Yusa的密码学课堂-CBC第一课

发表于 2021-03-05 更新于 2021-03-15 分类于 Challenge， 2020， SWPU CTF 2020， Crypto
Challenge | 2020 | SWPU CTF 2020 | Crypto | Yusa的密码学课堂-CBC第一课

点击此处获得更好的阅读体验

WriteUp来源

官方WP

题目考点

- *CBC翻转*

解题思路

这一题的考点是CBC的字节翻转，需要对CBC模式具有一定了解

可见在解密时是先进行AES解密，随后异或iv(或者前一组密文)才得到明文。

在这一题中，我们的用户名在二组（除去iv），所以在第二次交互我们修改第一组密文的对应字节，就可以让用户名对应的字节翻转。

改了第一组密文的一个字节后，解密时整个明文会乱掉，不满足`yusa*4`的条件，对此我们需要最后一次交互改整个iv，计算规则就是: `原来的iv^第一组明文(乱)^"yusa"*4`

- ***本文作者：** CTFHub*
- ***本文链接：** https://writeup.ctfhub.com/Challenge/2020/SWPU-CTF-2020/Crypto/jhDNJ3rS2q5PZAS8FrUKJj.html*
- ***版权声明：** 本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2020 # Crypto # SWPU CTF 2020
Yusa的密码学课堂-ECB
miniobs