2.4 Insecure Direct Object References

1. **Use of prepared statements (parameterized queries)**
   Banking uses PreparedStatement with bind variables to construct and execute SQL statements in JAVA.

2. **Input Validation**
   Banking is a web based application, the request data from browser to server will be passed using request headers and request parameters. All the request fields coming from the client are validated using white list validation to prevent cross site scripting.
   User defined method validateParameter() is used for input validation which checks each character of the request field with a range of allowed characters.
   User defined methods escapeJavaScript(), escapeHTML() and escapeURL() will sanitize the output data before flushing it into client browser.
   escapeJavaScript() will escape all characters except immune JavaScript characters and alphanumeric characters in the ASCII character set. All other characters are encoded using the \\xHH or \\uHHHH notation for representing ASCII or Unicode sequences.
   escapeHTML() will escape the characters with equivalent HTML entities obtained from the lookup map. Lookup map will have entities such as amp, quot, lt, gt etc.
   escapeURL() will encode the URL using URLEncoder class.
   White list validation is also used to restrict Image/signature/excel upload and to check rights for every operation performed by user.

3. **Image Content validation**
   Signature upload will check for image type and image content using the inbuilt classes (ImageIO and JarFile) available in java.

4. **Field validation**
   Field level validations exist for all mandatory fields. Database too had limits on the type and the length of data. Blacklisted characters are not allowed in the mandatory fields. Nevertheless, Banking has free-text fields, which takes all data, entered by the user, as a String.

5. **Restriction on Blacklist characters**

   Similar to white list validation black list validation is also used for validating the request fields. Banking uses blacklist validation to check whether the request xml contains unwanted tags like scripting tag, html tag, anchor tag etc inside the xml content. It is also used for the advance summary field's validation to check whether proper request fields are coming from the browser.

Below table shows the list of bad characters which should not be allowed in URL path but the Banking operations requires many of the below characters to be passed in the request. So Banking will encode the below bad characters before sending them through the URL and same will be decoded at the server to prevent the hacker from modifying the request.

Bad URL Characters(Unsafe Characters)	
&	//
<	./
>	/.
;	/*
\"	*.
\'	~
%	\
)	25%
(	%25u
+	%25U
,	%00-%1f, %7f-%ff
" " (space)	%00-%1f and %7f-%ff
-	%25u and %25U

6. Restriction on Script/Html tags

Banking has blacklist validation for unwanted tag in xml like scripting tag or html tag inside xml content particularly in the header

2.5 Security Misconfiguration

1. Configuration files

Configuration files are securely placed inside the Classes folder of the WEB-INF folder which is not publicly accessible.

2. **Exception handling in java**

Different types of exceptions can rise in application. Java exceptions handled using try catch blocks available in java. Sometimes we use the Throw statement to throw an exception which is caught by the catch block. Caught exceptions will be written into the log files for the debug purpose when ever required. Whenever any exception occurs in application, proper information used to send to the front end user by showing alert.

3. **Exception handling in oracle database**

Database exceptions handled using EXCEPTION statement available in PL/SQL. Caught exceptions will be written into the log files for the debug purpose. And proper error message created to send the same in response to the user.

4. **Package lockout situation handled in backend**

Application will be hanged in an oracle system package lockout situation. Locked objects will be released manually using SQL scripts or through database restart.

We have handled cursor lock out problem in the required packages.

5. **Auto generated password:**

The password is generated by the system accordance to the password policy. The salt is also be generated every time the password is changed by using predefined algorithm.

The salt concatenated with auto generated password and SHA-512 hash applies on the resultant which results the password digest.

Once the successful generation of password digests both salt and password digest is stored in the DB.

6. **Custom password:**

The password is keyed in by the administrator / user accordance to the password policy. The salt is generated every time the password is changed by using predefined algorithm.

The salt concatenated with the password input and SHA-512 hash applies on the resultant which results the password digest.

Once the successful generation of password digests both salt and password digest is stored in the DB.

Oracle Banking Payments does not provide any default user/password. User and password needs to be created at the time of installation.

7. **Sand Box for File Upload**

The application uses a sandbox for placing files that are uploaded via the signature/image upload screen. The sandbox is placed in a specified location (the location will be specified in the properties file) on the server.

8. BI Publisher Reports – generation and access

The application uses a sandbox for placing the generated reports file into a sandbox area. The sandbox is placed in a specified location (the location will be specified in the properties file) on the server. The application validates if the user has explicit Rights to generate Reports.

