Security and Legal Compliance of Oracle's Cloud based Product

Submitted By

Bhavya Choudhary

16MCEI04

DEPARTMENT OF COMPUTER ENGINEERING

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

May 2018

Security and Legal Compliance of Oracle's Cloud based Product

Major Project

Submitted in partial fulfillment of the requirements

for the degree of

Master of Technology in Computer Science & Engineering

(*Information & Network Security*)

Submitted By

Bhavya Choudhary

(16MCEI04)

Guided By

Prof. Pooja Shah

DEPARTMENT OF COMPUTER ENGINEERING

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

May 2018

Certificate

This is to certify that the major project entitled **"Security and Legal Compliance of Oracle's Cloud based Product"** submitted by **Bhavya Choudhary (Roll No: 16MCEI04)**, towards the fulfillment of the requirements for the award of degree of Master of Technology in Computer Science and Engineering(Information & Network Security) of Nirma University, Ahmedabad, is the record of work carried out by her under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this project, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Prof. Pooja Shah
Guide & Associate Professor,
CE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr. Sharada Valiveti
Coordinator M.Tech - CSE (INS),
CE Department,
Institute of Technology,
Nirma University, Ahmedabad

Dr. Sanjay Garg
Professor and Head,
Institute of Technology,
Nirma University, Ahmedabad.

Dr. Alka Mahajan
Director,
Institute of Technology,
Nirma University, Ahmedabad

Statement of Originality

I, **Bhavya Choudhary**, **16MCEI04**, give undertaking that the Major Project entitled " **Security and Legal Compliance of Oracle's Cloud based Product**" submitted by me, towards the fulfillment of the requirements for the degree of Master of Technology in **Computer Science Engineering***(Information & Network Security)* of Institute of Technology, Nirma University, Ahmedabad, contains no material that has been awarded for any degree or diploma in any university or school in any territory to the best of my knowledge. It is the original work carried out by me and I give assurance that no attempt of plagiarism has been made.It contains no material that is previously published or written, except where reference has been made. I understand that in the event of any similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

_____

Signature of Student

Date:

Place:

Endorsed by

Prof .Pooja Shah

(Signature of Guide)

Acknowledgements

It gives me immense pleasure in expressing thanks and profound gratitude to Prof. Pooja Shah, Associate Professor, Computer Engineering Department, Institute of Technology, Nirma University, Ahmedabad for her valuable guidance and continual encouragement throughout this work. The appreciation and continual support she has imparted has been a great motivation to me in reaching a higher goal. Her guidance has triggered and nourished my intellectual maturity that I will benefit from, for a long time to come.

It gives me an immense pleasure to thank Dr. Sanjay Garg, Hon'ble Head of Computer Engineering Department, Institute of Technology, Nirma University, Ahmedabad for his kind support and providing basic infrastructure and healthy research environment.

A special thank you is expressed wholeheartedly to Dr. Alka Mahajan, Hon'ble Director, Institute of Technology, Nirma University, Ahmedabad for the unmentionable motivation she has extended throughout course of this work.

I would also thank the Institution, all faculty members of Computer Engineering Department, Nirma University, Ahmedabad for their special attention and suggestions towards the project work.

- Bhavya Choudhary

16MCEI04

Abstract

The Project "Security and Legal Compliance of Oracle's Cloud based Product" is about making the product ready according to Oracle's security policies.RCOM is delivered as a cloud service, which provides retailers with faster and easier deployments in a highly scalable, reliable, and secure environment. Security and Legal Compliance of RCOM is about making the product secure from the known web threats and making the product ready according to EUGDPR.The first chapter talks about the Oracle Retail and Omnichannel structure.The second chapter shows the literature survey carried out during the whole project work.Third chapter is about the product,it's objective to serve the customers. In the fourth chapter the Technical and Functional overview of the product is discussed.Fifth chapter shows the basic aspects taken care in order to secure the product.The sixth chapter covers the approach used in order to comply with EUGDPR policy.Where the Right to Access and Right to Forget were implemented into the product.

Contents

List of Figures

Chapter 1

Introduction

1.1 Retail World

Retail is tied in with having the correct item, at the opportune time, at the correct area, in right amount, and cost. Bringing together, Consolidating and expanding a lot of data accessible are a portion of the key difficulties in retail. Retailers need to relate things, areas, and providers, track buy orders, screen bargain pay, oversee recharging settings, and settle on valuing choices and total exchange data into the stock record at detailing levels.

In the retail world, the purchaser merchandise are sold and benefits are given to the clients to win more benefit. The client requests are fulfilled subsequent to recognizing them. Oracle Retail furnishes retailers with an entire, open, and coordinated suite of business applications, server, and capacity arrangements built to cooperate to enhance each part of their business. The client pays the dealer once the merchandise are traded or the administration is given. After installation, the client can pick one or a mix of installment techniques like credit/charge/money/blessing coupons. After this procedure, the client enters his points of interest, which is put away for review purposes, dedication plans, rebates or even simplicity of exchange next time.This data is exchanged between many other integrated system for their verification or authorization and is also stored in the database.

Thus, it is very important to secure the system so that this information is not mishandled and as per Oracle's Data privacy policy, every customer gets the right to know and delete all of his/her Personally Identifiable Information (PII) data stored with the

retailers.

1.2 Omni-channel Scenario

Omni-channel is a multichannel approach to sales which provides all the customers with a seamless shopping experience whether the customer is doing online shopping from a desktop or mobile device, by telephone or in a bricks and mortar store. That is,

- Order online/mobile/call center
  - Ship from Distribution Center(DC)
  - Ship from store
  - Pickup in-store with store inventory
  - Pickup in-store with DC inventory
  - Return to store
- Order in-store A
  - Ship from DC
  - Ship from DC, pickup in store A
  - Ship from store B
  - Ship from store B, pickup in store A
  - Pickup from store B

Figure 1.1: Omni-Channel Scenario

Thus, as shown in Figure Omni-Channel Scenario has a concept of “buy anywhere, pickup anywhere and return anywhere”.

Chapter 2

Literature Survey

This chapter would include the survey done in order to understand the security requirements of the product in a better way.

It was observed that while designing a product most of the security aspects are not taken into consideration which can result into making the product vulnerable to various attacks.Most common attacks have been taken into consideration and have been tried to avoid by performing various mitigation and various filters.

It is always better to have early security verification than to wait for penetration testing.These security verification should be performed very often and the newly introduced security policies should taken into consideration.

Also,Data privacy is a major issue of concern.Personal data is used for an individuals identity which in some also has the chances of being misused.Just like other laws in countries a law for data privacy is introduced which would cover the rights of the citizens of a nation to ask for the data privacy and also remove it from records whenever they wish to.[1]

Chapter 3

Oracle Retail Customer and Order Management system

3.1 Introduction

Oracle Retail Customer and Order Management system is planned as an independent endeavor application. To empower venture client and request administration, RCOM has been architected on a J2EE Java engineering, which encourages a successful reconciliation of client and request administration framework capacities into outer applications and accommodates the administration of basic business rationale over the endeavor.

Figure 3.1: Retail Flow

RCOM has been expected to have more prominent flexibility to arrange into the endeavor retail condition.. RCOM use the retail venture by uncovering stock, valuing,

advancement, client, and production network data. This combination from RCOM into the endeavor prompts enhanced fill-rates for client request, faster shipments of client arranges, and expanded stock turns. By offering a solitary and complete view of the client, RCOM gives retailers a reliable technique for creating,manging and viewing customer interactions for the greater part of a customer's channels and brands.

The application is composed and worked as a far reaching business-to-buyer endeavor arrange administration arrangement and gives incorporated business forms into the retail condition, such as into marketing and distribution center administration applications.

