Minesploit: Bitcoin White Hat Hacker Tool

A toolkit for pentesting bitcoin mining infrastructure

BTC++ 2026 / Edição Façanhas / Exploits Edition / Florianópolis, SC, Brazil

Meet the team

Johnny Santos

github.com/johnnyasantoss

Jayr Motta

github.com/jayrmotta

Lucas Balieiro

github.com/lucasbalieiro

The problem

- Bitcoin mining infrastructure has real security vulnerabilities

- No specialized framework exists for testing bitcoin mining systems

- Security researchers need accessible systems to test hypothesis

What is minesploit?

- Security research framework for testing Bitcoin mining software

- Composed of a Python library and an interactive shell

- Protocols: Stratum V1/V2, P2Pool implementations

- Utilities: CPU miner wrapper, networking, crypto helpers

Key Features

- 15+ implemented CVEs (Bitcoin Core, cgminer, Stratum) and even a zero day vulnerability

- Fluent, composable Python API

- Hypothesis-first design for rapid testing

Demo Time

Showing the framework

We found a new vulnerability!

Impact

- Pool Accountability Destroyed - Miners can inflate their reported hashrate

- Financial Fraud - Get paid for work never done

- Silent Exploitation - No obvious signs of cheating

Responsible disclosure

We contacted the Stratum V2 maintainers and reported this vulnerability.

They acknowledged it and we're authorized to demonstrate it here today.

Thank you