**Applied Cryptography (UE20CS314)**

**Hash Length Extension**

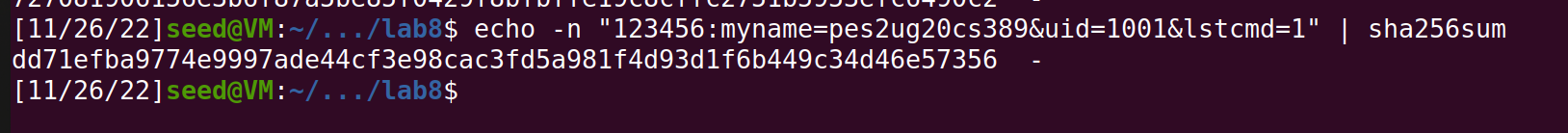
Name: Vishwa Mehul Mehta

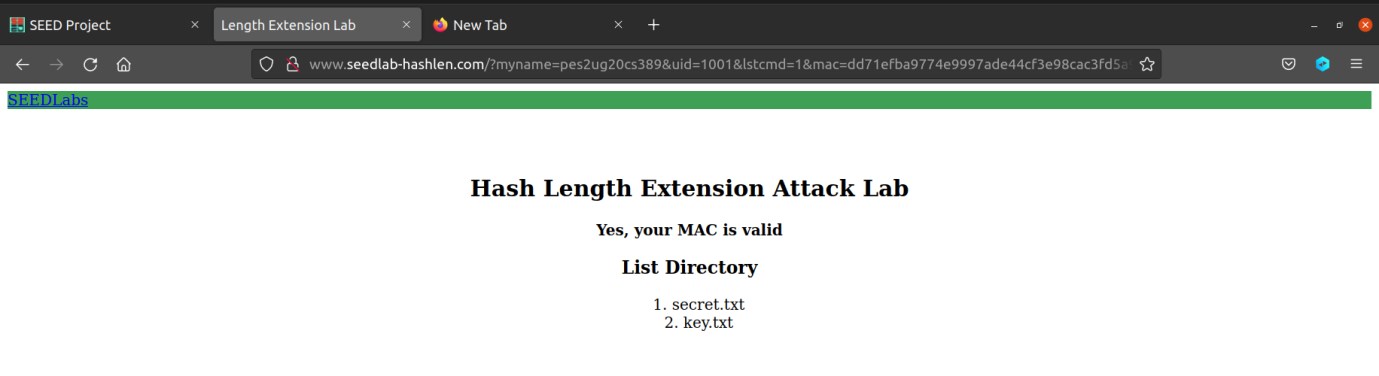
SRN: PES2UG20CS389

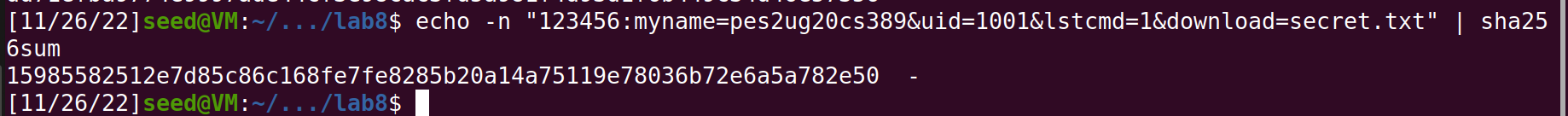
Section: F