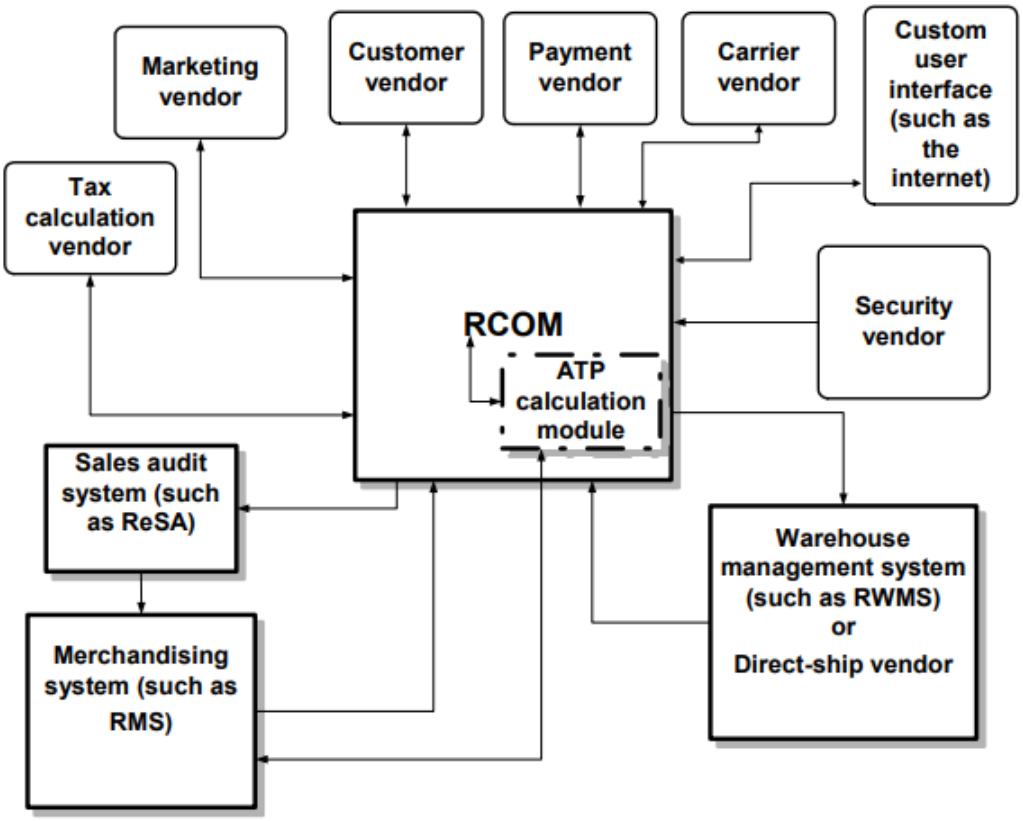


Figure 3.2: RCOM Components

3.2 Motivation

In today's retail culture of higher and higher consumer expectations, retailers are faced mainly with four key challengesLarge IT footprint required to run their on-

line retail business Retailers spend excessive time and resources managing their on premise commerce implementations. Unable to facilitate Omni-Channel scenarios Customers today demand to be able to "order anywhere" and "receive anywhere," which means retailers must be able to "fulfill from anywhere" in order to meet their customer demand and also customer expect to be able to choose where they will receive their products. Disconnected user experiences across all touchpoints A commerce platform today must provide a consistent, personalized, and optimized, experience across desktop, tablets, and mobile devices. Lack of customer and order visibility Customers need to be identified regardless of how they are interacting with the brand – online, in-store, or via the call center. Order information needs to be must be available, accurate, and complete at all touchpoints – online, in-store, and via the call center.

Thus there was need for a platform which incorporates all these requirements.

3.3 Objectives

- Deliver a Cloud Service OROCP is delivered as a cloud service, which provides retailers with faster and easier deployments in a highly scalable, reliable, and secure environment. OROCP requires a low upfront investment and a rapid return on investment and enables retail teams to focus on innovation and managing their business as opposed to managing their IT infrastructure. Return on Investment (ROI) and focus on innovation.

- Support Omni-Channel scenarios To support Omni-Channel scenarios starting in the browse process, moving all the way through the checkout flow, and then continues its support throughout the order lifecycle.

- Provide a consistent, personalized experience across touchpoints To provide a consistent, yet personalized experience across all touchpoints. OROCP ships with a fully responsive reference application or "Starter Store", consumer-facing native app. OROCP enables retailers to create and tailor content, and promotional "Experiences" based on consumer demographics, behavior, and device type.

- Provide a single view of customers and orders Order history provides information for all online, in-store, and call center orders My account customer information

changes will be reflected online, in-store, and in the call center. Loyalty points and awards can be viewed, earned, and used online, in-store, and in the call center. Out-of-the-box integrations with other Oracle Retail Cloud Services enable a single view of both customers and orders.

- Provide user an easy way to access their PII data Detail of any PII data of user saved by the application must be made available to the user when they request for it. Therefore, there is a need to create a user friendly approach to process this.

3.4 Internationalization

Support for worldwide nations and regions is added to RCOM. RCOM has a logic to decide whether a URL is right for the present region. Even if it isn't, it will divert the client to the right space. RCOM guarantees that the intricate rationale of deciding the present region is executed as it were once per ask. Once the district is resolved, RCOM stores the region in various distinctive areas with the goal that those areas can be utilized to recover the region:

- in an attribute for request in a cookie
- in an attribute for pipeline session

The cookie remains set for different requests in a similar session, so future sessions for browsing will know which region was already chosen by the client. The pipeline session will stay set until the pipeline session pruner erases it, so future perusing sessions could conceivably know which district was beforehand chosen by the client. At the point when the technique to discover district is conjured, it searches for the flow region in the following areas, in the order given. Once it finds a locale, it stops looking in the other areas:

- in an attribute for request
- preview session
- cookie
- geolocation for server side
- URL domain
- pipeline session

3.5 Site Manager

As name indicates this manages the site. The addition or formatting of following mentioned below are done through site manager

- Asset Types and Formats: There are numerous content asset types in the Site Manager like Ensemble asset (Ensemble formats are various ways to display information about an ensemble on the website), Ensemble collection (A collection of ensembles that have been set up as a group), Image asset (Image formats are various ways to display an image).

- Awards: Item awards relate to discounts on product and ensembles. The cart and address subtotals are dependent on the aggregated price total of all items. As a result, neither the shopping cart subtotal nor address subtotal can trigger an item price change.

- Email Tokens: Based on the information known about users, tokens will be used to populate personal information in the available email templates. There are two types of tokens:

  - Personalized tokens: These are based on things known about the user, such as their name or address.

  - Smart tokens: These represent general items (such as products in the Shopping Cart) but are dynamic and look to the users Shopping Cart, Wish List, or past orders for information. Any information that is in the pipeline session can be referenced via an email token, using the column name of the data structure to form the email token.

- Roles and Privileges: The users a are assigned different roles, depending on these roles the users are permitted to view or modify certain assets. Usually admin users are given all the privileges.

- Site Parameters: Site parameters are key/value pairs that are used to configure many different areas of OROCP. Site parameters and their values are all available through the Site Manager.

- User Group Conditions: User are placed into different group based on their profile based on which promotions, discounts are sent to the users.

Chapter 4

Technical and Functional Overview

4.1 Functionalities

Functionalities of the product are,

- Focused on Order Processing and Exception Management
  Managing flow of orders for the direct channel
  Capturing store orders for processing
  Managing business rules, fraud, and payment processing exceptions

- Supporting Customers After the 'Buy' Button
  Customer service focus for add/edit/modify/cancel
  Clear processing flow which can be communicated to your customer

4.2 Technology Used

The technologies used in the product,

- Java 8 JDK

- Web Services
  SOAP Web Service
  REST Web Service

- Data Access Layer
  Oracle 12c
  JDBC access layer

4.3 Architecture

The high-level architecture of Oracle Retail and its components

- Oracle Retail Platform:

  Oracle Retail Platform provides services to all Oracle Retail applications. It contains the, UI framework, and Manager/Technician frameworks. Oracle Retail Platform is not retail-specific.

- Commercial Services:

  Commerce Services implement business logic. Commerce Services define data and behavior for retail applications.

- Oracle Retail Applications:

  All Oracle Retail applications leverage the frameworks and services provided by Oracle Retail Platform and Commerce Services.

