Oracle Weblogic Server formsweb.cfg deployment file security

Mojtaba Eltayeb Abdellatief[1], Mohammed Ahmed Mohammed Alata [2], Samani A. Talab [3]

[1, 2]Dr, Computer Science, RedSea University, RedSea State, Sudan

[3] Prof, Computer Science, Neelain University, Khartoum State, Sudan

Abstract: *Oracle weblogic server is middleware application server which is used to deploy and host java and oracle forms applications, hosting oracle forms 11g, 12c requires using formsweb.cfg file which is plain text file in order to deploy the application for production, formsweb.cfg file is modified by weblogic service through enterprise manager interface in addition to the direct modification through any text editor, the file acts as a deployment point for oracle forms application where any modification to application related section affect the deployed application, this paper discusses security issues of using formsweb.cfg file, it also suggest securing the file through encryption which restrict access to the file by normal users and administrators. .*

Keywords: *Weblogic, forms, deployment, binary file, formsweb.*

1. Introduction

Weblogic Server is an application server of Oracle Corporation, a platform for developing and deploying multitier distributed enterprise applications, it is based on java and mainly targeted to serve and deploy J2EE application in the first place, it acts as middleware and it contains many services like web server functionality, connectivity services and business components in addition to load balancing, monitoring and caching mechanisms it also provide administrators with a set of tools to manage, deploy and troubleshoot the weblogic components and the deployed applications.

The Weblogic server is a Java EE application server which supports Java application and numerous web services. The Weblogic Server complete implementation of the Java EE 6 specification provides a standard set of APIs for creating distributed Java applications including Oracle forms that can access a wide variety of services, such as databases, messaging services and connections to external Enterprise systems. End - user clients can access these applications using Web browser or standalone Java clients. It also supports the Spring Framework, a programming model for Java applications which delivers an alternative to

Many aspects of the Java EE model.[1].

Oracle corporation integrates Forms and reports application with oracle weblogic, since oracle application server which is used to deploy oracle forms 10g oracle weblogic become the basic application server for deploying oracle forms application, oracle forms and report services installed after oracle weblogic component is installed, the forms require configuring oracle weblogic server with form service, oracle weblogic server install oracle forms service as logical managed server as a component of oracle weblogic which allows administering the form from the main oracle weblogic server administration console, the deployment process for oracle forms requires configuring a weblogic formsweb.cfg plain text file with application parameters, the file will be read by forms service and provide the client with the specific URL to run the application, it also control many behavior and properties of deployed application.

The forms is deployed as java application and it runs in clients using java applet plugin, while the forms servlet is written in java the forms services is written in c and C++, the forms connection and login from client will remain encrypted as long as the application uses HTTPS the application URL will look like http://server:8888/forms/frmservlet?config=testapp in this case the connection is not encrypted, we notice here the application name is (testapp) which is the configuration section in the formsweb.cfg deployment file.

The file as mentioned earlier is normal text file it can be managed by using oracle weblogic enterprise manager GUI as shown in figure 1, in addition to any text editor, this allows every user in the operating system to read its contents and modify it which affects the deployed application and it allows to gather information regarding deployed system easily including username and password for system login, the paper will focus in the risks of using the formsweb.cfg as deployment file.

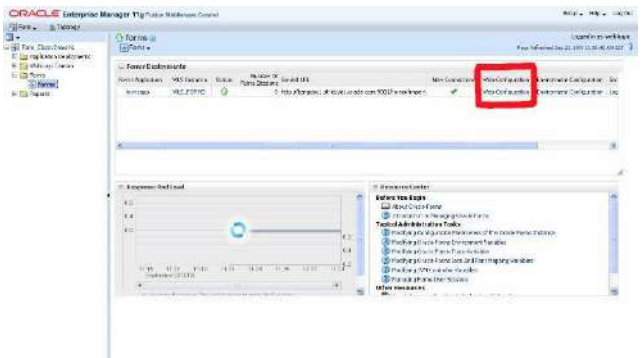

Fig -1: accessing formsweb.cfg using EM

2. Deploying forms using formsweb.cfg

In order to run oracle forms 11g, 12c application it require modifying the formsweb.cfg with the

appropriate parameters to enable the application to work as mentioned earlier, the formsweb.cfg file is a plain text file located at *$DOMAIN_HOME/config/fmwconfig/servers/WLS_FORMS/applications/formsapp_12.2.1/config/formsweb.cfg*

or where the weblogic server forms components is installed, the file supports many parameters, is organized in sections, every section related to specific application, in order to deploy oracle forms application new section should be created as shown following :

