Improving Oracle Retail Merchandising System and Oracle Retail Sales Audit using Functional and Software Security Assurance Testing

Thesis submitted in partial fulfilment of the requirements for the award of degree of

Master of Engineering

in

Information Security

Submitted By

Bhawna Gupta

(Roll No. 801633002)

Under the supervision of:

Dr. Maninder Singh

Professor (CSED)

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR INSTITUTE OF ENGINEERING AND TECHNOLOGY

PATIALA – 147004

June 2018

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "*Improving Oracle Retail Merchandising System and Oracle Retail Sales Audit using Functional and Software Security Assurance Testing*", in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Information Security* submitted in Computer Science and Engineering Department of Thapar Institute of Engineering and Technology, Patiala, is an authentic record of my own work carried out under the supervision of Dr. Maninder Singh and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Bhawna Gupta

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

Dr. Maninder Singh
Professor , CSED

ACKNOWLEDGEMENT

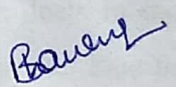
I would like to express my deepest appreciation to my mentor and thesis supervisor Dr. Maninder Singh for his constant support and motivation. He had been instrumental in guiding me throughout the thesis with his insights, constructive criticisms and interminable encouragement.

I would like to thank Oracle India Pvt. Ltd. I also wanted to thank my manager Jagadeesh Hosamane and all my team members who guided me throughout whole internship.

I would like to thank all the faculty members and staff of Computer Science and Engineering Department who were always there at the need of hour and provide all the help and facilities, which I required for the completion of this work.

I offer my deepest gratitude to my family for their support and affection and believing in me always. I also want to thank my friend who helped me in all possible ways towards the completion of my work.

Finally I thank the Almighty who gave me strength to complete the work.



Bhawna Gupta

ME (Information Security)

801633002

ABSTRACT

In this ever-changing technology world, being competitive and successful is important. This competition results in organizations to improve their short software development process timelines to produce high quality and efficient software. Various testing types are performed on product before it is released to the market. Earlier testing was considered a process that occur after software development is completed. But now testing is being performed at every phase of Software Development Life Cycle. Due to increase in security attacks organizations are performing software security assurance testing on their software along with functional testing.

Manual and automated testing are performed to ensure the efficiency of software. With time organizations are moving towards automated testing. Scripts and tools are used and trusted more than manual testing. Tools used are generic tools and can't depict the functionality of applications. Thus the reports generated contains a lot of false positive errors. Inspecting these false positives wastes a lot of time of developers. Thus it is important to not depend on automated testing alone. Manual testing must also be performed. Security testing should be performed by security experts manually as well as with tools. This will increase the efficiency of software and thus increase the revenue of organization as maintenance cost will be less.

Retail Merchandising System is one of Oracle's Retail product which deals in the functions like item management, replenishment, inventory management etc. Due to shifting to cloud micro services are being implemented and delivered to the customers. For auditing of retail operations Oracle provides Retail Sales Audit to the customers which can be integrated to the RMS. All the pricing related information that flows between RMS and ReSA is provided by Retail Pricing System. The above said testing i.e. functional and security testing was performed on two of the products RMS and ReSA to make sure the performance of the software is acceptable.

Table of Contents

Page

List of Figures

List of Screenshots

Chapter 1

Introduction

1.1 Merchandise Operations Management (MOM)

Retail industry deals in operations like buying the products in bulk, breaking that bulk into smaller pieces and then selling those pieces to gain profit. The major activities that takes place during the whole MOM process are :

- Planning : Planning is the phase in which decision of what item, in what amount and from which supplier items need to be ordered is taken. Along with this it also includes the activities like which supplier will be available for the delivery of the items, which warehouse to be used for the delivery or how many items need to be transferred from warehouse to the store etc.
- Buying : In this phase an order is being placed for the selected item against the selected supplier. Item, its quantity and warehouse to be delivered is decided in the planning phase.
- Merchandising and Inventory Management : After the ordered quantity is received then the Inventory management is done. Stock count of the received item will be revised or updated and the transfer of the item from warehouse to stores are being performed in this phase.

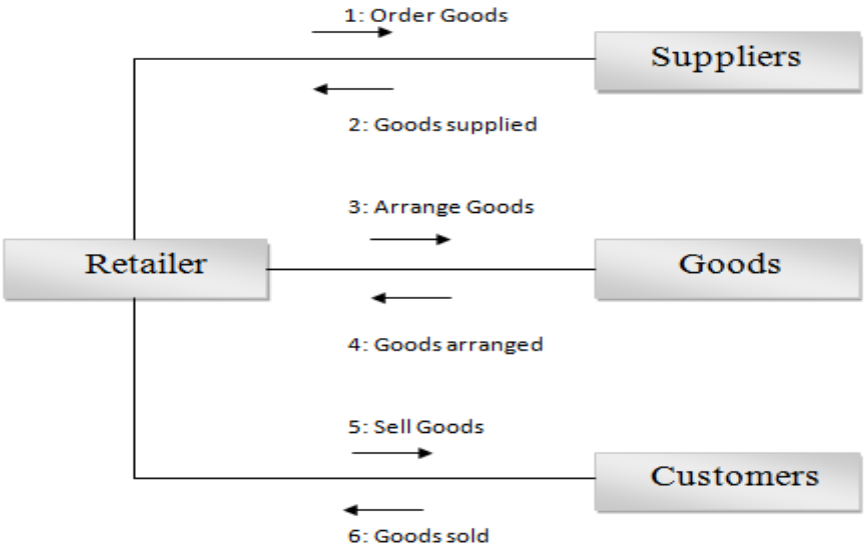


Figure 1.1 MOM Operations

- Selling and Customer Service : This includes selling of the products at store level and provide services to customers. This phase impacts on the inventory management.
- Support : Includes support for the customers.

1.2 Retail Merchandising System (RMS)

RMS is the central repository that records and controls all the data and maintains integrity of all the systems integrated to it. The main functions of RMS are inventory management, item maintenance and replenishment. Due to these key functions of RMS it is easy to have access to day-to-day merchandising activities that are critical in nature. This helps retailer to focus on the key decisions and achieve the sales and profit targets. As RMS is a web based and scalable application it supports bulk data without any problems.

Beside online application various others ways were needed to be introduced in 3 tier architecture to perform the above described operations. One of them is Web Services. Web Services is a client server application which helps in the communication between two devices over network. Various HTTP methods are used for communication. For example: “GET” method is used for getting information about any entity passed in URI (like item, order etc).

As RMS is a cloud based application, security is very important as there will be no direct database access. Data will be available from cloud. The connection as well as the data on the cloud must be secured while processing is being performed. Here processing include posting the data, getting the data, and updating the data etc.

1.3 Security in RMS

Security is the process of protection against potential harm from external threats. It is achieving a fearless state or state of freedom from any kind of threats. Application security is the protection of application from external threats by the use of hardware, software or any other potential methods. Security requirement needed to be taken care before and after software development. Some security measures are implemented before software development process is started like updated versions of JDK must be present for the use of cryptographic extensions.

1.3.1 Oracle Software Security Assurance Testing

Security in Oracle products is assured by Oracle Software Security Assurance (OSSA). OSSA encompasses constantly-evolving processes, procedures, and technologies implemented by Oracle to ensure that Oracle's products are meeting customers security requirements, while providing for the most cost-effective ownership experience.[1]

Figure 1.2 : Software Security Assurance[1]

OSSA is applied to every Oracle products. It will be applied to software components of hardware products also. Security is being considered at each phase of software development. Following are the major programs included in OSSA testing.

- Secure Development Standards

In this program of OSSA, design level security standards, secure coding standards and secure coding practices and trainings are included. Standards like Old and weak cryptography is banned, secure coding standards etc are to be followed while whole development process. Mandatory trainings are given to every employee in development sector.

Figure 1.3 : Secure Development Standards

- Secure Design

A secure application will be a result of secure design. Security architecture refers to the fundamental pillars: the application must provide controls to protect the confidentiality of information, integrity of data, and provide access to the data when it is required (availability) – and only to the authorized users [2]. Use of strong cryptographic libraries and Single Sign On (SSO) is mandatory and developers need to implement this in all the Oracle products.

- Security Tools and Testing

Both proactive and reactive testing are performed. Whenever any new functionality or module is added then a thorough testing is performed on it. Integrating it with application should not effect other modules functionality. In house tools and third party tools are used to configure scans on products before delivered to customers.

- Security Compliance

Newly acquired products are checked for security vulnerabilities before they are used by employees in any of the activities of software development life cycle. Exceptions are tracked and resolved.

- Security Evaluations

Third party product security evaluation against standards of 'what you mean when you say you are secure' i.e. checking if the product is as secure and bug free as it was said.

- Internal Security Assessments

In this the product is given to internal Ethical Hacking team for evaluation of security vulnerabilities.

- External Security Assessments

In this application is tested against common criteria, FIPS 140. Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST). This standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information [3].

- Critical Patch Updates and Security Alerts

Security patching is the most public evidence for ongoing assurance[1].Patches are provided in two ways. Predictable patches are those which are provided after periodic

time like after every four months etc. Cumulative Patches are those in which customer can install all the previous patched in a single patch update.

1.3.2 Testing Process

Testing is performed in two ways in most of organizations. Those are :

- Manual
- Automated

First test cases are created in Oracle Test Manager. Separate folders for different functionalities are created and in those folders test cases are created. Each test case contains information like what the test case is about, for what type of testing the test case was created, who is the owner of the test case, who updated the test case, what is the name and number of product etc. Along with this steps to recreate the test case is also written. After the test case is recreated (if no error exists) then it is passed otherwise it is failed.

In Manual testing, application is tested manually by recreating the test cases. The software is tested by performing the operation manually again and again without the use of tools. Tester plays a very important role in this as tester will execute the test cases manually. All the test cases created for UI manual testing are recreated and behaviour of the application is studied. If the application is behaving normally then the test case is passed otherwise a bug is created against it. There are also some cases in which the test case is passed but while checking another bug is found then again a bug is logged against it.

Advantages of Manual Testing :

- No environment limitations
- Programming knowledge is not required
- Recommended for software which has dynamically changing GUI design requirements.

In Automated testing, goal is the same but approach is different.

- Automation Testing
- WebInspect
- SoapUI

- Postman
- SQLSPLAT

Advantages of Automation Testing :

- Fast
- Reliable
- Comprehensive : A batch file can be created which will run without user interaction.
- Scalable and Modular : The RMS Automated Testing tool allows you to add as many records as you need with which to test across any number of scenarios. Your testing can span various technology platforms (including forms and ADF) and can encompass your end-to-end merchandising solution or just a single functional area.
- Flexible : Automation scripts validate the environment for stability, ensuring that all activities, such as a new migration, implementation, or a patch can be executed. Once the scripts run successfully with the desired results across all features, the system can be deemed stable and ready to be used and loaded with production data.

  Automated Regression Testing is the testing area in which you can leverage automation to the fullest extent. You can execute all previously executed test cases on the new build through automation. This ensures that testing is accurate and provides confidence that the product is working as expected. Automation also yields significant time savings for the regression cycle.

  Patch validation is often time consuming, since previously working features can be broken because of a new fix. Automation delivers huge savings in terms of time and testing. Retailers can either run the pre-defined accelerator kit or run their customized datasheets that encompass all their critical business work flows. With automation, you can expect that all the regression scenarios will work even after the new patch is applied, without breaking previously working features.
- Efficient : Quality assurance (QA) professionals have been required to spend numerous hours or days testing a new patch depending on its size and scope. Automated testing provides the QA team with a time-saving tool that allows

them to focus on other core business activities. The time saved with automation can free up resources and take the squeeze out of deadlines. The scripts and customizable datasheets offer significant time savings along with executable repeatable tests.

Chapter 2

Literature Review

Testing can be defined as gathering information on software's reliability [4]. It is the process in which software is tested against various set of inputs. Test cases are made and behaviour of the software is tested by recreating those test cases. Test cases covers both functional, non-functional i.e. security and other requirements of the software. There can be various sources which may result the errors in the programs [4].

- Not defining the user requirement correctly
- deciding the major functions of program
- gaps in designing individual software components
- coding/implementation of software

To determine all the errors in a program two approaches are used [4] :

- deterministic approach
- probabilistic approach

When test cases are made by taken into consideration the types of errors, then the approach is said to be deterministic. Probabilistic methods estimates the likelihood of undetected errors still present in the program. Probabilistic approach focuses on the effectiveness of test cases to detect the errors that are still present in the program. It is very important that tester have the correct data to test. If tester does not have the correct data set to test then it may result in undetected errors in program. Organizations use various test data management tools from the purpose of avoiding this like HP has its own HP Test Data Management .

2.1 Test Data Management (TDM) [5]

Test Data is any information (static/transactional) that is used as an input to perform a test. Test Data management is the process that ensures the data used by testing team is of right quality. It ensures that the test data contains all the necessary inputs that are needed for the testing the product. It should be of appropriate length- not too large in quantity like production data and also not too same to fulfil all the testing needs. But the requirement is purely dependent on the type of software.

2.1.1 Challenges for TDM [5]

- Often incomplete
- testing team may not access to all the data sources.
- some data may be used by other teams also.
- at code level may be logic relationships are hidden and testers may not be able to extract all the needed data.
- data dependencies
- large amount of time spend in data gathering etc.

After data is verified by the TDM, tester starts the job by executing various test cases. Study the results and report for errors if exists.

With time, the way of testing are also changing. According to Infosys, QA's need to shift their focus from traditional functional testing to customer experience [6]. The data set which a TDS system prepare, the input data should be customer experience. In this way reliability, performance of the application will increase [7].

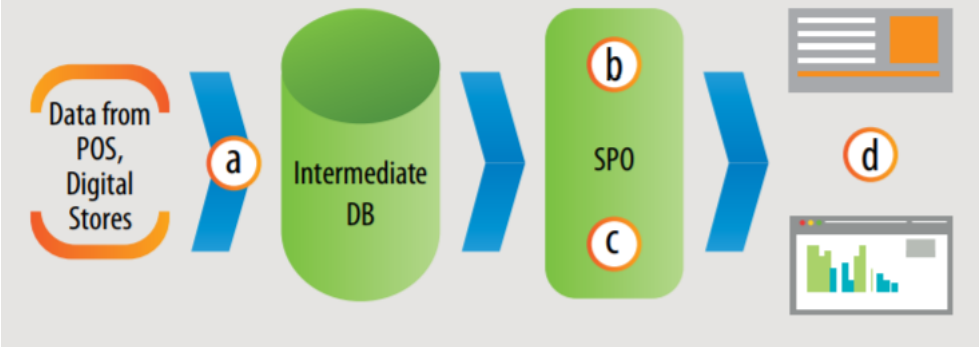


Figure 2.1 : Data Management System [7]

2.2 Introduction to Oracle Retail Merchandising System

Oracle Retail Merchandise System executes the core retail operations like inventory management, replenishment etc across countries, various channels, and business models which help retailers to establish a solid platform for growth and innovation.