- External Interfaces:

  Using frameworks and services, the applications are able to interface with other applications and resources

  Advantages of the Oracle Retail architecture include its object-oriented design and scalability. The system is designed to support existing systems and customer extensions. Oracle Retail Platform frameworks support integration by adhering to retail and technology standards. The multi-tier design of the architecture allows the application to support numerous types of infrastructure.

4.4 Database Data Model

RCOM groups schemas together into four databases: control, content, event, and reporting. In implementation, these databases can be entirely separate and may even exist on different database servers, or they can be included in just one database.

- Database: Control Description: Tables that manage administrative user accounts, groups, roles, and the privileges available within the site management tools. Auditing data is also stored here.

- Database: Content Description: Tables required to represent a site's virtual catalog, categorizations, ensembles, products, and sky-level product variants.

- Database: Event Description: Tracks all of the "events" that are generated by registered users, users with known email addresses, and anonymous users. Logically part of the "user" package, but schema supports physical distinction in order to provide the flexibility to track events in an alternative data store.

- Database: Reporting Description: Tables that contain the data presented in the Site Manager (Reporting) when reports are generated. These tables are populated by scripts that transform the data in the control and content databases and places the data here.

Chapter 5

Product Security

5.1 Security Aspects

During the product development it is always taken care to look at it from the security perspective,hence protect it from vulnerabilities.In order to do so we develop utilities to analyse the product from security perspective.

Figure 5.1: Retail Cycle

- Data Flow Aspect

  This utility identifies potential vulnerabilities that include corrupted information (client controlled info) put to possibly risky utilize. It checks the data flow between the site and a function call which is dangerous .

  For instance, the information stream analyzer distinguishes whether a client controlled information string of unbounded length is being replicated into a statically

estimated support, and recognizes whether a client controlled string is being utilized to develop SQL question content

- Control Flow Aspect

  This analyzer recognizes dangerous consequences of operations. By breaking down control stream ways in a program, the control stream analyzer decides if an arrangement of operations are executed in a specific request. For instance, the control stream analyzer recognizes time of check/time of utilization issues and uninitialized factors, and checks whether utilities, for example, XML readers, are designed legitimately before being utilized.

- Structural Aspect

  This analyzer recognizes the flaw in the structure. By breaking down control stream ways in a program, the analyzer decides if an arrangement of operations are executed in a specific request. For instance, the analyzer recognizes time of check/time of utilization issues and uninitialized factors, and checks whether utilities, for example, XML readers, are designed legitimately before being utilized.

- Semantic Aspect

  This analyzer recognizes possibly unsafe employments of functions and APIs at the intra-procedural level.

- Configuration Aspect

  It searches for errors and mistakes,mostly the one's which might not follow the policies.

- Buffer Analysis Aspect

  It detects the buffer overflow.

5.2 SQL Injection

A SQL infection comprises of injection of a SQL query by means of the information from the customer to the application. A fruitful SQL injection can read delicate information from the database, alter database information (Insert/Update/Delete), execute organization operations on the database, (for example, shutdown the DBMS), recoup the substance of a given document display on the DBMS record framework and at times

issue summons to the working framework. SQL injection attacks are a kind of attacks, in which SQL command are infused into information plane in order to affect the predefined SQL commands.[2]

Execution

Input validation is performed to guarantee just appropriately shaped information is entering the work process in a data framework, keeping malicious information from persevering in the database and activating glitch of different downstream parts. Input validation ought to occur as right on time as conceivable in the information stream, ideally when the information is gotten from the outer party.

A weak validation of input could lead to affecting the data flow of the application.An attack on the data flow could affect the Availability,Confidentiality and Integrity of the application.An attacker can provide a malicious input as a result the application can crash or some excess information can be fetched from the database.

Rather than preparing a black-list of unwanted inputs, a white-list is prepared about the acceptable inputs because there are high chances of some data to be missed in the black-list.An input that doesn't comply with the defined inputs list would be rejected.During the validation of input data some of the factors taken into consideration are the type of data,length of data, syntax.Also these security checking are done on both, the server-side as well as the client-side in order to avoid any loop hole

5.3 Cross-site scripting

Cross Site Scripting happens when dynamicallly created site pages show client input, for example, login data, that isn't appropriately approved, enabling an intruder to insert malicious script into the produced page and after that execute the content on the machine of any client that perspectives the site. This type of user interactive vulnerabilities require the client to trigger the execution of the malicious contents by means of an activity, for example, clicking a connection or moving the mouse pointer over the content.[4] In case of success, Cross Site Scripting vulnerabilities can be misused to control or take treats, trade off secret data, or execute vindictive code on end client frameworks. Proposals incorporate actualizing secure programming systems that guarantee legitimate filtration of user provided information, and encoding alluser provided information to counteract

embedded contents being sent to end user in a format that can be executed.[5]

Implication

XSS can by large be subdivided into two classifications: stored and reflected attack. The primary difference between the two is in the way of arrival of base at the server. Stored attacks are only that in some way stored in the server. The victim will recover and execute the malicious code in their program when a demand is made for the stored data. Reflected attack, then again, originate from elsewhere. This happens when user contribution from a web customer is instantly included by means of server side contents in a powerfully created website page. By means of some social designing, a victim can be attacked by the attacker, for example, through a malevolent connection or "fixed" shape, to submit data which will be changed to incorporate assault code and afterward sent to the real server. Injected code is then reflected back to the user's program which executes it since it originated from a trusted source of server. The implication of every sort of attack is similar.

The main problems associated with successful Cross Site Scripting attacks are:

- Account hijacking-An attacker can seize the client's session before the session lapses and do some activities with the benefits of the client who got to the URL, for example, issuing database questions and survey the outcomes.

- Malicious script execution-Many times users being unaware execute a script, or any Flash content which an attacker might have inserted into the site.

- Worm propagation-XSS can behave like a virus in some AJAX applications. The XSS payload can self-rulingly inject itself into pages, and effectively reinject a similar host with more XSS, which can all be finished with no hard refresh. In this way, XSS can send numerous requests utilizing complex HTTP strategies to propagate itself undetectably to the client.

- Information theft-Users can be directed to the attackers choice of site throught redirecting.

- Denial of Service-Most of the time the users are denied from the requested service asked by them in order to defame the service owner.

- Browser Redirection-Many times it happens that the user is redirected to the malicoius site unknowngly but the user thinks he is on the correct site as the URL remains the same. This is because not the entire page but just the frame is redirected.

- Manipulation of user settings-There are chances where the attacker changes the settings of user for notorious tasks.

Execution:

The attack string can be kept an eye on in order to know what the response should be. Like, if "(javascript:alert ('XSS')" is given as an attack string, it will also appear as the response. This shows that web application is HTTP request parameters values and without removing the response using it as a response.

The fix required here was, HTML Tag Injection attacks can be kept away from via validating all information, and legitimately encoding output. While approving client input, confirm that it coordinates the strictest meaning of substantial information possible. For instance, if a specific parameter should be a number, endeavor to change over it to a numeric information compose in programming dialect. While reflecting qualities into JavaScript or another configuration, make a point to utilize a kind of encoding that is suitable. Encoding information for HTML isn't adequate when it is reflected within a content or template. For instance, while reflecting information in a JavaScript string, we made a point to encode all non alphanumeric characters utilizing hex () encoding. In the event that you have JavaScript on your page that gets to risky data (like location.href) and composes it to the page (either with document.write, or by adjusting a DOM component), we made a point to encode information for HTML before composing it to the page.

There is no in-built function in JavaScript to do this, however numerous systems do. Approving client information ought to be done when it is gotten. Encoding information for show ought to be finished

5.4 Exposure of POST parameters in GET

Implication: RCOM, the GET and POST parameters are collapsed into a single data structure and served in the same manner. This is a security flaw as it leaves the exposure of sensitive data such as credit card numbers, email address in the GET URL. On the

off chance that a page acknowledges POST parameters as GET parameters, an attacker would have the capacity to impact change on sites through Cross-Site Request Forgery or use this plan defect with different vulnerabilities to assault the framework facilitating the web application.

