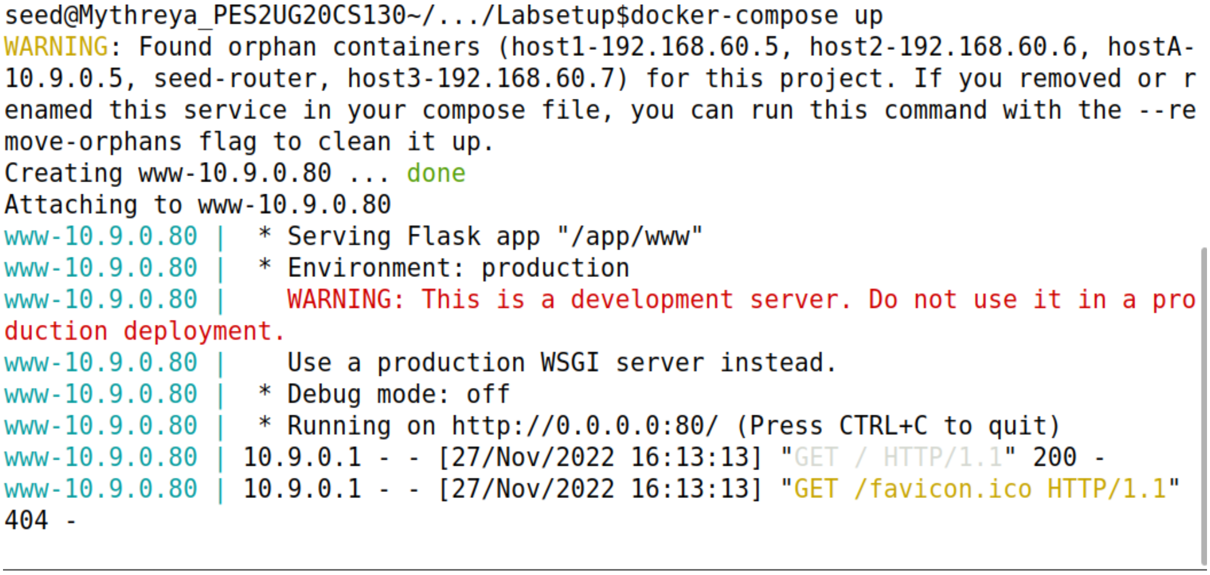
Crypto Lab - 9

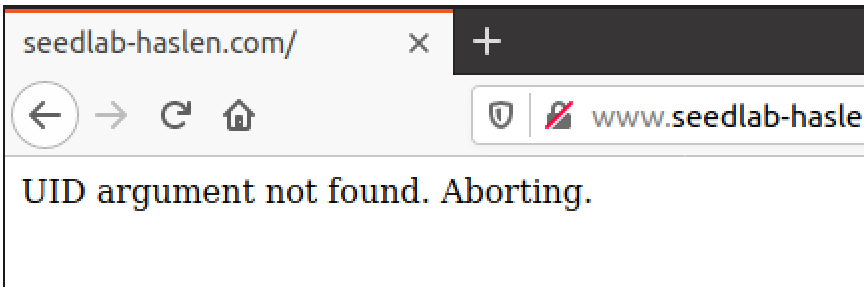
Name: H M Mythreya

SRN: PES2UG20CS130

Setting up docker



```
seed@Mythreya_PES2UG20CS130~/.../Labsetup$docker-compose up
WARNING: Found orphan containers (host1-192.168.60.5, host2-192.168.60.6, hostA-
10.9.0.5, seed-router, host3-192.168.60.7) for this project. If you removed or r
enamed this service in your compose file, you can run this command with the --re
move-orphans flag to clean it up.
Creating www-10.9.0.80 ... done
Attaching to www-10.9.0.80
www-10.9.0.80 |  * Serving Flask app "/app/www"
www-10.9.0.80 |  * Environment: production
www-10.9.0.80 |    WARNING: This is a development server. Do not use it in a pro
duction deployment.
www-10.9.0.80 |    Use a production WSGI server instead.
www-10.9.0.80 |  * Debug mode: off
www-10.9.0.80 |  * Running on http://0.0.0.0:80/ (Press CTRL+C to quit)
www-10.9.0.80 | 10.9.0.1 - - [27/Nov/2022 16:13:13] "GET / HTTP/1.1" 200 -
www-10.9.0.80 | 10.9.0.1 - - [27/Nov/2022 16:13:13] "GET /favicon.ico HTTP/1.1"
404 -
```

