unpackme.py

Medium | Reverse Engineering | picoCTF 2022 | packing

AUTHOR: LT 'SYREAL' JONES

Description

Can you get the flag?

Reverse engineer this Python program.

Hints

(None)

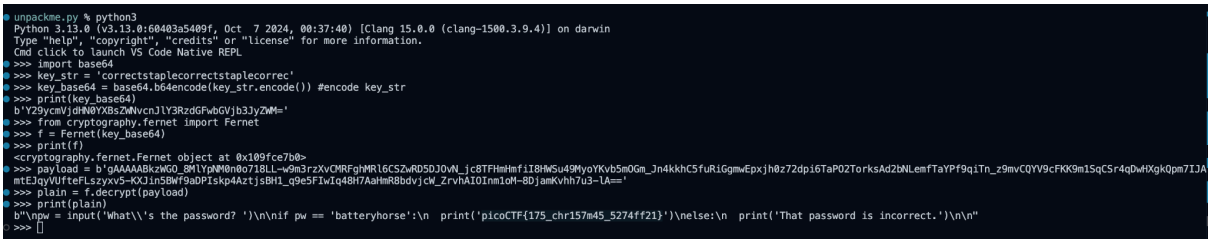
```
Resolving artifacts.picoctf.net (artifacts.picoctf.net)... 2600:9000:25fb:8c00:1
6:5ec5:2840:93a1, 2600:9000:25fb:7000:16:5ec5:2840:93a1, 2600:9000:25fb:6a00:16:
5ec5:2840:93a1, ...
Connecting to artifacts.picoctf.net (artifacts.picoctf.net)|2600:9000:25fb:8c00:
16:5ec5:2840:93a1|:443... connected.
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_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 :



Dapet flag : picoCTF{175_chr157m45_5274ff21}