Execution:

Utilizing any web tool peruse to the connection. Once got to add each POST parameter to the GET parameters rundown and re-ask for the page. On the off chance that a similar page shows up while asking for FullUrl with a HTTP GET ask for with all POST parameters in the URL, at that point this page is defenseless against this outline defect.

The Command framework for RCOM is designed in such a way that the same URL could be served by both GET and POST requests with the process behind being transparent to the user of the system. During analysis it was found that changing the existing framework to differentiate between GET and POST requests would require extensive re-factoring and was not desirable. All sensitive data handling URLs in RCOM had one of these patterns "user" or "card" or "payment" embedded as a part of the URL. The solution then provided was to write a filter which intercepts the doGet() method and if the URLs have the above mentioned pattern, a new Exception is thrown and error is logged stating that the method called cannot be served by GET but rather POST.

5.5 Identity Cloud Service Security

Process flow:

- User clicks on 'Can't sign in?'
- This will direct him to the user data request confirmation page which consists of form to enter the username.
- User submits his/her email address
- This username is mapped to the email id in the database,which sends a password changing link to the user
- User clicks the link through user data request instruction mail to access his data.

- The server takes UID from the link and user email from the database to generate a new token and then compares new token to the original token saved in the database for authentication.
- Only after successful authentication user is eligible to change the password.
- This link is set to expire within few minutes of time in order to avoid reuse of the link.