The major challenge is to handle the large bulk of data efficiently and provide vast amount of information available in a usable and consumable format. Due to flexible

and scalable nature of RMS it is capable of providing such information effectively. This feature of RMS reduces the cost and time to perform the complex day-to-day merchandising activities. Also it provides the information about the where the items are in their life-cycle i.e. replenishment attributes.

2.3 Functional Areas of RMS [8]

The following functional areas exist in the Oracle Retail Merchandising System (RMS). Each functional area has business processes designed to help you complete a task.

- Foundation Data - Merchandise Hierarchy
- Foundation Data - Organizational Hierarchy
- Item Maintenance
- Purchase Orders
- Deals
- Replenishment
- Contracts
- System Administration
- ORAAC – Oracle Retail Application Administration Control
- Cost and Price Management

2.3.1 Foundation Data – Merchandise Hierarchy [8]

Merchandise Hierarchy defines the products at different levels. The purpose is to track and manage inventory. The levels can be specified according to the requirement of the project. Item Attributing Management at merchandise hierarchy levels is done to improve data consistency thus improving analysis and operations.

Following are the levels of Merchandise Hierarchy in RMS :

- Company : It is the highest merchandise and organizational entity defined in RMS. Only one company can be defined.
- Division : It is the first level of merchandise hierarchy within an organization. This level is basically used for differentiating the item types. For example : Within an organisation there can be two divisions- Food and Clothing.
- Group : It is the second level in merchandise hierarchy. Divisions can have many groups. For example : In clothing there can be various groups –Winter clothing, Summer clothing etc.

- Department : The third level after Group is Department. A group can have multiple departments. Key information about how inventory is tracked and reported is stored at the department level. For example : Men's Clothes and Women's Clothes etc.
- Class : The fourth level below department in the merchandise hierarchy is Class. A department can have multiple classes. A class provides the means to group products within a department. For example : Shirts, Jeans etc.
- Subclass : The fifth level after class in the merchandise hierarchy is subclass. A class can have multiple subclasses. A subclass provides the means to classify products within a department/class combination. For example : Full sleeves shirt.

The examples here are flexible i.e. may vary company to company. It is also possible that for some organisations not all the merchandise hierarchy levels exists.

2.3.2 Foundation Data – Organizational Hierarchy [8]

Organizational Hierarchy gives the complete structural hierarchy from business perspective. It is the structure that enhances retailers ability to target selling outlets.

Following are the levels of Organizational Hierarchy :

- Company : It is the highest merchandise and organizational entity defined in RMS. Only one company can be defined.
- Chain : The next level after the company level in the organizational hierarchy. The definition of a chain is based on the needs of the company, but a chain can be used to group various store formats, concepts, and geographical locations within the organization.
- Area : The next level after the company level in the organizational hierarchy. The definition of an area is based on the needs of the company, but an area is used typically to define a geographical group within the organization. An area can belong to only one chain.
- Region : The next level after the company level in the organizational hierarchy. The definition of a region is based on the needs of the company, but a region can be used to group geographical locations within the organization. A region can belong to only one area.
- District : The next level after the company level in the organizational hierarchy. The definition of a district is based on the needs of the company,

but a district is used typically to group geographical locations within the organization. A district can belong to only one region.

- Channel : A channel is different modes to sell the items i.e. Internet, Bricks and Mortar, Telephone, Catalogues etc. We can assign channel to locations while creating virtual warehouse or store.

2.3.3 Item Maintenance [8]

This module is used for item creation and maintenance. Submission and approval of items also included in this.

Following are the operations in Item Maintenance module :

- Set Up Diffs : RMS allows you to create items with different differentiators. Differentiators are the attributes of item that define the item uniquely. Differentiators are used to differentiate the items based on different attributes like size, colour etc. Diffs are used to distinguish items by their characteristics.
- Create Items : RMS allows you to create six different kind of items like – Regular, Pack Items, Deposit Items, Consignment/Concession, Catch weight and Transformable. RMS also allows you to create child items for the items having transaction level greater than one. Along with the item attributes it is mandatory to give the supplier and supplier country details for that item. Vat and taxes are also calculated on the basis of the department chosen. It will also calculate unit retail for that item (per EA). Calculations are being performed by Oracle Retail Sales Audit System.
- Submit/Approval : Initially when item is created it is in worksheet status. When all the details filled are correct then only item can be submitted for further approval. Before placing order against an item it need to be in approved status.
- Reclassify Items : This is the process of moving an item or item list from one department or class or subclass to the another.

2.3.4 Purchase Orders [8]

Orders can be placed for approved items. Key elements for purchase orders are Supplier, Delivery Date, Items, Cost, Quantities and Locations. There are various constraints while placing the orders like there may be a supplier who has set a minimum quantity as a constraint. Then in that case retailer has to order according to

that quantity. In case of failing satisfying the constraints will also fail the order creation process. There are various types in which orders can be created.

- Manual Creation : New Order can be generated or Order from an Existing PO can be created.
- Automated : Automated orders can be created through Store Orders, Replenishment or Contracts.
- Vendor Managed Inventory (VMI) : Order is created via supplier.

Bracket costing, Deals, Scaling and Truck Splitting are the constraints that can be applied on the orders.

2.3.5 Deals [8]

Deals are a set of discounts and/or rebates negotiated with a supplier that share a common start and end date. A deal provides the means by which retailers can manage reductions in the supplier's purchase order cost of an item. Following type of deals are available in RMS. Deal contains Supplier or Deal Partner, Status, Active and Close Date etc. A deal partner, such as a manufacturer, distributor or wholesaler, that gives rebates to the retailer. Deals can be Annual, Promotional or PO-specific. In Annual deal no end date is required. It can be closed manually by user or automatically upon creation of a new annual deal for the supplier. Promotional deal is automatically closed on specific end date. In PO-specific deal start date is set to the orders not-before-date. No end date is required.

Deals can be created and edited in worksheet status. Once entered a deal must be submitted and approved via batch before it becomes active. Deals can be manually closed or deactivated. Deals can be purged after specified number of days (system option). The Recalculate orders indicator, if checked, will recalculate any approved, non-received orders that fall within the deal dates according to the new deal discounts. Deals are applied online by clicking the Apply Process button in the Purchase Order dialog. Then check the Apply Deals box in the Recalculation Options form. Deals will be applied in the nightly batch regardless if the user has hit the Apply button in the Ordering dialog. The discount can be applied when the PO is approved or when the PO is received.

2.3.6 Replenishment [8]

Replenishment is the process of automated ordering of items. It monitors retailers inventory conditions at item/location level. As reorder points are met, RMS replenishment generates orders or recommended order quantities to meet need.

The Retail Merchandising System Replenishment module helps reduce manual processes and increase efficiency by providing :

- Automation of recommended order quantity calculations
- Automation of ordering process from supplier to stores and warehouses
- Automation of transfer process from warehouses to stores

Purchase order generated through replenishment which can be to warehouse, direct to store. There are various Replenishment Methods to calculate the ROQ. Three of these methods don't use forecasts as part of their algorithm.

- Constant : It is the simplest method. In this method inventory is ordered when the user falls below the user defined "maximum". It will only consider the maximum defined by user and if the stock count is less than that it will automatically places the order.
- Min/Max : In this method the user will define the minimum and maximum stock . When the stock count is less than the minimum then it will place the order and fills to the maximum.
- Floating Point : It uses same principle as that of Min/Max. In Min/Max user gives a maximum number which will act as the maximum stock count , but in this the maximum will be calculated on the basis of the sales history(store) and issue history(warehouse). It needs 15 months of sales history for proper need calculations.
- Dynamic : This is the most complex replenishment method. It minimizes stock on hand, whilst preventing stock outs. It replenishes only quantity required between each replenishment cycle. It considers forecasted demand, review and lead times, and available inventory in calculation. Dynamic replenishment also considers the following attributes when calculating ROQ:
    - Service level: Determines the level of safety stock that is desired.
    - Inventory selling days: Desired inventory turn objectives.
    - Lost sales factor: Allows any lost sales in the last replenishment period to be factored into the next replenishment period.

2.3.7 Contracts [8]

In Oracle Retail, a contract is a binding agreement with a supplier to purchase a volume of items at a particular cost price over time. It improves supplier relationships by helping suppliers to plan their production in advance. It provides retailers with early margin figures and eliminates risk. The balance of the contract is decreased when an order is written against it, enabling commitment tracking. Stock is sourced from the best contract by replenishment according to predefined logic. Contract Orders are visible from PO and/or Contracts dialog. Item cost is defined on the contract at item/supplier level. Bracket costing, Deals, Scaling and Truck Splitting do not apply on contracts.

2.3.8 System Administration [8]

This module of RMS has all the system options. There are various system options that need to be enabled/disabled according to the situation. For example : There may be a case where a department level order need to be placed. In that case the department level indicator need to ne enabled in the System Administration. These setting are only available for Administration and the link will be hidden for all other users.

2.3.9 ORAAC – Oracle Retail Application Administration Console [9]

ORAAC is the security feature of the Retail Merchandising System. RAAC include the roles, duties and privacy policies that are applied on the RMS. This feature is only available for RMS administration. All the role based testing is done by taken into consideration the duties and roles being defined in RAAC. Admin can add/edit/delete any role and privileges for any user. RAAC also contains the documents related to RMS usage.

2.3.10 Cost and Price Management [8]

This module of RMS helps the retailer to change the cost as well as the price of an item. This can be used in case of sudden discounts like in fashion industry when a season ends then clothes are sold at less price. Cost Change button is also provided in the item search results as the same function can be used from there. The new cost/price will be effective only after a batch is run.

2.4 Unique Features of RMS [10]

1. Exception Based Retail : Persona-based dashboards provide the users with real-time information which highlights actionable or frequently monitored activities. The entire UI is focused on user behaviour, providing multiple methods to view, filter, and take action on items on their dashboard.
2. Eliminating Complexity : Oracle Retail Merchandising provides dashboards that highlight the work a user needs to focus on and the tools to resolve the issues direction from the dashboard as well as the way to go directly to the item requiring resolution. Contextual Business Intelligence(BI) provides the users additional information to aid in their decision making without having to search for the information.
3. Foundation Data Management : Oracle Retail Merchandising provides users with a complete application to manage the fundamental elements of their business such as organization and product hierarchies, locations, and suppliers. Items are classified within the merchandise hierarchy, which facilitates operational processing and reporting.
4. Enterprise Inventory : The Oracle Retail Merchandising System effectively handles the requirements of the fast-paced, multi-channel environment. New channels can be added as needed and the organizational hierarchy can be adjusted easily. Oracle Retail Merchandising provides real-time inventory visibility, the option to segregate inventory by channel and the ability to monitor all transactions, including sales, by channel.
5. Master Data Management : Oracle Retail Merchandising System is unique in that depending on the retailer's requirements; it can act as either the master or recipient for particular information. Orders can be created within the Merchandising System itself, be sent from an external system via standards-based web services, via integration with Assortment Planning or uploaded from a file.
6. Comprehensive Cost Tracking : Oracle Retail Merchandising manages supplier unit costs, bracket costs, and estimated landed costs. The solution automates the defaulting and calculation of estimated landed cost, which gives retailers a more objective basis for supplier cost evaluation and ensures more accurate inventory valuation in the purchasing cycle.

7. Multiple Replenishment Methods and Mass Maintenance : Replenishment of merchandise from suppliers or warehouses is achieved using either stock level methods or forecast driven methods. Mass maintenance assists with setup and size profiles are leveraged to populate stock value for fashion items. For grocery retailers, replenished quantities can be automatically divided between multiple suppliers and scaled to full truckloads.
8. Globalization : The Oracle Retail Merchandising System supports multi-currency, multiple legal entities, and multi-language in a single instance. In addition, the Merchandising System provides support for retailers who operate in multiple countries with multiple sets of financial books and centralized VAT processing provides additional flexibility.
9. Documented Business Processes and Implementation Tools : The key to unlocking the value of a merchandising system lies in a successful implementation. To help retailers and partners implement the solution as efficiently as possible in accordance with best practices, Oracle developed a robust set of implementation tools.
10. Complete, Seamless Integration : Retailers need world-class functionality and the ability to seamlessly interact across all areas of the organization. Oracle Retail Merchandising provides the platform for executing end-to-end retail processes.

2.5 Retail Sales Audit (ReSA)

Retail Sales Audit [11] is an Oracle application which describes the process of Point-of-Sale and check the accuracy of the order and other calculations. It ensures the integrity of audited data and provide smooth integration with other applications of retail. It balances the cash registers, store day totals etc. It is part of Merchandise Operations Management (MOM) Suite which help the retailer to reduce integration costs, improve internal control, increase productivity, and improve visibility to sales. Along with this it also manages foundation data, cost, inventory and financial processes.

2.5.1 Purpose and Benefits of ReSA [11]

ReSA takes input from Point-of-Sales and Order management System, process the input and provide the audited data to other applications like General Ledger

applications. It only allows single entry for sales data from external sources to maintain the integrity of the system. It validates the data by correcting the errors according to the rules which are pre-defined in it. These rules can be system defined and user defined. Users can view the audited data on various levels like store day level or cashier register level. It corrects the error in the data, which reduces the cost of integration with other applications.

2.5.2 ReSA Roles [11]

The user roles [11] provides a means of grouping privileges together for granting access to a user. The retailer can modify the roles to suit their business needs. The following are the default roles set up in ReSA :

- Auditor : A Sales Auditor is a person who is responsible for the daily reporting of sales, auditing and accuracy of the store sales. Ensuring deadlines are met, enclosing the store day register are also included in sales auditor responsibilities.
- Auditor Manager : Auditor Manager tasks is to manage the team to auditors. They act as the main point of contact for any query related to auditing. They also represent finance in meetings related to Point of Sales and sales.
- Finance Manager : Finance Manager's task is to maintain the financial accounting of a particular region.
- Administration : Maintaining administrative functions of the application is the major task of an admin. Employee maintenance, reference field maintenance are others responsibilities of an admin.

2.5.3 Integrating with Other Applications

SA can integrate with the following applications:

- Oracle Retail Management System (MS)
- Oracle Retail Invoice Matching (ReIM)
- Oracle Retail Point-Of-Service (ORPOS)

You can also set up SA to interface with third-party applications including general ledger applications.

2.5.4 ReSA Terminology

- Store Day : The time between the opening of the cash register at the start of business day and closing of register at the end of business day is defines as Store Day.
- Transactions : A transaction is a record of any event related to sales, return or exchange of items.
- Revisions : Revisions is the snapshots of the data. Before updating the data in the transaction table, a snapshot of that data is taken which is known as revisions. This process include following steps :
    1. Creating a new transaction record.
    2. Keeping the older version of record unchanged.
    3. Moving the older version data into revision tables.

Doing such will increase the efficiency as the records in the transaction tables decreases.

2.5.5 Totals definition

Totals can be defined as the total sales of a store at a particular store day. Totals are used to perform the store balancing, generate reports and export reports to the external systems. Totals can be defined in the system or can be imported as reported by POS or Order Management System.

2.5.6 Report Data

It allows you to generate various reports related to audit process like sales report, totals report etc.

