[hw0x09] writeup

莊翔旭, woolninesun, b04902083

Oracle's Revenge

漏洞：msgpack format
如果 `user = b'A'\*5, password = b'A'\*28`，packed message 會長成 `b'\x83\xa3usr\xa5AAAAA\xa3pwd\xbcAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\xa2vc\xda\x00(' + [40 bytes of vc]`。
`b'\xa2vc\xda'` 會在第三個 block 尾端，取出前三個 block，然後把 `b'\xda'` 變成 `b'\xa0'` 再傳空的 VC 就可以拿到 FLAG 了