**Computer Security HW0x9**

R08946007 資科所 蔡昀達

Nickname : r08946007

**Cathub Party**

1. 使用requests 設定cookie來跟server溝通拿到加密的flag
2. 根據上課助教透露，使用Padding oracle attack
3. 先將flag做base64 decode還有url unquote，因為這兩個卡很久QQ，通靈許久才發現
4. 從最後一個byte做xor把它變成合法的padding來搜正確的明文，訊息出現”What the flag”是decrypt出錯，”Your flag seem strange”是明文不符合，用這樣的方式去找出正確的flag
5. 最後解出來的flag是LAG{EE0DF17A410C90F86E88471346B6DA77E8C878200B37E60C53E9A56913211465}

不知道為什麼F不正確還在尋找原因但還是過了XD