b06705001 資管 3 楊力行 b06705001

HW9

這題我發現 flag 的長度雖然不同，但是與他之中的%的數量有關，因此我猜他是用 url 編碼過的，果然，在我進行轉碼之後 flag 都統一變成的 128 字節的字串，接著利用 padding oracle attack，從 1 到 255 由最後一位開始進行 XOR 再對題目進行 request，若成功 request，就可根據成功的數字得出有多少個填充的位元接著再挨個得對非填充的密文進行 XOR 查找應該就可以解出，但是因為我對於 request 語法的不熟悉，我沒能成功地解出來答案。