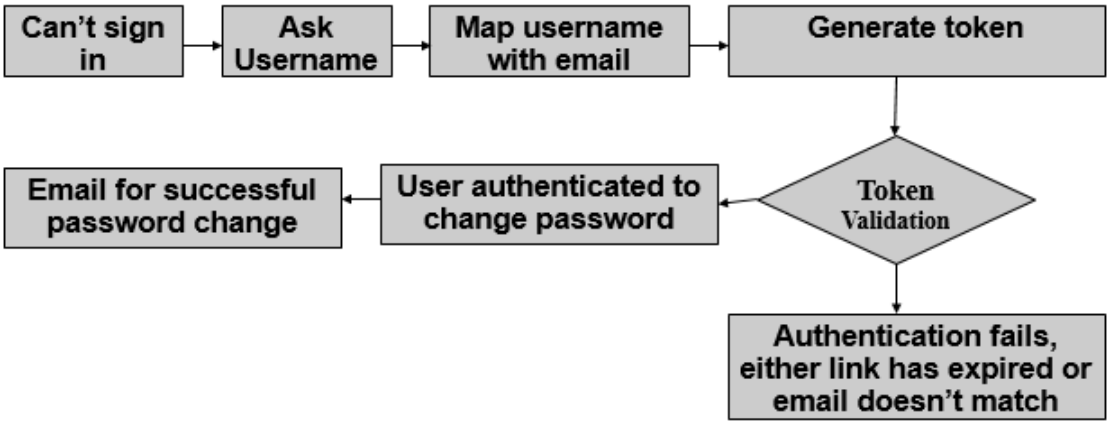


Figure 5.2: Process

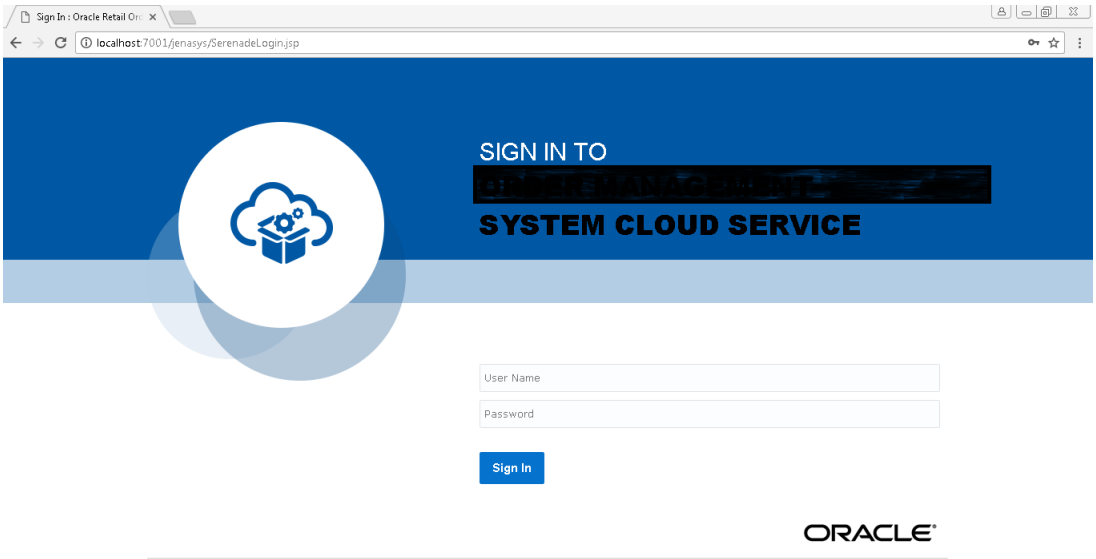


Figure 5.3: Older UI

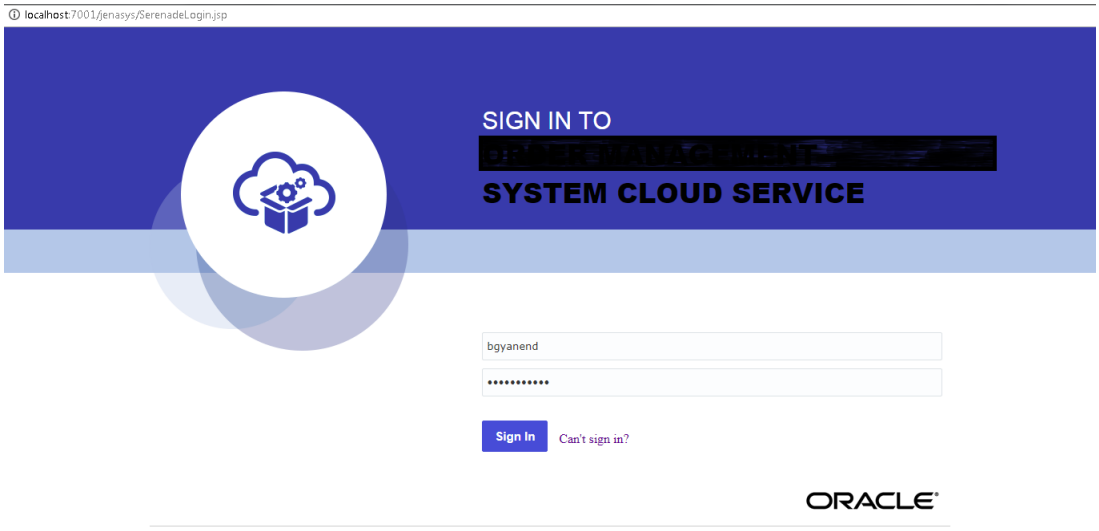


Figure 5.4: New UI

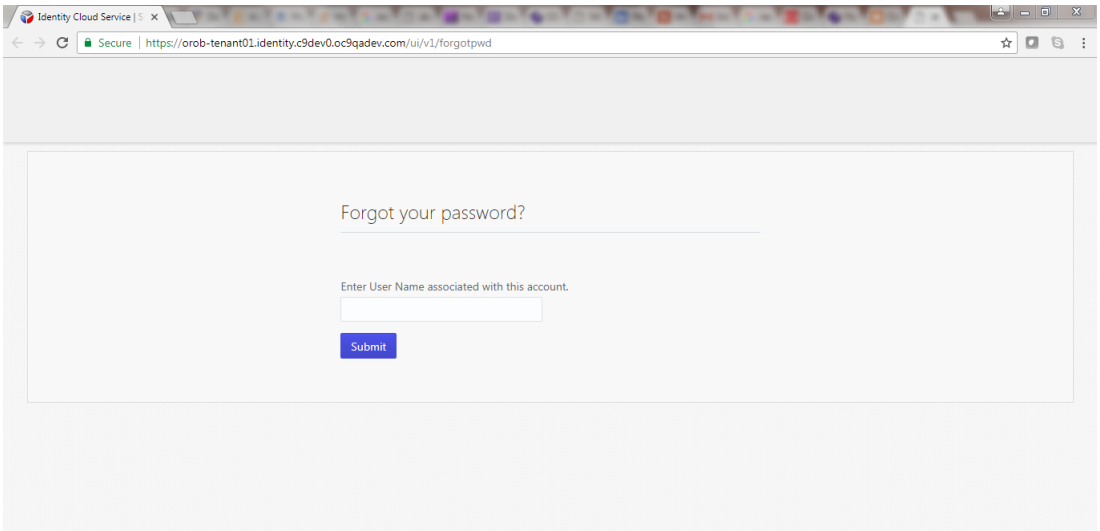


Figure 5.5: Ask for username

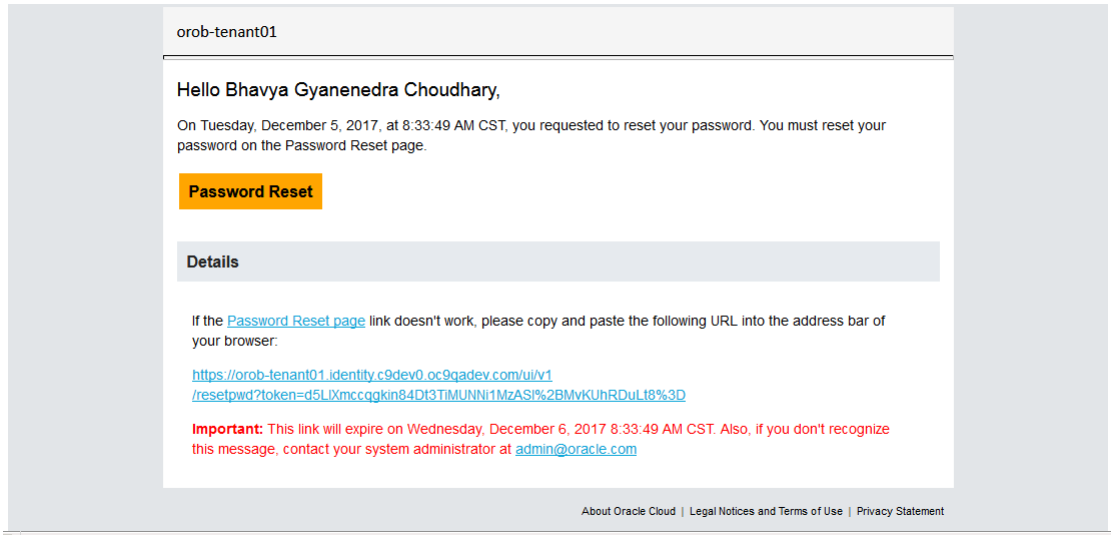


Figure 5.6: Email to change password

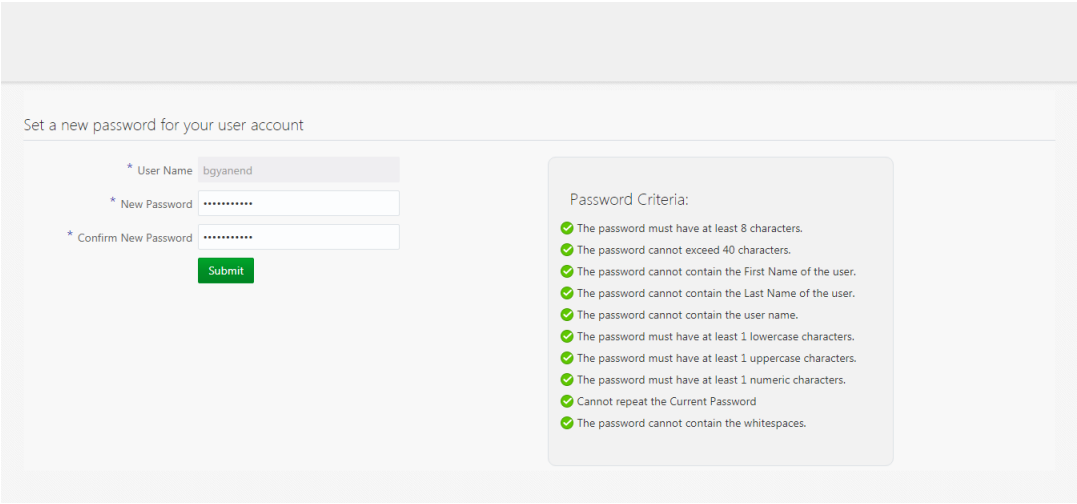


Figure 5.7: Reset Password Validation

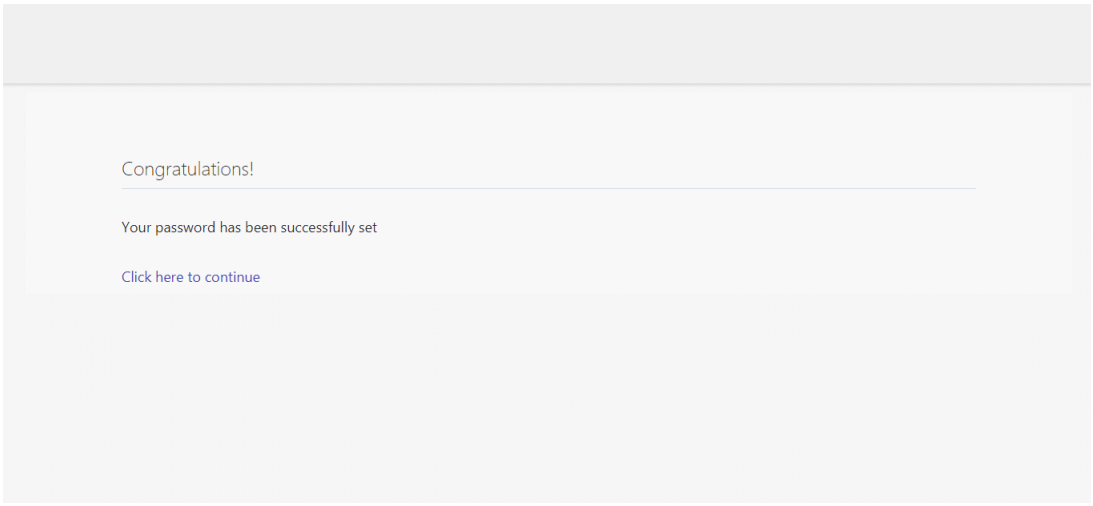


Figure 5.8: Reset Password successful

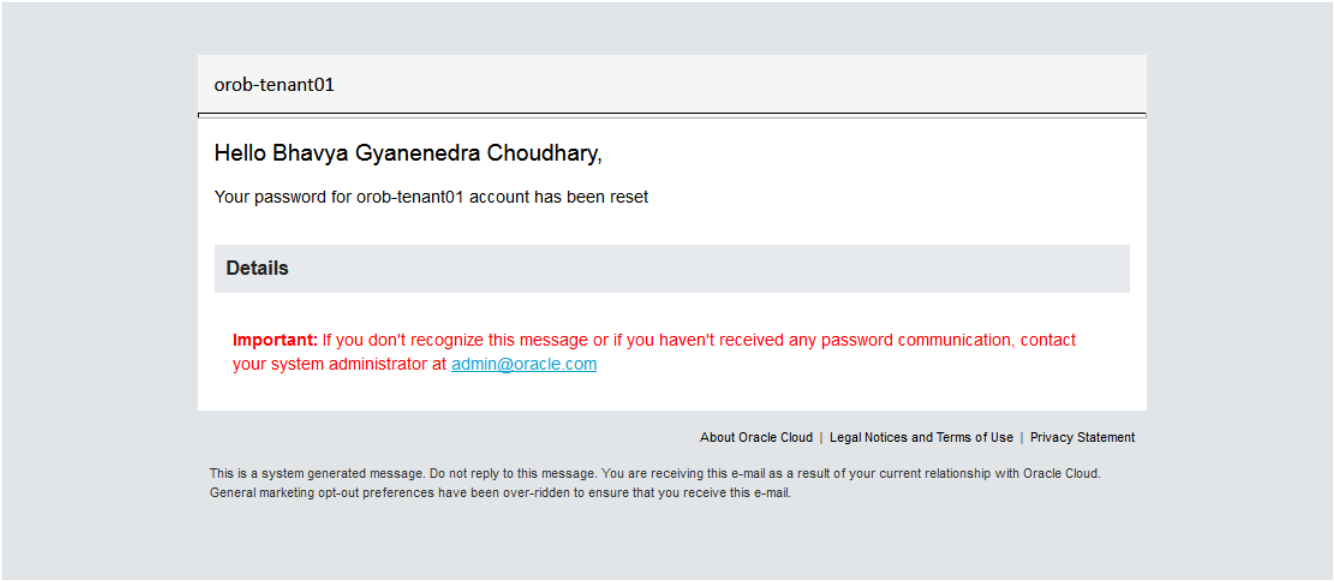


Figure 5.9: Email Change of Password Successful

Chapter 6

Legal Compliance

6.1 Overview

The main Legal Compliance of RCOM is based on the European Union General Data Privacy Regulations (EUGDPR). EUGDPR is a series of laws that affect all products that may contain personal information about residents of the EU. It is important to note that these regulations affect products regardless of where they are hosted, so OROCP is also subjected to these regulations if they are intended to hold the Personally Identifiable Information of EU citizens. The following terms are used to describe the actors involved in the handling and processing of PII data within the scope of the RGBU:

- **Data Subject** - The person whom the PII describes. In most cases within the RGBU (Retail Global Business Unit), this refers to a shopper, whether it is in the store or online. In some cases, this may refer to an employee of the retailer, or a corporate contact for a third party contractor to the retailer.
- **Data Controller** - The retailer. In a cloud environment, Oracle becomes the data custodian, but the retailer still retains ownership and control of the data.
- **Data Processor** - Applications that work with PII, including RGBU applications and any external applications with whom we share the data.

The data subject rights on which the work to be done are,

- **Right to Access:** Some portion of the extended privileges of information subjects plot by the GDPR is the privilege for information subjects to acquire from the

information controller affirmation in the matter of regardless of whether individual information concerning them is being processed, where and for what reason. Further, the controller might give a duplicate of the individual information, free of charge, in an electronic format. This change is a sensational move to information straightforwardness and strengthening of information subjects.

