**Applied Cryptography**

**Lab 6: Hash Length Extension Attack Lab**

Name: Siri N Shetty SRN: PES2UG22CS556

**Problem 1: Send Request to List Files**

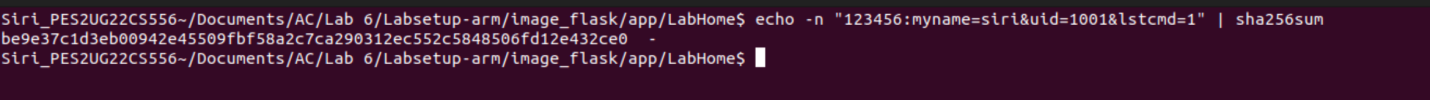
Step 1 : Finding UID.

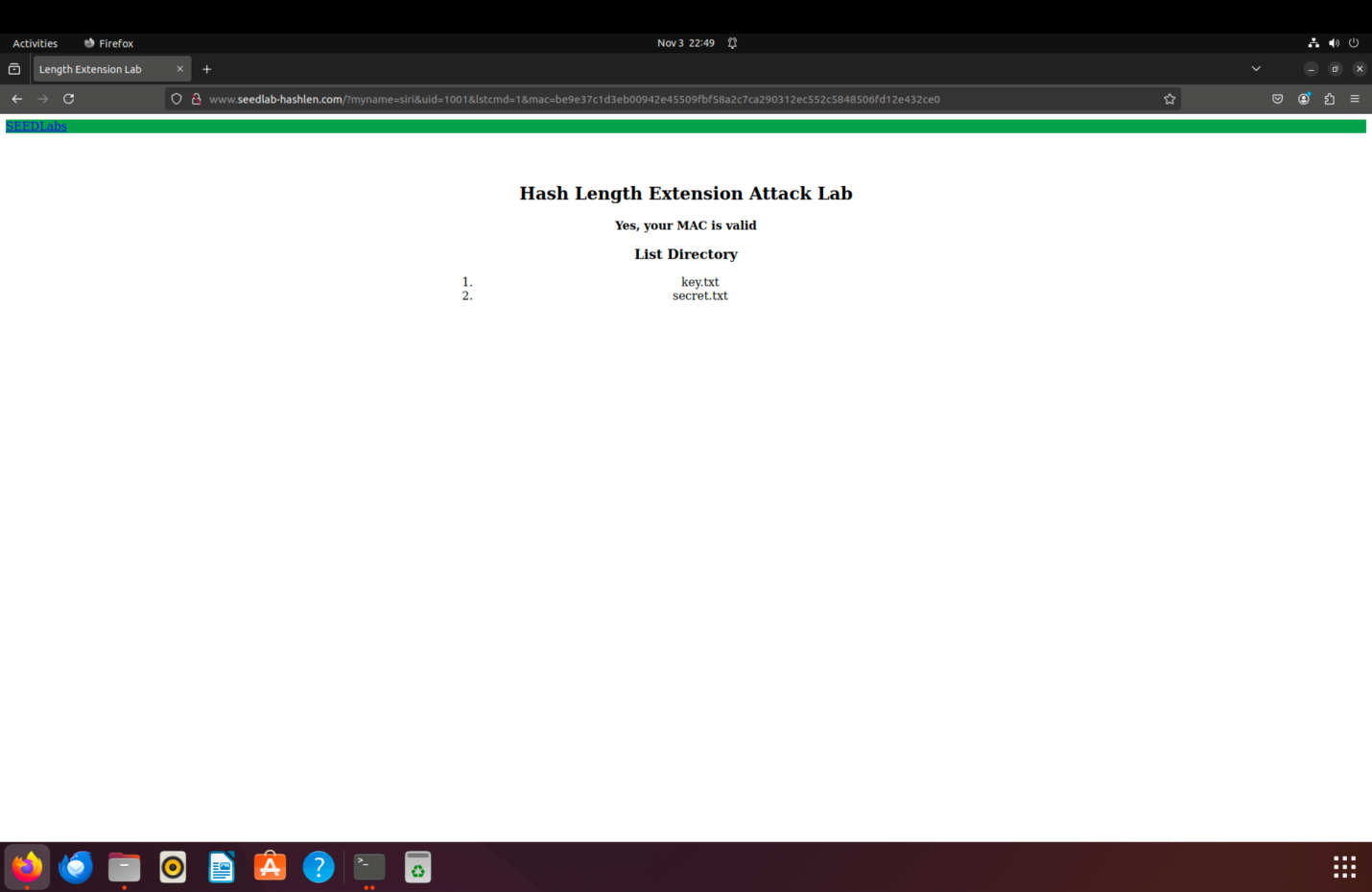
Step 2 : Calculating mac command

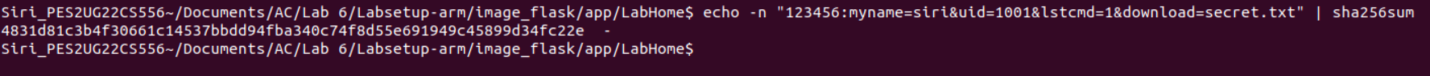
