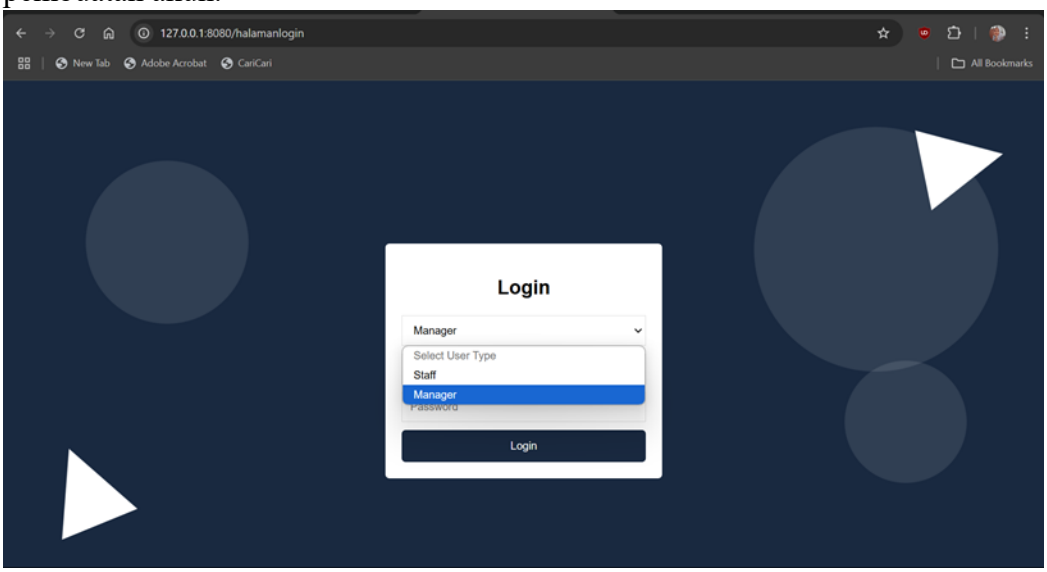
Klasifikasi Level Security Database PBL

1. **Authentication And Access Control**

   Penerapan Authentication And Access Control yang ada di website pbl-rks302 menggunakan Moderate Security. Di dalam moderate security terdapat basic authentication dengan pilihan role untuk izin akses login ke website nya. Yang termasuk di dalam basic authentication ialah username dan password yang dimana merupakan komponen utama untuk mengautentikasi pengguna.

   Lalu terdapat juga mode role. Pada gambar tersebut mode role ada dibagian dropdown select user type untuk pengguna dapat memilih peran yang sudah ditentukan pada saat pembuatan akun.



2. Data Encryption

Pada PBL ini, tepatnya tim PBL-RKS302, aspek data encryption jatuh pada kategori klasifikasi : **Moderate Security** (*Encrypts data either at rest or in transit, but lacks robust key management practices*./Mengenkripsi data baik pada saat tidak digunakan maupun pada saat dikirim, tetapi tidak memakai praktik manajemen kunci yang kuat.)

Mengapa? Hal ini dikarenakan tidak seluruh isi *database* dienkripsi, melainkan sebagian data yang dianggap sensitif tidak disimpan secara *plain*/jelas pada saat tidak diakses (*at rest*) yakni *value/*nilai password pengguna. Nilai ini disimpan pada database dengan hash MD5. Dan terlebih lagi juga, penggunaan enkripsi data juga tidak disertai dengan penggunaaan KMS (*Key Management System*/Sistem Manajemen Kunci) untuk menyimpan kunci-kunci master (*masterkey*) yang dibutuhkan pada saat enkripsi-dekripsi data. Sehingga semakin jelas bahwa aspek ini jatuh pada pilihan Moderate Security

3. Backup and Disaster Recovery

Apa yang dimaksud dengan pemulihan dan pencadangan bencana?

Untuk mempertahankan atau melanjutkan aktivitas perusahaan jika terjadi kehilangan data akibat kerusakan file, kerusakan data, serangan siber, atau bencana alam, pencadangan dan pemulihan bencana memerlukan pembuatan atau pembaruan salinan file tambahan secara rutin, menyimpannya di satu atau beberapa tempat terpencil, dan menggunakan salinan tersebut.

