

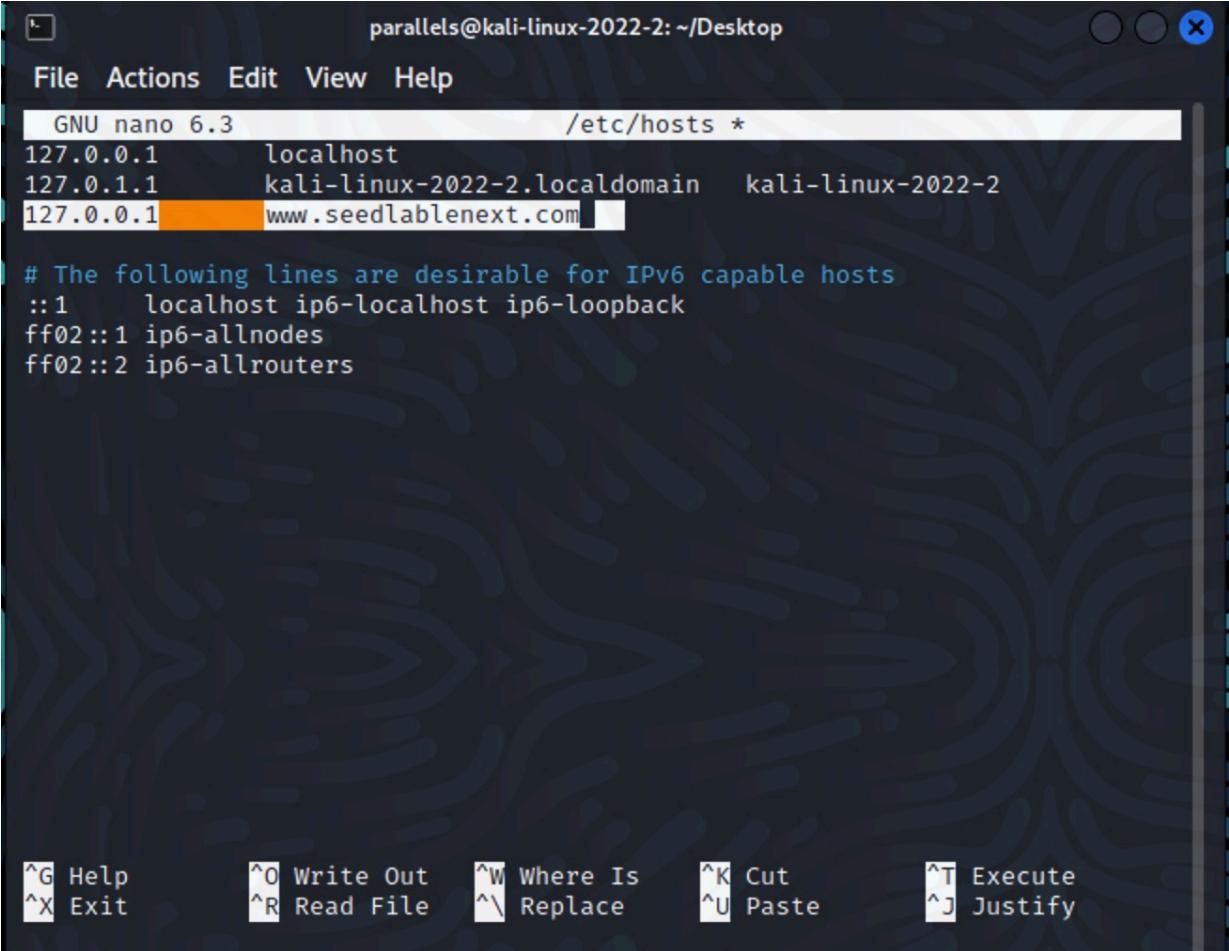
# Applied Cryptography

Name	Naman Choudhary
SRN	PES2UG20CS209
Section	D

## Hash Length Extension Attack Lab

### Lab Setup

Setting up the hostname



```
parallels@kali-linux-2022-2: ~/Desktop
File Actions Edit View Help
GNU nano 6.3          /etc/hosts *
127.0.0.1      localhost
127.0.1.1      kali-linux-2022-2.localdomain  kali-linux-2022-2
127.0.0.1      www.seedlablenext.com

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters

^G Help   ^O Write Out  ^W Where Is  ^K Cut    ^T Execute
^X Exit   ^R Read File  ^\ Replace   ^U Paste  ^J Justify
```

