Login-Error

发表于 2021-01-08 分类于 Challenge ， 2020 ， CSICTF ， Crypto
Challenge | 2020 | CSICTF | Crypto | Login-Error

点击此处获得更好的阅读体验

WriteUp来源

https://dunsp4rce.github.io/csictf-2020/crypto/2020/07/21/Login-Error.html

by `raghul-rajasekar`

题目描述

> *We forgot our credentials, help us to get the flag.*

题目考点

解题思路

On connecting to the server, we are presented with a prompt like this:

```
We implemented a really cool AES-encryption for our login, however in the process we forgot the username and password to the admin account.
We don't remember the exact credentials but the username was similar to c?i and password similar to c?f.
When we entered 'user:c?i' and 'pass:c?f' the portal spit out 2 hex strings :
74fe40821832d516552c931cb75dca4b5122d18d66c0d31361724e305cf103e1
74fe40821832d516552c931cb75dca4b9f06c892f2c94c75e8dd185410621e0a
The only way to login now is to enter 2 hex strings which decrypt to the correct credentials.
Enter username hex string :
Enter password hex string :
Error!!
```

Out of the two ciphertexts given, the first halves of each are the same. Hence, this is an indication that perhaps the first halves are a common IV value and the second halves are the encryptions of the plaintexts using AES in CBC mode. In CBC mode, the first block of plaintext is obtained by decrypting the first ciphertext block and XORing it with the IV value. Since only one block is present here, by changing the IV value sent for decryption, we could change the decrypted plaintext to anything we want. For example, for the username, assuming `user` *is a* `bytearray` *containing the AES encryption of* `"user:c?i"`*, we could turn it into a valid encryption of* `"user:csi"` *by doing* `user[6] ^= ord('?') ^ ord('s')`*, and similarly for the password. Submitting these new values gives us the flag.*

Flag

```
csictf{Sh4u!d_hav3_n0t_u5ed_CBC}
```

- *本文作者：* *CTFHub*
- *本文链接：* *https://writeup.ctfhub.com/Challenge/2020/CSICTF/Crypto/ePRE3csJpZfUDHfdZ9fiBF.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 # CSICTF
Quick Math
Rivest Shamir Adleman