2.6 Sensitive Data Exposure

1. Secure Transformation of Data (SSL)

The Oracle Banking Payments Installer allows a deployer to configure Oracle Banking Payments such that all HTTP connections to the Oracle Banking Payments application are over SSL/TLS. In other words, all HTTP traffic in the clear will be prohibited; only HTTPS traffic will be allowed. It is mandatory to enable this option in a production environment, especially when WebLogic Server acts as the SSL terminator.

A two-way SSL is used when the server needs to authenticate the client. In a two-way SSL connection the client verifies the identity of the server and then passes its identity certificate to the server. The server then validates the identity certificate of the client before completing the SSL handshake.

In order to establish a two-way SSL connection, need to have two certificates, one for the server and the other for client.This is required for de-centralized setup of application.

For Oracle Banking Payments, need to configure a single connector. This connector is related to SSL/TLS communication between host or browser and the branch which uses two-way authentication.

If the secure flag is set on a cookie, then browsers will not submit the cookie in any requests that use an unencrypted HTTP connection, thereby preventing the cookie from being trivially intercepted by an attacker monitoring network traffic.

Below configuration has to be ensured in weblogic.xml within the deployed application ear.

- Cookies are set with Http only as true
- Cookie secure flag set to true
- Cookie path to refer to deployed application

```
<wls: session-descriptor>
 <wls: cookie-http-only>true</wls: cookie-http-only>
</wls: session-descriptor>

<wls: session-descriptor>
<wls: cookie-secure>true</wls: cookie-secure>
 <wls: url-rewriting-enabled>false</wls: url-rewriting-enabled>
</wls: session-descriptor>

 <session-descriptor>
  <cookie-name>JSESSIONID</cookie-name>
  <cookie-path>/<DeployedApplicationPath></cookie-path>
  <cookie-http-only>true</cookie-http-only>
  <cookie-secure>true</cookie-secure>
  <url-rewriting-enabled>false</url-rewriting-enabled>
        </session-descriptor>
```

Always make sure Cookies are set with always Auth Flag enabled by default for WebLogic server .

2. Sign-On messages

Below table shows the general Sign-On messages which would be displayed to the user during invalid authentication.

Message	Explanation
User Already Logged In	The user has already logged into the system and is attempting a login through a different terminal.
Invalid User ID/Login.	An incorrect user ID or password was entered.
User Status is Disabled. Please contact your System Administrator	The user profile has been disabled due to number of dormancy days allowed for the user has exceeded the dormancy days configured in the system.
User Status is Locked. Please contact your System Administrator	The user profile has been locked due to an excessive number of attempts to login, using an incorrect user ID or password. The number of attempts could have matched either the successive or cumulative number of login failures (configured for the system).

3. CACHE Control in Servlet and jsp

There are three basic HTTP response headers that prevent a page from being cached to disk. Different browsers handle them in slightly different ways, so they need to be used in combination to ensure all browsers do not cache the specific page. These headers are "Expires", "Pragma" and "Cache-control". In addition, these headers can either be sent directly by the server or placed in the HTML code as HTTP-EQUIV META tags within the HEAD section. The "Expire" header gives a date at which point the page should expire and no longer be cached. Internet Explorer supports a date of "0" for immediately and any negative number for already expired. The "Pragma: no-cache" header indicates that the page should not be cached.

4. Clickjacking/Frame-bursting

Banking uses the X-Frame-Options HTTP response header to indicate whether or not a browser should be allowed to render a page in a <frame> or <iframe>. This is used to avoid Clickjacking attacks, by ensuring that the content is not embedded into other sites.

2.7 Missing Function Level Access Control

It is likely that users working in the same department at the same level of hierarchy need to have similar user profiles. In such cases, you can define a Role Profile that includes access rights to the functions that are common to a group of users. A user can be linked to a Role Profile by which you give the user access rights to all the functions in the Role Profile.

Application level access has implemented via the Security Management System (SMS) module.
SMS supports “ROLE BASED” access of Screens and different types of operations.
Banking Payments supports dual control methodology, wherein every operation performed has to be authorized by another user with the requisite rights.
Please refer 2.6 section of the SMS user manual for more details.

Apart from the role based access control particular functions , products can be restricted for user as described below.

***Disallowed functions**:* Function IDs or UI level restrictions can be provided for the user by including the function Ids in the disallowed list. This will restrict the user from accessing the UI. When accessed, an error message dialogue box will pop up saying-“User not authorized to access the screen”.

Disallowed account class: The user could be restricted to perform any operation using a particular a/c class. When disallowed, no accounts could be created by the user using the account class.

Disallowed products: The user could be restricted to use product(s) of any module(s), if disallowed. This is really required when restricting users department wise. For example, staffs of accounts department need not be given access to view the loans of customers.