- **Right to be Forgotten:** Also known as Data Erasure, the privilege to be overlooked qualifies the information subject for have the information controller eradicate his/her own information, stop facilitate spread of the information, and conceivably have outsiders end preparing of the information. The condition for erasing the information never again being applicable to unique purposes for preparing, or an information subjects pulling back cons.

6.2 Right to Access

The main tasks performed in Right to Access are:

- Generate PII data xml file
- Backend job to delete token

6.2.1 User Data Request

In site manager UI create user data request page

Problem Statement

The shopper or employee will have the right to request access to any personal information stored in client applications. They will contact the retailer to request this information and provide any necessary information. A new screen must be added to Site Manager for the retailer to submit this request on behalf of the customer.

Process Flow

- General public (data subject) user makes a phone call to data controller requesting his/her data.
- If call center representative has admin roles and privileges, will access user data request page in site manager, and will request for user name (email) from the data subject and submits it into the user data request form. If he doesn't have the privilege to do this then he forwards it to the site admin.

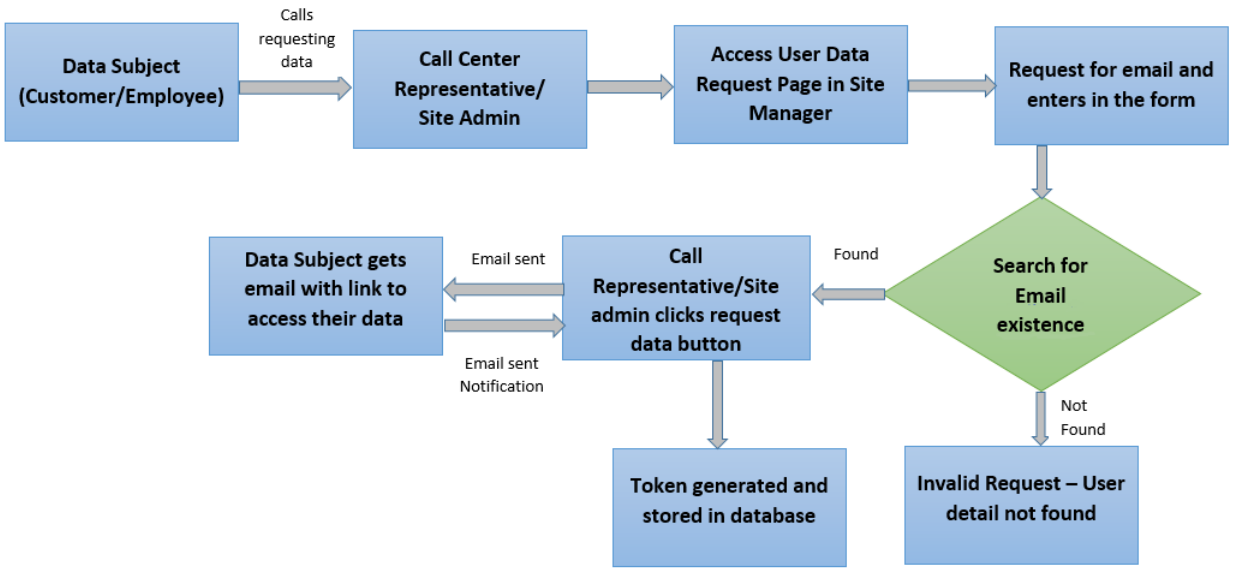


Figure 6.1: Process Flow

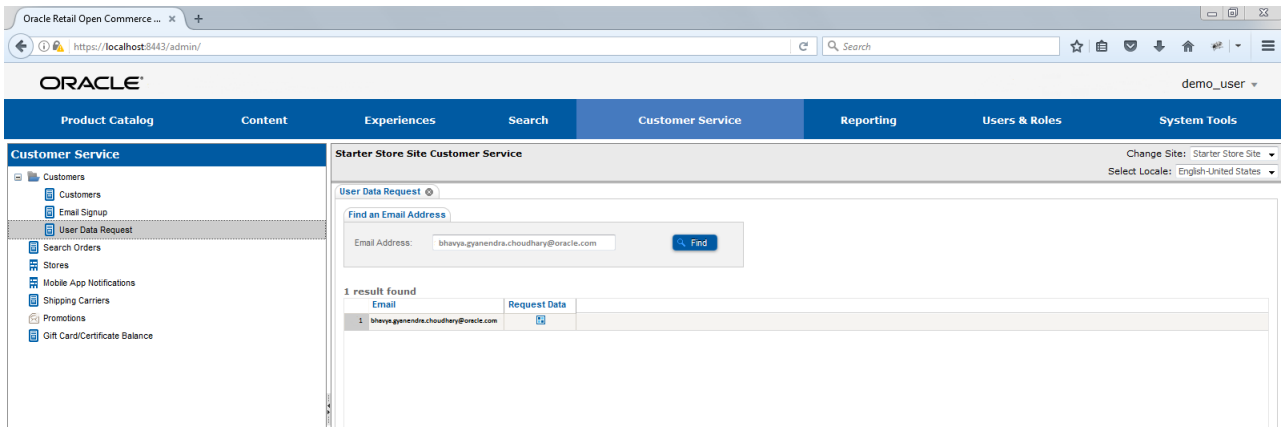


Figure 6.2: User Data Request Page in Site manager

- If the match for the email is found then call center representative/site admin clicks on request data option. During this server takes the email address and generate a token which is stored in database for validation and sends an email to the user with the link containing the Unique Identification number (Uid).
- Once the mail is sent, the call center representative/site admin will get the email sent to the user confirmation message displayed on the page.
- User view the email and click the link which takes them to user data request page in starter store UI.