The server program

```
parallels@kali-linux-2022-2: ~/Desktop/server
File Actions Edit View Help
└$ sudo nano /etc/hosts

└(parallels@kali-linux-2022-2)-[~/Desktop]
└$ unzip server.zip
Archive: server.zip
  creating: server/
  inflating: server/.gitignore
  inflating: server/run_server.sh
  creating: server/www/
  inflating: server/www/lab.py
  inflating: server/www/config.py
  inflating: server/www/__init__.py
  creating: server/www/templates/
  inflating: server/www/templates/index.html
  creating: server/LabHome/
  inflating: server/LabHome/secret.txt
  inflating: server/LabHome/key.txt

└(parallels@kali-linux-2022-2)-[~/Desktop]
└$ cd server

└(parallels@kali-linux-2022-2)-[~/Desktop/server]
└$ ls
LabHome  run_server.sh  www

└(parallels@kali-linux-2022-2)-[~/Desktop/server]
└$
```

```
└(parallels@kali-linux-2022-2)-[~/Desktop/server]
└$ ./run_server.sh
* Serving Flask app "www" (lazy loading)
* Environment: development
* Debug mode: on
* Running on http://127.0.0.1:5000/ (Press CTRL+C to quit)
* Restarting with stat
* Debugger is active!
* Debugger PIN: 445-062-230
```

