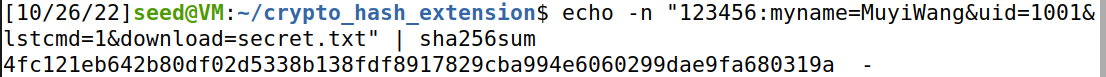
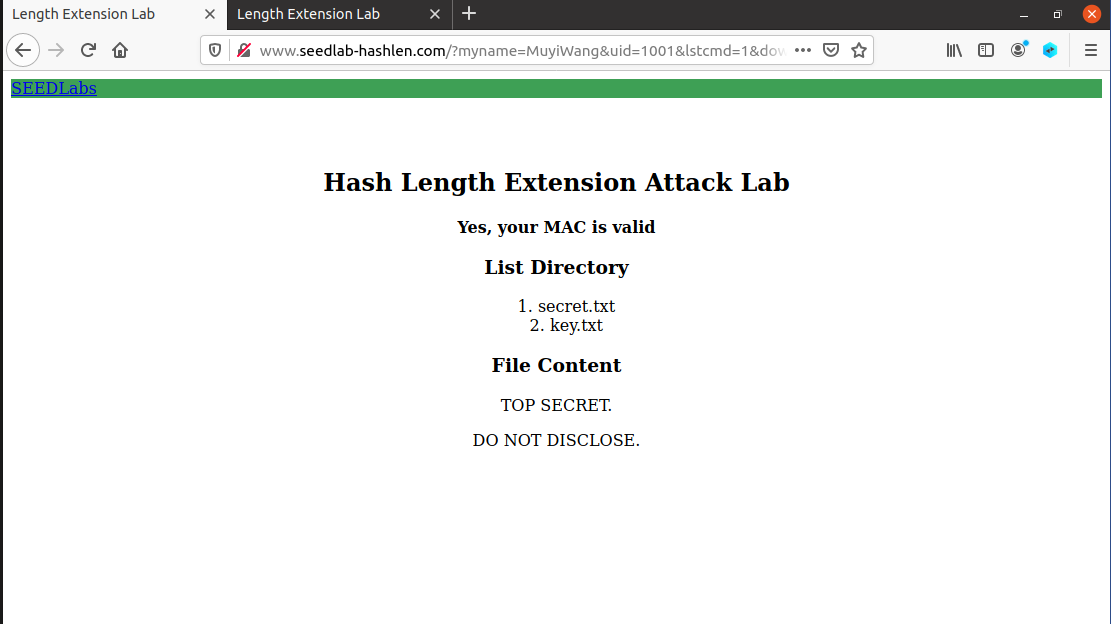
|  |
| --- |
| 哈尔滨工业大学（深圳） |
| **《密码学基础》实验报告** |
|  |
| Hash长度扩展攻击实验  学 院: 计算机科学与技术   |  |  | | --- | --- | | 姓 名: | 王木一 | | 学 号: | 200210231 | | 专 业: | 计算机科学与技术 | | 日 期: | 2022-10-26 | |

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. 计算mac



1. 访问

[www.seedlabhashlen.com/?myname=MuyiWang&uid=1001&lstcmd=1&download=secret.txt&mac=<](http://www.seedlabhashlen.com/?myname=MuyiWang&uid=1001&lstcmd=1&download=secret.txt&mac=%3c)上面生成的mac>



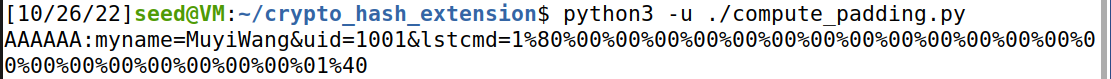
（实际这里应该是lstcmd=0，当时做的时候没注意到，不过也不影响download）

1. 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

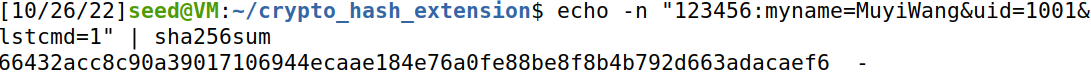
%80%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%01%50