6.2.2 Confirmation for the User Request

In starter store UI create user data request page confirmation page

Problem statement

The data subject on request will receive an email with instruction to obtain their PII data. A new screen must be added to Starter Store which contains a form for a user to enter their email address and which does the validation of the link (user).

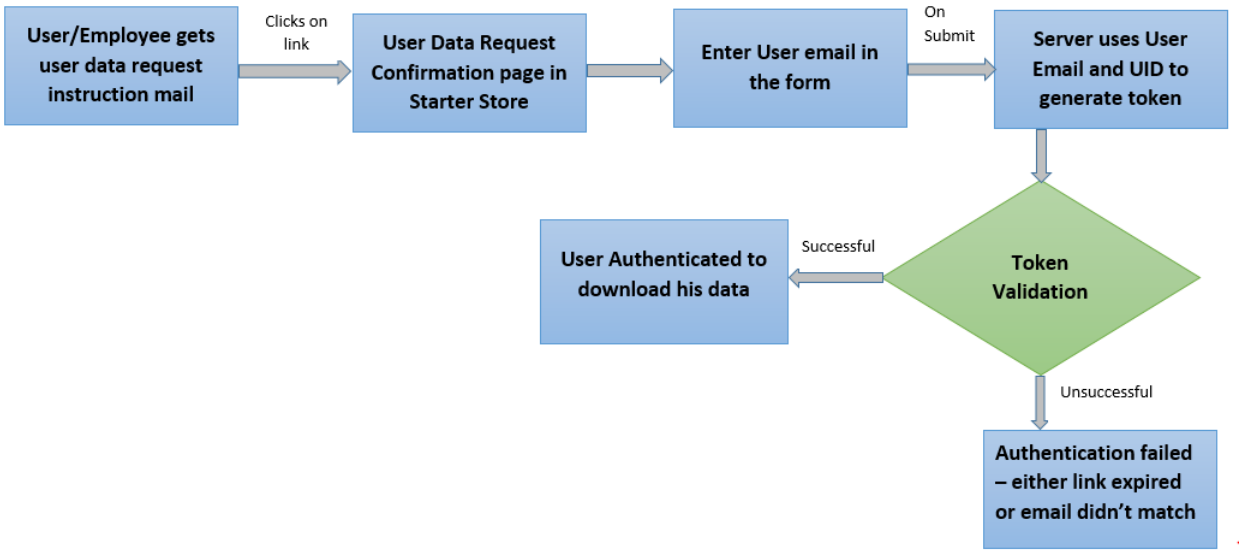


Figure 6.3: Process Flow

Process flow

- User clicks the link sent to him through user data request instruction mail to access his data.
- This will direct him to the user data request confirmation page (Figure 13) which consists of form to enter the user email.
- User submits his/her email address.
- RCOM server takes Uid from the link and user email from the form to generate a new token and then compares new token to the original token saved in the database for authentication.
- Only after successful authentication user is eligible to get his/her PII data.

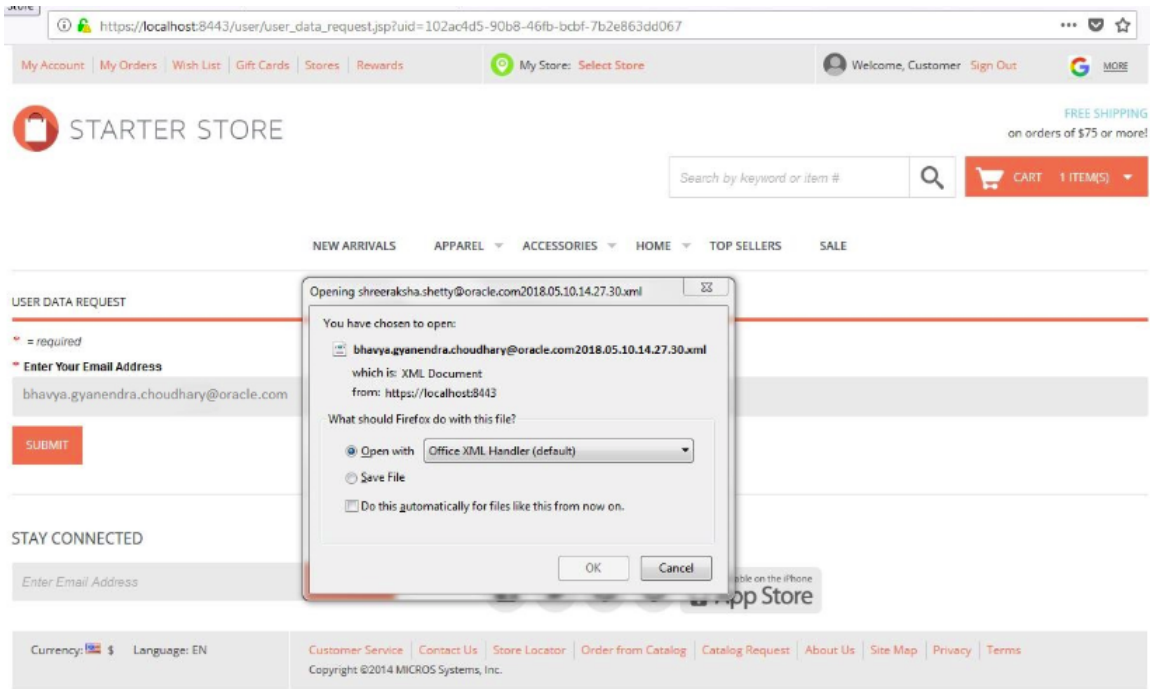


Figure 6.4: Popup for XML file download

6.3 Right to Forget

The main tasks performed in Right to Forget are:

- Block inactive user
- Anonymize PII data by email
- Don't send anonymize data to management system
- Don't send anonymize data to e-commerce website

6.3.1 User Data Removal Request

In site manager UI create user data request page

Problem Statement

The shopper or employee will have the right to request removal of any personal information stored in client applications. They will contact the retailer to request the removal of all the personal data on the client applications.Before removal of the clients personal data it is first checked that no orders are pending on the customer's name. A new screen must be added to Site Manager for the retailer to submit this request on behalf of the customer.

Figure 6.5: XML file

Process Flow

- General public (data subject) user makes a phone call to data controller requesting removal of his/her data.
- If call center representative has admin roles and privileges, will access user data removal request page in site manager, and will request for user name (email) from the data subject and submits it into the user data request form. If he doesn't have the privilege to do this then he forwards it to the site admin.
- If the match for the email is found then it is first checked that there exists no pending unfulfilled order on the customer's name.
- If there are no open orders then the call centre representative will click on anonymize data button.
- Once the anonymize data button is clicked, the entry for that email id is searched for in all the database and every information to it is permanently deleted from the database.

```
- <Card>
      <cc_number>**********1111</cc_number>
      <cc_type>VI</cc_type>
      <cc_name>Nancy Swan</cc_name>
      <subscription_id>9909000194231398</subscription_id>
  </Card>
- <Card>
      <cc_number>**********1111</cc_number>
      <cc_type>VI</cc_type>
      <cc_name>Nancy Swan</cc_name>
      <subscription_id>9909000192716788</subscription_id>
  </Card>
- <Card>
      <cc_number>**********1111</cc_number>
      <cc_type>VI</cc_type>
      <cc_name>Nancy Swan</cc_name>
      <subscription_id>9909000188954575</subscription_id>
  </Card>
- <Card>
      <cc_number>**********4444</cc_number>
      <cc_type>MC</cc_type>
      <cc_name>Nancy Swan</cc_name>
      <subscription_id>9909000188953742</subscription_id>
  </Card>
- <Card>
      <cc_number>**********5100</cc_number>
      <cc_type>MC</cc_type>
      <cc_name>Nancy Swan</cc_name>
      <subscription_id>9909000201619031</subscription_id>
  </Card>
- <Card>
      <cc_number>**********5100</cc_number>
      <cc_type>MC</cc_type>
      <cc_name>Nancy Swan</cc_name>
      <subscription_id>9909000201616664</subscription_id>
  </Card>
</cards>
</UserInfo>
<userRegistrationAccounts/>
- <ExternalSystems>
    <SystemName>RELATE</SystemName>
    <UserExternalSystemID> </UserExternalSystemID>
</ExternalSystems>
- <ExternalSystems>
    <SystemName>SERENADE</SystemName>
    <UserExternalSystemID>11809</UserExternalSystemID>
</ExternalSystems>
</user_data>
```