## Task 1:Send Request to List Files

Calculating the MAC address

```
(parallels㉿kali-linux-2022-2)-[~/Desktop/server]
└─$ cd LabHome

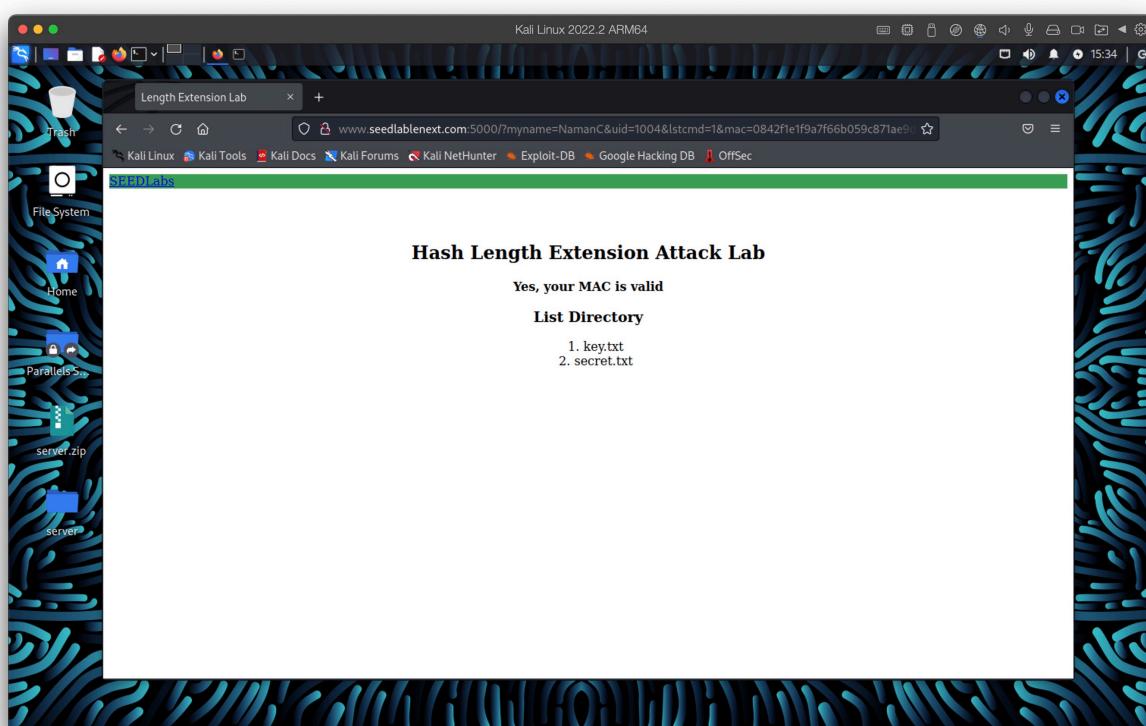
(parallels㉿kali-linux-2022-2)-[~/Desktop/server/LabHome]
└─$ ls
key.txt  secret.txt

(parallels㉿kali-linux-2022-2)-[~/Desktop/server/LabHome]
└─$ cat key.txt
1001:123456
1002:983abe
1004:98zjxc
1005:xcuijk

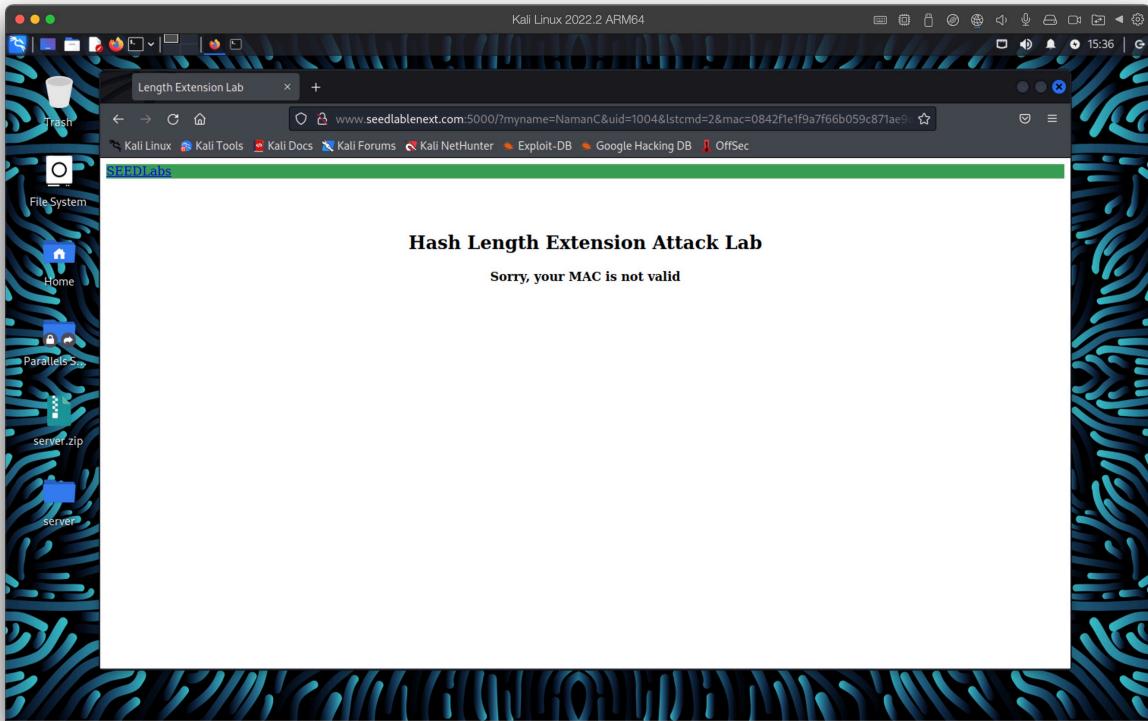
(parallels㉿kali-linux-2022-2)-[~/Desktop/server/LabHome]
└─$ echo -n "98zjxc:myname=NamanC&uid=1004&lstcmd=1" | sha256sum
0842f1e1f9a7f66b059c871ae9d7cd22311cf356173c3b4feab45e46dac5003f

(parallels㉿kali-linux-2022-2)-[~/Desktop/server/LabHome]
└─$
```