Untuk tingkat klasifikasis security pada PBL kami adalah moderate security, tingkat keamanan moderate mencakup praktik yang lebih baik daripada konfigurasi dasar, tetapi belum mencapai tingkat keamanan yang tinggi. Fokus utama kami pada tingkat keamanan ini adalah memastikan backup dilakukan secara teratur dengan pemulihan bencana (disaster recovery) yang jarang diuji atau memiliki batasan tertentu, serta kemungkinan tidak adanya enkripsi pada media penyimpanan.

Kelebihan dan Kekurangan moderate security kami:

Kelebihan:

- Backup rutin meminimalkan risiko kehilangan data akibat insiden,
- dan solusi TrueNAS menggunakan antarmuka yang mudah digunakan untuk memudahkan manajemen penyimpanan.
- Implementasi ini cukup efisien dari sisi biaya dan waktu karena tidak memerlukan konfigurasi enkripsi atau replikasi yang kompleks.

Kekurangan:

- Tanpa enkripsi, data rentan jika media penyimpanan jatuh ke tangan yang salah.
- Pengujian pemulihan bencana yang minimal dapat mempersingkat waktu pemulihan saat terjadi bencana.
- Tidak ada redundansi geografis, jadi risiko kehilangan data karena bencana fisik tetap ada.

4. Vulnerability Management

Pada Vulnerability Management yang kami terapkan berada dikategori Moderate Security. pembaruan perangkat lunak database dan pemindaian kerentanan secara berkala, tetapi ada kemungkinan adanya penundaan dalam penerapan patch atau pembaruan. Dampaknya: Penundaan ini memberikan celah waktu di mana kerentanan yang diketahui (disclosed vulnerabilities) belum ditangani, sehingga meningkatkan potensi eksploitasi, meskipun risikonya masih terkontrol dengan praktik mitigasi lain seperti firewall atau kontrol akses.

Adapun alasan mengapa Vulnerabiliy Management berada di Moderate adalah:

1. Pembaruan dan Patch Masih Dilakukan : Meskipun mungkin ada penundaan dalam penerapan patch, pembaruan tetap dilakukan secara berkala, yang secara signifikan mengurangi risiko eksploitasi kerentanan dibandingkan sistem yang benar-benar tidak diperbarui.
2. Pemindaian Kerentanan Tetap Ada : Karena pemindaian kerentanan dilakukan secara periodik, meskipun tidak seketat kategori High Security
3. Tidak Menggunakan Sistem Legacy : Menggunakan perangkat lunak yang masih didukung oleh vendor, sehingga pembaruan keamanan tetap tersedia, meskipun implementasinya mungkin tidak selalu cepat.
4. Ada Mekanisme Keamanan Tambahan
5. Risiko yang Lebih Terkontrol

5. Compliance and Standards

Tingkat Keamanan Sedang: Sebagian Memenuhi Standar Keamanan, dengan Pemeriksaan Berkala

Website ini dikembangkan untuk manajemen penyimpanan barang dengan dua peran pengguna, yaitu Manager dan Staff. Fitur utama dari website ini mencakup pengelolaan inventaris, pencatatan penerimaan barang, serta pengawasan alur persetujuan dan pengelolaan stok barang. Manager memiliki hak akses lebih luas, termasuk menerima atau menolak barang yang akan diterima, sedangkan Staff hanya dapat melakukan pencatatan dan pemeliharaan stok.

Penting untuk memastikan bahwa website ini sesuai dengan berbagai compliance dan standards yang berlaku untuk menjamin keamanan data pengguna dan kelancaran operasional. Oleh karena itu, berikut adalah penjelasan mengenai compliance dan standards yang diimplementasikan dalam pengembangan website ini.

Alasan Website Masuk dalam Kategori "Tingkat Keamanan Sedang"

Penerapan Beberapa Standar Keamanan

Perlindungan terhadap Serangan Web Umum

Perlindungan terhadap serangan web adalah bagian penting dari keamanan aplikasi web. Serangan-serangan ini dapat merusak sistem atau mencuri data sensitif jika tidak diatasi dengan tepat.Ada beberapa antispasi seranga yang sudah kami lakukan pada web kami berikut

SQL Injection

SQL Injection terjadi ketika penyerang mengirimkan kode SQL berbahaya melalui input form atau URL untuk mengeksekusi query SQL yang tidak diinginkan di database.

