p4-team / ctf

Watch 79   Star 295   Fork 63

<> Code   ⓘ Issues 0   ⑂ Pull requests 0   ▦ Projects 0   ⎍ Pulse   � Graphs

Branch: master ▾   ctf / 2016-01-29-nullcon / crypto_2 /

Create new file   Find file   History

Pharisaeus formatting of crypto 2

Latest commit 3044dd3 on 1 Feb 2016

..

📄 README.md	formatting of crypto 2	a year ago
📄 The_extract.txt	Adding stubs for nullcon 2016	a year ago

📖 README.md

Caesar (Crypto, 400p)

```
Some one was here, some one had breached the security and had infiltrated here.
All the evidences are touched, Logs are altered, records are modified with key as a text from book.
The Operation was as smooth as CAESAR had Conquested Gaul.
After analysing the evidence we have some extracts of texts in a file.
We need the title of the book back, but unfortunately we only have a portion of it...
```
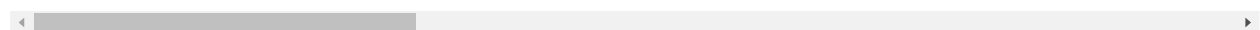
PL ENG

Dostajemy plik a z treści zadania wynika, że może być on szyfrowany za pomocą szyfru Cezara. Uruchamiamy więc prosty skrypt:

```
import codecs

with codecs.open("The_extract.txt") as input_file:
    data = input_file.read()
    for i in range(26):
        text = ""
        for x in data:
            c = ord(x)
            if ord('a') <= c < ord('z'):
                text += chr((c - ord('a') + i) % 26 + ord('a'))
            elif ord('A') <= c < ord('Z'):
                text += chr((c - ord('A') + i) % 26 + ord('A'))
            else:
                text += chr(c)
        print(text)
```

Który wypisuje wszystkie możliwe dekodowania, wśród których mamy:

```
Dr. Sarah Tu races against time to block the most dangerous Internet malware ever created, a botnet called QUALNTO. W

Hanna's condition is misleading. In her coma state, she is able to build a zsychic bridge with FBI Szecial Agent Jasc

Tough and street-smart Jason McNeil doesn't believe in visions or telezathic messages, and he fights the voice inside

When an extremely dangerous arms dealer and cybercriminal discovers that Sarah blocked his botnet, he kidnzs Sarah.
```

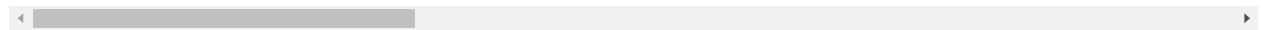Pochodzące z książki `In the Shadow of Greed` co jest flagą.

ENG version

We get a file and the task description suggests that the encryption is Caesar. Therefore we run a simple script:

```
import codecs

with codecs.open("The_extract.txt") as input_file:
    data = input_file.read()
    for i in range(26):
        text = ""
        for x in data:
            c = ord(x)
            if ord('a') <= c < ord('z'):
                text += chr((c - ord('a') + i) % 26 + ord('a'))
            elif ord('A') <= c < ord('Z'):
                text += chr((c - ord('A') + i) % 26 + ord('A'))
            else:
                text += chr(c)
        print(text)
```

Which prints all possible decryptions where we can find:

```
Dr. Sarah Tu races against time to block the most dangerous Internet malware ever created, a botnet called QUALNTO. W

Hanna's condition is misleading. In her coma state, she is able to build a zsychic bridge with FBI Szecial Agent Jaso

Tough and street-smart Jason McNeil doesn't believe in visions or telezathic messages, and he fights the voice inside

When an extremely dangerous arms dealer and cybercriminal discovers that Sarah blocked his botnet, he kidnzs Sarah.
```

Coming from `In the Shadow of Greed` book, which is the flag.