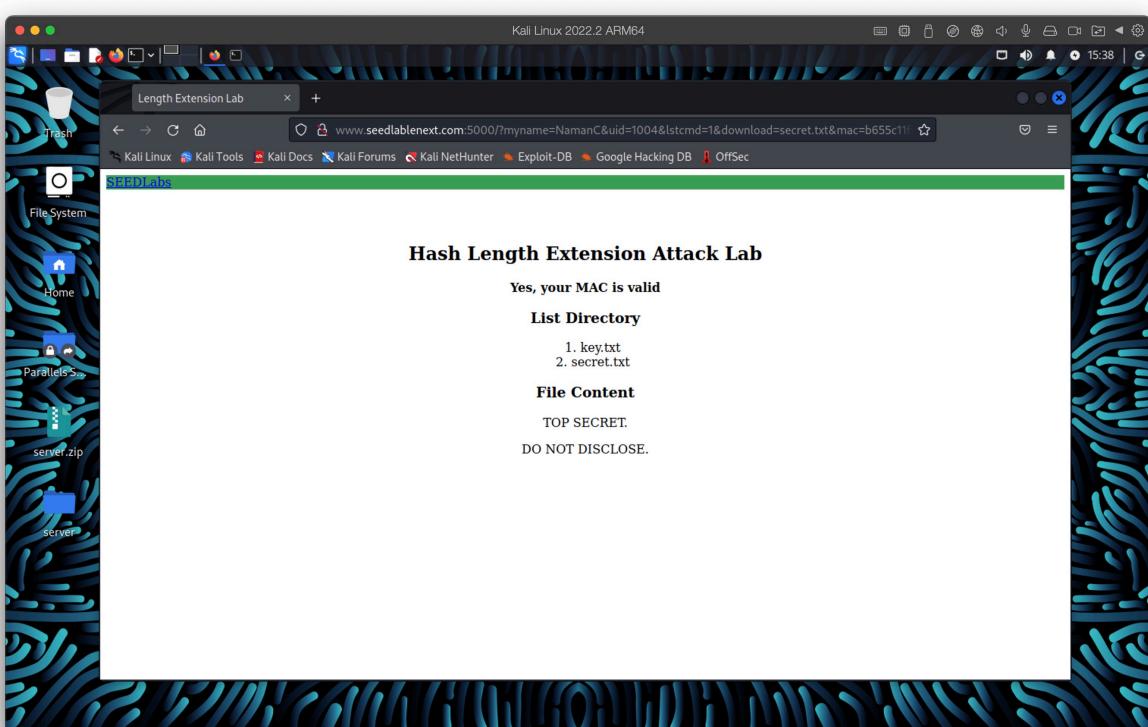
Result on the website



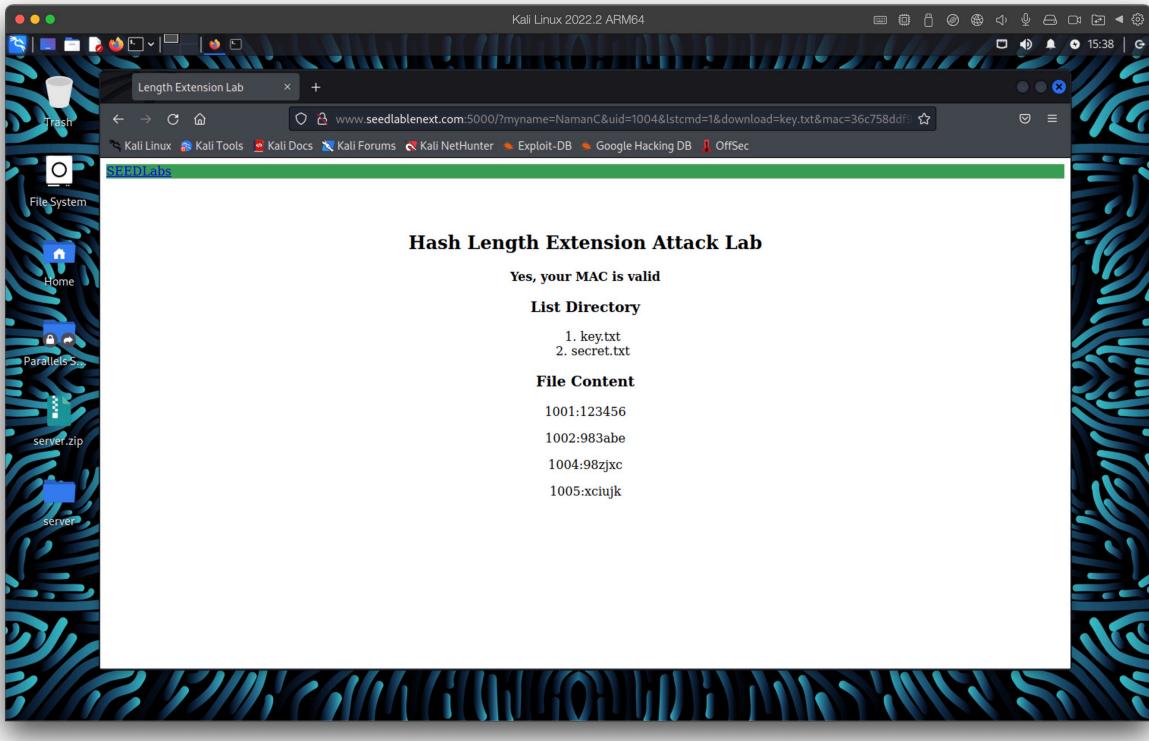
When an invalid MAC is given



### Contents of secret.txt



### Contents of key.txt



## Task 2:Create Padding

A screenshot of a terminal window on Kali Linux. The terminal shows Python code generating a payload and printing padding bytes. The code uses `lenfield=(len(payload)\*8).to\_bytes(8,'big')` and `padding=b'\x80' \* b'\x00'\* (64-len(payload)-1-8) + lenfield` to create a payload of length 64. It then prints the padding bytes. In