**APPLIED CRYPTOGRAPHY**

NAME: VISHWAS M

SRN: PES2UG20CS390

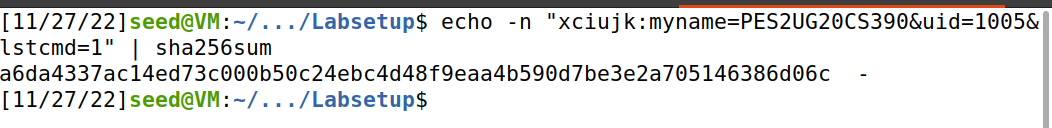
SEC: F

LAB: Hash Length Extension Lab

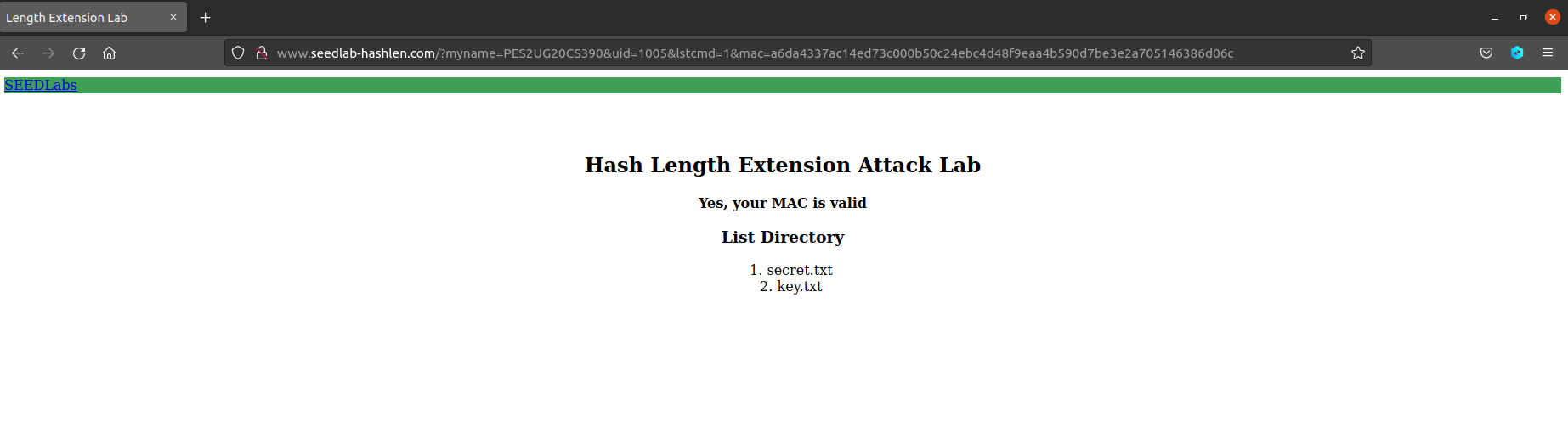
Task1: Send Request to List Files

Step1: Finding the uid

Step2: Calculating MAC



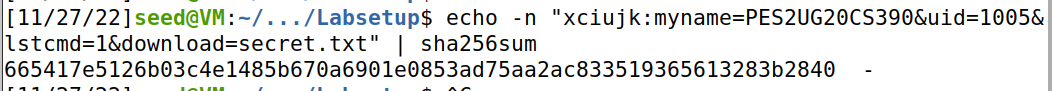
Step3: Sending the Request