1. 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>*



1. 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。

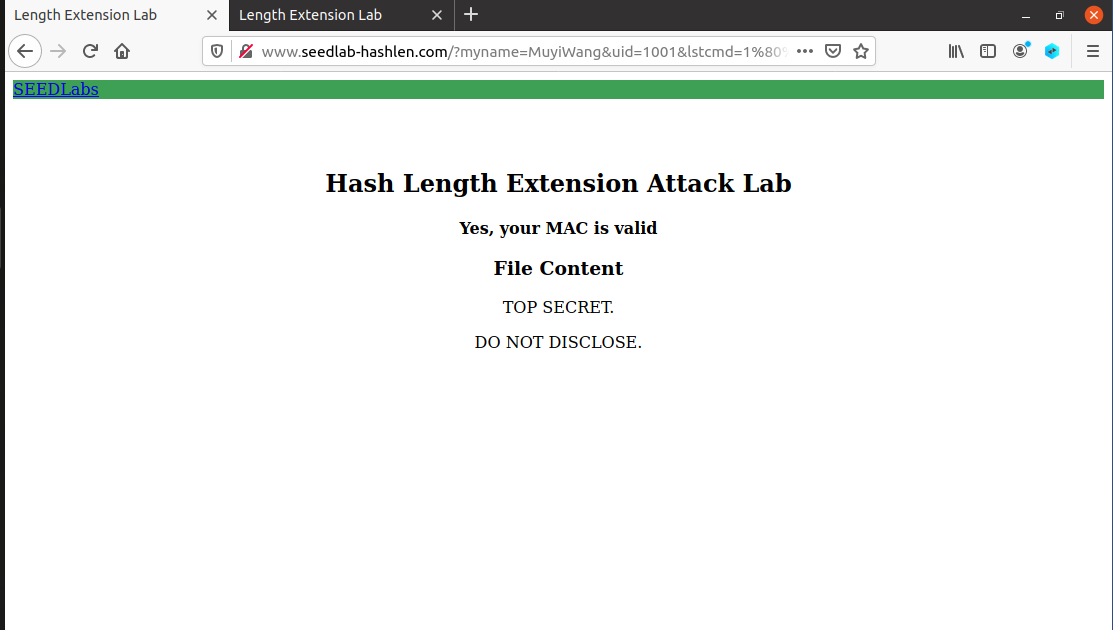
http://www.seedlab-hashlen.com/?myname=<name>&uid=<uid>

&lstcmd=1<padding>&download=secret.txt&mac=<new-mac>

1. new-mac生成



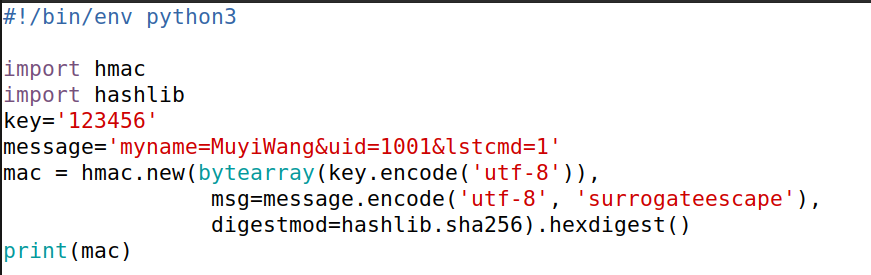
1. 进行长度攻击





1. 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。
2. 正常访问（改为HMAC后正常使用lstcmd=1命令）