the background, a browser window shows the 'Hash Length Extension Attack Lab' page with the message 'Yes, your MAC is valid' and a list of files and their hashes.

## Task 3:Compute MAC using Secret Key

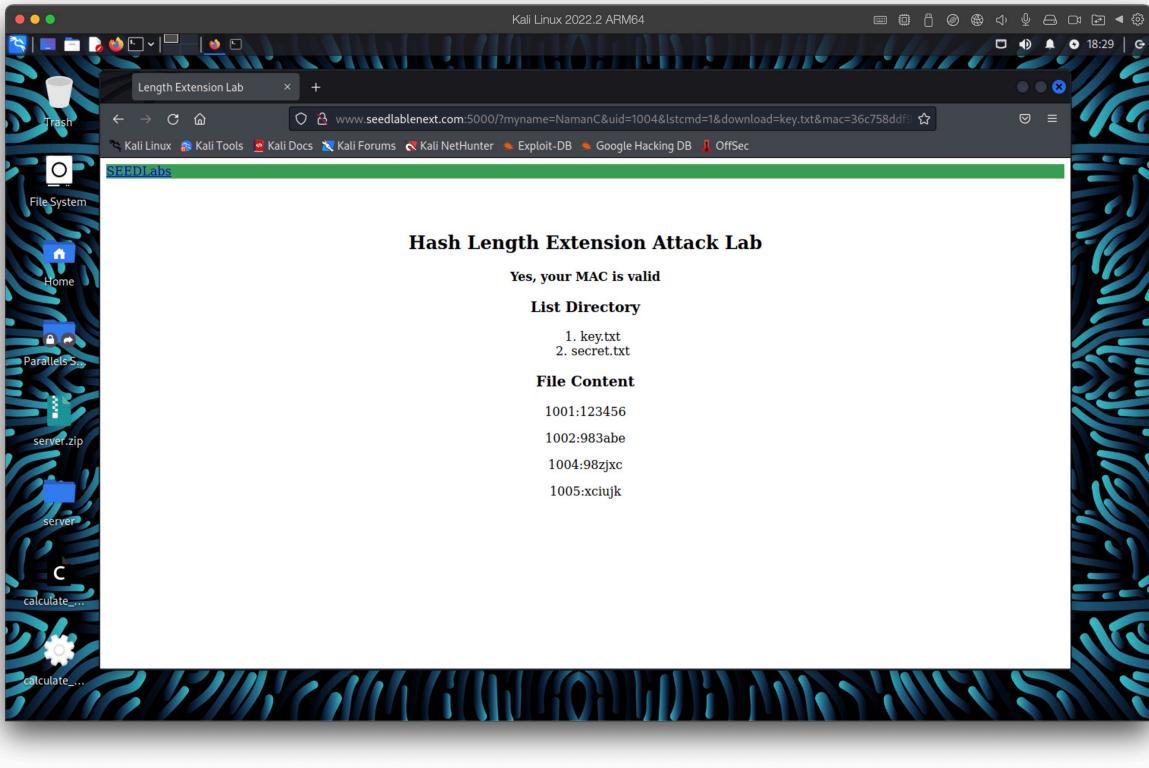
## Using Python to create padding

```
(parallels㉿kali-linux-2022-2)-[~/Desktop]
$ gcc calculate_mac.c -o calculate_mac -lcrypto -w

(parallels㉿kali-linux-2022-2)-[~/Desktop]
$ ./calculate_mac
eb71f88b08909fa9fe582c994a6f620b739045287104bf44fad9a2d0e28d6bf3

(parallels㉿kali-linux-2022-2)-[~/Desktop]
$
```