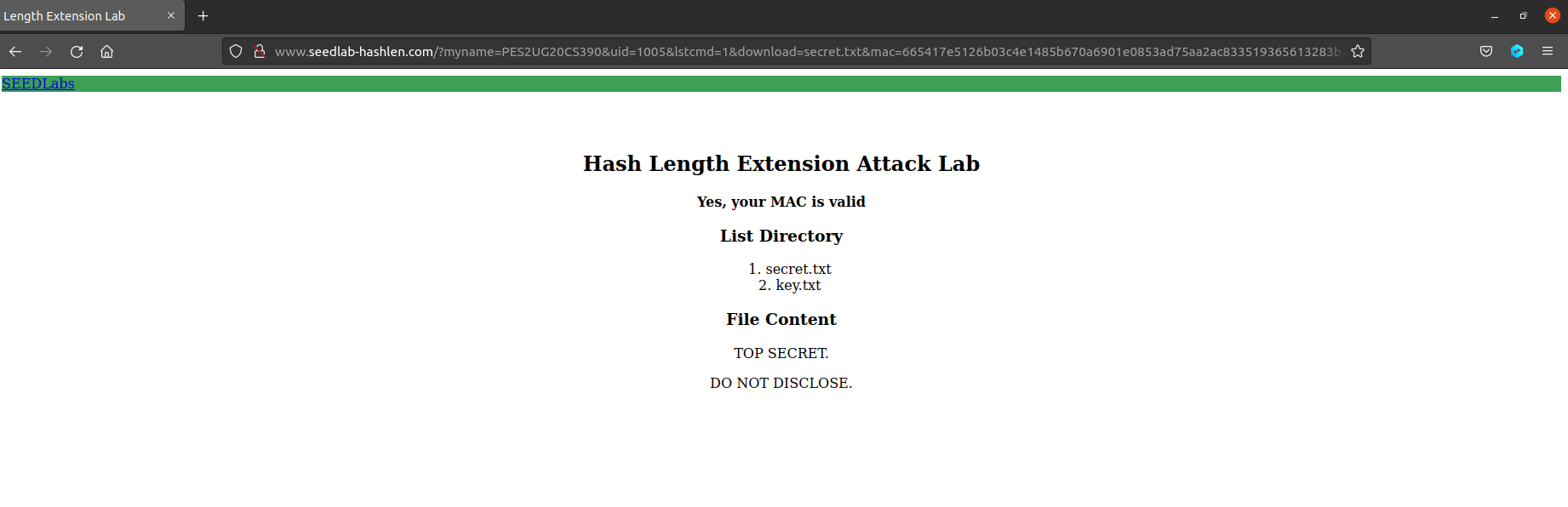
We are just finding the directory list from the above steps.

Step1: Finding uid

Step2: Calculating MAC

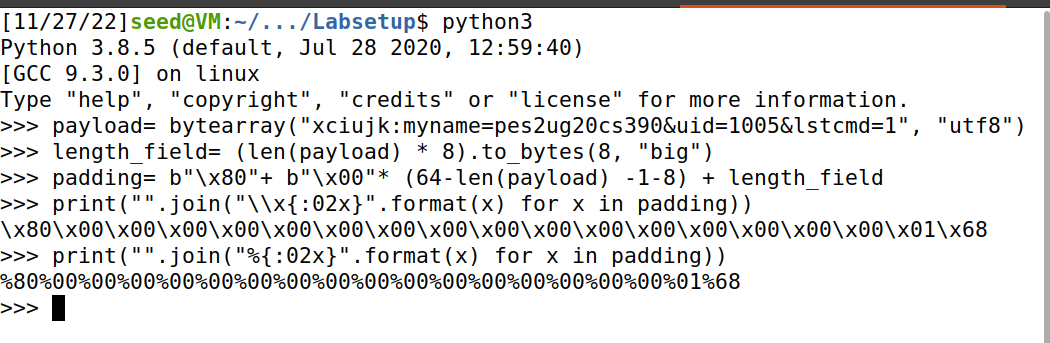


Step3: Sending the Request



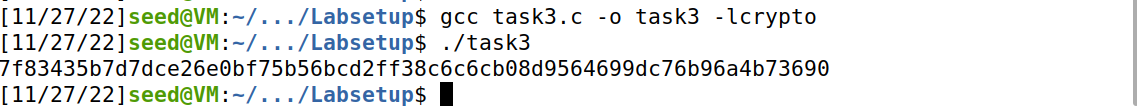
We are finding the contents from secret.text which is displayed in the above screenshots.