Step 3 : Sending the request

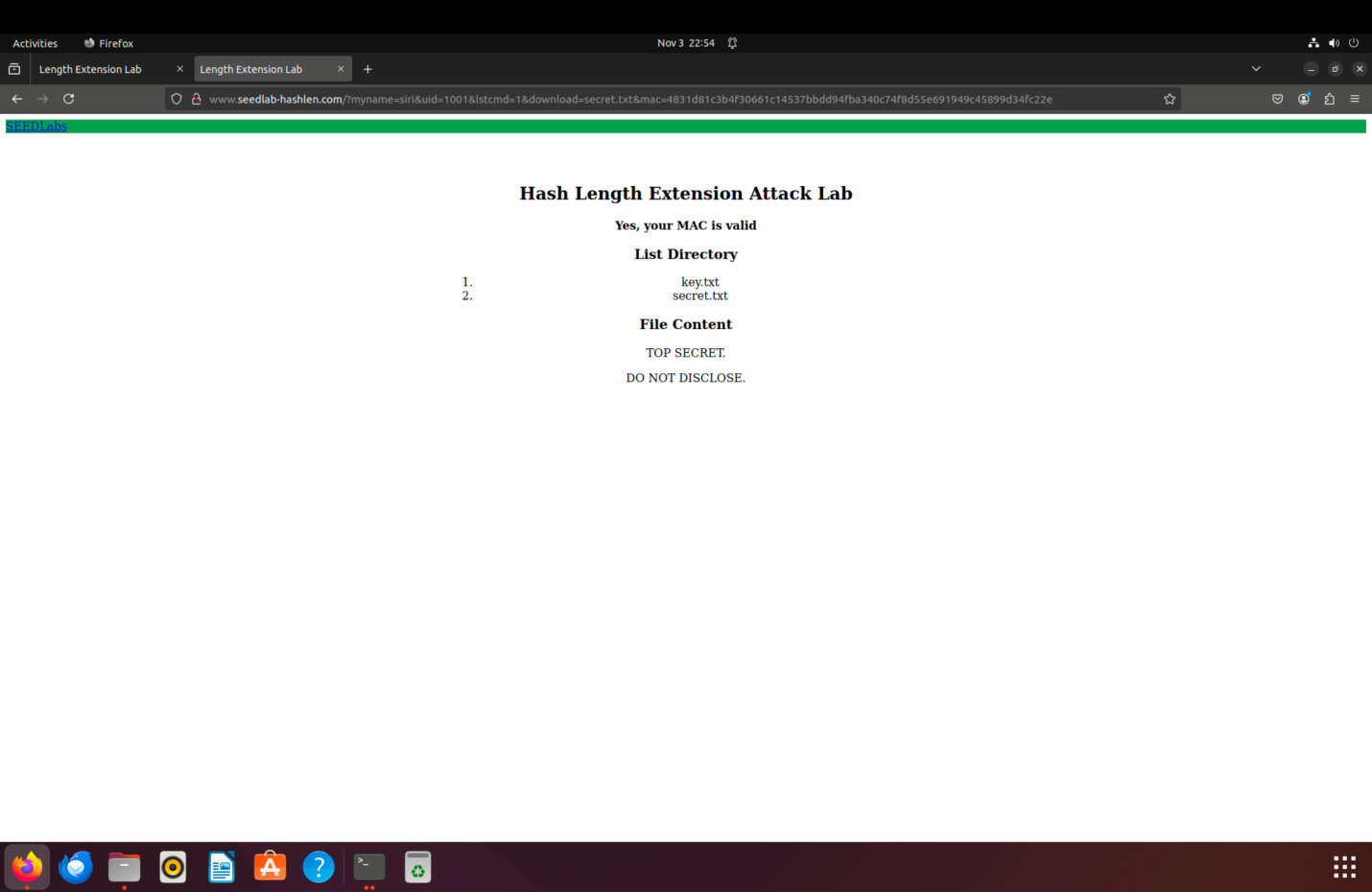
Step 4 : Cmd with download secret.txt

Step 5 : Sending request for download secret.txt

Expected Deliverables -   
i) Code Output Screenshot for step 2

ii) Code Output Screenshot for step 3

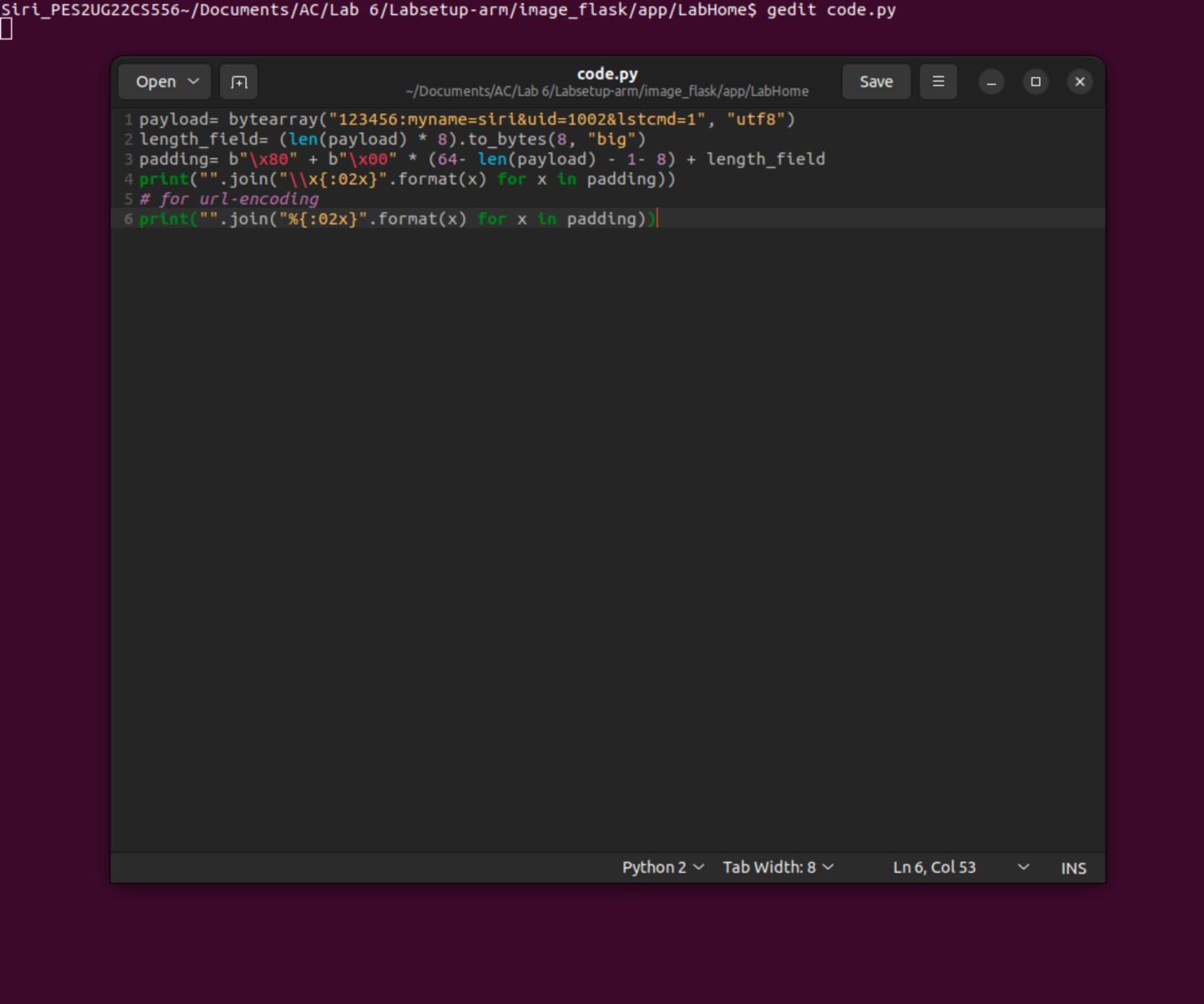
iii) Code Output Screenshot for step 4

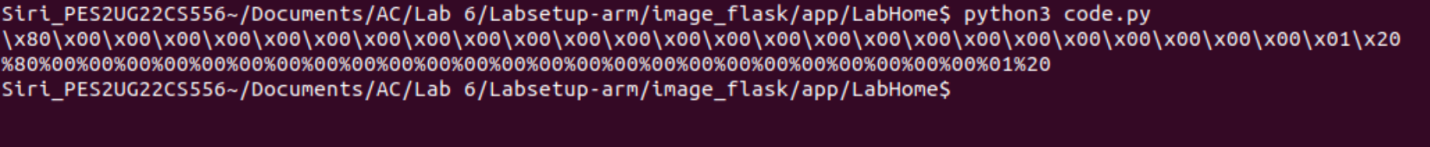
iv) Code Output Screenshot for step 5

**Problem 2 : Create Padding:**

Step 1 : Creation of code file.

Step 2 : Run the code file.

Expected Deliverables -   
i) Output Screenshot for step 1

ii) Code Output Screenshot for step 2

**Problem 3 : The Length Extension Attack**

Step 1a : Creation of code file.