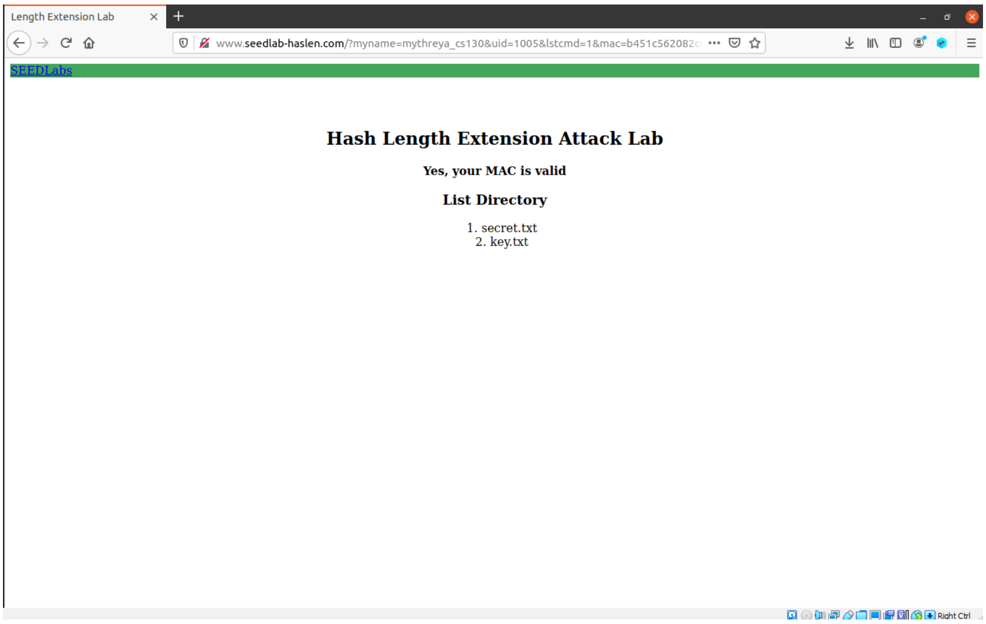


UID argument not found. Aborting.

Task 1: Accessing website with proper mac

Calculating mac using sha256sum
uid:key pair used → 1005:xciujk

```
seed@Mythreya_PES2UG20CS130~/.../Labsetup$echo -n "xciujk:myname=mythreya_cs130&
uid=1005&lstcmd=1" | sha256sum
b451c562082cd93cf5fbc028ab7928df85ac28786cf006d02c1c5a53b848f651  -
```


Length Extension Lab
www.seedlab-haslen.com/?myname=mythreya_cs130&uid=1005&lstcmd=1&mac=b451c562082c
SEEDLabs
Right Ctrl

