



Medium Reverse Engineering picoCTF 2022 packing

AUTHOR: LT 'SYREAL' JONES

Hints ?

## Description

Can you get the flag?

Reverse engineer this [Python program](#).

```
Resolving artifacts.picotf.net (artifacts.picotf.net)... 2600:9000:25fb:8c00:1  
6:5ec5:2840:93a1, 2600:9000:25fb:7000:16:5ec5:2840:93a1, 2600:9000:25fb:6a00:16:  
5ec5:2840:93a1, ...  
Connecting to artifacts.picotf.net (artifacts.picotf.net)|2600:9000:25fb:8c00:  
16:5ec5:2840:93a1|:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 527 [application/octet-stream]  
Saving to: 'unpackme.flag.py'  
  
unpackme.flag.py    100%[=====>]      527  --.-KB/s   in 0s  
  
2026-01-15 11:50:57 (83.8 MB/s) - 'unpackme.flag.py' saved [527/527]  
  
unpackme.py % file unpackme.flag.py  
unpackme.flag.py: Python script text executable, ASCII text, with very long line  
s (305)  
unpackme.py %
```

isinya :

```
import base64
from cryptography.fernet import Fernet

payload = b'gAAAAABkzWGO_8MlYpNM0n0o718LL-w9m3rzXvCMRFghMR16CSZwRD5DJOvN_jc8TFHmH
mfI8HWSu49MyoYKvb5mOGm_Jn4kkhC5fuRiGgmwEpxjh0z72dpI6TaPO2TorksAd2bNLem
fTaYPf9qiTn_z9mvCQYV9cFKK9m1SqCSr4qDwHXgkQpm7IJAmteJqyVUfteFLszyxv5-KXJ
in5BWf9aDPISkp4AztjsBH1_q9e5FIwIq48H7AaHmR8bdvjcW_ZrvhAIOInm1oM-8DjamKv
hh7u3-lA=='
```

  

```
key_str = 'correctstaplecorrectstaplecorrec'
key_base64 = base64.b64encode(key_str.encode()) #encode key_str
f = Fernet(key_base64)
plain = f.decrypt(payload)
```

```
exec(plain.decode())
```

Coba jalankan kode per baris dengan menampilkan output pada setiap fungsi :

```
● unpackme.py & python3
Python 3.13.1 (v3.13.1:69403a54d9f, Oct  7 2024, 00:37:40) [Clang 15.0.0 (clang-1500.3.9.4)] on darwin
Type "help", "copyright", "credits" or "license" for more information.
Cmd click to launch VS Code Native REPL
>>> import base64
>>> key_str = 'correctstaplecorrectstaplecorrect'
>>> key_base64 = base64.b64encode(key_str.encode())
>>> print(key_base64)
b'YycavVJdhN0XbZuNvcnJlY3RzdGFnb0Vjb3JyZM='
>>> from cryptography.fernet import Fernet
>>> f = Fernet(key_base64)
>>> print(f)
<cryptography.fernet.Fernet object at 0x100fce7b8>
>>> payload = f.encrypt(b'What is the password?')
mtEjgyUftefLszxxv5-KXJjnS8wF9abPskp4Aztjs8H1_qe5FIw1q48l7AamIn8bdv;ck_ZrvIA01m1oH-8DjamKvhnu7u-1A=='
>>> plain = f.decrypt(payload)
>>> print(plain)
b"What\\'s the password? "
>>> npw = input('What\\\'s the password? ')
print('picoCTF{175_chr157m45_5274ff21}')
else:
    print('That password is incorrect.')
>>> []
```

Dapat flag : picoCTF{175\_chr157m45\_5274ff21}