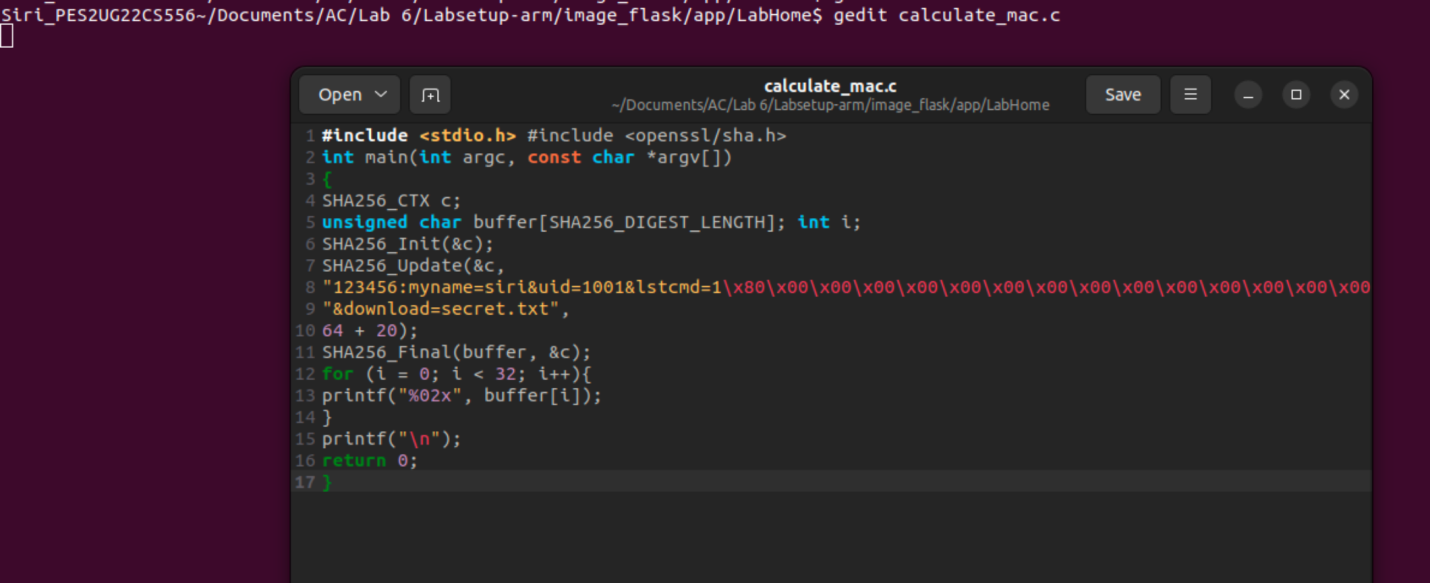
Step 1b: Compile and run the code

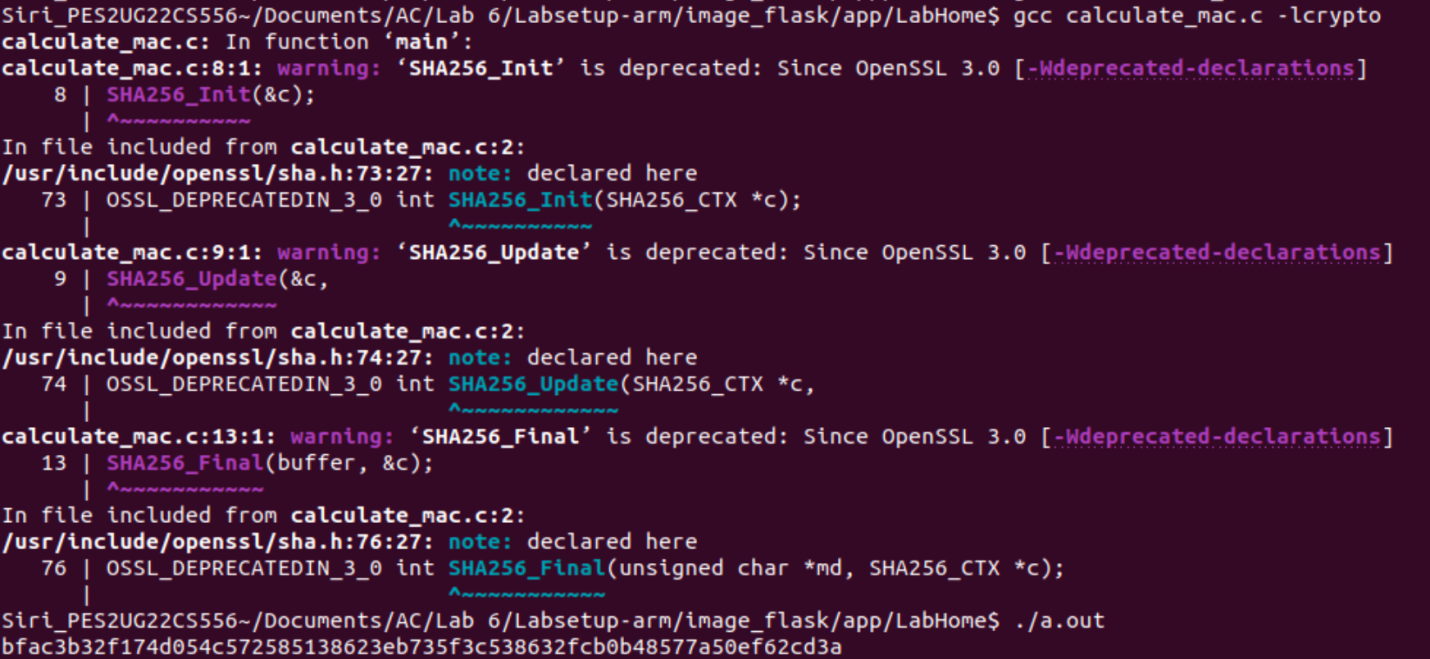