2.6 ReSA Process [11]

2.6.1 Defining Totals

A total is a summation of two or more entities. For example a retailer can define totals as sum of all the sales at the end of a business day. There are two activities that plays role here :

- Creating Totals definition
- Managing totals definition

2.6.2 Defining Audit Rules

As a retailer you may want to validate the sales records with your own records. ReSA has a functionality where retailers can add their own audit rules which is known as

Rule Definition. On the basis of rules, two results are possible – Pass/Fail. In case of failure errors also need to be defined. ReSA allow retailer to define error related to the audit rules.

- Creating Audit rules
- Managing Audit rules

2.6.3 Auditing Transactional Data

At the end of the day, totals are calculated, reports are being generated and all of these are transmitted to the head office. Following are the errors that need to be viewed from the perspective of Sales Auditor.

- Error list
- Totals
- Missing transactions
- Import and export log

2.6.4 Exporting Data

Once the auditing process is complete the audited data is generated which can be send to various other systems. Exporting it means getting the data from ReSA database and write the data into the format accepted by the external system (in this case Retail Merchandising System).

Steps followed to export the data :

- Totals are first corrected i.e. any missing entry or sales is corrected in the totals.
- The audited data is written into the interface file. The format of the file depends on the integrated system.
- A batch is run which will extract the transactions with Passed, Non-Fatal and Delete status and put that data into staging tables. Staging tables are the temporary tables where validation of data is checked before the data is moved to actual tables. In the staging tables additional changes are done to validate the data then only it is transferred to other systems.
- Revision entries are created for the updated transactions
- After all revision entries are created, the reversed transactions are deleted from the transaction tables.

2.7 Web Services in RMS

Web Services [12] is a services provided by one application on an electronic device to another. It is a client server application which is used to communicate between two devices over network. Sometimes these are referred to as software system which provides the functionality of interoperability machine to machine communication. Web Services are the standards/protocols which need to be followed for information exchange between two devices over network.

There are many technologies that are used to create software. Communication among these application directly is not possible due to compatibility issues. Web services are the intermediate between these applications to communicate.

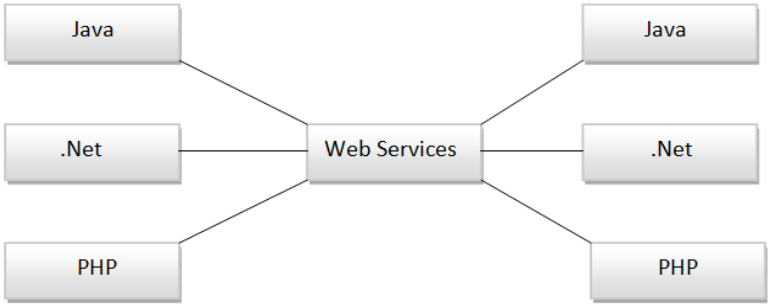


Figure 2.2 : Web Services

There are two types of web services :

- SOAP web services
- RESTful web services

2.7.1 SOAP Web Services

SOAP stands for Simple Object Access Protocol. It is a XML based protocol that can be used for accessing web services. As XML is a platform and language independent which concludes SOAP is also platform-language independent.

In SOAP based web services WSDL document is loaded. WSDL stands for Web Services Description Language , It is a XML based document in which all the operations that a web services can perform are defined. On loading this WSDL to a web testing application will create the ports for all the different functions described in it.

Advantages of SOAP Web Services :

- As SOAP is a protocol , it has its own set of rules that need to be followed for communication

- SOAP has its own security features known as WS-Security.
- It is platform and language independent so SOAP services can be written in any language and executed in any platform.

2.7.2 RESTful Web Services

REST stands for Representational State Transfer. It is an architecture not a protocol which means other than HTTP other protocols can also be implemented on this.

Advantages of RESTful Web Services [13].

- As it is an architecture so there is no restriction which makes it fast. It consumes less resources.
- RESTful web services are platform and language independent.
- Being an architecture RESTful web services can use SOAP web services as the implementation.
- It permits various data formats like Plain Text, HTML, JSON etc.

2.8 Software Security Assurance Testing

According to Functional and Security Testing Organization ZENQ which is a Hyderabad based organization , when a software is tested for vulnerabilities then the percentage that at least one serious vulnerability will appear in website is explained in the below Figure 2.3.

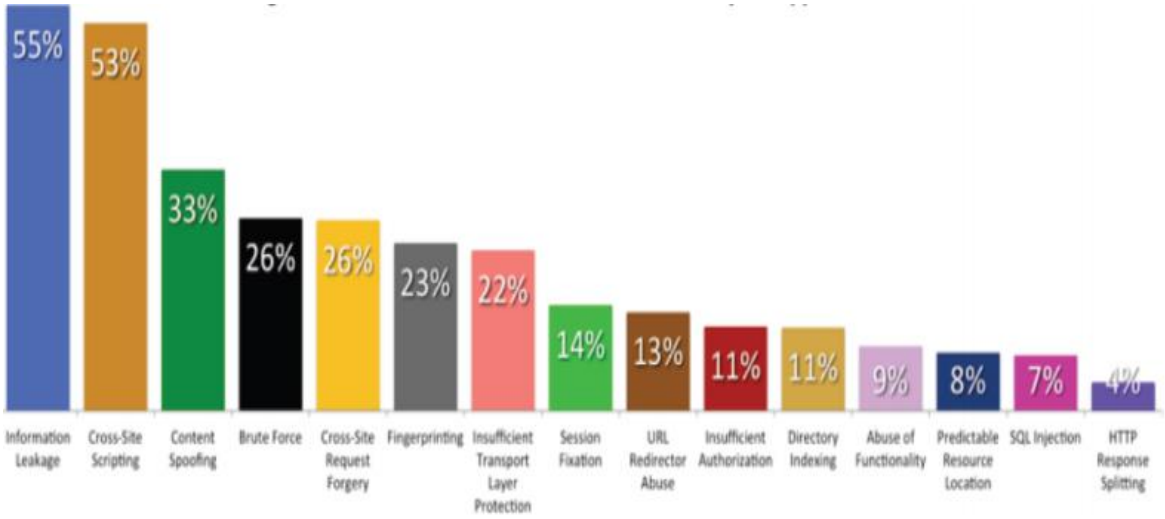


Figure 2.3 : ZENQ vulnerability assessment [14]

In general four basic requirements need to be addressed in every application for security assurance :

- Confidentiality

- Integrity
- Availability
- Non-Repudiation

It is important if security is taken into consideration from the initial call. When a client gives its requirement, then it is the task of organization to understand the requirements properly and explain client about the security process being followed. [14]

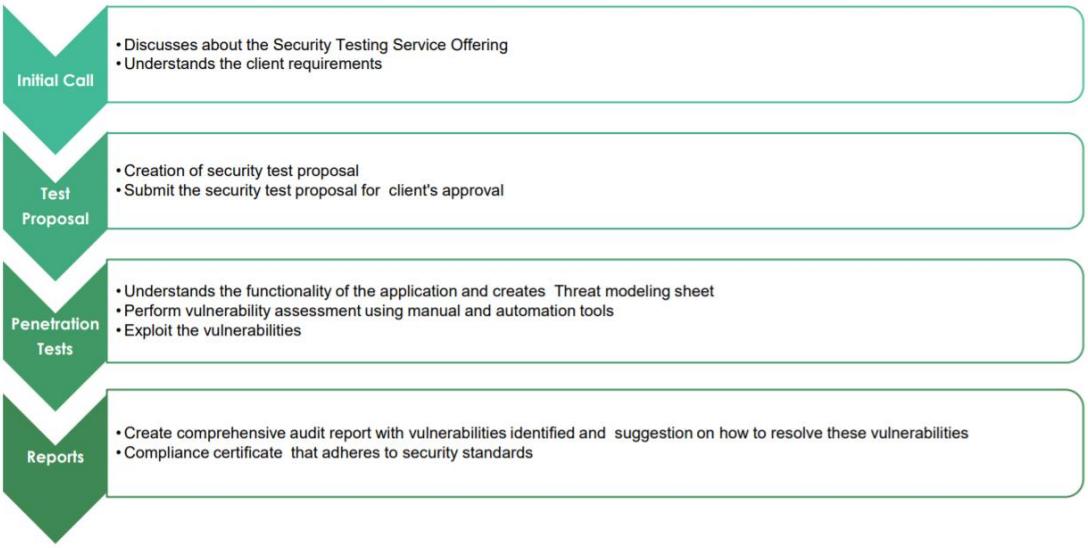


Figure 2.4 : Testing Process Flow by ZENQ [14]

Here creating the security proposal means explaining the whole security considerations for application. Various policies can also be implemented on the application to make it secure. Security policy means what could be securing for a system, organization or other entity[15]. Different security policies can be implemented at the software level. Mostly, these are traceable in the literature and reported practices, to one or more of the following :

- Authentication Policy
- Access Rights and Control Policy
- Confidentiality of Data
- Data Classification Procedures
- Non-repudiation

- Business Continuity Policy
- Virus Protection
- Event Log and Audit Trails
- Backup & Recovery
- Incident Management, Intrusion Detection and Forensic Analysis

2.8.1 Oracle Software Security Assurance

Oracle believe in "Security built in, not bolted on" [16] i.e. security vulnerabilities are checked at all the phases of software development life-cycle and not only at the end. Oracle's goal is to make the Oracle products as well the systems used by the customers for the products secure.

- Secure Development Standards

In this program of OSSA, design level security standards, secure coding standards and secure coding practices and trainings are included. It is believed that the maximum number of vulnerabilities and threats corresponding to each requirement can be taken care of right from requirements phase itself [17].

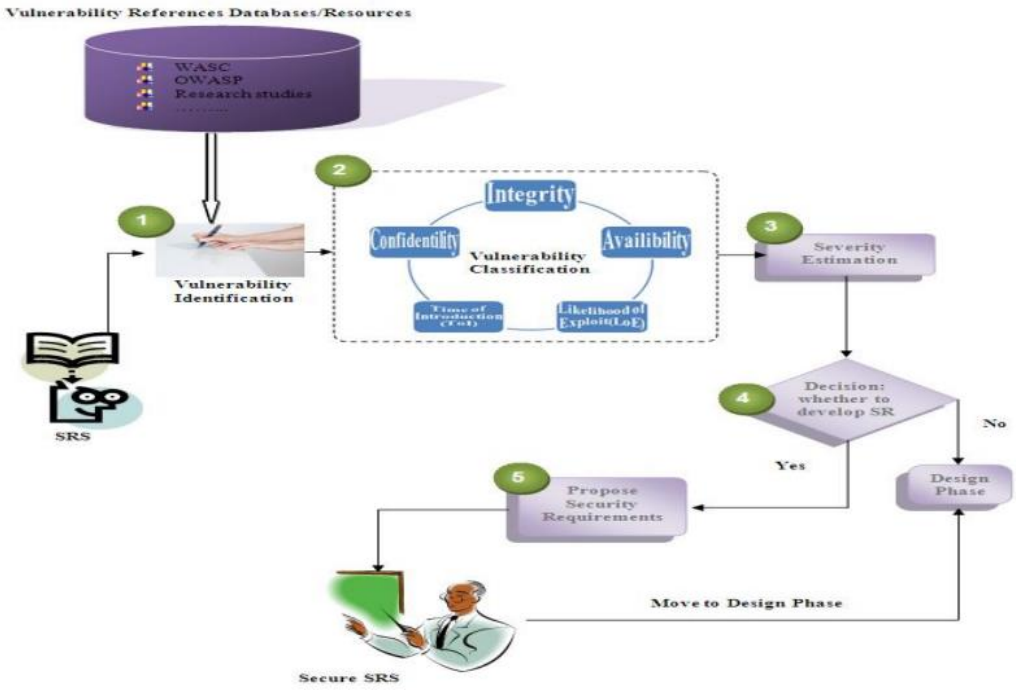


Figure 2.6 : Security at Requirement Phase

When SRS is prepared for a software then security should be considered. Figure 2.6 [18] shows the process can be used to eliminate vulnerabilities from the first phase itself.

Secure Coding Standards : A guide is provided for developers which explains all the secure coding standards that needs to be taken care while creating software. This guide is also referred by testers to ensure the secure coding standards. General security areas , design principles and common vulnerabilities are explained in this document [19]. Along with this it also includes topic like data validation and user management etc. Some of the secure coding standards are :

- Input Validation and Data Sanitization (IDS)
- Do not ignore returned value by methods.
- Validate method arguments
- Do not use obsolete classes and methods.
- Do not use finalizers etc.

Risk assessment summary is also given for each standard which includes the severity, likelihood, remediation cost and priority etc.

- Secure Design
- Security Tools and Testing

Comprehensive security analysis and testing is performed using in house and third party tools.

Comprehensive Security Analysis and Testing [19] **:** Security testing at Oracle includes both functional and non-functional activities for verification of product quality. It is the task of QA team to perform Functional Security Testing as a part of normal product testing cycle. In this QA engineer will check all the security consideration implemented in the application with the consideration given in FSD. Non-functional Security Testing verify the security assurance of Oracle products, including the remediation of security vulnerabilities and resistance to attacks. There are two categories in which this is done which are as follows :

Static Code Analysis : This type of testing is done during whole development life cycle of product. This type of testing is efficient in finding vulnerabilities like Buffer Overflow and memory leaks in C/C++ code and resource handling issue in J2EE , incorrect system configuration and improper user credentials etc.

Dynamic Code Analysis : Dynamic Analysis always takes place in the later phases of software development life cycle. This type of testing depends on specialized tools

(manual or automatic). Automatic tools employ fuzzy inputs to the application and study the behaviour of application in case of vulnerabilities, while manual tools needs hand modification but provide accuracy and precision.

- Security Compliance [1].
- Security Evaluations [1]
- Internal Security Assessments [1]
- External Security Assessments [1]
- Critical Patch Updates and Security Alerts

The requirements of OSSA after product development are assured by performing manual and automated testing. Various gaps were found while studying. Some of the gaps are like :

- RMS is shifted from 2 tier architecture to 3 tier architecture for cloud implementation, so web services implementation was needed to support micro services architecture.
- Security testing was done only with HP WebInspect tool. There were no security related test cases in Oracle Test Manager.
- Test cases and test data was not according to the new requirements.
- More focus was on testing with tools. For dynamic applications manual testing is must to find bugs.

Chapter 3

Problem Statement

Due to demand in the cloud services, Retail Merchandising System is shifted from 2 tier to 3 tier architecture. In 2 tier architecture there is direct link between logic and database. But in 3 tier architecture a middleware is in middle of logic and database, due to shifting from 2 tier to 3 tier , UI was the only way in which customers could interact with application. In case of urgency, customers were unable to use some features of RMS due to many restrictions in the modules from front end.
Also before releasing the product, thorough functional and security testing needs to be done. Performing testing manually is a very difficult task. Each and every combination needs to be tested for data validation and functionality checking.

In manual testing, testers and developers generates test cases, runs the system manually, try to find out defects in the system by comparing expected outcomes with the actual outcomes. Manual testing is better for the smaller size systems. Also cost is lower and it is more likely to find real user issues. But at the same time manual testing is repetitive and time consuming. Also manual testing requires skilled and experienced staff to cover all type of errors. Oracle RMS is a large application and needs a lot of man power to test the application. So to deal with all these kind of problems, automated testing is required.

