

```
# 1. I took key_str = 'correctstaplecorrectstaplecorrec' and encoded it in base64 to get the
valid key for Fernet.
# 2. I initialized Fernet (key_base64) and called decrypt (payload) to decrypt the data.

# 3. I read the plaintext (a small Python script) — it contains a password check
(batteryhorse) and the flag in the clear.

# 4. I extracted the flag from the script :
```

```
import base64
from cryptography.fernet import Fernet

payload =
b'gAAAAABkzWGWvEp8gLI9AcIn5o-ahDUwkTvM6EwF7YYMZ1E-_Gf9rcNYjxIgX4b0ltY6b
cxKarib2ds6POclRwCwhsRb1LOXvt4Q3ePtMY4BmHFFZlIHLk05CjwigT7hiI9p3sH9e7Cp
k1uO90xbHbuy-mfi3nkmn411aBgwxyWpJvykpuBIG_nty6zbox3UhbB85TOis0TgM0zG4h
t0-GUW4wTq2_5-wkw3kV1ZAisLJHzF-Z9oLMmwFZU0UCAcHaBTGDF5BnVLmUeCGTgzVLSNn
6BmB61Yg=='
key_str = 'correctstaplecorrectstaplecorrec'
key_base64 = base64.b64encode(key_str.encode())
f = Fernet(key_base64)
plain = f.decrypt(payload)

print(plain.decode())
```

THE FLAG : picoCTF{175_chr157m45_85f5d0ac}
~Z4que