Step 2 : Loading the URL

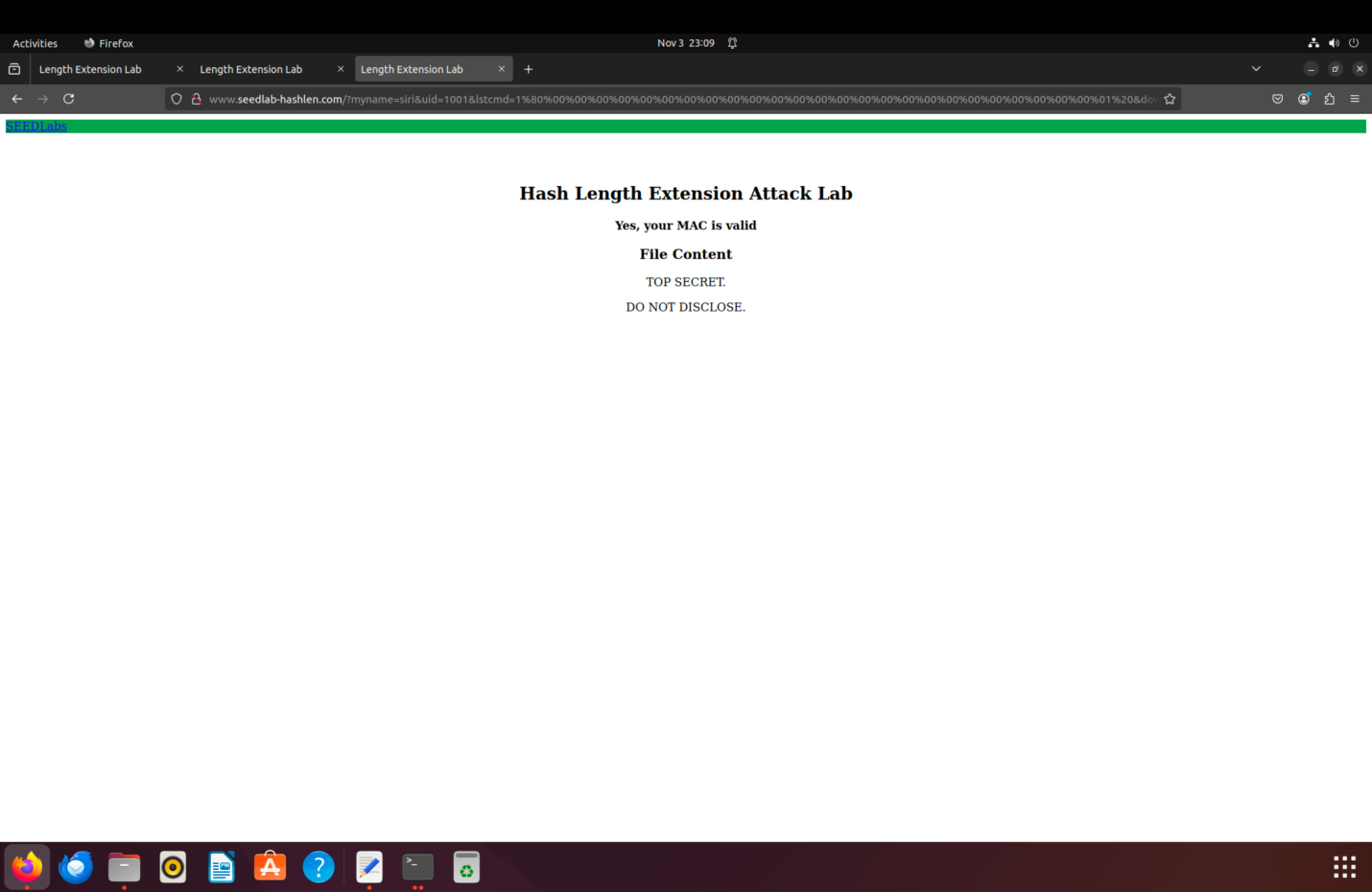
Step 3a : Generate New MAC

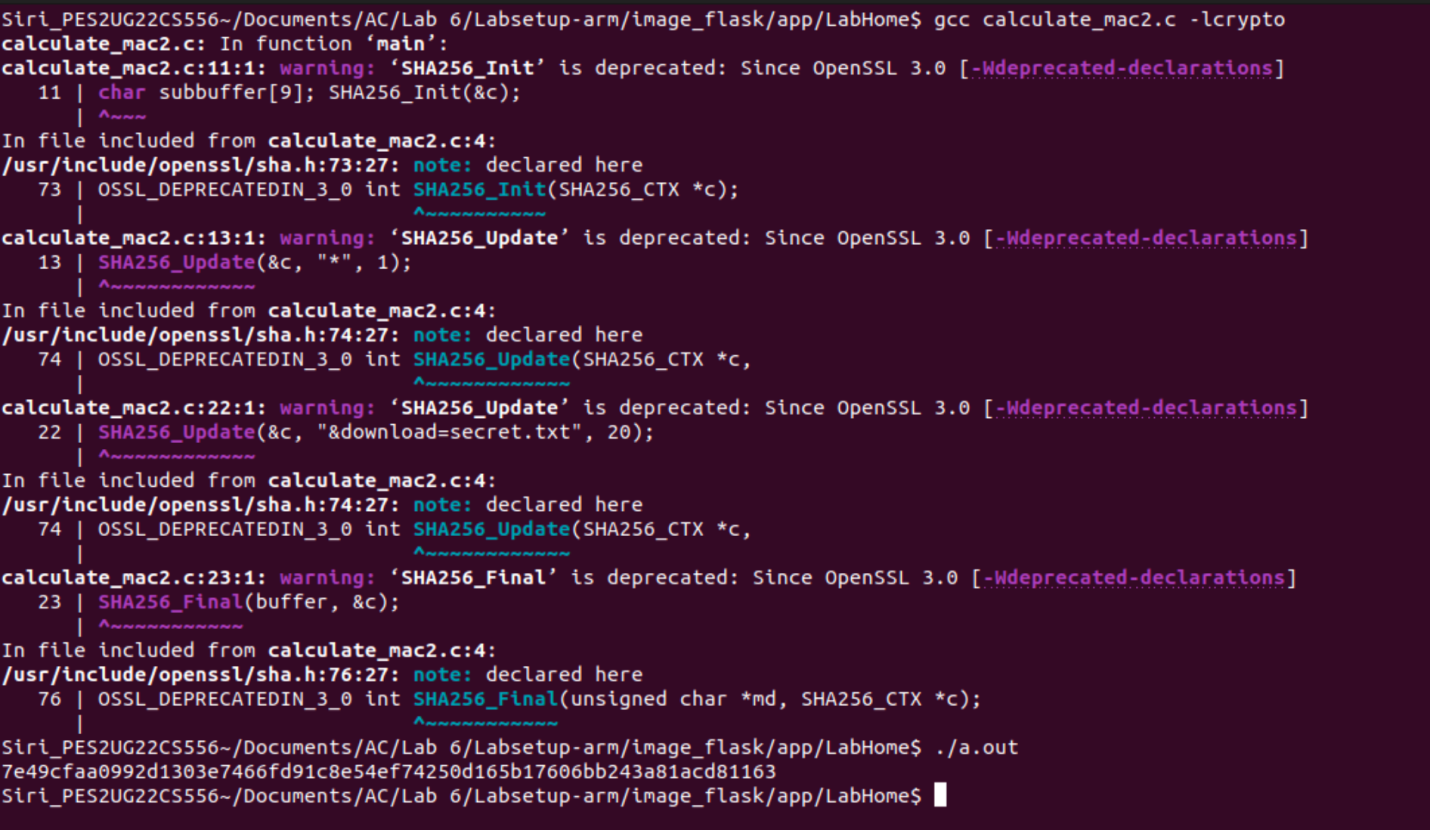