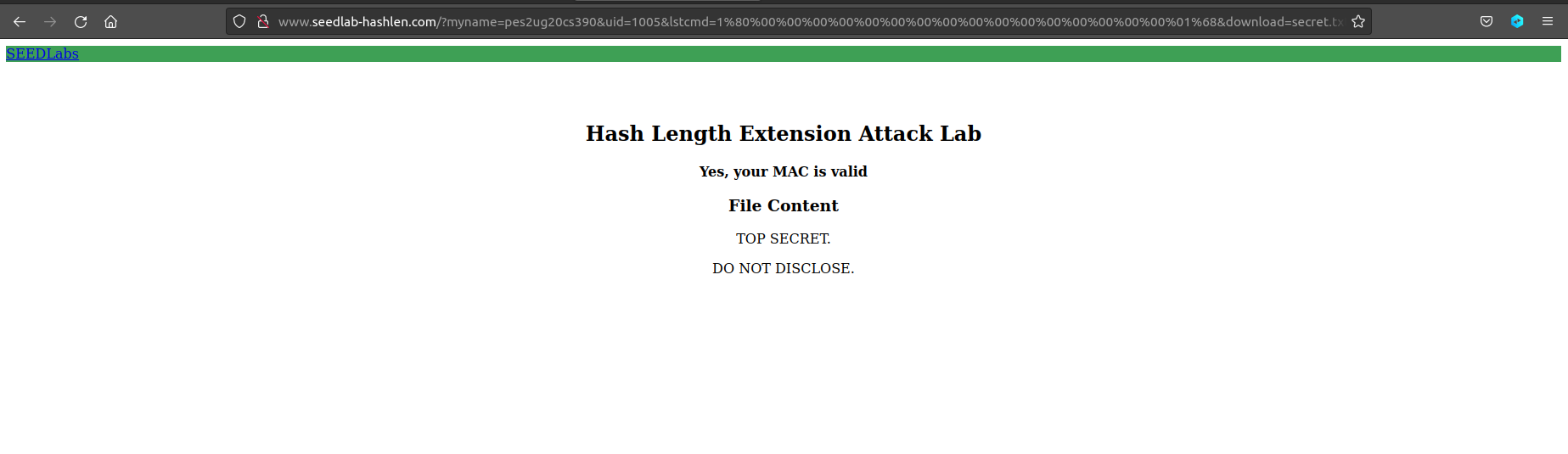
Task 2: Create Padding



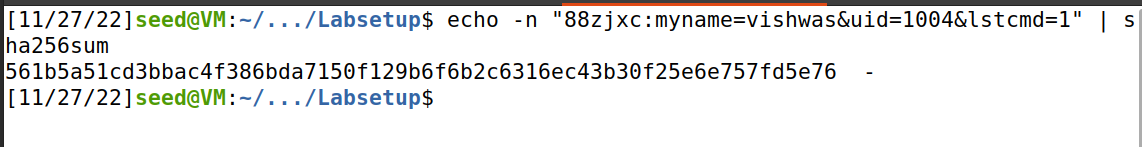
We can observe the URL and hash padding.