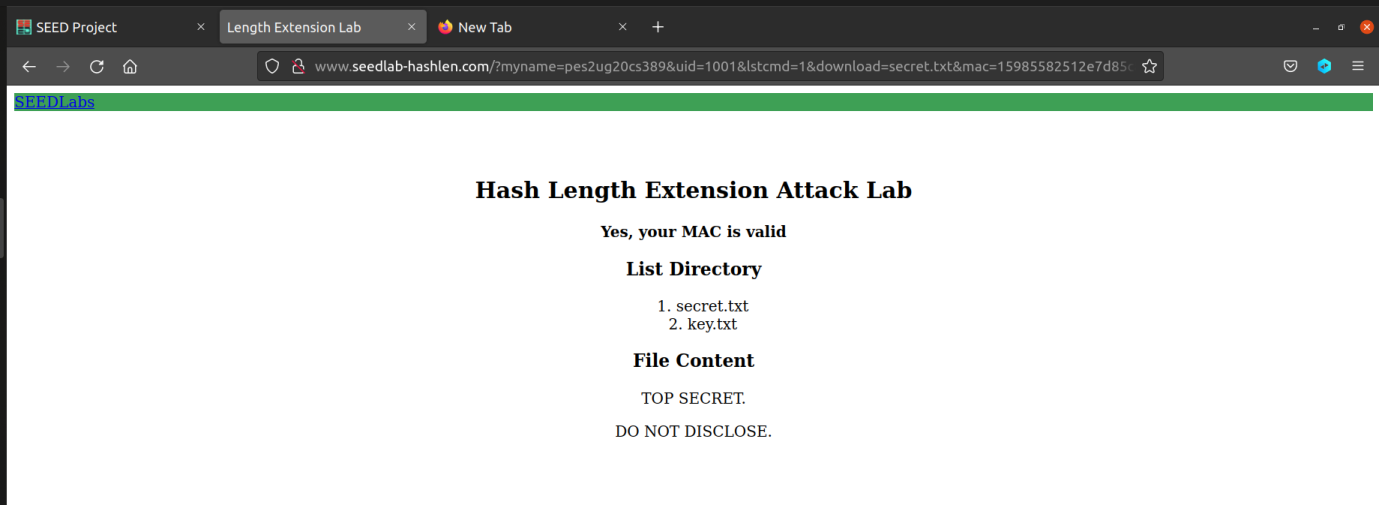
Task 1:

Screenshot:







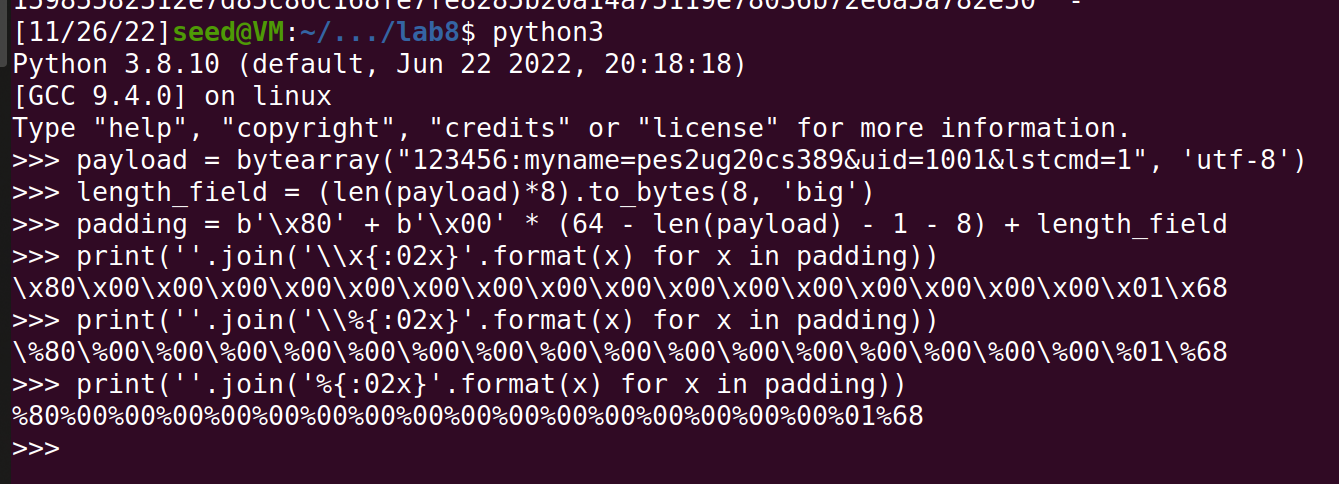


Observation:

We get the contents of the file secret.txt along with its contents and also list the directory with key.txt and secret.txt.

