Analysis of the RuCTF 2017 Olympiad

3ch

You could've used GET CSRF in the image element, redirecting bot posting photos to the password changing form, allowing to log in on behalf of its name and see the flag.

Captain Election

Imagine we have **n** voters and **m** mixers (in the MixNet terminology) Let **P(v_i)** be the probability of tracing voter **i**. Note, that all voters are homomorphous, so this probability should be equal, let's call it p. The probability that at least one of the voters will be compromised is

1 - (1 - p)^n

For the individual participant it's possible to show that:

p = (k / n)^m

Combining everything together

1 - (1 - (k / n)^m)^n < 0.01
k < n * (1 - (1 - 0.01)^(1 / n))^(1 / m)

Flag

File only has 3 chunks: IHDR, IDAT and IEND. IHDR and IEND are too short to have a flag hidden in them, so the most probable container is IDAT, which is compressed using Deflate.

Before every row, there's a byte responsible for choosing filter for this row. This byte has 5 possible values. Despite the image being colorless, this byte is changing from one row to another, which indicates that the flag is hidden there.

All 5 possible values are used, so it seems reasonable to assume that the data was encoded in the five-digit number system. After converting this number to 256-digit number system, this number becomes a byte sequence, containing flag.

Attraction

Task statement has several hits about the used programming language. Using the list of programming languages, it's relatively simple to find TRAC - language that was developed in 1959 and implemented in 1964. When it's clear what to look for, it's enough to run the given program, its output is the answer.

There might have been some problems with conflicting versions of this language, however, considering how small the instruction set is, bruteforcing the right command was possible.