As cloud is emerging with its plenty of advantages, clients are also moving towards the cloud solution. Oracle has its own cloud and many products of the Oracle are available on cloud. Oracle has also decided to move automation of RMS on the cloud. The on prem solution for the automation needs to query the database for retrieving the values. But on cloud, the database access will not be available. So the problem is to find out the solution through which we can ensure that our test script has successfully passed without querying the database.

With increase in technology, attacks also increases. Before the release of the application, it needs to be tested from functional as well as security aspects. Manually

testing it for security is difficult as many manipulated requests need to be send and behaviour of application need to be studied. So automated testing is necessary.

Chapter 4

Objectives

The main objectives are listed below :

- To implement client side RESTful web services.
- To perform functional and security testing of RMS and ReSA
- To perform functional and security testing of RMS Web Services

Chapter 5

Implementation of Client side RESTful web Services

To get information about various entities web services were needed. RESTful web services were developed for that. For testing those web services client side code was written in OpenScript. A switched case script was written which displays all the web services entities that can be queried. On selecting one of them will ask for the parameter/s . For example : Lets assume a customer want to know about a particular item, then first he has to select the item entity. Then he will be asked to pass the item number whose information he wants. On providing the parameter script will create an excel file containing all the information of that item.

5.1 Characteristics [12]

- RESTful web services are stateless
- The services use HTTP method explicitly
- The services are accessible through Uniform Resource Identifiers (URIs)

5.2 Relationship between HTTP verbs and SQL

HTTP methods like “GET” and “POST” are used by developers to describe the appropriate action like “CREATE”,”UPDATE” or “SELECT” etc.

Action	SQL	HTTP
Create	Insert	PUT
Read	Select	GET
Update	Update	POST
Delete	Delete	DELETE

- GET is used to retrieve data.
- POST is used to create a new resource.
- PUT is used to update the existing resource.
- DELTE is used for deleting the data or resource.

5.3 Usage of RESTful Web Services [21]

- The web services are completely stateless. A good test is to consider whether the interaction can survive a restart of the server.
- REST is used for limited profile devices like mobile devices.

5.4 REST request

A parameter is passed in URI in the case of GET operation. JSON data is received as response of GET request. In case of POST operation, JSON data is passed in the body of the request. In the response, success/failure response is received.

Figure 5.1 : GET request-response

5.5 API Flow

A request is send from the client which will have all the headers and the parameters necessary for the request. Errors are received if any of the request properties are missing.

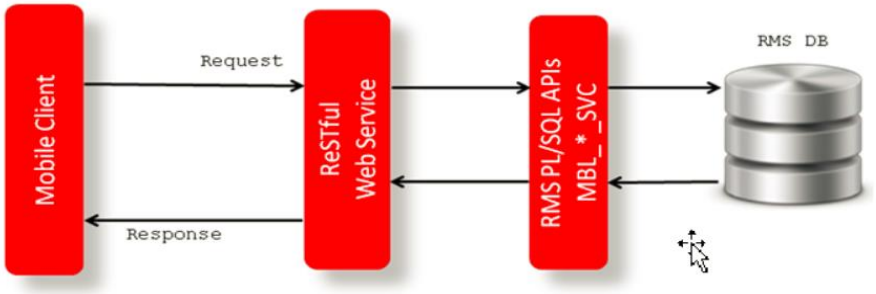


Figure 5.2 : API Flow

5.6 Process

A generalized script was prepared for all the entities. When the user will select the entity he is asked to give entity number as parameter , then according to the parameter final URI will be prepared.

Now this URI will be used in GET request of REST services. After sending the request, response will be send by the REST services which is in JSON format.

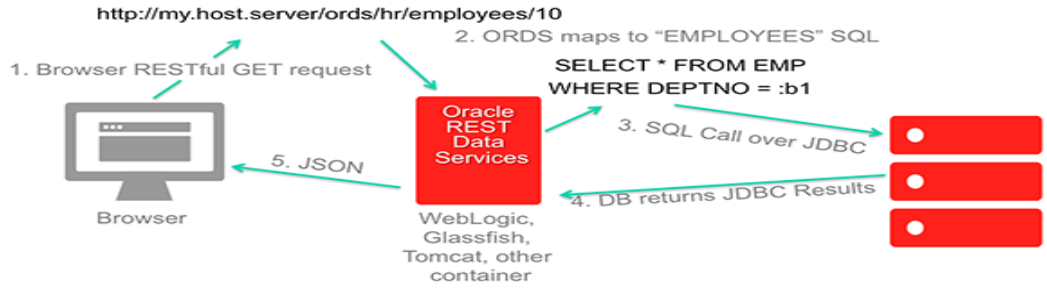


Figure 5.3 : Process flow of REST request [22]

5.6.1 JSON

JSON stands for JavaScript Object Notation. JSON is a syntax for storing and exchanging data. JSON is text, written with JavaScript object notation. When exchanging data between a browser and a server, the data can only be text. JSON is text, and we can convert any JavaScript object into JSON, and send JSON to the server. Sample of JSON received in the response in Screenshot 4.1 .

Screenshot 5.1 : JSON response

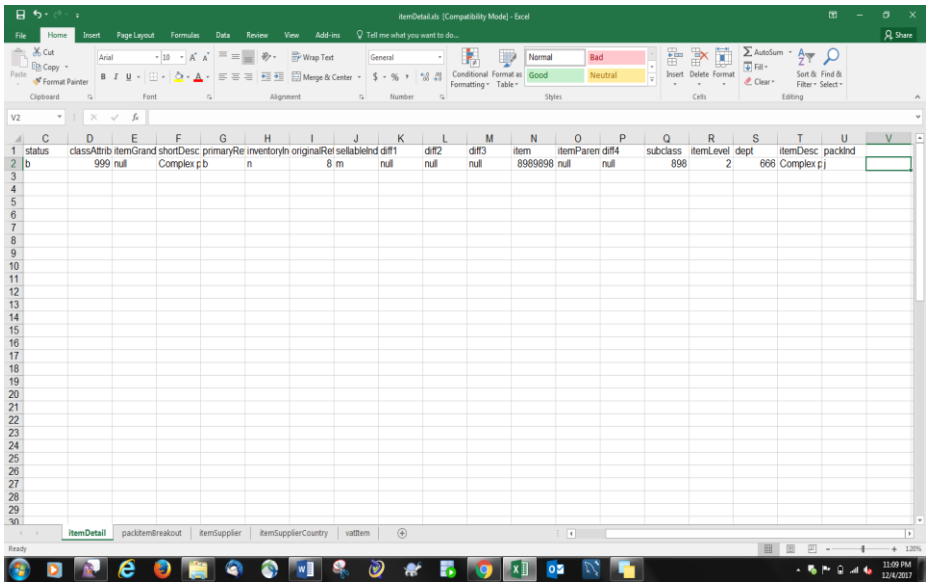
As user can not understand the JSON format so it need to be converted into readable format.

5.6.2 JSON to Excel

Conversion of JSON to Excel was done using ArrayList of HashMaps. HashMap is a Map based collection class that is used for storing Key & value pairs, it is denoted as HashMap<Key, Value> or HashMap<K, V>. This class makes no guarantees as to the order of the map. It is similar to the Hashtable class except that it is unsynchronized and permits nulls. The final excel sheet may or maynot contain multiple Excel worksheets depending upon the JSON response we got. If the JSON

response has metadata JSON then a new Excel sheet will be created within the main sheet and the metadata will be stored in that sheet and so on. In this way desired output is achieved.

Final Excel sheet may look like as shown in Screenshot 5.2 :



Screenshot 5.2 : Final Excel Sheet

In this way testing of Client side RESTful Web Services were performed.

Chapter 6

Functional and Software Security Assurance Testing of RMS and ReSA

Functional testing is the testing in which the tester tests the functionality of every module in the software individually and integrated to other modules. Functional testing includes unit testing, integration testing and regression testing etc. Whereas security testing is scanning the application for security vulnerabilities. Sending various manipulated requests to application and observing the behaviour of application is done in this.

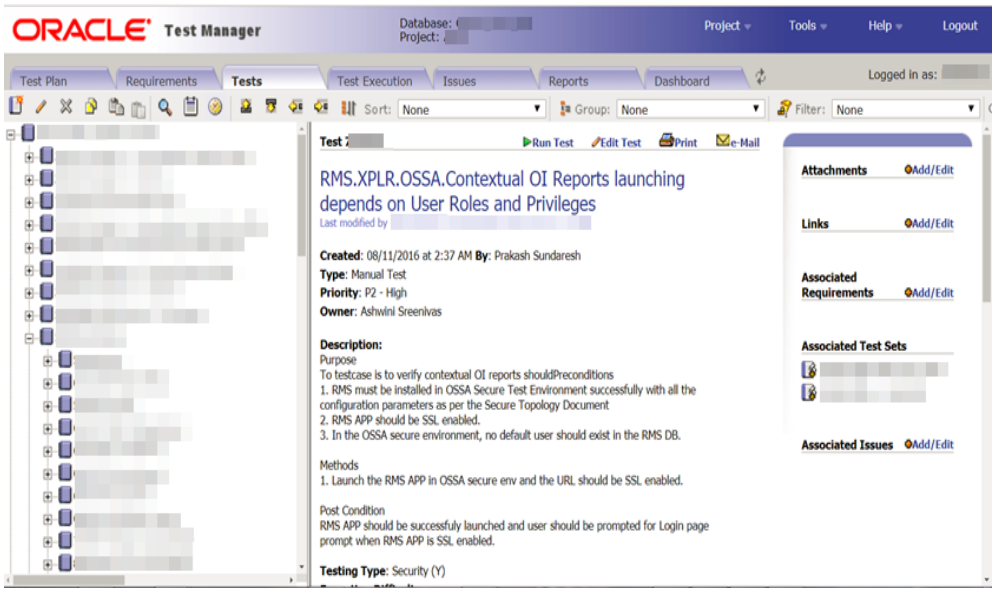
Testing is a process not a single activity. There are steps that need to be followed to complete it. Oracle has its own policies, steps and techniques that need to be followed for successful completion of the testing process.

6.1 Oracle Test Manager (OTM)

Oracle uses Oracle Test Manager [23] as a test process management solution for building the test cases. Due to its flexible nature and easy-to-use feature whole testing process can be created and managed on it. It provide integrated platform to manage the planning of test cases, steps, activities and the reports generated from those tests. Oracle Test Manager is a complete solution for testing web based and service oriented applications.

6.1.1 Benefits of OTM

- Its structured approach reduces test cycle time.
- It provides efficient and simple way to schedule or run the test cases.
- Reusability of test cases is also provided by OTM.
- Supports all types of testing i.e. manual, automation .



Screenshot 6.1 : OTM

As shown in the screenshot, test cases were created after reading specifications from Functional Specification Document (FSD). FSD is a document which contain all the specifications, functionalities a software must perform. QA Engineers reads the documents and create folder structure in OTM. Each folder is dedicated to specific entity. Under a folder various test cases were created according to the need and functional requirement of the entity.

6.1.2 Test Cases in OTM

Test Cases in OTM has various attributes like :

- Title of the test case
- Purpose of the test case
- Creator, owner of the test case along with last updated by feature.
- Type of test case i.e. Manual test/Automated test
- Type of testing i.e. Functional/Security Testing
- Description
- Steps to recreate the test case
- Run the test case- it also has fail option inside it
- Edit the test case etc.

For manual testing simply the test cases were recreated and passed and failed according to the behaviour of the application.

6.2 OpenScript

Software testing is the crucial part of Software Development Life Cycle. Different kind of approaches have been introduced for testing the software in a way that all the requirements are being covered. Manual testing is necessary part of Software Development Life Cycle, which requires lots of manpower and also it is time consuming. After that, automation testing was introduced. Oracle uses OpenScript for automation. OpenScript is a great tool developed by Oracle to support automation of Oracle Application Testing Suite. It supports Oracle Forms, Application Development Framework, JD Edwards, and also Web applications. It has great in-built report generation functionality which can give step by step execution details. It is based on record and playback functionality. Developers can record actions and then can transform those actions into executable test scripts which can be reusable.

6.2.1 Features of OpenScript [24]

1. Record and Playback : Using Record and Playback User can record the browser activities in Firefox or IE. User's actions are recorded and transformed into executable scripts. After recording, user has option to playback. The same thing can be played again with playback button.
2. Integrated tools : Oracle Test Manager (OTM) can be used to manage the test scripts after generation of automation scripts based on script type like load testing, functional testing etc.
3. Flexible Execution : It shows particular execution result to the user. It shows error messages, warning messages, success messages etc.
4. Modular : OpenScript supports Oracle ADF applications, Web, Oracle Forms Applications, Siebel Applications and Web Services. It has support for Java APIs so it can support anything in which Java API is associated.

6.2.2 Automation using OpenScript

Test scripts were written in Open Scripts for Functional Automation Testing of RMS. Excel sheets were generated which will be taken as input by the test scripts. The automation flowchart has been shown in Figure 5.1

A – Picks the Datasheet key prefix to run.

B – Based on the Datasheet key prefix records with status record is

picked for execution.

C – Based on Action the respective function is called from Test Engine Library.

1 – If excepted or actual Databank from the batch file is set to Forms environment, respective functions are called form Forms library.

2 – If excepted or actual Databank from the batch file is set to ADF environment, respective functions are called form ADF library.

3 – If the Action is 'CREATE' and scenario is executed successfully in Forms and/or ADF value is stored.

3A – Created value will be updated in Datasheet file, under Generated Data Work-sheet.

4 – After successful execution data will be downloaded from Database.

5 – If execution is successful in Forms and ADF then validation is carried on.

