Srp

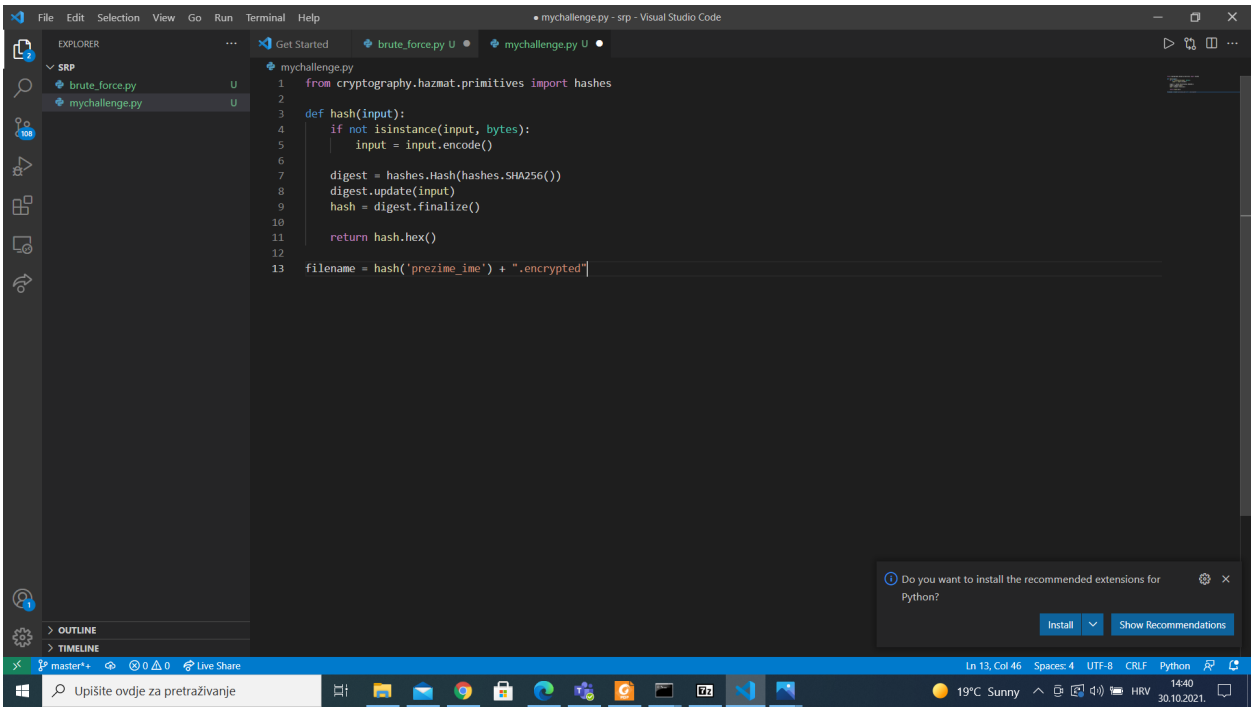
2.lab vjezba

Za vjezbu smo trebali desifrirati enkriptirani plaintext.

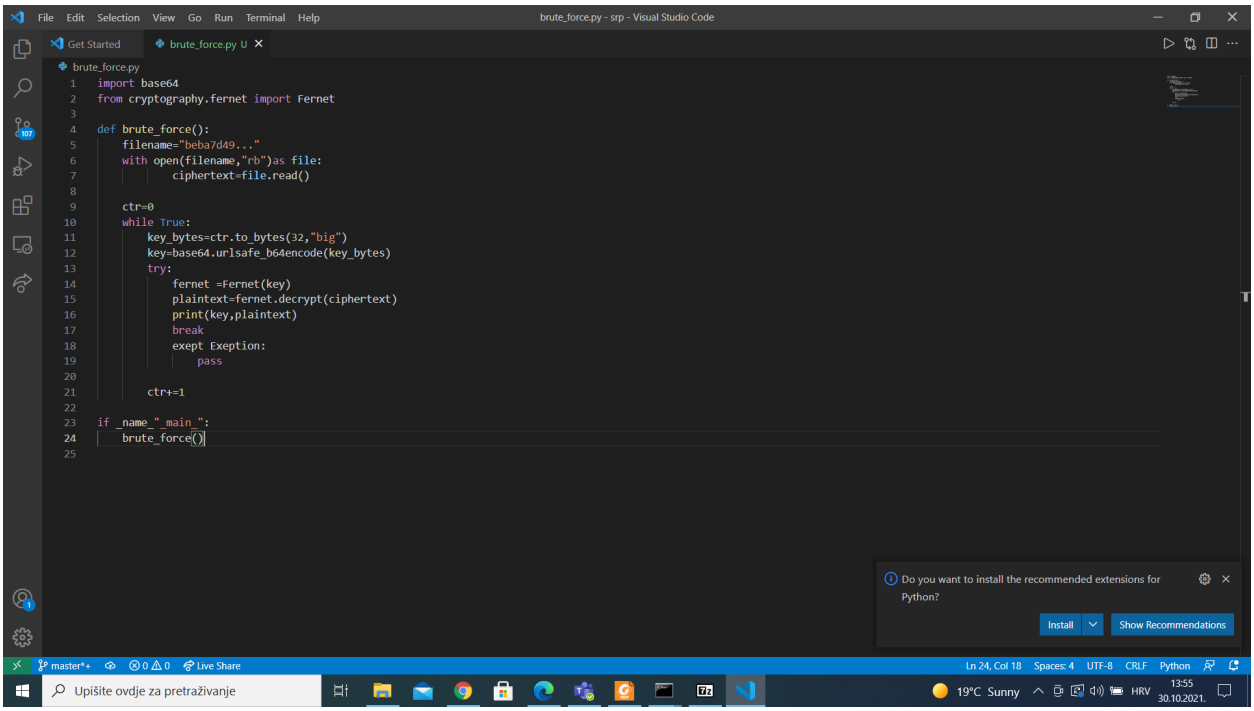
Enkriptiran je koristenjem high level sustava za simetričnu enkripciju iz biblioteke Fernet:

Otkrili smo osobni izazov koji je namijenjen nama pomocu

```
from cryptography.hazmat.primitives import hashes

def hash(input):
    if not isinstance(input, bytes):
        input = input.encode()

    digest = hashes.Hash(hashes.SHA256())
    digest.update(input)
    hash = digest.finalize()

    return hash.hex()

filename = hash('prezime_ime') + ".encrypted"
```



Nakon toga trebamo brute force algoritmom otkriti kljuc za dekripciju ciphertexta



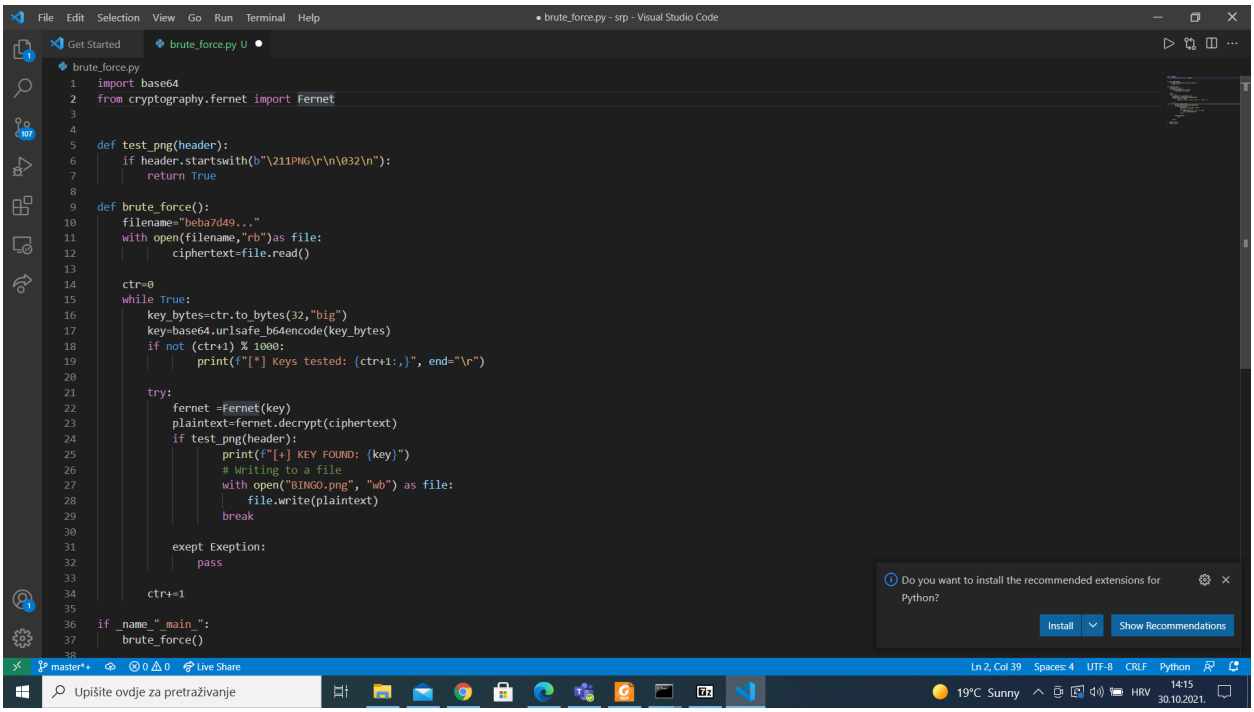
Problem nam stvara beskonacna petlja i kako izaci iz nje.

Saznali smo da je nas plaintext slika png formata sa odredenim headerom te smo stvorili koja testira je li prvi dio plaintexta trazeni format:

```
def test_png(header):
if header.startswith(b"\211PNG\r\n\032\n"):
return True
```

Spremimo nas plaintext u file:

```
if test_png(header):
print(f"[+] KEY FOUND: {key}")
# Writing to a file
with open("BINGO.png", "wb") as file:
file.write(plaintext)
break
```



Program generira kljuc te otvorimo BINGO.png u nasem direktoriju

Untitled