CTF hw9

> b05902127 劉俊緯

Oracle's Revenge

> flag{\xb5_O2ac1e_is_Ev3rywher3\x05\x05\x05\x05\x05}

- 利用CBC的cipher可變動msg的原因，達到將vc的長度變成0，成功繞過vc檢查。
- 首先，既然要利用block的cipher來控制msg，那麼就必須挑一個無害的參數。不然被改爛的cipher解回去就會炸掉。因為pwd並沒有做任何事，所以pwd是一個可以改爛的好選擇。
- 再來，我們稍微分析一個msgpack就可以知道：除了開頭的magic number以外，其他都是用len(key),key,len(value),value來存成一串bytes的。而這些規則都是有機可尋。例如長度就是\xa0 + len()。
- 因此我們稍微控制一下長度，就可以讓我們比較好改寫vc長度。而詳細構造大概是長這樣。

```
1234567890123456
----------------
-*usr*01234*pwd*
0123456789012345
678901234567*vc*
```

  - * 表示長度。一開頭的-表示magic number。
- 因此就把這串打上去，在將第二個block的最後一個bytes^(0xda)^(0xa0)，就能把原本是0xda的長度改成0x0a。因此vc就會變成一個空字串。
- 而我們接下來把改寫的token還回去，在輸入一個enter，就可以繞過去了。