Securing a Multi-Tenant SaaS Application Using Cello

techcello

Following document outlines various security aspects by categorizing into 3 major areas that are required by any SaaS Application and also how they are addressed by CelloSaaS:

1. Application Vulnerability Protection
2. Data Security and Access Control Mechanism
3. Security Certification

1) Application Vulnerability Protection

A) Security Threat Counteract Measures

I) Microsoft .Net Framework Support

The Admin Portal of CelloSaaS Framework is built on top of Microsoft ASP.Net MVC; the built-in security features are available out of the box with regards to following security threats

1) XSRF [Cross Site Request forgery]

2) XSS [Cross Site Scripting]

II) CelloSaaS Support

In addition to the built-in security protection modes, Cello provides additional security features that consummate Microsoft .Net framework security measures with respect to XSRF, XSS & SQL Injection attacks to name a few.

B) Unauthorized Access

CelloSaaS provides access control policy which enables the application to restrict unauthorized access to various business functionality

I) This feature is supported via Tenant Licensing.

II) Graphical User Interface level security policy configuration that is capable of restricting the user access to application resources at the first place.

III) Access control policies are also available for defining service access which prevents unauthorized access to the services that may be exposed by the application other than via Graphical User Interface.

2) Data Security

This section explains about various data security aspects such as:

A) Cello Managed Metadata

Cello metadata managed by CelloSaaS are secured using CelloSaaS Security mechanism via appropriate access control check and validations.

B) Securing Data at Rest

Sensitive data that are handled by Cello are persisted in the data store after encryption / hashing so data at rest cannot be interpreted.

C) Securing Data In-Transit

Cello is compliant with the well-established security mechanisms like HTTPS [Transport layer Security / Security Socket Layer] which enables secure exchange of data over the wire.

D) Security Modes

Security Modes that are supported are Encryption / Hashing, with Encryption [AES] being the default.

E) Application Data Security

Application developers can make use of a simple API that will take care of Encryption / Hashing of the sensitive data.

F) Data Isolation

Data Isolation helps the application to handle tenant specific data at ease by making use of auto tenant isolation, security scanners that act at the lower level to give more control on data accessed by the application at any given point of time.

G) Access Control Security

I) Presentation Tier

Page level access control lists or policies are configured in the application that enforces security at the presentation tier.

II) Service Tier

CelloSaaS provides options to automate on-demand permission check both in a custom or an automated fashion.

In case of automated access control enforcement, access control policies configured are used to validate against any service call that is made by the presentation tier to access data.

In case of custom access control enforcement, there are API's exposed from CelloSaaS libraries that helps the developer perform necessary access control enforcement.

III) Role Based Access Control

Tenant Users / administrators gain access to various application resources based on Roles & Privileges that are governed by the Product / Tenant Administrators. Roles are in-turn bound to privileges which are the lower level on security hierarchy that determines the access rights to business services for any user at a given instant.

H) Fine Grained Data Security

Apart from the default RBAC [Role Based Access Control] mechanism, CelloSaaS provides a more fine grained control mechanism which gives flexibility to control data access at the following levels:

1. Entity [Business Object]
    a. Secure access to an entity
2. Records
    a. Secure access to records within an entity
3. Fields
    a. Secure access to the fields within an entity

The enforcement mapping and updates can be done in GUI [Graphical User Interface]

3) External Security Certification [Veracode]

Cello has gone through Security Testing from Veracode. Veracode is a market leader in identifying CWE/SANS and OWASP Vulnerabilities.

Cello has met the requirements for Application Business Criticality - Level 5 (Highest)

Note: Any application that complies to the best practices suggested by Cello gets the above features out of the box.