

To solve this, we can make a quick solve script to test whether each password was pwned and, if yes, how many times using the **Have I Been Pwned api**:

```
import requests
import hashlib

def check_password_pwned(password):
    sha1_password = hashlib.sha1(password.encode('utf-8')).hexdigest().upper()
    first5_chars = sha1_password[:5]
    rest_of_hash = sha1_password[5:]
    url = f"https://api.pwnedpasswords.com/range/{first5_chars}"
    response = requests.get(url)
    if response.status_code == 200:
        hashes = response.text.splitlines()
        for hash_entry in hashes:
            hash, count = hash_entry.split(":")
            if hash == rest_of_hash:
                return int(count)
    return 0

with open("leaked.txt", "r") as file:
    passwords = file.readlines()
for password in passwords:
    password = password.strip()
    count = check_password_pwned(password)
    if count > 0:
        print(f"Password '{password}' has been pwned {count} times.")
```

The correct password is the one with the most amount of pwns (1204 at the time of writing).