Reverse Engineering Report

Lakshit Verma

August 14, 2024

LIT CTF — revsite2

watch ads for a free flag, with amazing data integrity (patent not pending) URL: http://litctf.org:31785/

We were given a website which incremented a variable by clicking a button. When the variable reached $10 \wedge 18$ we would get the flag. Inspecting the script running the site we found it ran WASM, which was the code we had to reverse to get the flag.

Things I learned in this challenge:

1. **WASM decompiling:** Using tools such as `wat2wasm` and `wasm2js` to decompile and convert WASM to more readable languages.
2. **WASM reversing:** Understanding WASM syntax and logic.
3. **Using the Ghidra WASM plugin:** Found this out after the CTF ended.

After looking at other writeups and on the Discord it turned out it performing the summation

$$y = \sum_{x=0}^{10^{18}-1} (8x^3 + 3x^2 + 3x + 8)$$

Putting the valu