RBAC (Role-Based Access Control)

untuk membatasi hak akses pengguna berdasarkan peran mereka. Ini memberikan kontrol yang baik terhadap siapa yang dapat mengakses data dan melakukan operasi di website.

Keamanan data sensitif, seperti password, disimpan dengan menggunakan algoritma enkripsi seperti **bcrypt**, yang memastikan perlindungan data pengguna yang baik.

6. Resilience Againts Common Attacks

High Security:

- Disini kami menerapkan yang namanya Parameterized Queries atau Prepared Statements dengan tujuan untuk terhindar dari yang namanya serangan SQL Injection
- lalu, kami juga menerapkan yang namanya Filtering Input Validation agar terhindar dari berbagai serangan injeksi salah satunya XSS Stored, Serangan Stored XSS terjadi ketika input berbahaya dari pengguna disimpan di database dan kemudian dieksekusi di browser pengguna lain. dengan memfilter input pengguna di browser yang kami gunakan menggunakan htmlspeciaalchars(), maka serangan XSS tersebut tidak akan tersimpan kedalam database yang menyebabkan XSS Stored.
- Lalu, kami juga menerapkan RBAC (Role-Based Access Control) untuk membagi hak akses pengguna dalam database berdasarkan peran mereka. Misalnya, User A hanya dapat melakukan UPDATE, sedangkan User B memiliki akses untuk DELETE dan INSERT. Dengan RBAC, setiap pengguna hanya memiliki hak akses yang sesuai dengan tugasnya, sehingga jika seorang penyerang berhasil menyusupi akun dengan hak akses terbatas, mereka tidak dapat meningkatkan hak akses tersebut untuk melakukan tindakan berbahaya seperti menghapus data atau mengubah konfigurasi penting. Hal ini secara efektif mencegah serangan Privilege Escalation.
- lalu, kami menggunakan rate limiting. dimana, rate limit yang kami gunakan untuk mencegah yang namanya serangan brute force
- selanjutnya, kami melakukan monitoring terhadap database tersebut menggunakan siem, dengan melakukan monitoring, kami jadi tau aktivitas yang terjadi di belakang layar selama proses databse tersebut berjalan dan juga untuk meilihat perilaku dari seorang penyerang ketika melakukan akses di database kami.

7. Isolation and Segmentation

high security

- pertama disini kami menggunakan yang namanya firewall, Firewall digunakan untuk membatasi akses ke sumber daya tertentu, menentukan apa saja yang boleh diakses, dan memblokir akses yang tidak diizinkan. Selain itu, firewall yang kami gunakan memiliki fitur stateful inspection, di mana setiap paket data diperiksa berdasarkan status koneksinya, memastikan hanya koneksi yang sah yang diizinkan masuk atau keluar.
- Lalu, selain firewall, kami juga menambahkan VLAN (Virtual Local Area Network) sebagai bagian dari strategi isolation and segmentation. Dengan menggunakan VLAN, kami dapat memisahkan jaringan menjadi beberapa segmen yang terisolasi, meskipun secara fisik berada pada infrastruktur yang sama. Setiap VLAN memiliki kontrol akses yang lebih ketat, sehingga hanya perangkat atau pengguna yang diberi izin yang dapat berkomunikasi antar VLAN. Salah satu penggunaan utama VLAN adalah untuk menciptakan isolated environment for sensitive data, di mana data sensitif atau sistem kritis dapat dipisahkan dari bagian lain dari jaringan. Misalnya, server yang menyimpan data penting dapat diletakkan dalam VLAN khusus yang hanya dapat diakses oleh pengguna atau sistem yang memiliki hak akses tertentu, sehingga mengurangi risiko pencurian atau kebocoran data. Dengan cara ini, VLAN tidak hanya membantu dalam segmentasi jaringan, tetapi juga memperkuat proteksi terhadap data yang lebih sensitif.