Disallowed branches: The user could be restricted to access branches other than his own branch (reporting branch). He can be given access to login from other branches of the bank at an approval from authenticated person, an action which again requires manual authorization.

2.8 Cross-Site Request Forgery (CSRF)

In case of XMLHttpRequest objects, the XMLHttpRequest object sets a custom HTTP header in the request, with the header value being the Cross-site request forgery token; the server then verifies for the presence of such a header and the Cross-site request forgery token. This serves as a protection at endpoints used for XMLHttpRequest requests, since only XMLHttpRequest objects can set HTTP headers (apart from Flash; and both cannot make cross-domain requests).

2.9 Using Components with Known Vulnerabilities

Source code scanning done using the latest fortify to identify the sources code issue and will provide the proper fix for the reported issues.

3rd party libraries scanning for every release has been done to validate if any security issues rise for any of the components or not. Update the 3PL with latest security patch or upgraded to latest version.

2.10 Unvalidated Redirects and Forwards Network Security

Application uses 302 redirect wherever required. Banking UBS uses response.sendRedirect(newURL);

3. Securing Gateway Services

Different applications deployed on disparate platforms and using different infrastructure need to be able to communicate and integrate seamlessly with Oracle Banking Payments in order to exchange data. The Oracle Banking Payments Integration Gateway will cater to these integration needs.

The integration needs supported by the Gateway can be broadly categorized from the perspective of the Gateway as follows:

- Inbound application integration – used when any external system needs to add, modify or query information within Oracle Banking Payments
- Outbound application integration – used when any external system needs to be notified of the various events that occur within Oracle Banking.

3.1 Inbound Application Integration

Oracle Banking Payments Inbound Application Gateway provides XML based interfaces thus enhancing the need to communicate and integrate with the external systems. The data exchanged between Oracle Banking Payments and the external systems will be in the form of XML messages. These XML messages are defined in FCUBS in the form of XML Schema Documents (XSD) and are referred to as 'FCUBS formats'.

FCUBS Inbound Application Integration Gateway uses the Synchronous and Asynchronous Deployment Pattern for addressing the integration needs.

The Synchronous Deployment Pattern is classified into the following:

- Oracle Banking Payments EJB Based Synchronous Inbound Application Integration Deployment Pattern
- Oracle Banking Payments Web Services Based Synchronous Inbound Application Integration Deployment Pattern
- Oracle Banking Payments MDB Based Asynchronous Inbound Application Integration Deployment Patten

3.2 EJB Based Synchronous Deployment Pattern

The Enterprise Java Beans (EJB) deployment pattern will be used in integration scenarios where the external system connecting to Oracle Banking Payments is 'EJB literate', i.e., the external system is capable of interacting with Oracle Banking Payments based upon the EJB interface. In this deployment pattern, the external system will use the RMI/IIOP protocol to communicate with the Oracle Banking Payments EJB.

In this deployment pattern the EJB displayed by Oracle Banking Payments will be a stateless session bean. The actual request will be in the form of an XML message. After the necessary processing is done in Oracle Banking Payments based on the request, the response is returned to the external system as an XML message. The transaction control for the processing will stay with the Oracle Banking Payments EJB.

3.3 Web Services Based Synchronous Deployment Pattern

The web services deployment pattern will be used in integration scenarios where the external system connecting to Oracle Banking Payments wants to connect using standards-based, inter-operable web services.

This deployment pattern is especially applicable to systems which meet the following broad guidelines:

- Systems that are not 'EJB literate', i.e., such systems are not capable of establishing connections with Oracle Banking Payments based upon the EJB interface; and/or
- Systems that prefer to use a standards-based approach

In this deployment pattern, the external system will use the SOAP (Simple Object Access Protocol) messages to communicate to the Oracle Banking Payments web services.

The services displayed by Oracle Banking Payments are of a 'message based' style, i.e., the actual request will be in the form of an XML message, but the request will be a 'payload' within the SOAP message. After the necessary processing is done in Oracle Banking Payments based on the request, the response is returned to the external system as an XML message which will be a 'payload' within the response SOAP message. The transaction control for the processing will stay with the Oracle Banking Payments.

3.4 HTTP Servlet Based Synchronous Deployment Pattern

The HTTP servlet deployment pattern will be used in integration scenarios where the external system connecting to Oracle Banking Payments wants to connect to Oracle Banking Payments using simple HTTP messages.
This is especially applicable to systems such as the following:

- Systems that are not 'EJB literate', i.e., are not capable establishing a connections with Oracle Banking Payments based upon the EJB interface; and/or
- Systems that prefer to use a simple http message based approach without wanting to use SOAP as the standard
-

In this deployment pattern, the external system will make an HTTP request to the Oracle Banking Payments servlet.