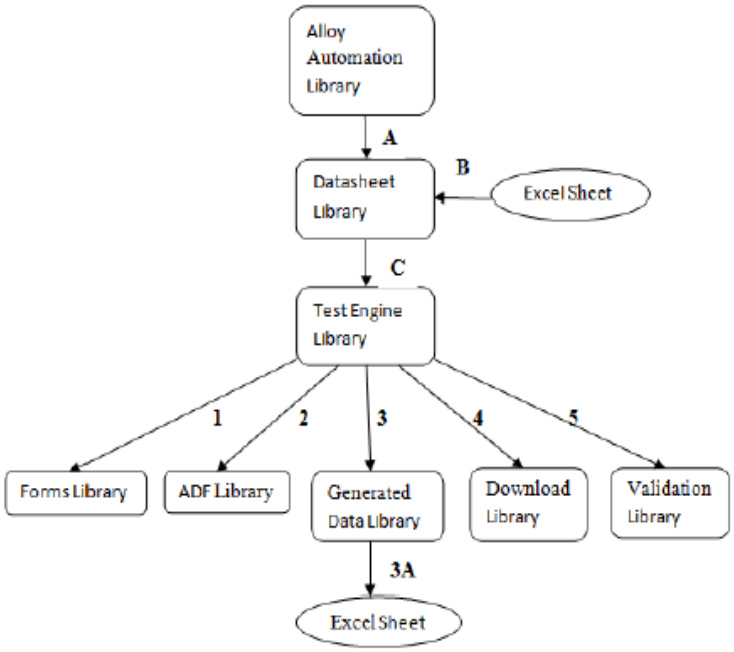
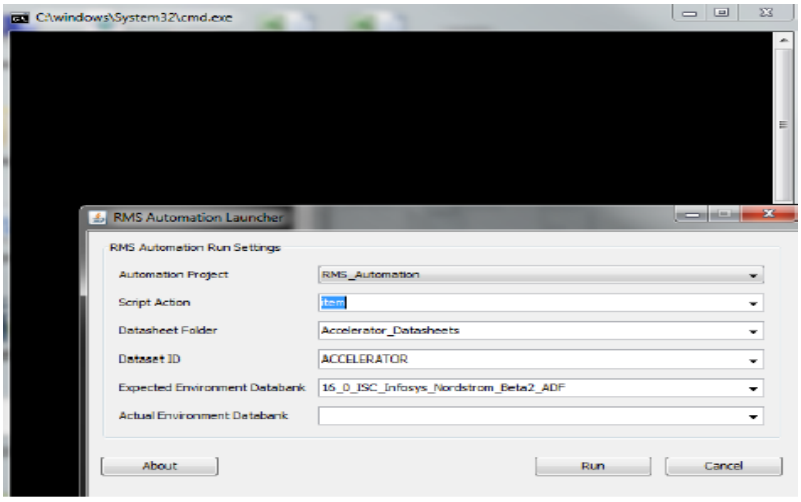


Figure 6.1 : Automation flowchart

6.2.3 Running the tests

To run and test the scripts locally, run the OpenScript -> RMS_Automation -> Batch -> RMS_Automation.bat file as Administrator.



Screenshot 6.2 : RMS Launcher

Automation Project: Different Projects that can be run through automation.

Script Action: Datasheet to run.

Datasheet Folder: Folder from which the data should be fetched.

Dataset ID: Specifies the records that are to be created from the given datasheet.

Expected or Actual Environment Databank: The environment in which the records should be created.

After entering all the required data, click “Run” to start the execution. Now the script will fetch the item datasheet from the path specified.

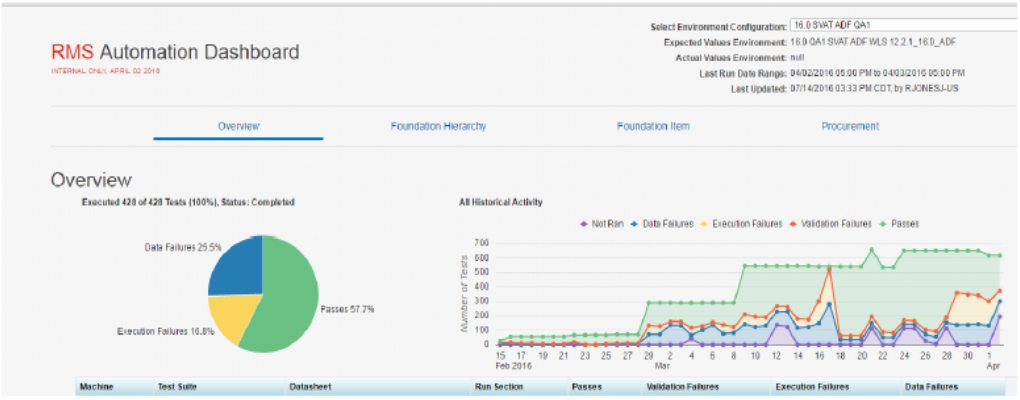
In the parent sheet all the records with the Dataset as “ACCELERATOR” and Status as “Always” will be created.

6.2.4 Result Validation

OpenScript gives users the privilege to generate the reports for whatever they are developing or testing. It gives the pass and failure count for the tests with detailed description.

Datasheet	Passes	Validation Failures	Execution Failures	Data Failures	Total	Run Time	Results Link
Organization Hierarchy	7	0	0	0	7	00:15:17	Organization Hierarchy Test Results
Store	3	0	0	0	3	00:18:16	Store Test Results
Warehouse	2	0	0	0	2	00:24:20	Warehouse Test Results

Figure 4.6: Result Report



Screenshot 6.3 : Automation Result Report

6.2.5 Analysis

OpenScript is very useful platform for testing the applications. The user will have to run the batch file to trigger the automation. Input data can be inserted through the excel sheets.

6.2.6 Advantages

- Robust architecture.
- Supports simultaneous execution.
- Supports all browsers.
- Detailed test execution report. Shows particular failure point so resolving the error becomes easy.

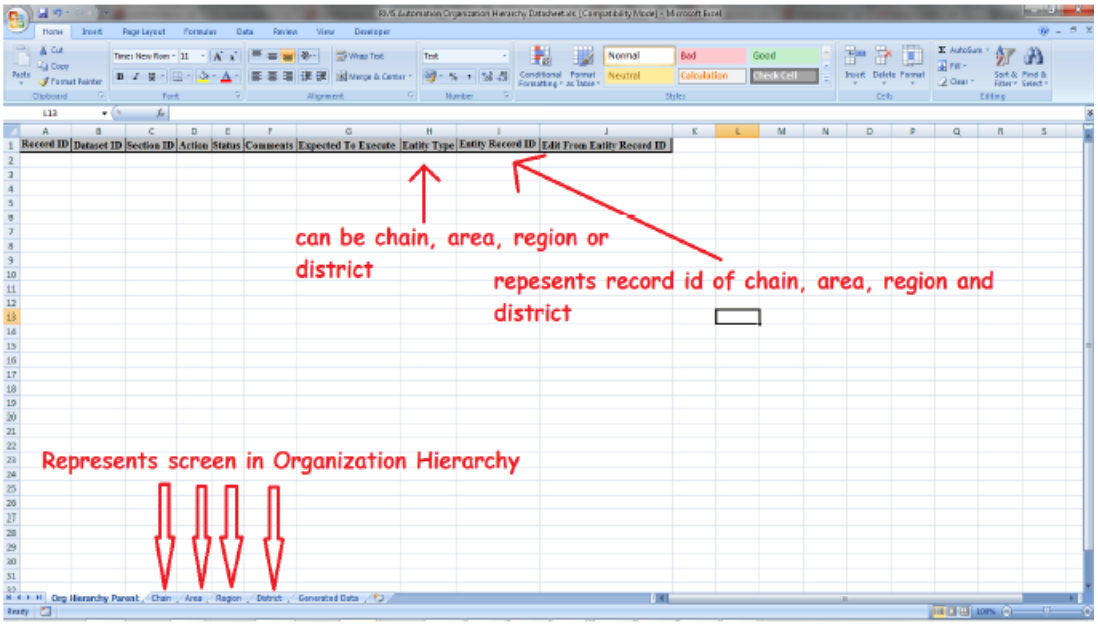
6.2.7 Customized Datasheet Creation

The framework which is currently being used by Oracle for automation testing requires lots of manual efforts for creation of datasheets. The purpose of this task is to reduce the manual effort and make the automation testing completely automated.

The purpose of automation testing is to test the software automatically to check whether all the requirements for the system are being met. The obvious advantages of the automation testing is that it is faster than manual testing, it requires less human resources and it is less prone to the human errors. The current framework which is being used by Oracle for the automation testing is taking input from excel sheets and

test the system with that data. These input spreadsheets are the test cases defined for the software. These test cases are written in a particular format in which the scripts written for the automation will take them as an input data to the software and fill them in the system. After completion of testing, the automation report will be generated with number of passed and failed test cases. Based upon the generated report, one can figure out the bugs in the system which are the cause of failures.

The current framework is doing extremely fine with taking input data from excel datasheets, filling them in the system and testing the system. But here the major part is creating the datasheets with all the required test cases. Now the testers are generating the test cases and writing them into the datasheets. But as we know, the humans are more prone to the error and also there are chances of mistakes while creating datasheets which cause problem in the testing going forward and will lead to the non-existing bugs. Also, the customers are not aware of how to fill the datasheets. And filling large amount of data is tricky part. Therefore, to avoid these problems, "Customized Datasheet Creation" was introduced. As per this project, the datasheets will be created automatically without any human intervention. The idea is to fetch data from database which already exists and convert them into the existing required datasheet format. Thus, the datasheets will be automatically created and can be uploaded directly to the system. This saves time and also it is very user friendly.

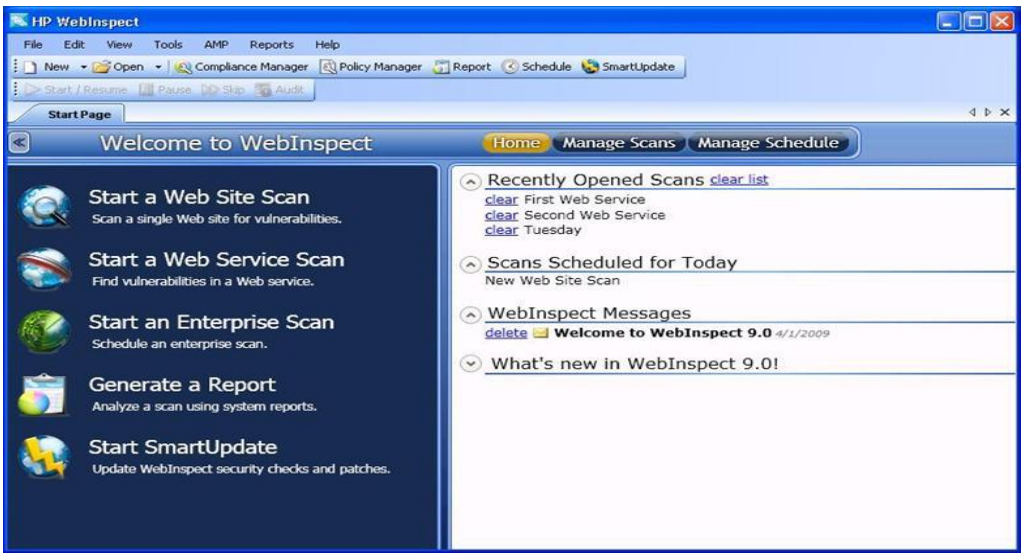


Screenshot 6.4 : Customized Excel Sheet Format

After automation testing , next step is to perform automation and security testing using WebInspect tool.

6.3 WebInspect tool

WebInspect [25] is a professional tool by HP which is mainly used for security testing of dynamic applications. It is used for testing application and web services also. There are options to which gives user to configure scan according to the need. It also provide the network authentication option if scan is to be performed outside from organization network. It also gives a facility to record the authentication macro and reuse that for future use. Enabling traffic analyser will give user a facility to keep the track of the network traffic. Scan/Scan details both can be imported/exported. It send various attacks to the application to ensure the security of the application. In the end a report is generated which will include all the vulnerabilities found in the application. It depends on the user if he/she wants to create the report for attacks sent (request with responses).



Screenshot 6.5 : WebInspect Web Site scan

Along with this logs and errors can also be exported in WebInspect which helps in the case of investigation when the vulnerabilities are found.

6.3.1 Advantages [25]

- Saves time when large enterprise application is scanned with it.
- Shows results with requests and responses.
- Facility of download various kinds of reports.

- Language independent.

6.3.2 Disadvantages [25]

- Tools are designed to test in a specific way and in a specific structure. Due to this it is possible many vulnerabilities are not figured by WebInspect.
- It has a list of payloads that it uses for every web application testing. It doesn't consider the type of application and requests.
- There could be false positive in the list of vulnerabilities found by it as it uses generic approach for testing.

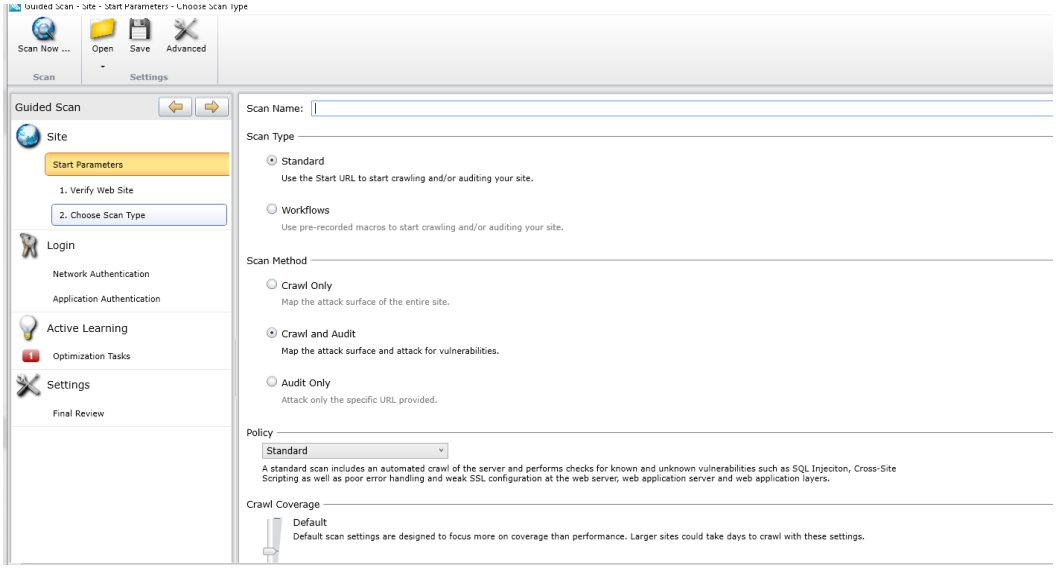
6.3.3 Feature of WebInspect [25]

- Tree Structure : It uses crawl and audit procedure. Thus presents you with hierarchical structure of the application.
- Customized view : It gives you a customized view to view the results in a sorted form. For example : First all high vulnerabilities will be shown then medium and so on.
- Scanning Policies : It gives you option to edit and customize the scanning policies.
- Manual Attack Control : With this option you can actually simulate a true attack and see what is happens with the application.
- Report Generation : A customized report can be generated according to the need of user.
- Remediation : Along with the vulnerability report, it gives the fix that can be implemented to fix that vulnerability.
- Web Services Scan : It also gives you an option to scan web services.

6.3.4 WebInspect Standard/Workflows Scan

When WebInspect is started , a start screen is displayed in which you can select the type of scan you want to perform like application scan/web services scan. Select the application scan for application testing. Next screen will be displayed. In that screen you then have to select the type of testing you wish to perform.

