KevOrr [fithack-2017] Added crypto/encryption-program-leaked Latest commit f75ddd9 17 days ago

..

Cryptographic_program.py	[fithack-2017] Added crypto/encryption-program-leaked	17 days ago
README.md	[fithack-2017] Added crypto/encryption-program-leaked	17 days ago
sol.py	[fithack-2017] Added crypto/encryption-program-leaked	17 days ago

README.md

Crypto - Encryption Program Leaked

Description

> The encryption program and secret key leaked out!!
>
> key = eglafdsewafslfewamfeopwamfe encrypt = 5857342f555c2528182b55175e5f543a14540a0617394504380a0e52

Attachments

Cryptographic_program.py

Solution

We are given a python script that takes a message and a key, and "encrypts" the message. Of course, it's not actual encryption, and they're essentially just XORed together. Pseudocode for the encryption program:

```
message = 'FIT{flag...}'
key = 'eglafdsewafslfewamfeopwamf'

message, key = pad_end(reversed(message), key, fillvalue=0)
encrypted = xor(message, key)
```

This of course can be reversed by finding `reversed(xor(message, key))` .

We are given the key and the ciphertext, which is hexdumped, so first we need to get the original ciphertext. After that, we reverse the encryption using the above scheme. Once we do that we get the string `RklUe2Ixcl9uM192d3JoMV83NX0` . This looks like base64-encoded data. When we decode this, we get the flag.

Flag

```
FIT{b1r_n3_vwrh1_75}
```