DateMarch 5, 2017 | **Name ***

[Pragyan CTF] Evil Corp

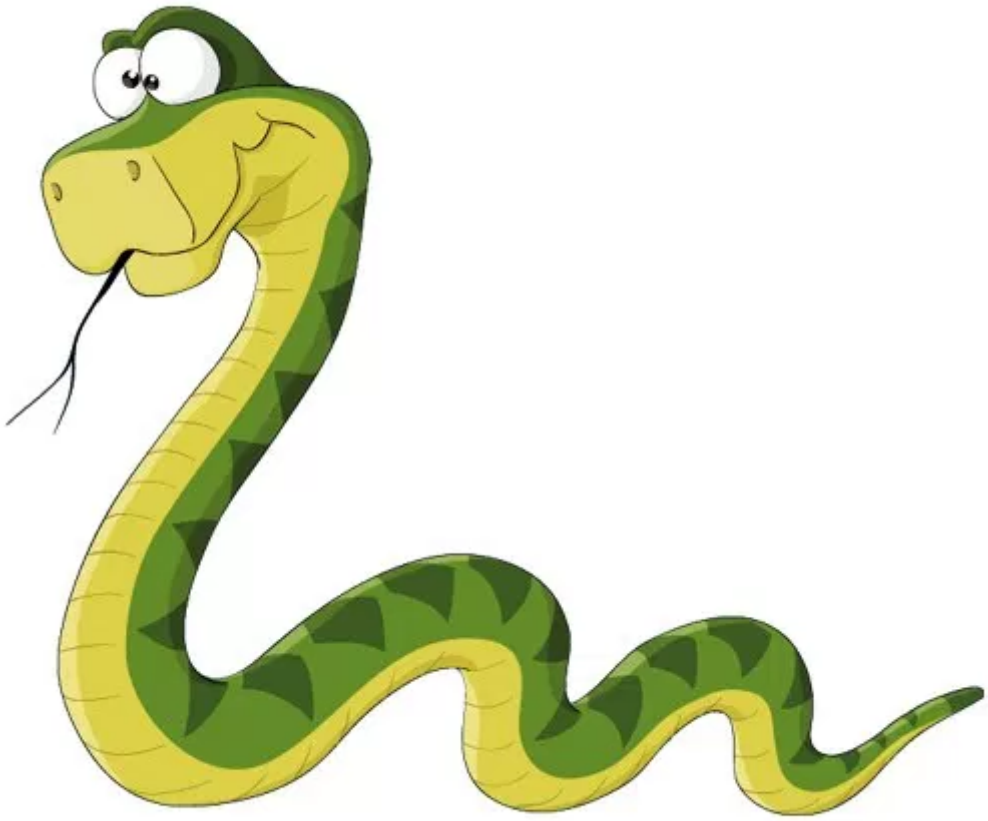
Standard

Description:

> fsociety has launched another attack at Evil Corp. However, Evil Corp has decided to encrypt the .dat file with a CBC cipher. Reports reveal that it is not AES and the key is relatively simple, but the IV might be long. And remember, fsociety and evilcorp are closely linked.
>
> **Hint!** Snakes serve the fsociety. Hmmm.
>
> **Hint!** fsociety and evilcorp are too close, even 16 characters long together. Damn
>
> fsociety_new.dat

This challenge was tricky for lot of people, the riddle was hiding in the questions itself. The challenge doesn't require high skills, just understanding the meaning behind the words and hints.

From the question we know it's a CBC cipher, but which? I got it just after the first hint was released, something to do with **snakes**. hmm... Serpent! Serpent is another term for Snake, and there's Serpent-CBC cipher.

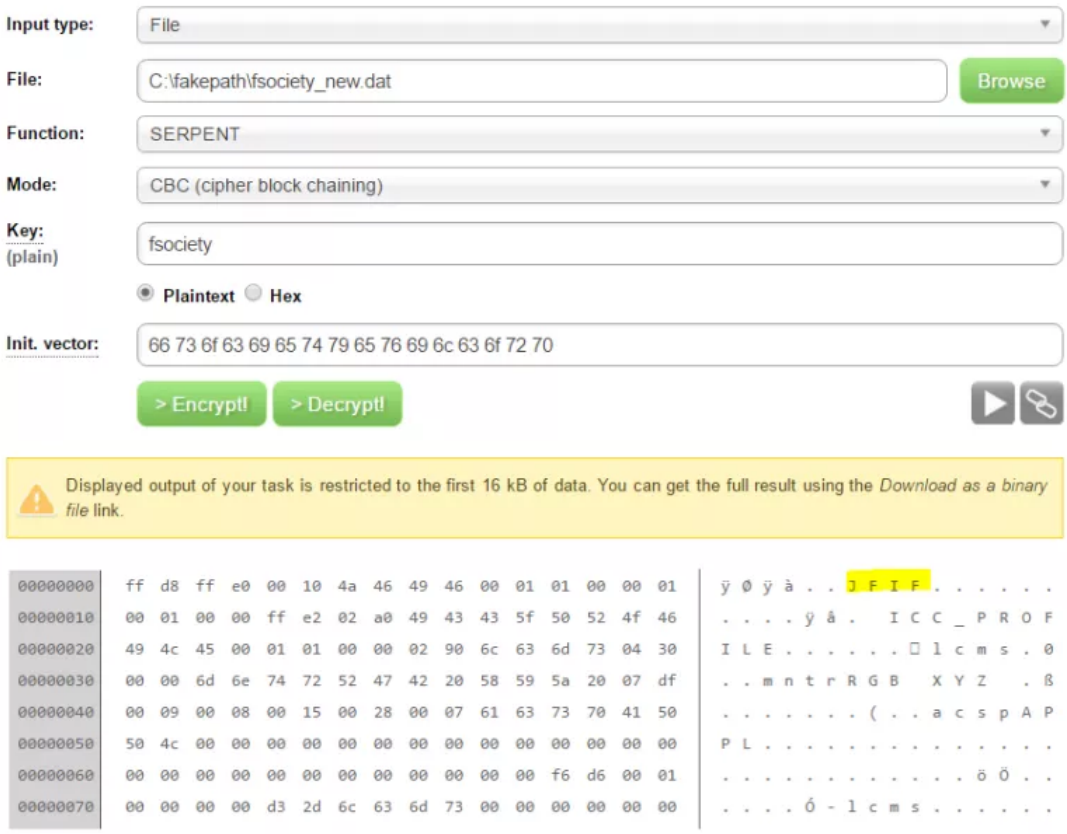


What about the IV? We know several things about the IV:

1. The length of Serpent-CBC IV must be 32 bytes,
2. Most of the Serpent decrypters are taking the IV as hex sequence
3. in the question: "but the IV might be long"
4. in the Hint: "even 16 characters long together...fsociety and evilcorp are closely linked".

So, this made me believe that the IV is "fsocietyevilcorp" because len(hex("fsocietyevilcorp"))==32.

So we now know the algorithm and the IV, what is the Key? The question says "the key is relatively simple". So I tried online with some simple and "obvious" keys until I recognize a valid header of file and found that the key was "*fsociety*".



We got a leet JPEG image with the flag:

The flag was **pragyanctf{hellofriend}**