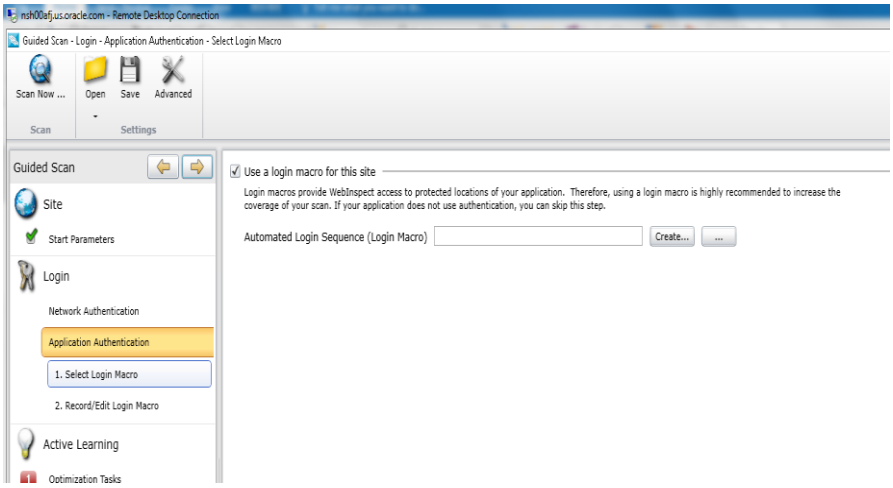
- Standard Scan
- Workflows



Screenshot 6.6 : Standard/Workflows Scan

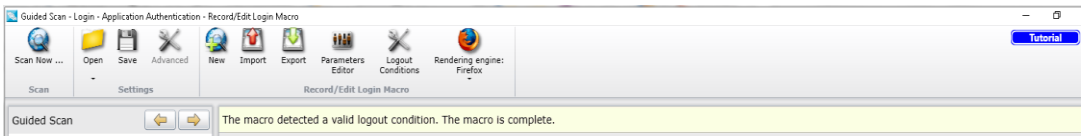
In Standard scan you can scan the full application. WebInspect uses crawl and audit technique to scan the whole application where as in workflows a specific workflow is configured for scan. This is used when small functionality is changed in the application. In that case whole scan I not needed thus this functionality is used.

After selection of scan type and method, Login to application need to be done. For this a login macro can be recorded and exported for future use or already created login macro can be reused by importing it.



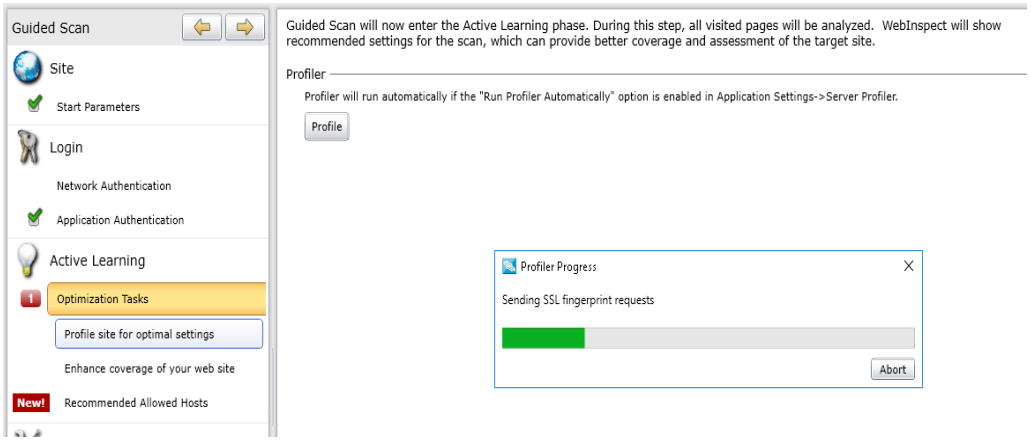
Screenshot 6.7 : Login Macro WebInspect

The following screen displays the import export options and also logout options detection in WebInspect.



Screenshot 6.8 : Import/Export Login Macro

After the scan is configured, WebInspect will check the profile of application, enable SSL connections etc.

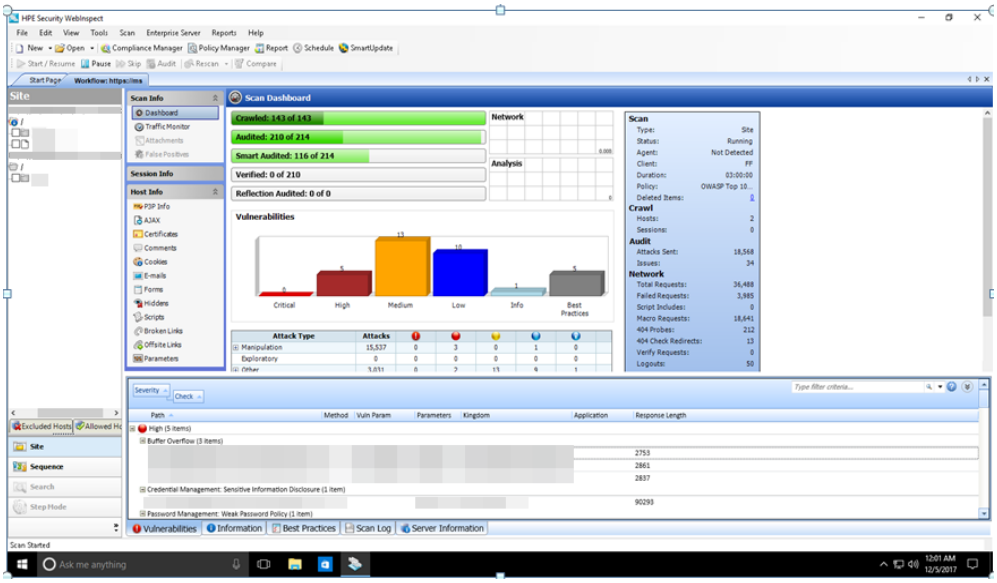


Screenshot 6.9 : Profile Progress

You can enable HTTP traffic and also you can use the false positives from previous scan. While scanning you will see the screen shown in Screenshot 5.10.

The screen has three panes :

- Navigation Pane : The navigation pane have 4 views.
    1. Site view : This view shows the hierarchical view of the site and also highlights the section in which vulnerability is found.
    2. Sequence View : Shows the sequence in which WebInspect traversed the hierarchical structure.
    3. Search View : Helps to search HTTP components like all sessions or cookies.
    4. Step View : It shows all the steps and URLs scanned by WebInspect.



Screenshot 6.10 : WebInspect Panes

- Information Pane : This pane contains the scan info. It has all the links related to scan information.
    - ➢ Dashboard : It gives the comprehensive view of the scan. It displays the vulnerability type, HTTP request, HTTP response etc.
- Summary Pane : It is at the below of window. This pane will display the results of the scan. Vulnerabilities will be displayed in this pane. Selecting the vulnerability will show the description of the vulnerability.

6.3.5 Reporting

After scan completion reports can be generated from Reports->Generate Report.

After the reports are generated an excel sheet is created by the use of the generated reports. In that report vulnerability number, its description , type of vulnerability and fix is given for the developer to solve the vulnerability. The same process is performed for ReSA.

6.4 SQLSplat

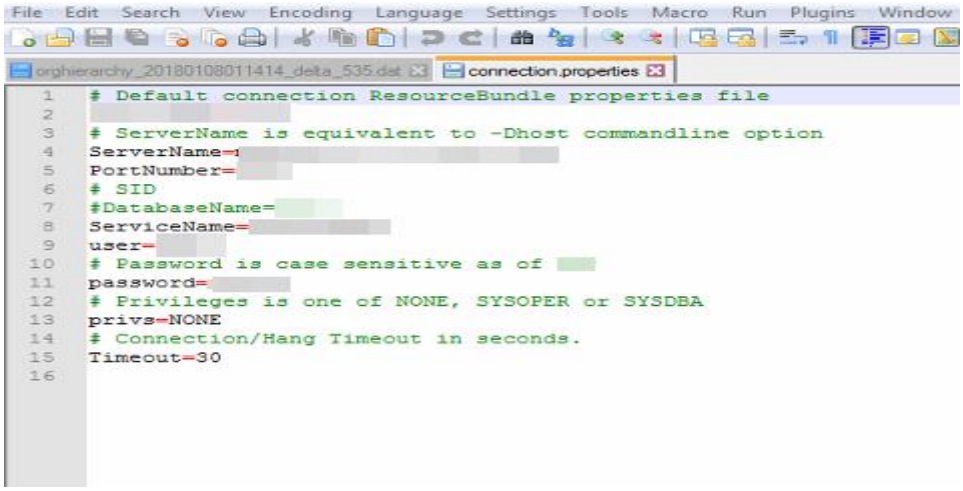
After WebInspect scan the code based functionality testing is complete. But database also need to be scanned against all the SQL vulnerabilities which is a part of OSSA testing. This is performed with Oracle SQLSPLAT tool.

SQLSplat is a fuzzer used to test PL/SQL stored procedures and functions. It's purpose is to uncover Denial of Service, elevation of privilege, and SQL Injection vulnerabilities within an application.

If a PL/SQL script was created, then the tester must use a tool such as SQL Developer or SQLPlus to run the script against the database. The person executing SQLSplat is then responsible to evaluate the output of the fuzzing operations.
SQLSplat is a command-line application. In general it works by :

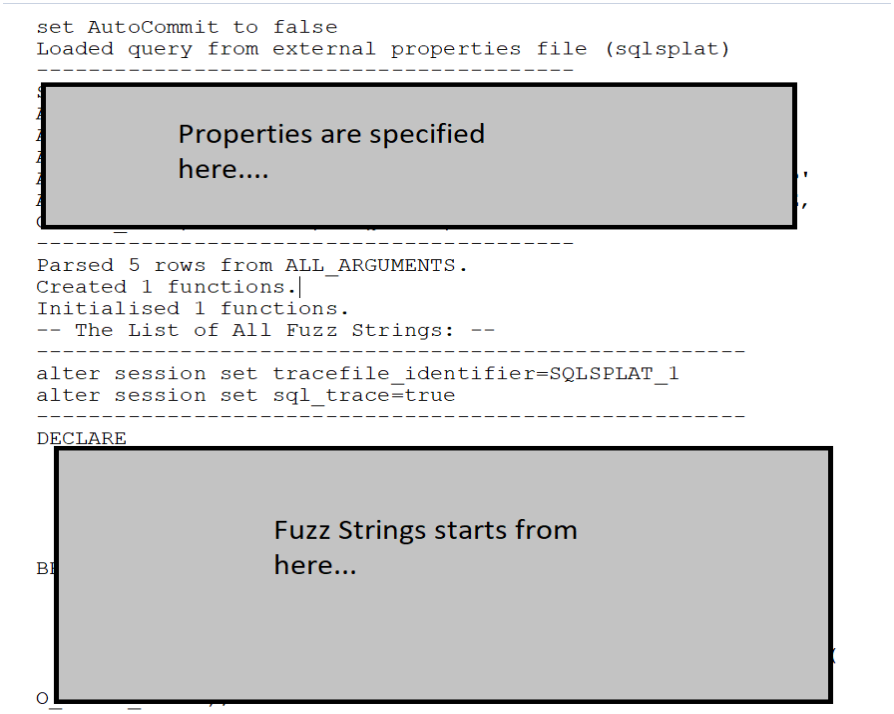
- Reading configuration files and command line arguments to determine what values to use during the fuzzing operation, the stored procedures/functions to fuzz and other tweaks to its behaviour. While a general purpose set of values is provided, some effort should be made to include known good values in order to execute as much targeted code as possible.
- Establishing a connection to the database.
- Querying tables to obtain the signatures of the target PL/SQL stored procedures and functions.
- Either

a) Based on the information obtained during steps 1 and 3, creating an executable PL/SQLScript that can be executed later. This script will contain lots (hundreds or possibly thousands) of calls to the targeted stored procedures or functions, each one using a different value based on parameter type and the configuration files.
b) Dynamically calling the targeted stored procedures or functions using the same values as in 4a. Note: SQLSplat may commit or roll back after each call, depending on the configuration used. Following figure shows the connection file of SQLSplat.



Screenshot 6.11 : Connection file SQLSplat

A copy of the actual database schema is created and SQLSPLAT query is fired on newly created database. After the successful execution of the query an output file is created automatically which includes all the request and responses, sessions , arguments and variables passed etc. It is task of QA to verify the file and create another file based on the output file which includes the vulnerabilities with description. This file will be used to verify the bugs and fixation of bugs also.



Screenshot 6.12 : Output.txt file SQLSPLAT

6.4.1 Advantages of SQLSplat

- Simplicity of use
- Point and fire at any Oracle DB version

- Simple configuration of argument inputs
- Ca test everything or focus on specific package procedure or function

6.4.2 Disadvantages of SQLSplat

- No support for dynamic generation of fuzz strings
- Large amount of logging output

SQLSplat is a wonderful tool for finding vulnerabilities in database.

Chapter 7

Functional and Software Security Assurance Testing of RMS Web Services

After shifting from 2 tier to 3 tier architecture, UI was the only way using which customers could interact with application. In case of urgency, customers were unable to use some features of RMS due to many restrictions in the modules from front end. For example customer wants to create an order for a specific date but RMS doesn't allow to create orders after v-date. In that case web services is the only solution that could help a customer. Due to this reason web services were implemented. Before releasing the web services, functional and OSSA testing is mandatory.

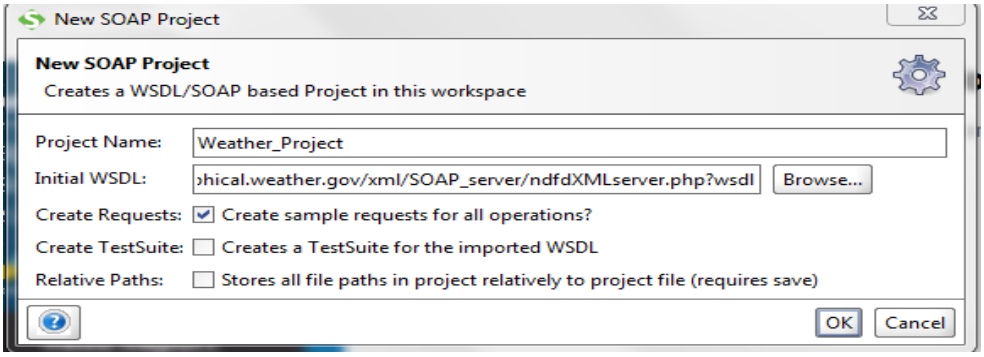
Oracle use various tools to perform such testing. Below are the tools I used for web services testing.

7.1 SoapUI

SoapUI is a tool used for Web Services testing. Web Services can be RESTful or HTTP based services. It is completely free tool which can be used to perform Functional Testing, Performance Testing, Interoperability Testing, Regression Testing and much more. Test cases can be recorded for later use. It is java based application so it can run on any operating system. Security test cases can also be implemented in it. Security tests can be implemented on the existing test cases.

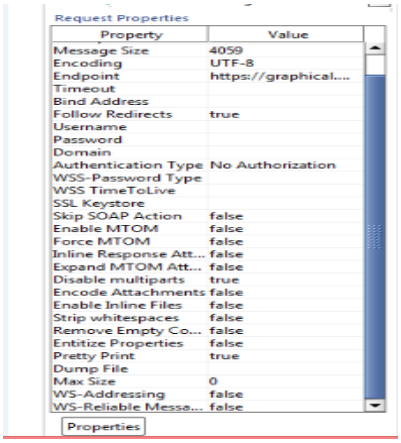
7.1.1 SOAP web services testing using SoapUI

For SOAP web services testing first select SOAP from File menu. Give the name of project and the WSDL for the SOAP request.



