Mark Seliternikov
picoCTF - caesar [100 points]

קיבלנו את המפתח לאתגר, אבל התוכן אשר נמצא בתוכו מוצפן:

picoCTF{dspttjohuifsvcjdpoabrkttds}

באתגר מרומז שזה הוצפן בשיטת caesar, שזו שיטה שבה האותיות מסובבות מספר מקומות ממקומם הרגיל. כלומר, אם מסובבים ב 3+ מקומות אז a יהיה d.

החלטתי לנסות את שיטת brute force ולגלות את כל ה-26 אפשרויות לקוד אם אני משנה את מיקום האותיות בשיטת caesar. זה הסקריפט שכתבתי ב-C:

```c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int main()
{
    // the encrypted text with caesar
    char *s = "dspttjohuifsvcjdpoabrkttds";
    // the length of the text
    int length = strlen(s);
    // a variable holding the ASCII value
    int c;

    // loop over all 26 possibilities
    for(int i = 0; i < 26; i++)
    {
        // loop over the whole text, in this case the encrypted flag
        for(int ii = 0; ii < length; ii++)
        {
            // doing some ASCII math
            c = s[ii] + i;
            // if it goes higher than 'z' then it rotates to the start of the ABC
            if(c > 122)
            {
                c -= 26;
            }
            printf("%c", c);
        }
        printf("\n");
    }
    return 0;
}
```

לאחר מכן בדקתי מה יצא הפלט:

```
dspttjohuifsvcjdpoabrkttds
etquukpivjgtwdkeqpbcsluuet
furvvlqjwkhuxelfrqcdtmvvfu
gvswwmrkxlivyfmgsrdeunwwgv
hwtxxnslymjwzgnhtsefvoxxhw
ixuyyotmznkxahoiutfgwpyyix
jyvzzpunaolybipjvughxqzzjy
kzwaaqvobpmzcjqkwvhiyraakz
laxbbrwpcqnadkrlxwijzsbbla
mbyccsxqdrobelsmyxjkatccmb
nczddtyrespcfmtnzyklbuddnc
odaeeuzsftqdgnuoazlmcveeod
pebffvatgurehovpbamndwffpe
qfcggwbuhvsfipwqcbnoexggqf
rgdhhxcviwtgjqxrdcopfyhhrg
sheiiydwjxuhkrysedpqgziish
tifjjzexkyvilsztfeqrhajjti
ujgkkafylzwjmtaugfrsibkkuj
vkhllbgzmaxknubvhgstjcllvk
wlimmchanbylovcwihtukdmmwl
xmjnndiboczmpwdxjiuvlennxm
ynkooejcpdanqxeykjvwmfooyn
zolppfkdqeboryfzlkwxngppzo
apmqqglerfcpszgamlxyohqqap
bqnrrhmfsgdqtahbnmyzpirrbq
crossingtherubiconzaqjsscr
```

באפשרות האחרונה ממש ניתן לראות שיש בה מילים לכן הסקתי שזה אכן ה-flag.
בדקתי אם התשובה נכונה והיא אכן נכונה!

<u>מה למדתי</u>

זאת הייתה הפעם הראשונה שניסיתי את שיטת ה-brute force ולמדתי קצת להשתמש בה.