Task 2:

Screenshot:

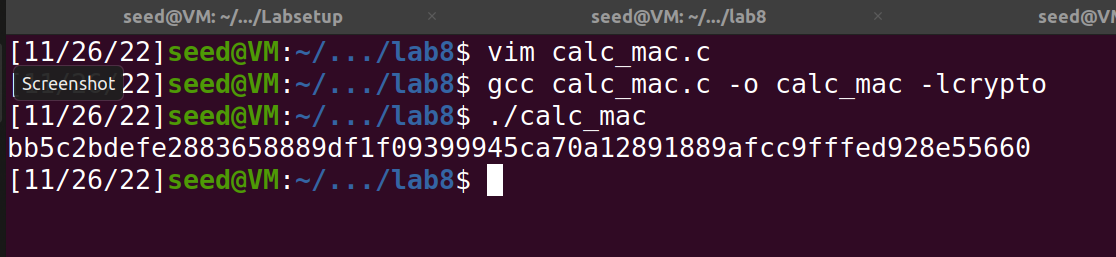


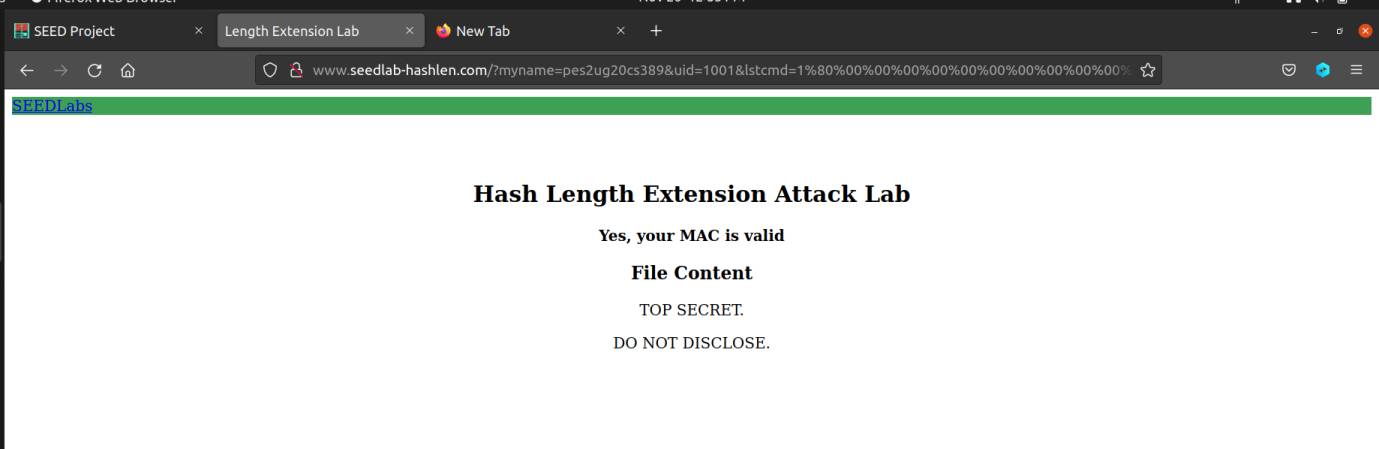
Observation:

We generate the url and hash padding.

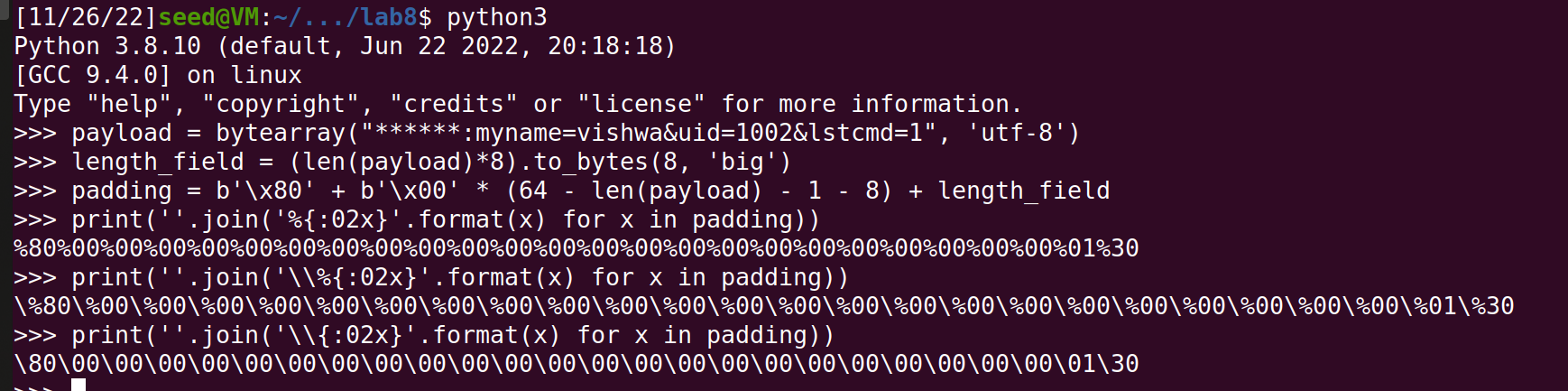
Task 3:

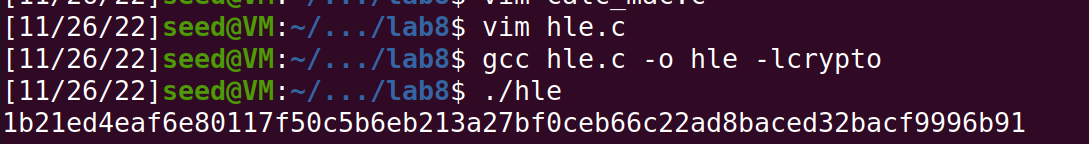
Screenshot:

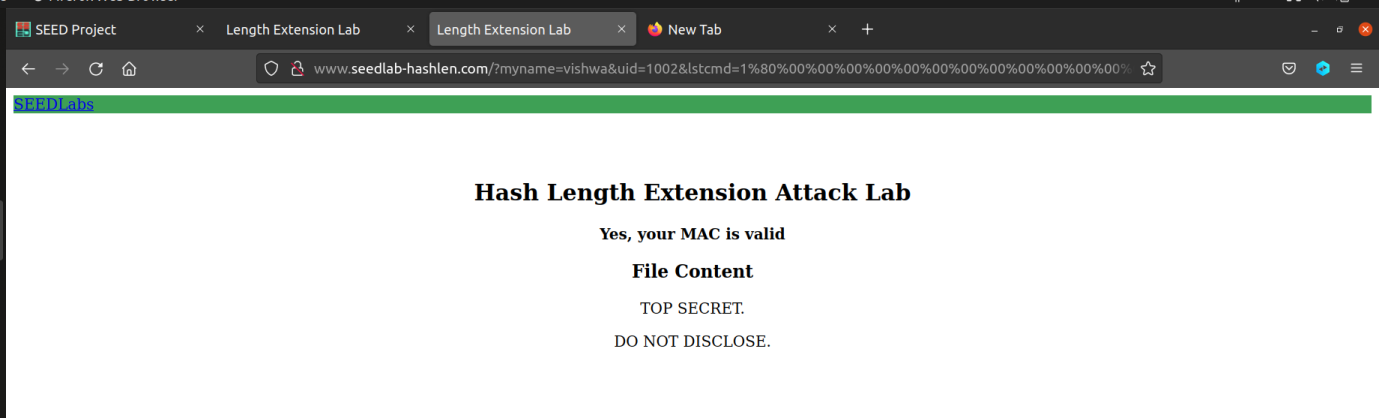




Without key:





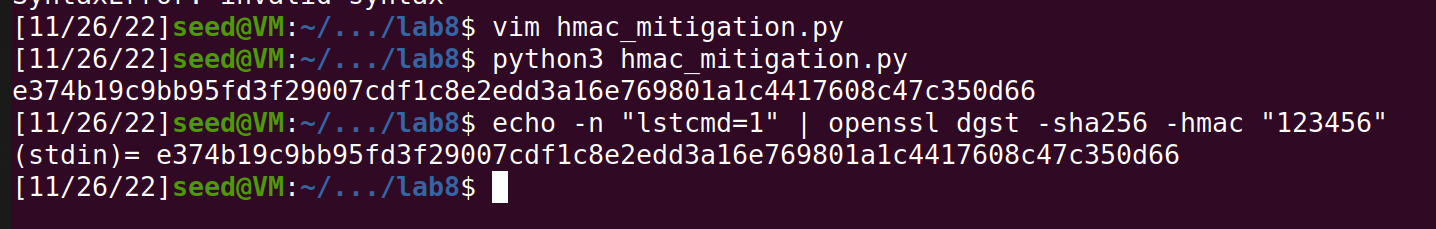


Observation:

The attack is successful and we can see the contents of the file secret.txt even though it is not a valid MAC address. We do both the attacks with the key and without it.

Task 4:

Screenshot:



Observation:

We use hmac to avoid the length extension attack as the mac generated will not be same for the extended length and the original address without padding and will thus fail to authenticate the address.