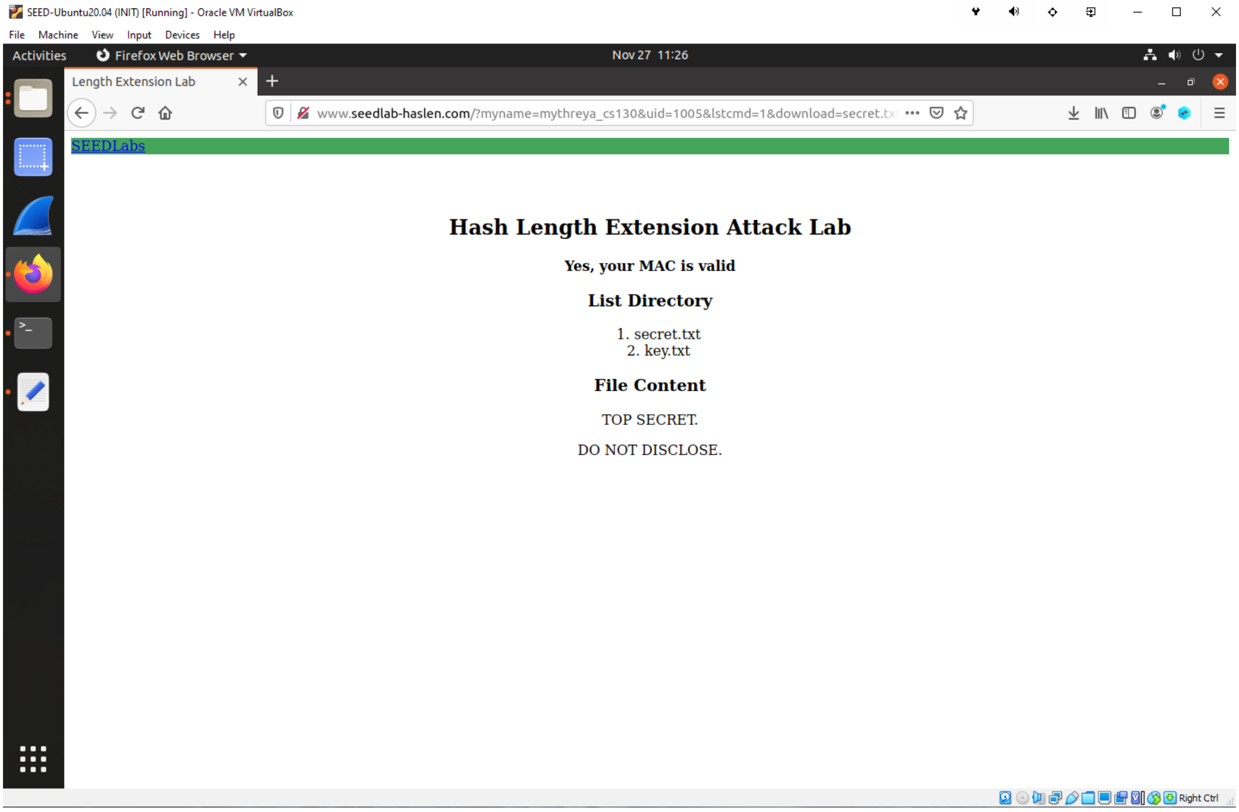
Hash Length Extension Attack Lab

Yes, your MAC is valid

List Directory

1. secret.txt
2. key.txt

We can see the contents of secret.txt by sending a query “download=secret.txt”


SEED-Ubuntu20.04 (INIT) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Activities
Firefox Web Browser
Nov 27 11:26
Length Extension Lab
www.seedlab-haslen.com/?myname=mythreya_cs130&uid=1005&lstcmd=1&download=secret.tx
SEEDLabs
Right Ctrl

