哈尔滨工业大学（深圳）

《密码学基础》实验报告

Hash 长度扩展攻击实验

学　院: 计算机科学与技术

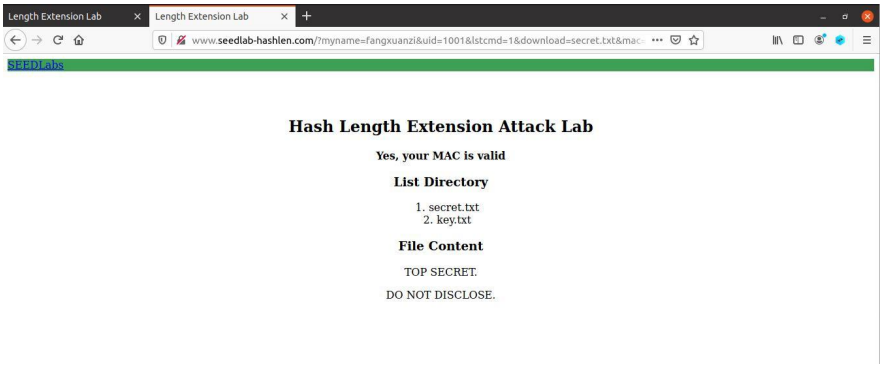
姓　名: 房煊梓

学　号: 210010101

专　业: 智能强基—计算机

日　期: 2023-10-19

1、 请发送一个`download`命令到服务区，myname 的信息修改为你自己的姓名拼音，并且记录你得到的响应内容（截图显示）。



2、 为消息<key>:myname=<name>&uid=<uid>&lstcmd=1 创建对应 padding，其中`<key>`和`<uid>`的实际内容应该从`LabHome/key.txt`文件中得到，myname 依然用你自己的姓名。

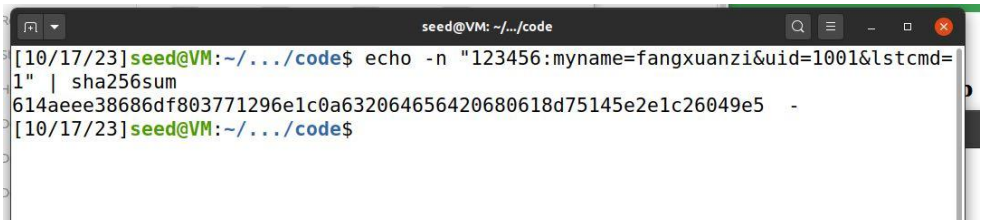
结果类似这样，红色部分可以参考代码换成 AAAAAA，不影响填充的内容：

```
123456:myname=SEEDManual&uid=1001&lstcmd=1
%80%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%01%50
```

```
[10/17/23]seed@VM:~/.../code$ chmod +x compute_padding.py
[10/17/23]seed@VM:~/.../code$ ./compute_padding.py
AAAAAA:myname=fangxuanzi&uid=1001&lstcmd=1%80%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00
%01%50
[10/17/23]seed@VM:~/.../code$
```

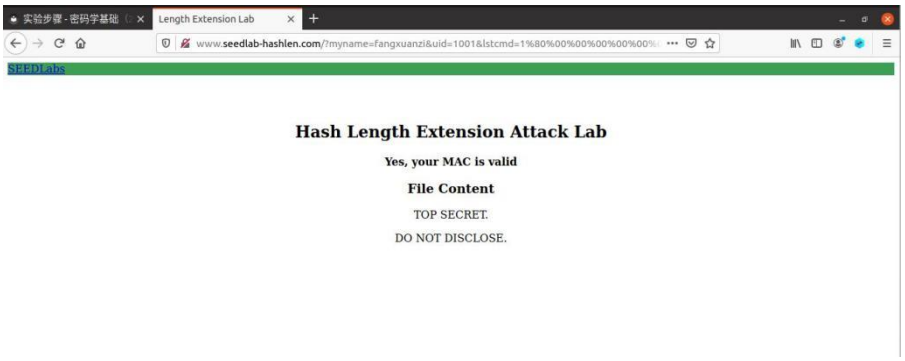
3、 为下面的请求生成一个有效的 MAC，其中`<key>`和`<uid>`的实际内容应该从`LabHome/key.txt`文件中得到，name 就是自己的姓名拼音。

http://www.seedlab-hashlen.com/?myname=<name>&uid=<uid>&lstcmd=1&mac=<mac>



4、 发送构造好的新请求到服务器，padding 是上面获取到的信息，记录收到的服务器响应并截图。

http://www.seedlab-hashlen.com/?myname=<name>&uid=<uid>&lstcmd=1<padding>&download=secret.txt&mac=<new-mac>



5、 用 HMAC 算法修改代码后，记录使用长度攻击的结果，根据收到的服务器响应进行截图。