Figure 6.6: XML file

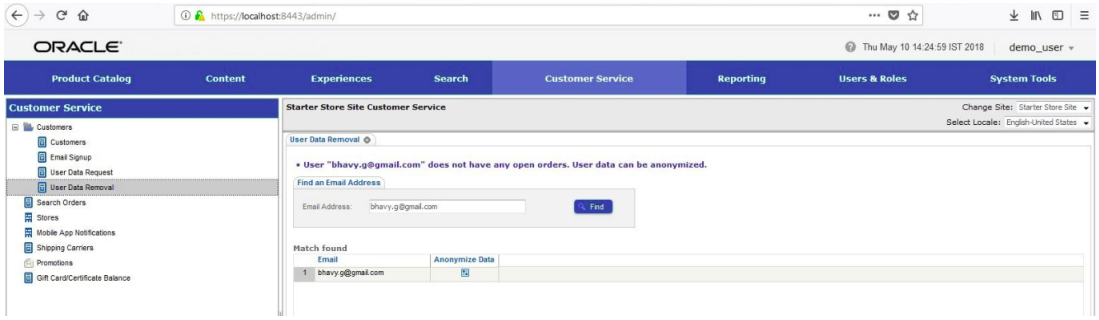


Figure 6.7: Anonymization of User Data

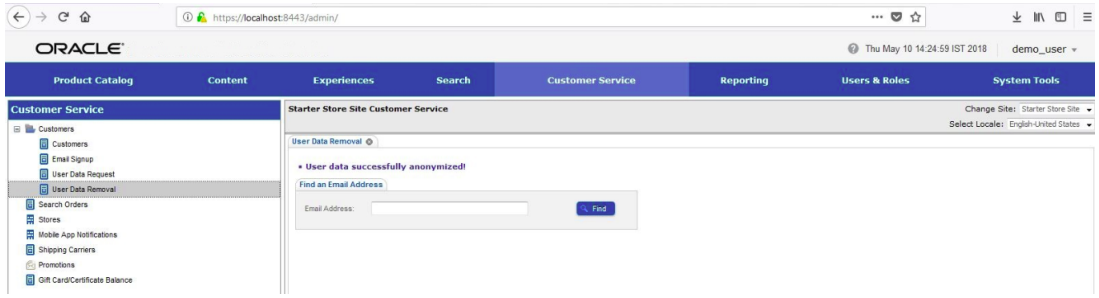
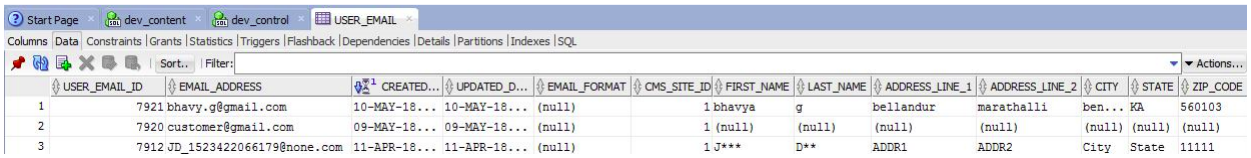
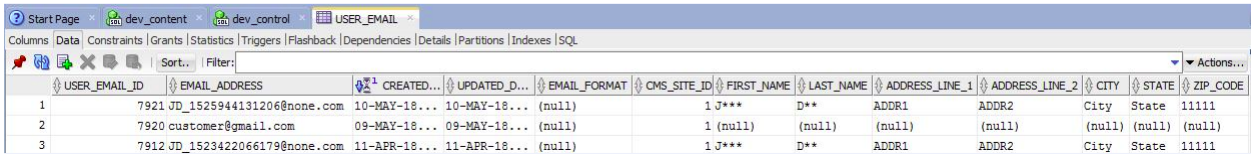


Figure 6.8: User Data Anonymized



	USER_EMAIL_ID	EMAIL_ADDRESS	CREATED...	UPDATED_D...	EMAIL_FORMAT	CMS_SITE_ID	FIRST_NAME	LAST_NAME	ADDRESS_LINE_1	ADDRESS_LINE_2	CITY	STATE	ZIP_CODE
1	7921	bhavy.g@gmail.com	10-MAY-18...	10-MAY-18...	(null)	1	bhavya	g	bellandur	marathalli	ben...	KA	560103
2	7920	customer@gmail.com	09-MAY-18...	09-MAY-18...	(null)	1	(null)	(null)	(null)	(null)	(null)	(null)	(null)
3	7912	JD_1523422066179@none.com	11-APR-18...	11-APR-18...	(null)	1	J***	D**	ADDR1	ADDR2	City	State	11111

Figure 6.9: Database before deleting user details



	USER_EMAIL_ID	EMAIL_ADDRESS	CREATED...	UPDATED_D...	EMAIL_FORMAT	CMS_SITE_ID	FIRST_NAME	LAST_NAME	ADDRESS_LINE_1	ADDRESS_LINE_2	CITY	STATE	ZIP_CODE
1	7921	JD_1525944131206@none.com	10-MAY-18...	10-MAY-18...	(null)	1	J***	D**	ADDR1	ADDR2	City	State	11111
2	7920	customer@gmail.com	09-MAY-18...	09-MAY-18...	(null)	1	(null)	(null)	(null)	(null)	(null)	(null)	(null)
3	7912	JD_1523422066179@none.com	11-APR-18...	11-APR-18...	(null)	1	J***	D**	ADDR1	ADDR2	City	State	11111

Figure 6.10: Database after deleting user details

Chapter 7

Conclusion and Future Scope

7.1 Conclusion

At the end of the project work on the product it can be concluded that even the biggest of brand names now adays lack the smallest of loopholes in their softwares which can be exploited easily.Hence,timely scanning of the softwares at regular interval is required.Like in my project work basic security flaws in the product where mended.Also,the implementation GDPR policy is a very good step towards securing the softwares in the world.

7.2 Future Work

As a part of GDPR, work on Right to Access and Right to Forget was done on the product.Once it has been released some other rights which are a part of GDPR would also be implemented.

Bibliography

[1] Bitar, Hadi, and Björn Jakobsson. "GDPR: Securing Personal Data in Compliance with new EU-Regulations." (2017)

[2] Clarke-Salt, Justin. SQL injection attacks and defense. Elsevier, 2009.

[3] Fergerson, Julie S., Christopher L. Fowler, and Risser C. Estes. "System and method for secure transaction order management processing." U.S. Patent No. 5,966,697. 12 Oct. 1999.

[4] Guamán, Daniel, et al. "Implementation of Techniques, Standards and Safety Recommendations to Prevent XSS and SQL Injection Attacks in Java EE RESTful Applications." New Advances in Information Systems and Technologies. Springer, Cham, 2016. 691-706.

[5] Gupta, Shashank, and Brij Bhooshan Gupta. "Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art." International Journal of System Assurance Engineering and Management 8.1 (2017): 512-530.

[6] Howard, Michael, and Steve Lipner. The security development lifecycle. Vol. 8. Redmond: Microsoft Press, 2006.

[7] Johnson, Robert. Security policies and implementation issues. Jones Bartlett Publishers, 2014.

[8] Long, Fred, et al. The CERT Oracle Secure Coding Standard for Java. Addison-Wesley Professional, 2011.