Wells-read WRITEUP

By opening the downloadable zip provided, we saw two files:

- **The Time Machine by H. G. Wells.txt**: contains some text;
- **words.txt**: contains a list of words.

By analyzing the text, we found out that some words were strange, containining one character changed. So, we thought about extracting those characters by comparing each word in the text with the ones in the wordlist provided.

We coded a Python3 script to do this work, which you can find below, using a regex to check whenever the flag started to appear in the logs.

```
import string
import re

# Save wordlist in a list
wordList = []
wordList_lower = []
with open("words.txt", "r") as fp:
    lines = fp.readlines()
    for line in lines:
        wordList.append(line.strip())
        wordList_lower.append(line.strip().lower())

# Read text from file
with open("text.txt", "r") as fp:
    text = fp.read()

# If you want to skip to the part of the text where the flag is, uncomment this l
# text = text[68500:]

# Start the parsing word per word
out = ""
punctuation = re.sub(r'[\_|\{|\}|\:]', '', string.punctuation)
for word in text.split():
    # Skip punctuation that could generate false positives
    skip = False
```

```
        for punc in punctuation:
            if punc in word:
                skip = True
                break

        if skip:
            continue

        # Check if lowercase word is in the wordlist
        word_lower = word.lower()
        if word_lower in wordList_lower:
            continue

        # Search for words in the wordlist with only one character different
        diff = []
        for w, w_lower in zip(wordList, wordList_lower):
            tmp = []

            # Check only words with same length
            if len(w) == len(word):
                for a, b in zip(word, w):
                    if a != b:
                        tmp.append(a)

            if len(tmp) == 1:
                diff.append(tmp[0])
                break

        # If the current word has been altered, append the changed character to the o
        if diff:
            out += diff[0]
            print(out)

        # Do we have the flag in the output?
        flag = re.search(r'\{FLG\:.+', out)
        if flag:
            print("FLAG: ", flag.group(0), "\n")
```

Finally, the flag appeared: `{FLG:1_kn0w_3v3ryth1ng_4b0ut_t1m3_tr4v3l}`