BRO64

Author: BIT SENTINEL

[Publish Date]

European Cyber Security Challenge

1.Initial Write-Up

Description

Betaflash, let's go to Cuba and dance amigo !!

The flag is with brackets ('ctf{sha256'}) but you have to submit it in the CTF{sha256} format.

Find the flag.

2.Challenge specifications

- Category: Cryptography
- Difficulty: Medium
- Estimated time: 1h – 2h

3.Questions and answers

What is the flag ?

ctf{f38deb0782c0f252090a52b2f1a5b05bf2964272f65d5c3580be631f52f4b3e0}

4.Artefact hashes

FILES	MD5	SHA256
deployment.yaml	E12B8626B299F38475C0404626A17411	885C805FD6E9CB742267C0B1F13C759ABA532640349CDC28B11B38C0AE1C3612
docker-compose.yml	9FD241DA9B6977FA62A8BB083101F9BD	20EC028091A915F24E5A054E92DB244097A8365248CDC0EC57D46B46F4399848
Dockerfile	5B66EBB2427BFF87BED57161913B4133	487613B6877AFCF3BD9C2E68C4F0FA73869D791F734067F3BAF7E87ED1653735
server/app.py	1439C7C690C2C4B837F9CB0959B654FD	C86334236CBBC3EE7EC985E732C0A22365E9DC5DE8FB0FB660C0F31DB8D1CEAD
solver/solver.py	E293301C83D4918B787A777F9619E112	DD4205BE055E7020CF02527C119ABAA34B969B16D5A5D626CB256D5FE85A2E14

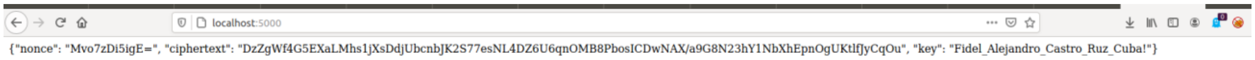
5.Tools needed

- sudo apt-get Install python2
- sudo apt-get Install python2-dev
- sudo apt-get install python2-pip
- pip2 install flask
- pip2 install pycryptodome

6.Walkthrough (writeup)

The challenge is chacha20 encryption.

1) Go to localhost:5000

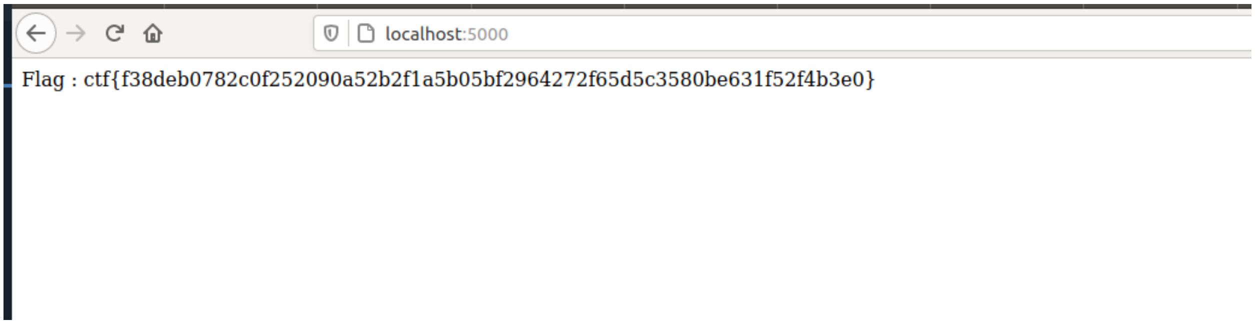


{"nonce": "Mvo7zDi5igE=", "ciphertext": "DzZgWf4G5EXaLMhs1jXsDdjUbcnbJK2S77esNL4DZ6U6qnOMB8PbosICDwNAX/a9G8N23hY1NbXhEpnOgUKtlfJyCqOu", "key": "Fidel_Alejandro_Castro_Ruz_Cuba!"}

2) You have nonce, encryption and key. Create basic decoder of chacha20.

```
from flask import Flask
import json
from base64 import b64encode
from Crypto.Cipher import ChaCha20
from Crypto.Random import get_random_bytes
from base64 import b64decode

app = Flask(__name__)
key_enc = "Fidel_Alejandro_Castro_Ruz_Cuba!"

@app.route("/")
def about():
    plaintext = b' '
    key = key_enc
    result='{"nonce": "Mvo7zDi5igE=", "ciphertext":
"DzZgWf4G5EXaLMhs1jXsDdjUbcnbJK2S77esNL4DZ6U6qnOMB8PbosICDwNAX/a9G8N23hY1Nb
XhEpnOgUKtlfJyCqOu"}'
    try:
       b64 = json.loads(result)
       nonce = b64decode(b64['nonce'])
       ciphertext = b64decode(b64['ciphertext'])
       cipher = ChaCha20.new(key=key, nonce=nonce)
       plaintext = cipher.decrypt(ciphertext)
       x= "Flag : " + plaintext
    except ValueError, KeyError:
      print("Incorrect decryption")
       return x



if __name__=="__main__":
    app.run()
```

3) Extract the flag



```
Flag : ctf{f38deb0782c0f252090a52b2f1a5b05bf2964272f65d5c3580be631f52f4b3e0}
```

7. References

http://www.byronknoll.com/braille.html