

Medium

Reverse Engineering

picoCTF 2022

packing

AUTHOR: LT 'SYREAL' JONES

Hints ?

## Description

(None)

Can you get the flag?

Reverse engineer this [Python program](#).

```
Resolving artifacts.picocft.net (artifacts.picocft.net)... 2600:9000:25fb:8c00:16:5ec5:2840:93a1, 2600:9000:25fb:7000:16:5ec5:2840:93a1, 2600:9000:25fb:6a00:16:5ec5:2840:93a1, ...
Connecting to artifacts.picocft.net (artifacts.picocft.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-w9m3rzXvCMRFghMRl6CSZwRD5DJOvN_jc8TFHmH
mfiI8HWSu49MyoYKvb5mOGm_Jn4kkhC5fuRiGgmwEpxjh0z72dpi6TaPO2TorksAd2bNLem
fTaYPf9qiTn_z9mvCQYV9cFKK9m1SqCSr4qDwHXgkQpm7IJAmTEJqyVUfteFLszyxv5-KXJ
in5BWf9aDPIskp4AztjsBH1_q9e5FIwIq48H7AaHmR8bdvjcW_ZrvhAIOInmloM-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 3.13.0 (v3.13.0:60483a5409f, 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.
>>> import base64
>>> key_str = 'correctstaplecorrectstaplecorrec'
>>> key_base64 = base64.b64encode(key_str.encode()) #encode key_str
>>> print(key_base64)
b'Y29ycmVjdHNOYXBsZWVucnJlY3RzdGFwOGVjb3JyZWw='
>>> from cryptography.fernet import Fernet
>>> f = Fernet(key_base64)
>>> print(f)
<cryptography.fernet.Fernet object at 0x109fce7b0>
>>> payload = b'gAAAAABuKwQ0_041VpM0n0e718LL-wm3rzVxCHRFghMR16CSz-R05DJD-wL_jc8TFHmHf.iT8HwGud9MyoYkvb5m0Gm_Jn4kKhC5fuRiGmwEpxjh0z72dp.i6TaP02TorksAd2bNLemfTaYPf9qITn_z9mVCQYV9cFKX9m1SqCSr4qdW4XgkQpm7IJA
mtIqyVUffteFLzyyvs-KXjins5BwF9a0Piskp4AztjsBH1_q8e5Fiwiq48H7Aahm88bdvjcw_ZrvhA10Inm10M-80jamkvhh7u3-1A='
>>> plain = f.decrypt(payload)
>>> print(plain)
b'npw = input('What\'s the password? ')\n\nif pw == 'batteryhorse':\n    print('picoCTF{175_chr157m45_5274ff21}')\nelse:\n    print('That password is incorrect.')\n\n"
>>>
```

Dapet flag : picoCTF{175\_chr157m45\_5274ff21}