For this deployment pattern, Oracle Banking Payments will display a single servlet. The actual request will be in the form of an XML message. This XML message is embedded into the body of the HTTP request sent to the Oracle Banking Payments servlet. After the necessary processing is done in Oracle Banking based on the request, the response is returned to the external system as an XML message which is once again embedded within the body of the response HTTP message. The transaction control for the processing will stay with the Oracle Banking.

3.5 MDB Based Asynchronous Deployment Pattern

The MDB deployment pattern is used in integration scenarios where the external system connecting to Oracle Banking Payments wants to connect to Oracle Banking Payments using JMS queues.

This is especially applicable to systems such as the following:

- Systems that prefer to use JMS queues based approach without wanting to wait for the reply
-

Here external system sends messages in XML format to request queue on which an MDB is listening. When a message arrives on the queue, it is picked up for processing. After the necessary processing is done in Oracle Banking Payments, based on the request, the response is sent to the response queue as an XML message.

3.6 Outbound Application Integration

The Outbound Application Integration is also called the Oracle Banking Payments Notify Application Integration layer. This application layer sends out notification messages to the external system whenever events occur in Oracle Banking Payments.

The notification messages generated by FCUBS on the occurrence of these events will be XML messages. These XML messages are defined in FCUBS in the form of XML Schema Documents (XSD) and are referred to as 'FCUBS formats'

3.7 Securing Web Services

Web services can be secured by applying security policies available in web logic sever. We can attach two types of policies to Web Logic Web services and clients at design and deployment time.
Oracle WSM policy : We can attach Oracle Web Services Manager(WSM) policies to Web Logic JAX-WS Web services and clients

Web Logic Web service policy: This policies are provided by Oracle Web Logic Server and can be attached to any web service deployed in Web Logic.
We can use Oracle Enterprise Manager Fusion Middleware Control to attach Oracle WSM security policies to Web Logic Java EE Web services and clients.
We can attach policies to Web Logic Web services at both design time and after the Web service has been deployed.
At design time, use the weblogic.jws.Policy and weblogic.jws.Policies JWS annotations in JWS file to associate policy files with Web service. We can associate any number of policy files with a Web service, although it is up to us to ensure that the assertions do not contradict each other. We can specify a policy file at the class level of our JWS file.

After the Web service has been deployed, use the Oracle Web Logic Server Administration Console to attach Web Logic Web service policies to Web Logic Web services.

3.8 Accessing Service and Operation

In a message it is mandatory to maintain a list of Service Names and Operation Codes. This information is called Gateway Operations.
A combination of every such Service Name and Operation Code is mapped to a combination of Function ID and Action. Every screen in Oracle Banking Payments is linked with a function ID. This information is called Gateway Functions.
User can gain access to an external system using the Gateway Functions. The Function IDs mapped in Gateway Functions should be valid Function IDs maintained in Oracle Banking Payments. Hence, for every new Service or Operation being introduced, it is important that you provide data in Gateway Operations and Gateway Functions.

3.9 Gateway Password Generation Logic for External System Authentication

As a secure configuration password authentication should be enabled for the external system maintained. The same can be verifying in External system detail screen level.
Once these features enable, system will validate for Encrypted password as part of every request sent by the External System.
The Message ID which is present as part of the header in Request XML, is considered as hash. External System generates an unique Message ID, which is functional mandatory field in the header. Create a Message Digest with SHA-512 algorithm.
The hash created from the previous step and the password in clear text together is encrypted in AES encryption method. Apply Base64 encoding to encrypted value and send to the Oracle Banking Payments gateway.

3.10 XSD Validation and Input Validation

Oracle Banking Payments supports the XSD validation for all types Gateway. Each node in request xml is getting validated with the corresponding webservice XSD's.

Restriction on Script/Html tags

Banking Gateway has blacklist validation for unwanted tag in xml like scripting tag or html tag inside xml content particularly in the header

3.11 List of Services

COCategoryTypeService
COCurrencyPairService
COCurrencyRateTypeService
COCurrencyService
FCUBSPXService

3.12 List of Interfaces

Generic Interface
Document Management System Interface
SWIFTNet Services Integrator Messaging Hub Interface
Oracle Identity Manager Interface

Development Security Guide
[Novemeber] [2018]
Version 14.2.0.0.0
Oracle Financial Services Software Limited
Oracle Park
Off Western Express Highway
Goregaon (East)
Mumbai, Maharashtra 400 063
India

Worldwide Inquiries:
Phone: +91 22 6718 3000
Fax:+91 22 6718 3001
www.oracle.com/financialservices/