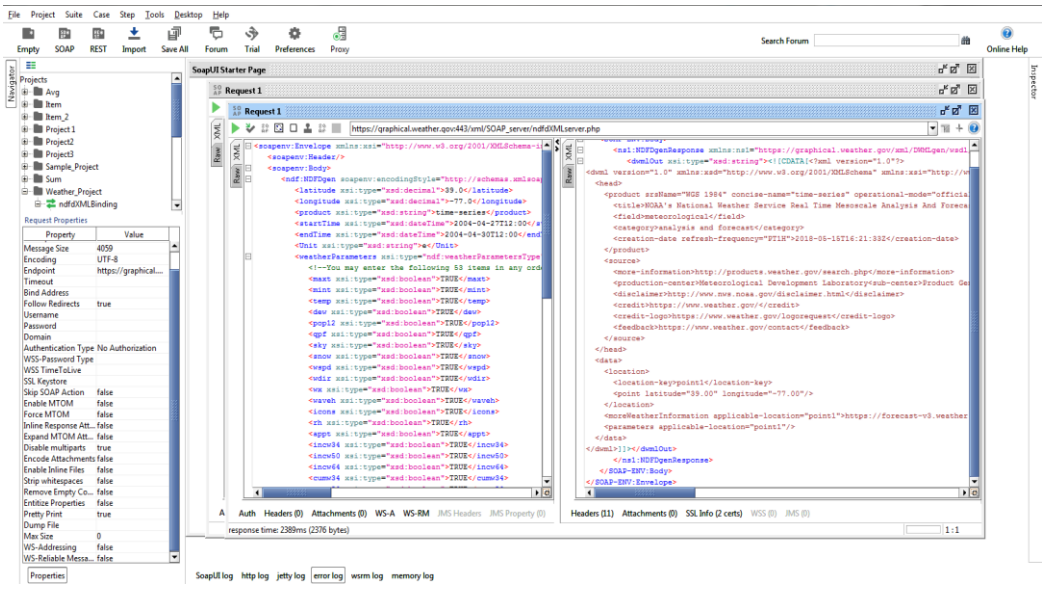
Screenshot 7.1 : SOAP project

A WSDL is a web services description language. It is an XML document in which all the functions related to an entity are defined. When ok is clicked a SOAP project will be created and WSDL will be loaded which will create all the ports (functions). Expanding the port will display the request. Selecting the request will display the request properties.



Screenshot 7.2 : SOAP Request Properties

You can set the username/password and other properties of request in the request properties window. On double clicking the request, an xml request will be displayed in the request window. To create the request replace the '?' with correct arguments. To send the request click on small green button present at the left of request pane. A response will be received which can be success or failure message.



Screenshot 7.3 : SOAP request/response

For functional testing various combination of data are passed as arguments and request is send. The responses received are studied for the behaviour of web services. For security testing request properties are changed. Incorrect username/password are send with SOAP request. In case of incorrect request properties , failure should be received as response. Role based testing was also performed i.e. user credential of the user who doesn't have privilege to access the entity were send in SOAP request and responses were studied.

7.1.2 Advantages

- It automatically updates the requests and response when WSDL changes.
- It has a user-friendly UI
- It has its own security features.

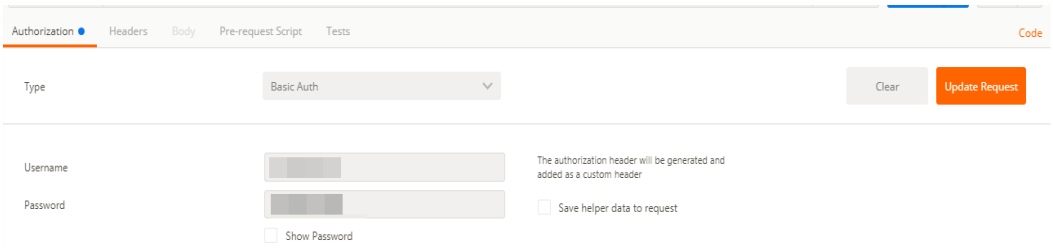
7.1.3 Disadvantages

- Having assertion on JSON response is not easy. It gives issues if request contains special characters.
- Creating scripts with SOAP requires lot of steps.

7.2 Postman

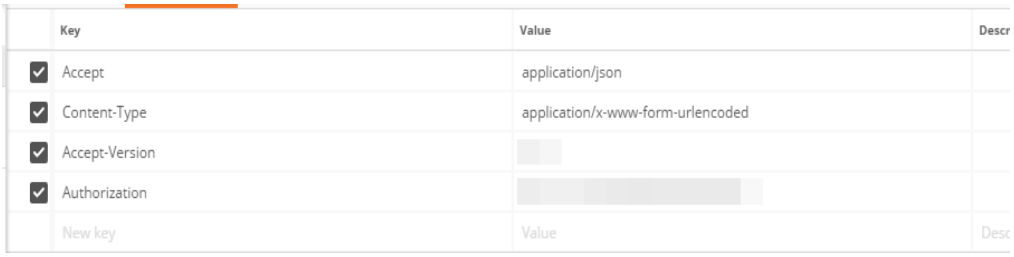
Postman is a Chrome extension and application which is use to send RESTful requests. It is a very light weight and fast application. Groups can be created for similar requests and also test can be created for verification of response received. It supports various HTTP methods – GET, POST, UPDATE, DELETE etc.

One can add authentication to the request if the application requires authentication before displaying information requested. In web services testing authentication was added. It will be added to header section of request when update request is clicked.



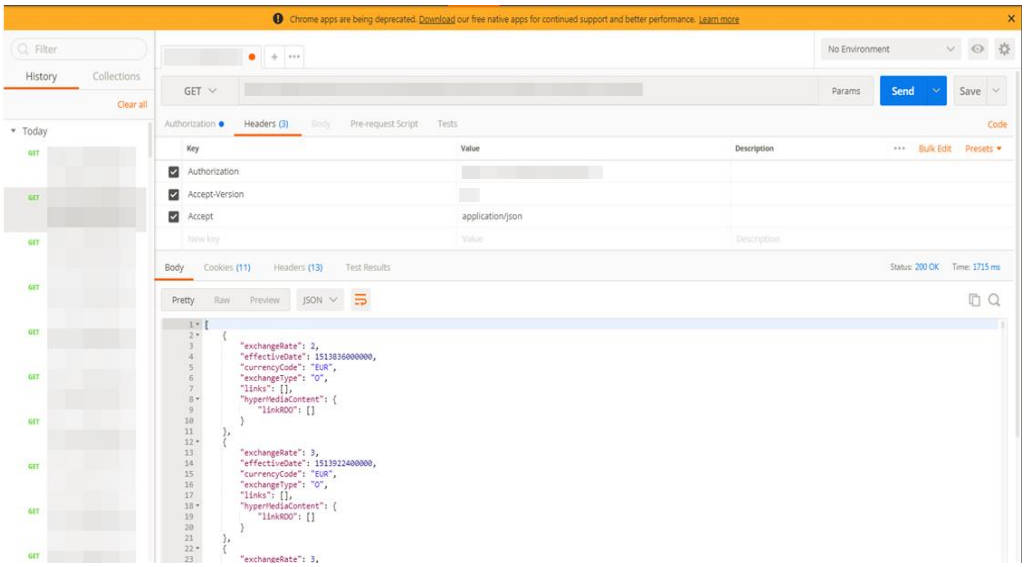
Screenshot 7.4 : Authorization header

Other headers were also added. Figure shows the headers added to the request.



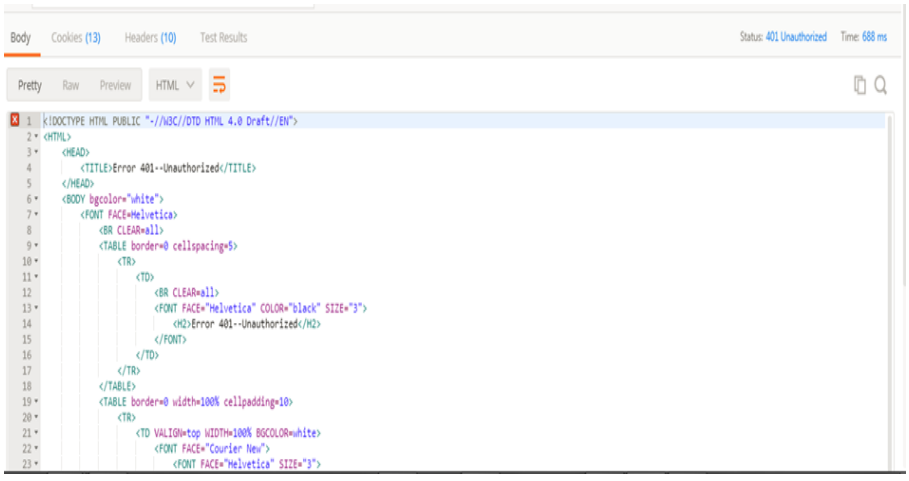
Screenshot 7.5 : Postman Request Headers

After request was send, response was received which was in JSON format. Below is one of the request and response received.



Screenshot 7.6 : RESTful Request/Response

In OSSA testing, wrong header were passed like wrong authorization header or wrong version of application. When wrong headers were passed it was observed that error response was received.



Screenshot 7.7 : Error response in Postman

7.2.1 Advantages

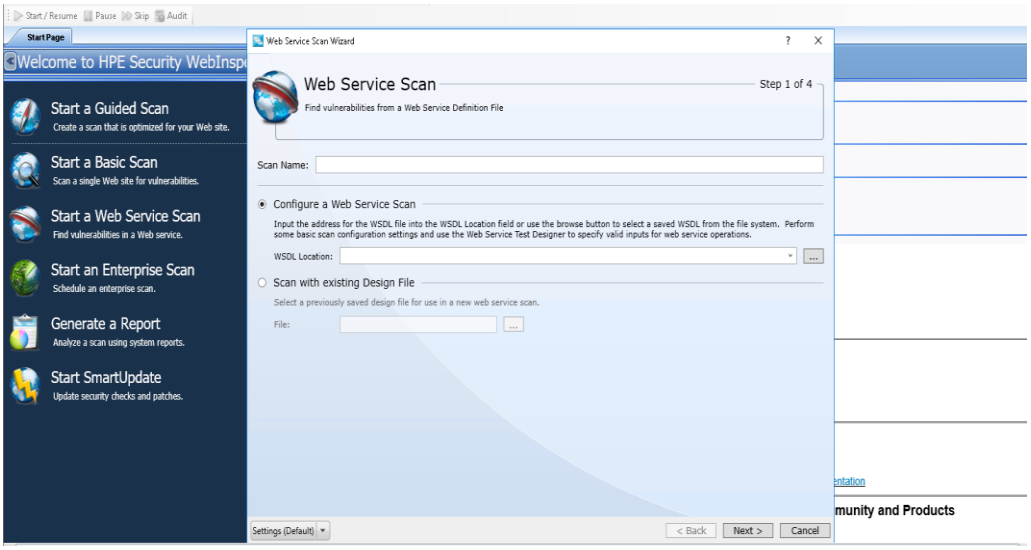
- It is lightweight and fast.
- Test cases can be added to verify the response.
- It is easy to create test suites.
- Different environments can be created.

7.2.2 Disadvantages

- Monitoring test cases is difficult.
- Codeless is not possible in postman.

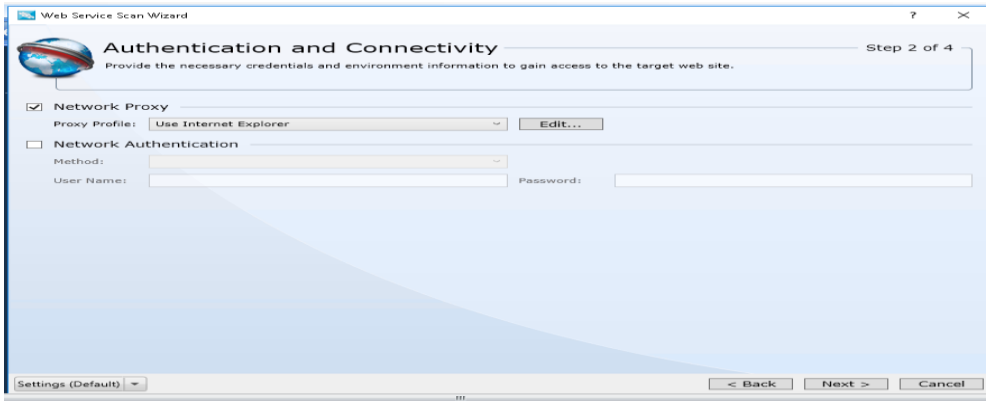
7.3 WebInspect

WebInspect [25] is a professional tool by HP which is mainly used for security testing of dynamic applications. It is used for testing application and web services also. There are options to which gives user to configure scan according to the need. It also provide the network authentication option if scan is to be performed outside from organization network.



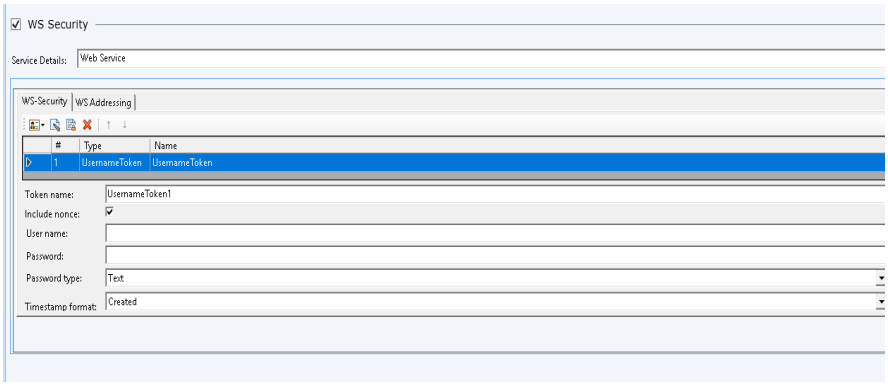
Screenshot 7.8 : WebInspect Web Service scan

After selecting the web service scan, scan name was given. Here either you can give the WSDL url or browse it from local computer. There is also an option to scan from existing design file. After selecting a new window will appear where web inspect will ask for network proxy and network authentication. For network proxy “Firefox” and no network authentication was given as the scan was configured in Oracle Network only.



Screenshot 7.9 : Authentication Web Services

After this WebInspect launch web designer file which create the ports of WSDL. Arguments were passed in the XML's of each port. Along with this WS-Security parameters were passed.



Screenshot 7.10 : WS-Security

After this scan was started. WebInspect send many attacks on web services and study the responses received. On basis of those responses it decide whether vulnerability exists or not. A report was generated at the end which include the vulnerability type, description along with the fix to resolve the issue. An Excel was generated from that report and was send to DEV spocs for fixation of vulnerabilities.