Table 1: some of formsweb.cfg parameters

id	*Content*	*content*
1	envFile	Specifies the name of the environment configuration file. Default value from ormsweb.cfg is default.env
2	Form	Specifies the name of the top level Forms module (fmx file) to un.Default value from formsweb.cfg is test.fmx. This parameter is a runform parameter.
3	height	Specifies the height of the form applet, in pixels
4	Userid	Login string. scott/tiger@ORADB. This parameter is a runform parameter.
5	Width	Specifies the width of the form applet, in pixels
6	ssoCancelUrl	Specifies the Cancel URL for the dynamic resource creation DAS page
7	ssoDynamicResourceCreate	Specifies whether dynamic resource creation is enabled if the resource is not yet created in the OID
8	ssoErrorUrl	Specifies the URL to redirect to if ssoDynamicResourceCreate is set to false
9	ssoMode	Specifies whether the URL is protected in which case, mod_osso is given control for authentication or continue in the FormsServlet if not. Set it to true in an application-specific section to enable Single Sign-On for that application.
10	ssoProxyConnect	Specifies whether session should operate in proxy user support or not. Set ssoProxyConnect to yes to enable for particular application. Default value is no. This parameter is a sub-argument for otherparams
11	debug	Allows running in debug mode.
12	EndUserMonitoringEnabled	Indicates whether End User Monitoring integration is enabled
13	EndUserMonitoringURL	Indicates where to record End User Monitoring data.
14	host	Specifies the host for the debugging session. This parameter should be used for debugging purposes only. It identifies the host on which the forms engine process is started
15	Port	Supports tracing and logging
16	Archive	Comma-delimited list of archive files that are used or downloaded to the client.
17	Codebase	Virtual directory you define to point to the physical directory ORACLE_HOME/forms/java, where, by default, the applet JAR files are downloaded from
18	imageBase	Indicates where icon files are stored. Legal values: codeBase, which indicates that the icon search path is relative to the directory that contains the Java classes. Use this value if you store your icons in a JAR file (recommended).
19	jpi_classid	Sun's Java Plug-in class ID. formsweb.cfg specifies an appropriate value
20	jpi_codebase	Sun's Java Plug-in codebase setting. formsweb.cfg specifies an appropriate value.

21	jpi_download_page	Sun's Java Plug-in download page. formsweb.cfg specifies an appropriate value.
22	jpi_mimetype	Parameter related to version of Java Plug-in. formsweb.cfg specifies an appropriate value.
23	baseHTML	The default base HTML file.
24	baseHTMLjpi	Physical path to HTML file that contains Java Plug-in tags. Used as the baseHTML file if the client browser is not on Windows and the client browser is either Firefox or IE without the IE native settings.
25	HTMLafterForm	HTML content to add to the page below the area where the Forms application is displayed.
26	HTMLbeforeForm	HTML content to add to the page above the area where the Forms application is displayed.
27	HTMLbodyAttrs	Attributes for the <BODY> tag of the HTML page.
28	pageTitle	HTML page title, attributes for the BODY tag, and HTML to add before and after the form.
29	background	Specifies the .GIF file that should appear in the background. Set to NO for no background. Leave empty to use the default background.
30	colorScheme	Determines the application's color scheme. Legal values: Teal, Titanium, Red, Khaki, Blue, BLAF, SWAN, Olive, or Purple. Default value from formsweb.cfg is teal.

Below is some of the most used parameters :

1- [sampleapp]

2- form=main.fmx

3- userid=scott/tiger

4- pageTitle= Sample Application title

5- width=1024

6- height=768

7- separateFrame=true

8- imageBase=codebase

9- archive=frmall.jar,my_icons.jar

10- envFile=/path/to/myapp.env

The [sampleapp] contains the name of the application which will be called from client web browser, the section name must be unique and can't be repeated, it also didn't accept spaces between its characters which may confused the client when calling the application.

The (form) tag require the main form binary fmx file which will be requested when section name called, it is usually holds the main or login form.

The (userid) parameters represent the database username and password if required which is an optional component, it allows the client to access the application directly without username or password, or in case of using logical username and password for application, the administrator must provide the username and password parameters with the appropriate values to allow the application to request the logical user later.

The (PageTitle) parameter display the application title in web browser, it accept any characters with any character length.

The (width) and the (height) represent the forms size in the browser, it controls the application dimensions regardless of the dimensions used in design time, it can be dynamically stretched by assigining 100% value which allow the application to stretch according to client browser width and height.

The (separateFrame) parameter determines whether the forms application appears within a separate window or in the browser window, this parameter accepts Boolean values whether true or False.

The (imageBase) parameter indicates where icon files are stored in the server to allow the application to use it.

(archive) parameter is a Comma-separated list of archive files that are used when the browser detected is neither Internet Explorer using native JVM nor JInitiator.

The Formsweb.cfg file contains many parameters to configure and control forms applications some of the parameters is very critical and can cause deployment problems for that carful modification is required.

After adding and modifying application parameters to the new section created in the formsweb.cfg, the application can be accesses by calling below URL:

http://server:port/forms/frmservlet?config=secname

the server and port should be replaced by the real weblogic server name or http server if load balancing is used, and http or form service port which is 8888 or 9001, the secname should be replaced with the section

name created in the sample above which was (sampleapp).

