mengkonfigurasi secara manual informasi yang dijabarkan oleh format log kombinasi menjadi format standar untuk Log Transfer |
| * Done * Not Done * N/A | Aktifkan Log Pengacu atau Log Agent jika format log kombinasi tidak tersedia |

|  |  |  |
| --- | --- | --- |
|  | * Done * Not Done * N/A | Buatlah nama-nama file log yang berbeda untuk situs Web virtual yang berbeda yang mungkin di implementasikan sebagai bagian dari suatu Web server fisik tunggal |
| * Done * Not Done * N/A | Gunakan identitas pengguna remote sebagaimana yang ditentukan dalam RFC 1413 |
| * Done * Not Done * N/A | Simpanlah log pada suatu host yang terpisah (syslog) |
| * Done * Not Done * N/A | Pastikan terdapat kapasitas yang cukup untuk log |
| * Done * Not Done * N/A | Arsipkan log berdasarkan pada persyaratan organisasi |
| * Done * Not Done * N/A | Periksa kembali log harian |
| * Done * Not Done * N/A | Periksa kembali log mingguan (untuk trend long- term yang lebih banyak) |
| * Done * Not Done * N/A | Gunakan tool analisis file log yang otomatis |
| **18.** | **Melakukan pembuatan backup Web server** | |
| * Done * Not Done * N/A | Buatlah suatu kebijakan backup Web server |
| * Done * Not Done * N/A | Lakukan back up Web server secara differential atau incremental berbasis harian hingga mingguan |
| * Done * Not Done * N/A | Buatlah back up Web server secara penuh berbasis mingguan hingga bulanan |
| * Done * Not Done * N/A | Buatlah back up arsip secara periodik |
| * Done * Not Done * N/A | Pelihara suatu copy otoritatif situs Web |
| **19.** | **Melakukan pemulihan terhadap suatu kebobolan/insiden** | |
| * Done * Not Done * N/A | Laporkan insiden kepada pihak tanggap insiden keamanan komputer dari organisasi |
| * Done * Not Done * N/A | Isolasi sistem yang bobol atau ambil langkah-langkah lain untuk memagari serangan sehingga informasi tambahan dapat dikumpulkan |
| * Done * Not Done * N/A | Periksa host-host yang serupa untuk menentukan jika penyerang juga membobol sistem-sistem lain |

|  |  |  |
| --- | --- | --- |
|  | * Done * Not Done * N/A | Konsultasikan, sebagaimana mestinya, dengan manajemen, konsultan hukum, dan kantor penegak hukum secara cepat. |
| **20.** | **Analisis intrusi yang terjadi** | |
| * Done * Not Done * N/A | Mengembalikan sistem seperti semula |
| * Done * Not Done * N/A | Menguji sistem untuk memastikan keamanan |
| * Done * Not Done * N/A | Menghubungkan kembali sistem ke jaringan |
| * Done * Not Done * N/A | Monitor sistem dan jaringan terhadap tanda-tanda bahwa penyerang berusaha mengakses kembali sistem atau jaringan kembali. |
| **21.** | **Scanning Kerentanan & Penetration Test** | |
| * Done * Not Done * N/A | Melakukan secara berkala scan kerentanan pada Web server, konten yang dihasilkan secara dinamis, dan jaringan pendukung |
| * Done * Not Done * N/A | Lakukan update scanner kerentanan sebelum pengujian |
| * Done * Not Done * N/A | Perbaiki kekurangan yang teridentifiikasi oleh scanner kerentanan |
| * Done * Not Done * N/A | Lakukan Penetration Testing pada Web server dan infrastruktur jaringan pendukung |
| * Done * Not Done * N/A | Perbaiki kekurangan apapun yang teridentifikasi oleh uji penetrasi |
| * Done * Not Done * N/A | Gunakan suatu mekanisme otentikasi yang kuat (misal, pasangan kunci publik/privat, otentikasi dua- faktor) |
| * Done * Not Done * N/A | Batasi host yang dapat digunakan untuk mengelola secara remote atau mengupdate konten pada Web server dengan IP address dan ke jaringan internal |
| **22.** | **Menggunakan protokol yang aman (misal, SSH, HTTPS)** | |
| * Done * Not Done * N/A | Terapkan konsep least privilege pada administrasi yang dilakukan secara remote dan update konten (misalkan meminimalkan hak akses untuk kedua hal ini) |
| * Done * Not Done * N/A | Rubah akun atau password default dari perangkat atau aplikasi administrasi yang dilakukan secara remote |
| * Done * Not Done * N/A | Tidak membolehkan administrasi dilakukan secara remoter melalui internet kecuali dengan menggunakan Secure Shell atau VPN |
| * Done * Not Done * N/A | Tidak melakukan sharing file Web server pada jaringan internal |