Step 3b: Generate a new padding

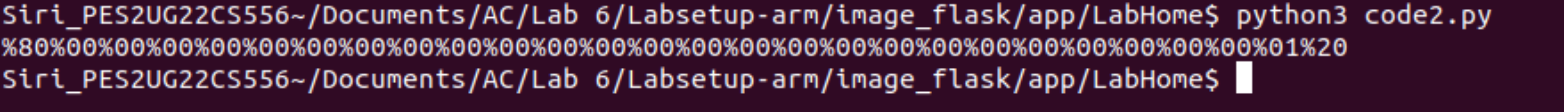
Step 4 : Visit the generated URL

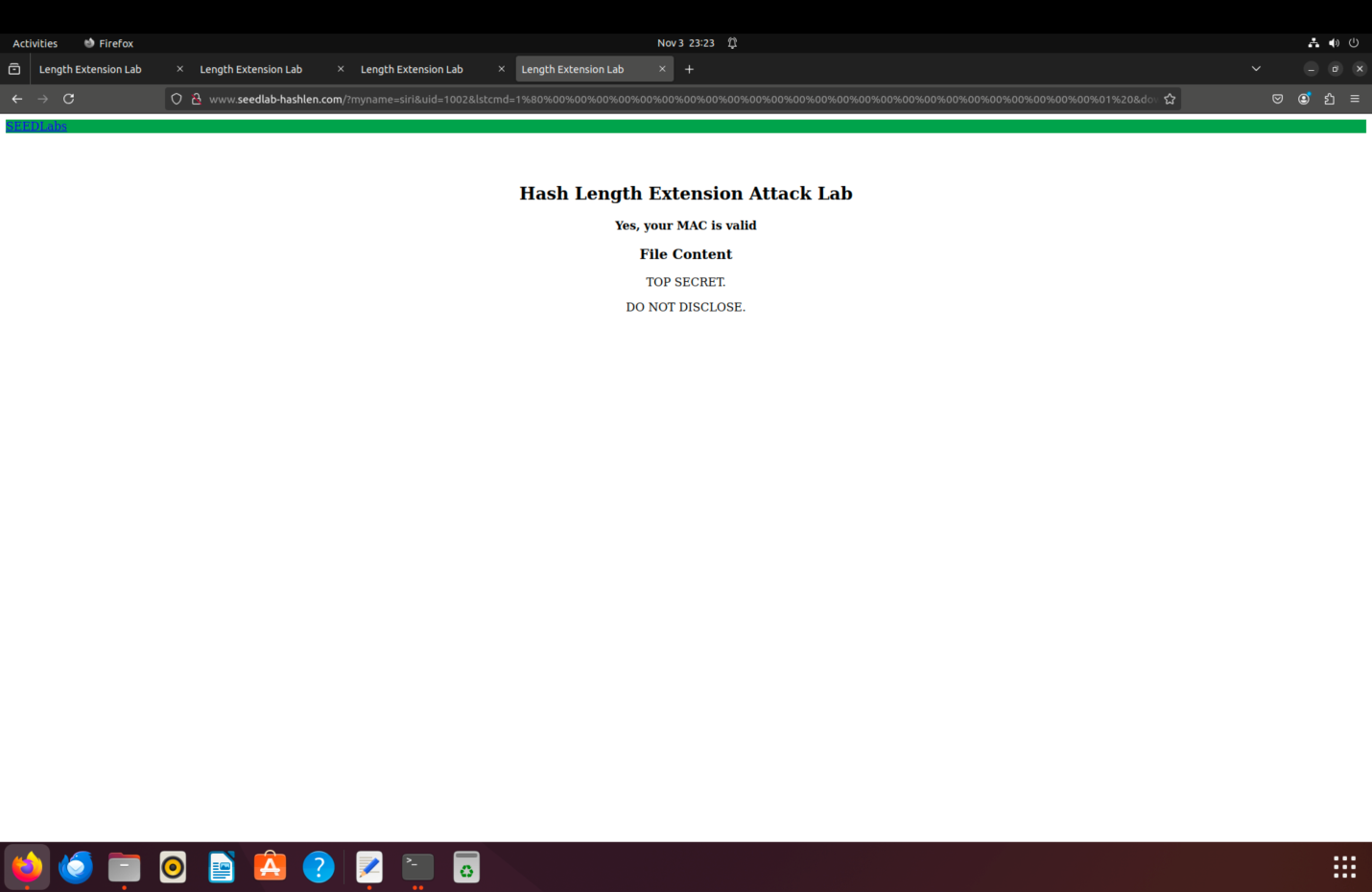
Expected Deliverables -   
i) Code Output Screenshot for step 1a