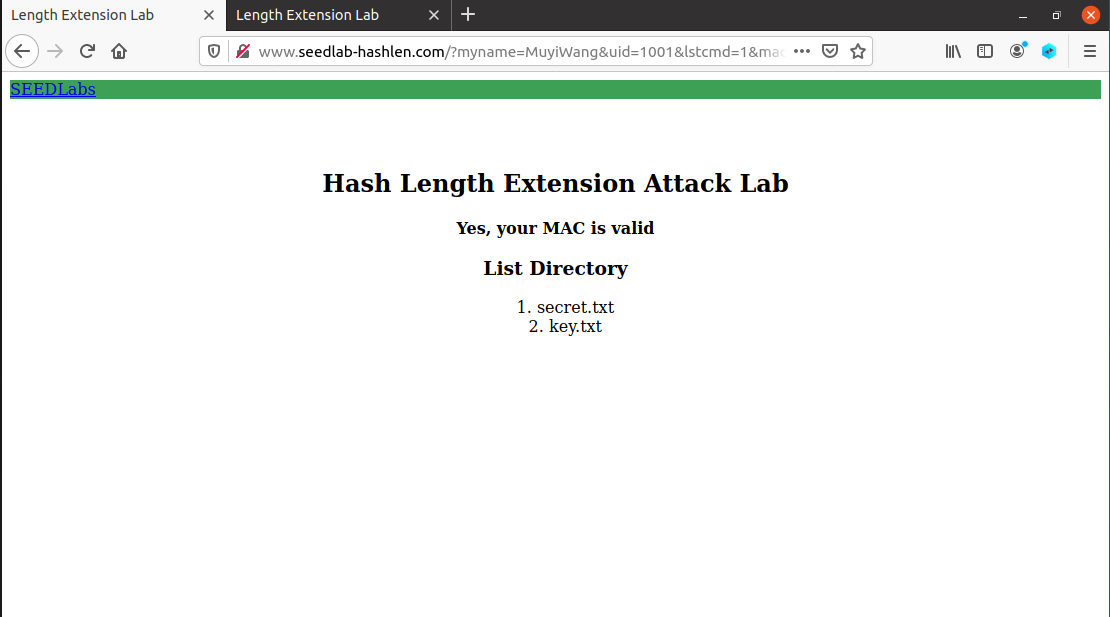
修改mac生成函数



生成mac

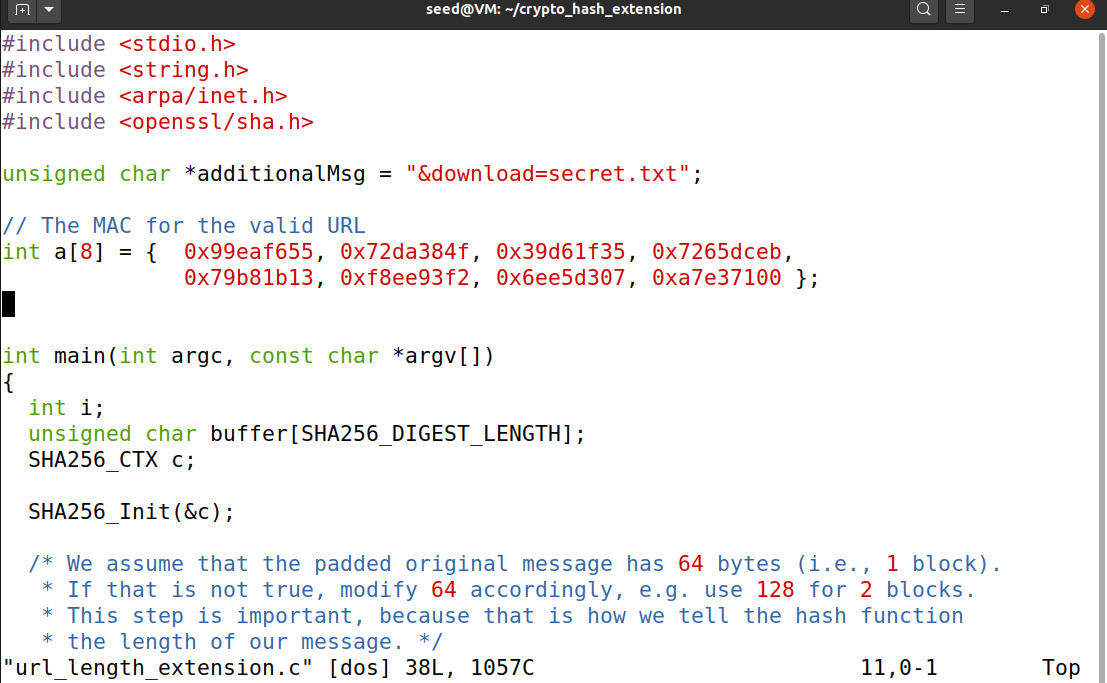


访问成功



1. 敌手在不知道已经换成HMAC的情况下进行长度攻击，仍和之前一样计算padding，计算新mac

生成new-mac





访问失败