Hash Length Extension Attack Lab

Yes, your MAC is valid

List Directory

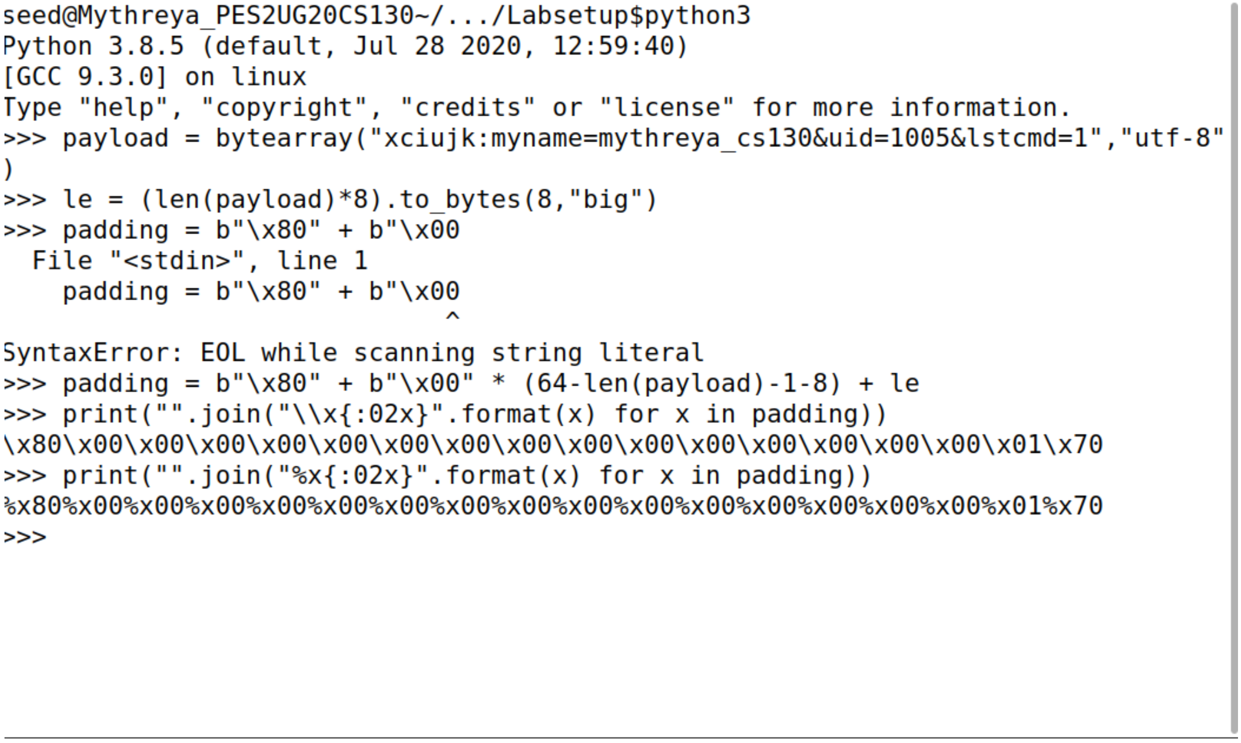
1. secret.txt
2. key.txt

File Content

TOP SECRET.

DO NOT DISCLOSE.

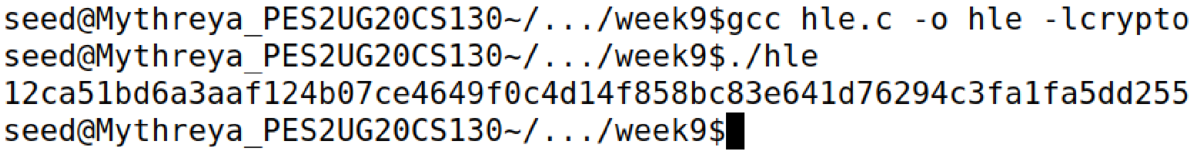
Task 2: Construct padding for sha256



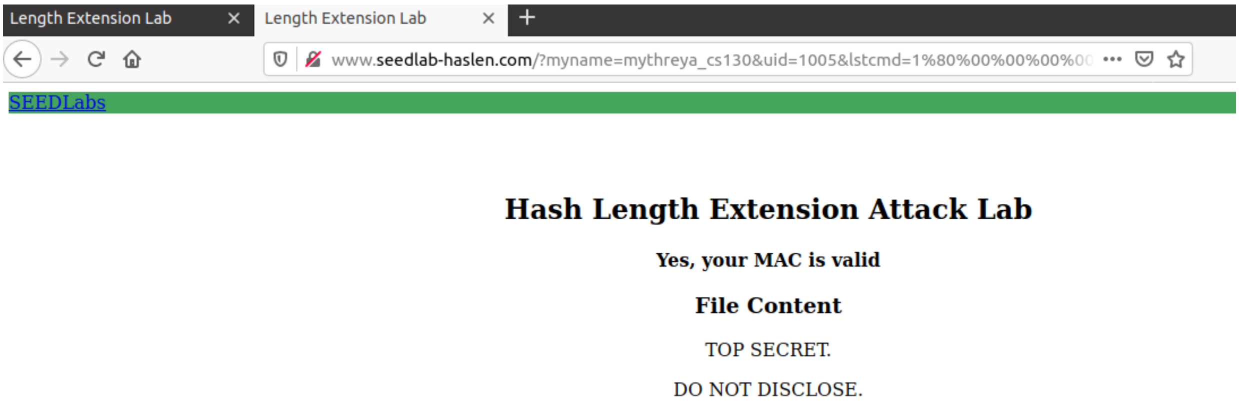
```
seed@Mythreya_PES2UG20CS130~/.../Labsetup$python3
Python 3.8.5 (default, Jul 28 2020, 12:59:40)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> payload = bytearray("xciujk:myname=mythreya_cs130&uid=1005&lstcmd=1","utf-8"
)
>>> le = (len(payload)*8).to_bytes(8,"big")
>>> padding = b"\x80" + b"\x00
  File "<stdin>", line 1
    padding = b"\x80" + b"\x00
                               ^
SyntaxError: EOL while scanning string literal
>>> padding = b"\x80" + b"\x00" * (64-len(payload)-1-8) + le
>>> print("".join("\\x{:02x}".format(x) for x in padding))
\x80\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x01\x70
>>> print("".join("%x{:02x}".format(x) for x in padding))
%x80%x00%x00%x00%x00%x00%x00%x00%x00%x00%x00%x00%x00%x00%x00%x00%x00%x01%x70
>>>
```