3. Discussion

The formsweb.cfg file can be Accessed and configured using oracle weblogic enterprise manager which is GUI for managing the weblogic components the enterprise manger allows modifying the formsweb parameters securely because the login to the enterprise manager is secured with user name and password, the file also can be modified directly using and text editor from the operating system because it is a normal plain text file, using the enterprise manager method is safe because it controls who is accessing the file in the first place and also it controls how the data modified in the file because it protect the main key and allows only modifying values as shown in figure 2

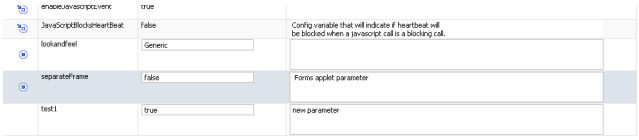

Fig -2: Configuring formsweb.cfg parameters using Enterprise Manager.

Usually the text file is located in *$DOMAIN_HOME/config/fmwconfig/servers/WLS_FORMS/applications/formsapp_[xxxx]/config/*

The path above May different depending on installation platform, the above path is for windows environment.

The file as mentioned earlier is plain non-encrypted text file format, it is readable by any user accessing the operating system with appropriate privilege, it also can be modified by any remote user, this allow extracting data belong to deployed application causing noted risk as :

1- Application parameters theft: As an example an enterprise organization with 30 database application deployed, the application parameters configured including section, forms path, optionally usernames and passwords, jpi parameters, the mentioned parameters and other parameters allows attacker to get basic information against organization systems and their location which help compromising their data from database using stolen credentials or database related data from forms application using disassembling tools, the plain formsweb.cfg help the attacker to identify which forms related to which application with their form path in addition to login credentials if username and password is configured in the formsweb.cfg.

2- Wrong parameters: Directly modifying formsweb.cfg by users may lead to corruption due to wrong parameters modification or accidently changing running application parameters, the fault will stop specific application from running which cause downtime.

3- Big text file issues: The deployment file is organized in to sections but the file is still one file, there is no mechanism to distribute the configuration across many parts or partitioning the file to speed up the read and write operation, also big text files in many circumstances get corrupted easily comparing with Other small ones.

3.1 SUGGESTED SOLUTION:

Encrypting formsweb.cfg file will help securing the application data and parameters inside, it will restrict normal users from extracting information from the file as shown in figure -3 , and will be the only way to access the file is through the oracle weblogic enterprise manager which is secured using username and password, the result will secure the file against information theft as well as wrong parameters issue, the encryption can be implemented by the enterprise manager itself which is the only tool writing to the formsweb.cfg, the decryption process is required for the forms service in order to read the file too, because when the oracle weblogic server initialized the forms servlet reads the forms related files, the formsweb.cfg will be read to allow clients accessing application by calling application section from the file so while the file is encrypted the form servlet should support reading the encrypted file to process it.

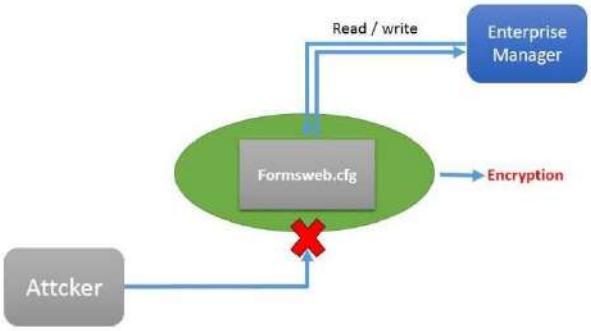

Figure 3: securing formsweb.cfg file using Encryption.

4. Conclusion

formsweb.cfg is the file responsible for deploying oracle forms application in oracle Webslogic Server, formsweb.cfg as plain non encrypted text file allows attackers to extract information regarding running database application, it allows direct modification by user which results entering wrong parameters, the paper suggest encrypting the deployment file and modify the forms servlet to support the encryption, securing the formsweb.cfg file helps securing both database application and oracle weblogic server too against compromising confidential data.

References

[1] Oracle Corporation, Introduction to Oracle weblogic Server 10.3.6, E13752-07, July 2015.

[2] J. Oracle Corporation. Fusion Middleware Forms Services Deployment Guide 11g Release 2 (11.1.2) E24477-03, November 2012.

[3] Swati Thacker: Oracle® Fusion Middleware Forms Services Deployment Guide 11g Release 1 (11.1.1) E10240-07. 2, 2014. June 2012.

[4] Bálint Varga-Perke : Automated Security Testing of Oracle Forms Applications, May 15, 2015.

Authors' Biographies

Mojtaba Eltayeb is a PhD in Computer science, he has been working in IT field for 14 Years, currently he is working as senior Oracle Database administrator in Sea ports Corporation.

Mohammed Ahmed Mohammed Alata a PhD In Information Technology, he is working in Red Sea University.

Prof Samani A. Talab is a computer science professor, he has been working in IT filed since 1990, and currently he is the vice-president of Neelain University.