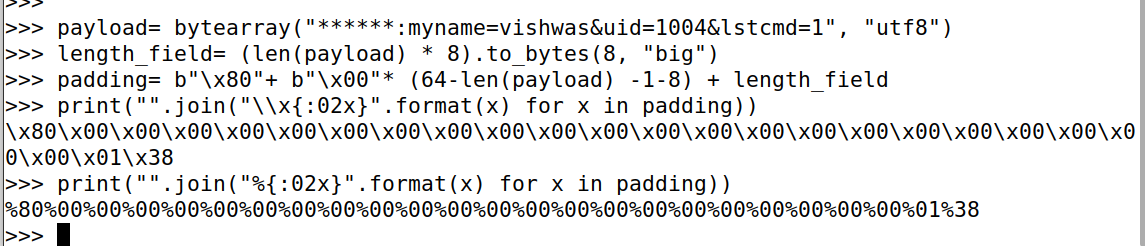
Task 3: The Length Extension Attack

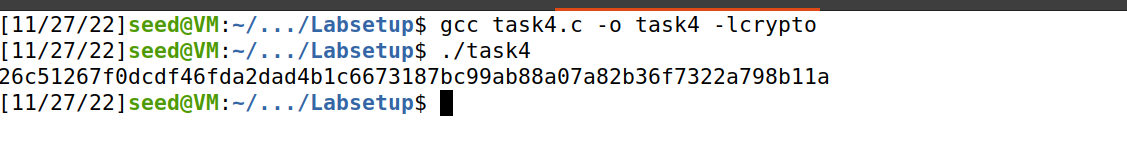


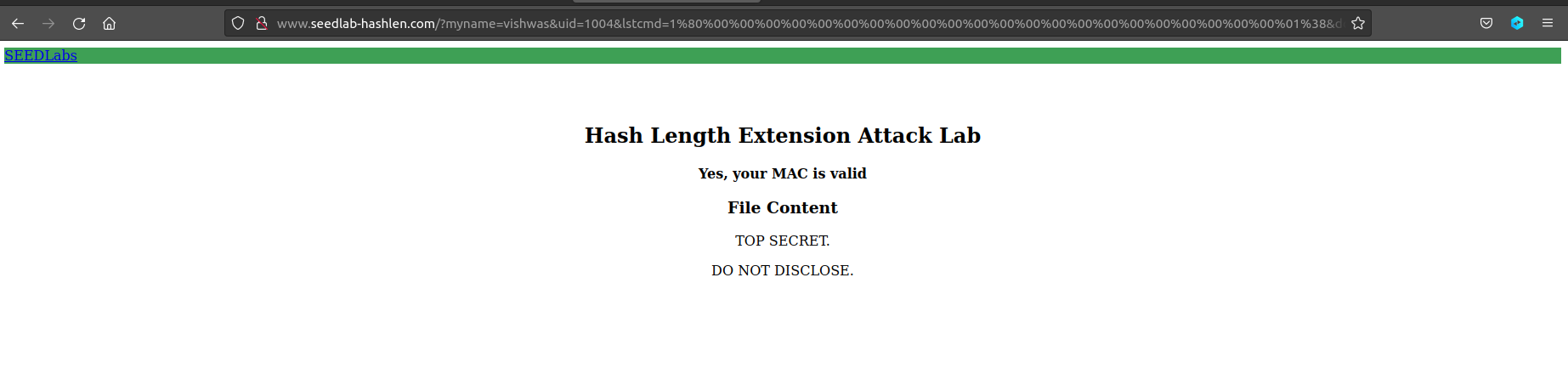


Without key:



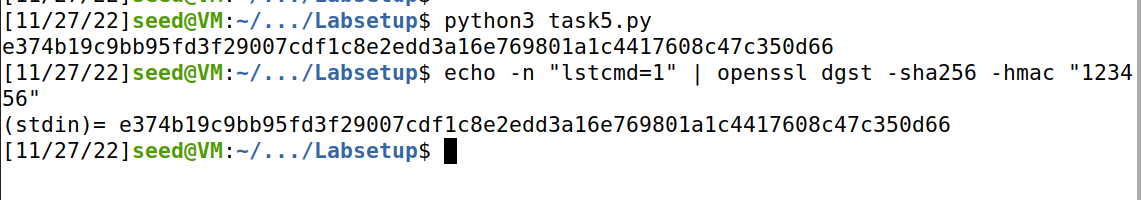






The attack is successful and we can see the contents of the file secret.txt even though it is not a valid MAC address. We do both the attacks with the key and without it.

Task4:



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.