Task 3

New hash generated after padding:



```
seed@Mythreya_PES2UG20CS130~/.../week9$gcc hle.c -o hle -lcrypto
seed@Mythreya_PES2UG20CS130~/.../week9$./hle
12ca51bd6a3aaf124b07ce4649f0c4d14f858bc83e641d76294c3fa1fa5dd255
seed@Mythreya_PES2UG20CS130~/.../week9$
```



Length Extension Lab
Length Extension Lab
www.seedlab-haslen.com/?myname=mythreya_cs130&uid=1005&lstcmd=1%80%00%00%00%00
SEEDLabs

Hash Length Extension Attack Lab

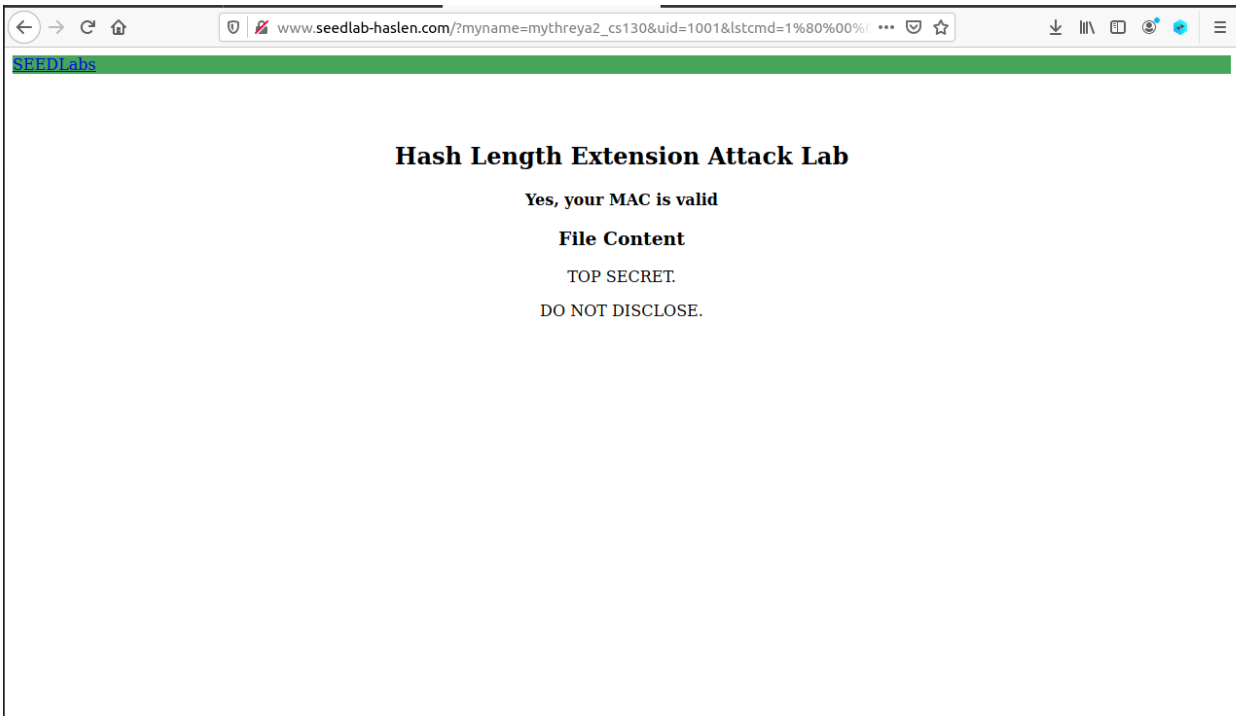
Yes, your MAC is valid

File Content

TOP SECRET.

DO NOT DISCLOSE.

Generating Hash without uid:key pair



www.seedlab-haslen.com/?myname=mythreya2_cs130&uid=1001&lstcmd=1%80%00%

SEEDLabs

Hash Length Extension Attack Lab

Yes, your MAC is valid

File Content

TOP SECRET.

DO NOT DISCLOSE.

With the help of sha256 padding we can access the secret.txt without the need to know uid:key pair.