Extropy CTF

Background

Extropy - Blockchain consultancy since 2015

Main areas - Auditing / Education

Workshops - 2 day and 4 week ZKP

Aims

Improve awareness of security

Gamify process

Provide community resources

Vulnerabilities included

1. Re entrancy
2. Size mismatch -> felt and U256
3. Addresses : lack of verification
4. Possibility of censorship by sequencer

Sources

Audits

1. Chain security - Maker DAO DAI Bridge
2. Peckshield - xBank audit

Next Steps

Cairo - more potential vulnerabilities

Warp - investigate how known solidity vulnerabilities map to cairo