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