ii) Code Output Screenshot for step 1b

iii) Code Output Screenshot for step 2

iv) Code Output Screenshot for step 3a

v) Code Output Screenshot for step 3b

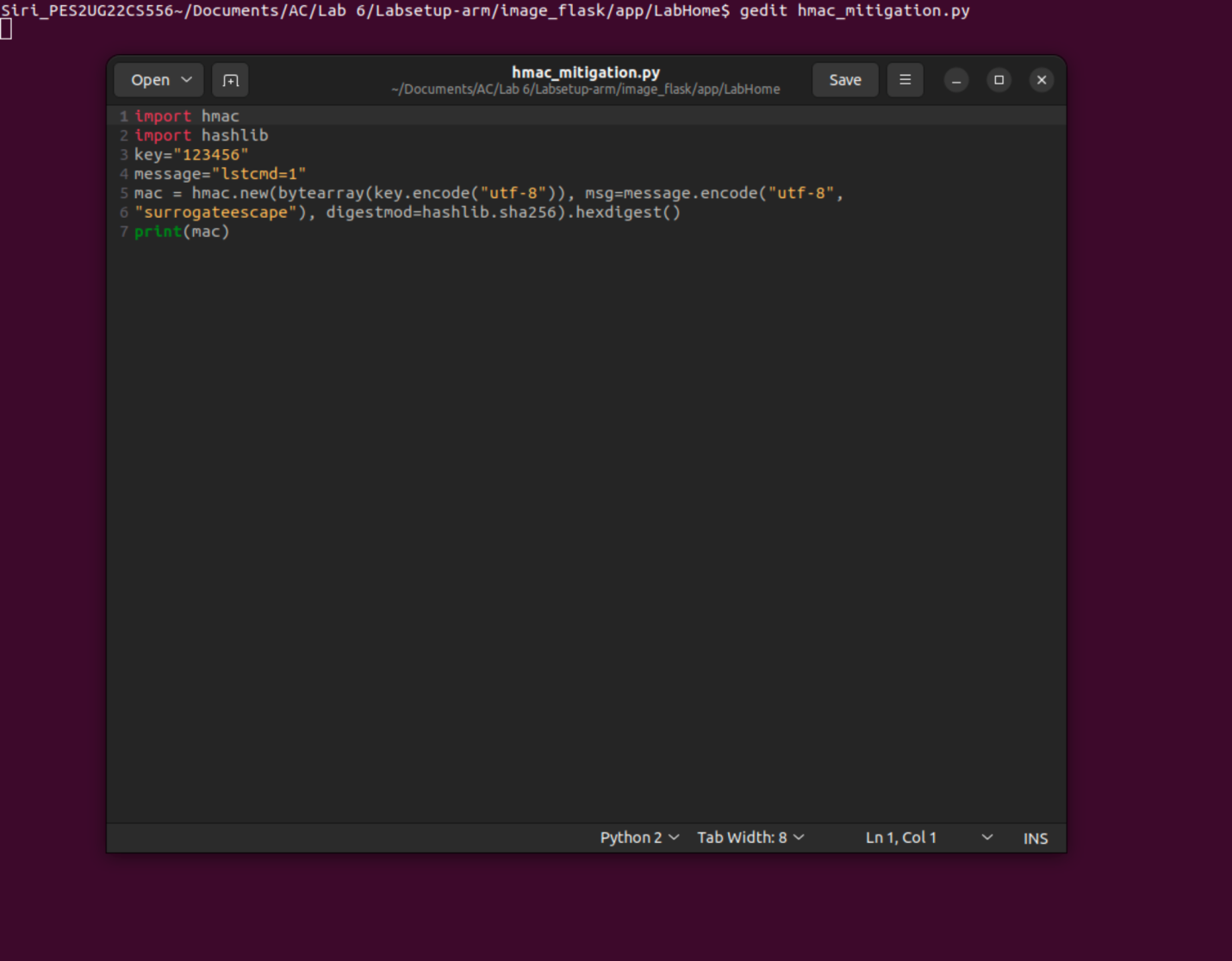
vi) Code Output Screenshot for step 4

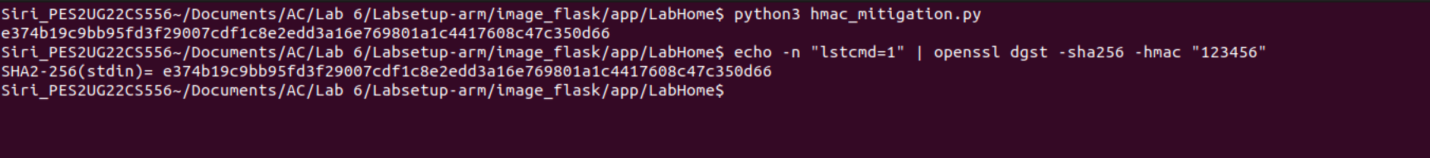
**Problem 4 : Mitigation Using HMAC**

Step 1 : Create the code file

Step 2 : Run the commands

Expected Deliverables –

i) Code Output Screenshot for step 1

ii) Code Output Screenshot for step 2

iii) Describe why a malicious request using length extension and extra commands will fail MAC verification when the client and server use HMAC.

HMAC involves using a secret key in both the generation and verification of the MAC. Unlike simple hash functions vulnerable to length extension attacks, HMAC adds security by incorporating the secret key, which prevents attackers from predicting or generating valid MACs for modified messages. This makes it resistant to length extension attacks because any modification to the message or commands would require knowledge of the secret key to create a valid MAC, which the attacker does not possess. Therefore, any malicious attempt to alter the message or add commands without the correct HMAC will fail verification.