## Website output

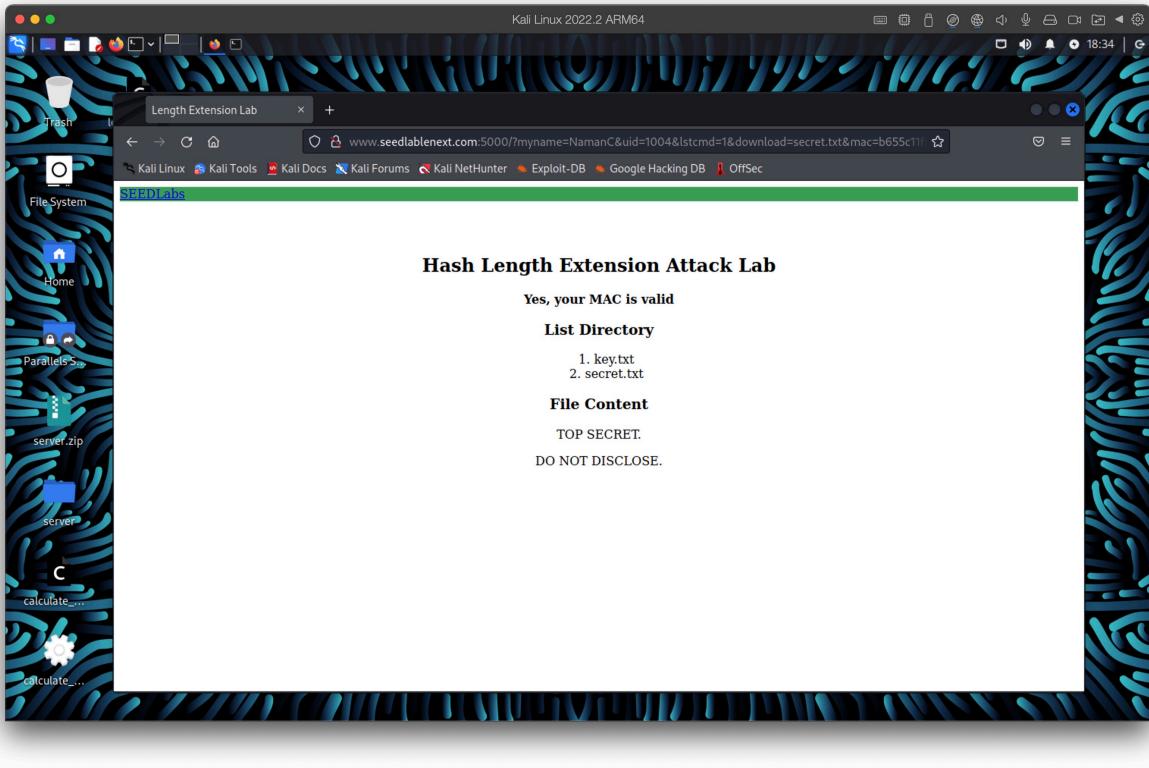


## Task 4: Length Extension Attack

```
(parallels@kali-linux-2022-2) [~/Desktop]
$ gcc length_ext.c -o length_ext -lcrypto -w

(parallels@kali-linux-2022-2) [~/Desktop]
$ ./length_ext
eb71f88b08909fa9fe582c994a6f620b739045287104bf44fad9a2d0e28d6bf3
```

Website output



## Task 5: Attack Mitigation using HMAC

Using Python to calculate HMAC

```
>>> import hmac
>>> import hashlib
>>> key='98zjxc'
>>> message='lstcmd=1'
>>> hmac.new(key.encode('utf-8')),msg=message.encode('utf-8','surrogateescape'),digest
mod=hashlib.sha256).hexdigest()
'b2bfbb4f616a5bebc13642dae5606d02aa693cc091f251dd2f1e7d03bd9acd10'
>>> █
```

File Content

TOP SECRET  
DO NOT DISCLOSE.