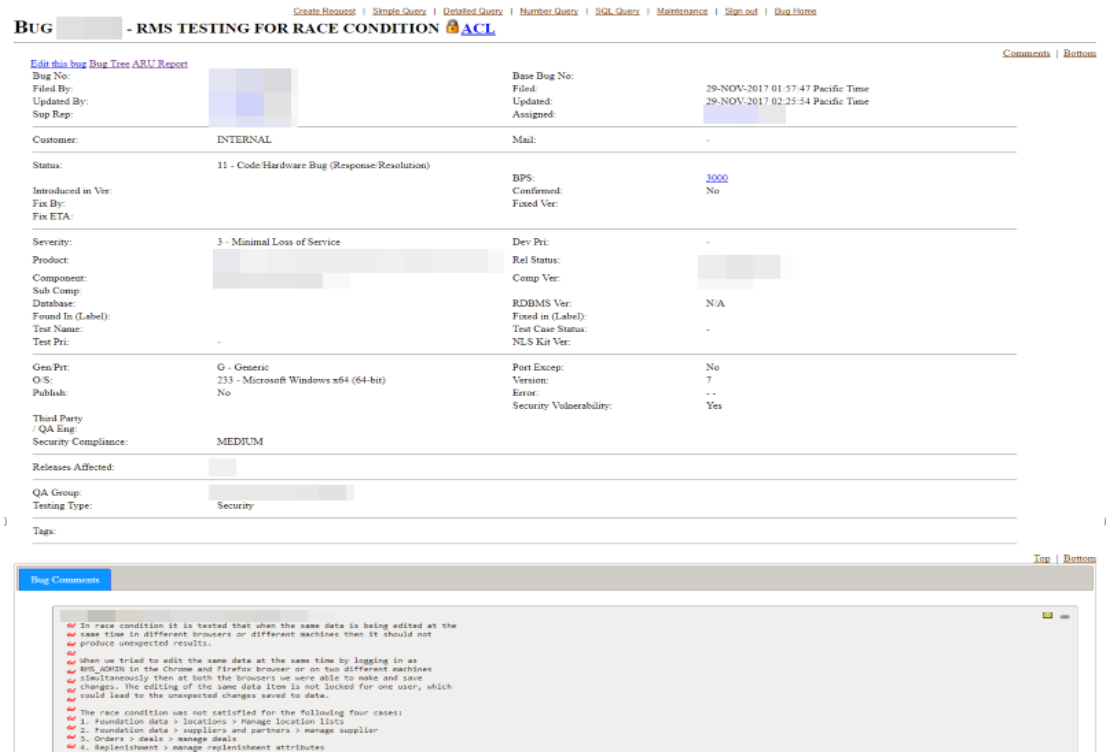
In this way OSSA testing is performed on web services before its release.

Chapter 8

Observations and Result

8.1 BugDB

While performing Functional and Software Assurance Testing many bugs were found. Whenever an error was found, a bug is raised by QA-Testers in BugDB. BugDB is Oracle's application which is used by employees to raise bugs found against the application.



Screenshot 8.1 : BugDB

When ever a bug is fixed, then it is again send back to QA team for verification.

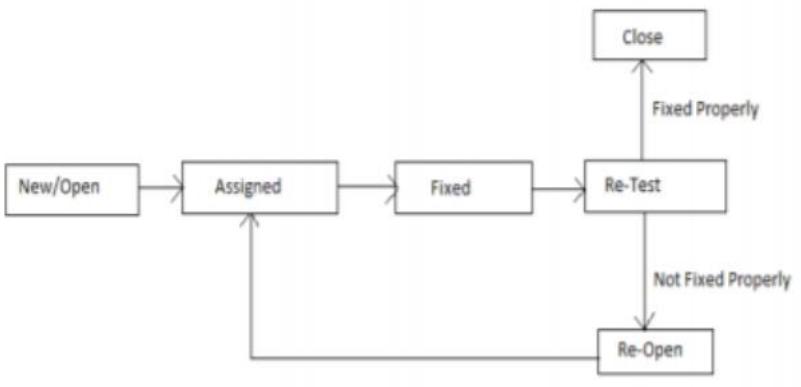


Figure 8.1 : Bug Life Cycle [26]

Closing of bug happen only after it is being verified by the QA tester.

8.2 Manual Testing Efficiency

It was observed that manual testing is time consuming but is more efficient. The number of functional bugs found using manual technique were higher in number than those found using WebInspect tool. Not only the number were higher but also the True Positive percent was also higher in case of manual testing. False Positive comes in case of manual testing only when the tester is confused about the functionality of the application. A true positive means the error predicted by tool is a true bug. A false positive is a state where error predicted is not a bug. The following figure explains the calculations for efficiency of manual testing.

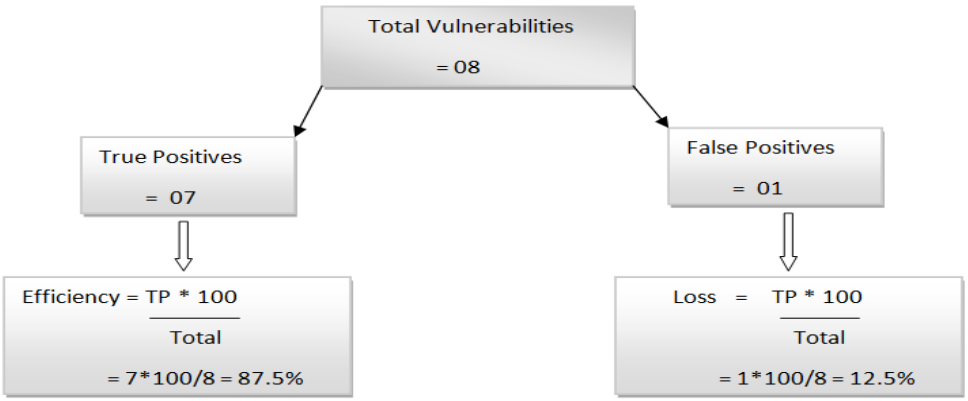


Figure 8.2 : Manual Testing Efficiency

8.3 Automation Testing Efficiency

Automation is good for functional testing. Automation was able to find more issues than manual and its efficiency is also comparable to manual. The failure that happened is also due to lack of functional knowledge.

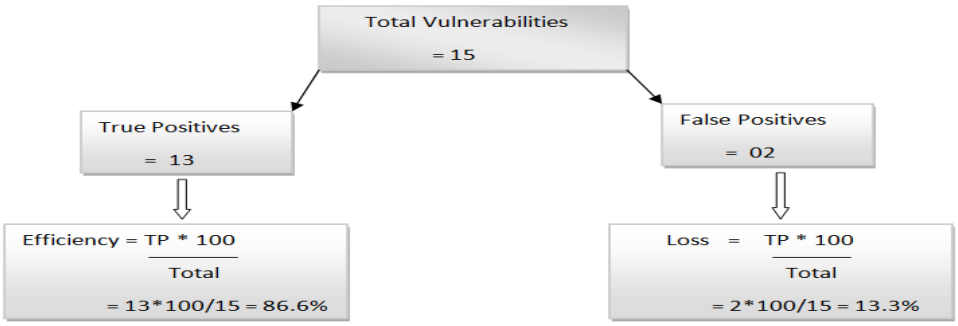


Figure 8.3 : Automation Testing Efficiency

Tester creates the test cases and scripts and if tester has lack of functional knowledge it results in gaps in test scripts too.

8.4 WebInspect Efficiency

In case of WebInspect the reports generated by WebInspect tool have more vulnerabilities than both automation and manual testing. But the rate of false positive is much greater than true positive in that report. For both web services and application testing this behaviour was observed. Also WebInspect was not able to find functional issues. It is most suitable for security testing than functional testing.

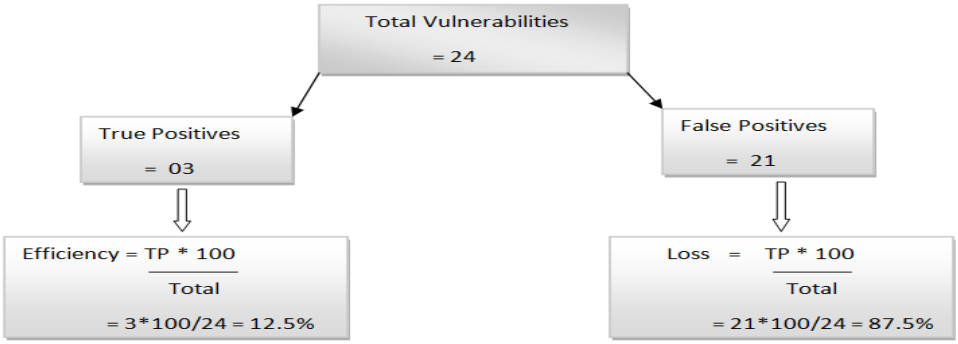


Figure 8.4 : WebInspect tool Efficiency

Thus we can say that depending only on tools for security testing is not a right choice.

Chapter 9

Conclusions and Future Scope

No software is bug free. Testing is a very crucial process. Each and everything need to be checked with precession before the product is released. Organizations are using various techniques for software testing. Test cases are written and on basis of those testing is performed. But it was observed that no probabilistic methods were taken in consideration while performing testing. Test cases were made on the basis of deterministic approach where test cases that will fail for particular error are made. If may be possible that beside from those errors others error are there in the program. But the test cases will not consider that point. Along with this Automation scripts are also written by testers for testing the functionality of software are used which checks the software by providing various combination of inputs. For security testing, companies mainly depends upon security testing tools.

The reason behind using tools is lack of functional information of the application. Also security analysts/experts in organizations are very less in number. It is observed that organizations doesn't have appropriate number of security analysts as needed. A regular QA-analyst is performing the job of security analyst. Due to lack of knowledge many security as well as functional bugs are missed from being found out. Along with that the tools used are the generic tools. They are programmed for specific applications and with fixed steps. They can't examine the functionality of applications correctly which results in more false positives.

Thus it is concluded both manual and automatic testing are necessary. Organizations must hire appropriate number of security experts for analysing security of software. Proper training should be provided to employees so they know the functionality of the software before starting testing it. This will decrease the false positives in manual as well as automation testing.

References

[1] *Owasp.org*, 2018. [Online]. Available: https://www.owasp.org/images/1/15/AppSecEU2012_Oracle.pdf. [Accessed: 05- Jun- 2018].

[2] *Owasp.org*, 2018. [Online]. Available: https://www.owasp.org/images/1/15/AppSecEU2012_Oracle.pdf. [Accessed: 01- Aug- 2018].

[3] *Nvlpubs.nist.gov*, 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.140-2.pdf. [Accessed: 10- Feb- 2018].

[4] "Software quality assurance: Testing and validation - IEEE Journals & Magazine", *Ieeexplore.ieee.org*, 2018. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1456077 , 1980. [Accessed: 25- Jan- 2018].

[5] *Infosys.com*, 2018. [Online]. Available: https://www.infosys.com/it-services/validation-solutions/white-papers/documents/test-data-management-software.pdf. [Accessed: 14- Apr- 2018].

[6] *Infosys.com*, 2018. [Online]. Available: https://www.infosys.com/it-services/validation-solutions/white-papers/documents/qa-strategy-succeed.pdf. [Accessed: 19- Mar- 2018].

[7] *Infosys.com*, 2018. [Online]. Available: https://www.infosys.com/it-services/validation-solutions/white-papers/documents/leveraging-advanced-validation.pdf. [Accessed: 23- Jan- 2018].

[8] *Docs.oracle.com*, 2018. [Online]. Available: https://docs.oracle.com/cd/E79623_01/rms/pdf/16022/rms-16022-ug.pdf. [Accessed: 09- Feb- 2018].

[9] "Oracle Retail Application Administration Console", *Docs.oracle.com*, 2018. [Online]. Available: https://docs.oracle.com/cd/E79623_01/rms/pdf/16021/html/impl_guide/oraac.htm. [Accessed: 03- Apr- 2018].

[10] *Oracle.com*, 2018. [Online]. Available: http://www.oracle.com/us/products/applications/047076.pdf. [Accessed: 02- Jul- 2018].

[11] *Docs.oracle.com*, 2018. [Online]. Available: https://docs.oracle.com/cd/E79623_01/rms/pdf/160C/resa-160-ug.pdf. [Accessed: 20- Jun- 2018].

[12] "Web Services in Retail Applications", *Docs.oracle.com*, 2018. [Online]. Available: https://docs.oracle.com/cd/E76310_01/pdf/160/html/operations_guide/webservices.htm. [Accessed: 13- Apr- 2018].

[13] *Oracle.com*, 2018. [Online]. Available: http://www.oracle.com/technetwork/database/database-cloud/public/restful-wp-1844130.pdf. [Accessed: 11- Feb- 2018].

[14] *Zenq.com*, 2018. [Online]. Available: https://zenq.com/Portals/0/SecurityTestingWhitePaper-v15.pdf. [Accessed: 21- Mar- 2018].

[15] S. K. Pandey, K. Mustafa – "Security Assurance: An Authentication Initiative by Checklist" / [Accessed 18 Mar. 2018].

[16] Rincon, D. (2018). *Oracle X6-2 Security and Architecture - Cornerstone Data Systems, Inc.*. [online] Cornerstone Data Systems, Inc. Available at: https://cdsiusa.com/oracle-x6-2-security/ [Accessed 8 Jan. 2018].

[17] S. K. Pandey, S. Rehman, K. Mustafa, S. I. Ahson – "Security Assurance – The Requirements Way" /[Accessed 23 Jan. 2018].

[18] Rajendra Kumar and Mustafa K – "Security Requirements Development Framework (^{S}RDF)" /[Accessed 24 Jun. 2018].

[19] Oracle.com. (2018). [online] Available at: http://www.oracle.com/us/support/library/software-security-assurance-2293569.pdf [Accessed 10 May 2018].

[20] Owasp.org. (2018). *Security by Design Principles - OWASP*. [online] Available at: https://www.owasp.org/index.php/Security_by_Design_Principles [Accessed 2 Aug. 2018].

[21] Docs.oracle.com. (2018). *Chapter 11 Introduction to Web Services (The Java EE 6 Tutorial)*. [online] Available at: https://docs.oracle.com/cd/E19798-01/821-1841/gijti/index.html [Accessed 24 Jun. 2018].

[22] Schd.ws. (2018). [online] Available at: https://schd.ws/hosted_files/utougtrainingdays2018/38/King_CreateRestfulServicesORDSUTOUGW.pdf [Accessed 8 Apr. 2018].

[23] Docs.oracle.com. (2018). *Oracle Test Manager Tutorial*. [online] Available at: https://docs.oracle.com/cd/E25294_01/doc.920/e15487/chap5_otm_fm.htm [Accessed 11 May 2018].

[24] Docs.oracle.com. (2018). *Getting Started With OpenScript*. [online] Available at: https://docs.oracle.com/cd/E25294_01/doc.920/e15488/opscrpt_get_started.htm [Accessed 12 Apr. 2018].

[25] Dl.packetstormsecurity.net. (2018). [online] Available at: https://dl.packetstormsecurity.net/papers/attack/WebInspect.pdf [Accessed 17 Apr. 2018].

[26] Annals-csis.org. (2018). [online] Available at: https://annals-csis.org/proceedings/rice2017/pliks/18.pdf [Accessed 29 May 2018].