QuillAudits

Audit Report
April, 2022

For

ENREX

Contents

Scope of the Audit

The scope of this audit was to analyze and document the Enrex staking programs codebase for quality, security, and correctness.

Checked Vulnerabilities

We have scanned the smart contract for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that we considered:

- Missing signer checks
- Missing ownership checks
- Missing rent exemption checks
- Signed invocation of unverified programs
- Solana account confusions
- Re-initiation with cross-instance confusion
- Arithmetic overflow/underflows
- Numerical precision errors
- Loss of precision in calculation
- Incorrect calculation
- Casting truncation
- Exponential complexity in calculation
- Missing freeze authority checks
- Insufficient SPL-Token account verification
- Over/under payment of loans
- Reentrancy
- Unsafe Rust code
- Outdated dependencies
- Redundant code

Techniques and Methods

Throughout the audit of smart contract, care was taken to ensure:

- The overall quality of code.
- Use of best practices.
- Code documentation and comments match logic and expected behavior.
- Token distribution and calculations are as per the intended behavior mentioned in the whitepaper.
- Implementation of spl-token standards.
- Efficient use of gas.
- Code is safe from other vulnerabilities.

The following techniques, methods and tools were used to review all the smart contracts.

Structural Analysis
In this step, we have analysed the design patterns and structure of smart contracts. A thorough check was done to ensure the smart contract is structured in a way that will not result in future problems.

Static Analysis
Static analysis of smart contracts was done to identify contract vulnerabilities. In this step, a series of automated tools are used to test the security of smart contracts.

Code Review / Manual Analysis
Manual analysis or review of code was done to identify new vulnerabilities or verify the vulnerabilities found during the static analysis. Contracts were completely manually analysed, their logic was checked and compared with the one described in the whitepaper. Besides, the results of the automated analysis were manually verified.

Gas Consumption
In this step, we have checked the behaviour of smart contracts in production. Checks were done to know how much gas gets consumed and the possibilities of optimization of code to reduce gas consumption.

Issue Categories

Every issue in this report has been assigned to a severity level. There are four levels of severity, and each of them has been explained below.

Risk-level	Description
High	A high severity issue or vulnerability means that your smart contract can be exploited. Issues on this level are critical to the smart contract's performance or functionality, and we recommend these issues be fixed before moving to a live environment.
Medium	The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on this level could potentially bring problems, and they should still be fixed.
Low	Low-level severity issues can cause minor impact and or are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.
Informational	These are severity issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

Number of issues per severity

Type	High	Medium	Low	Informational
Open	0	0	0	0
Acknowledged	0	0	0	0
Closed	0	0	2	0

Introduction

During the period of **March 24, 2022, to March 28, 2022** - QuillAudits Team performed a security audit for Enrex programs.

https://github.com/Enrex-io/staking-contract/

The code for the audit was taken from the repository of Enrex:

V	Date	Commit Hash
1	March	88bed1d22415a438bf8aa0fa93f57465620c7e35
2	March	c0b95bf2e2cccf4a229483ff361373c23ef89cf7

Mainnet Contract Address :-

https://solscan.io/account/2BkjfP3SzHe1sfBiYS61A6cffJtgJcTy5qaRGbhQCY22

Issues Found – Code Review / Manual Testing

A. Program – enrex_stake

High severity issues

No issues were found.

Medium severity issues

No issues were found.

Low severity issues

1. **Integer Overflow**

```
lib.rs - Line 43:
    pub fn fund_pool(_ctx: Context<FundPool>, amount: u64) -> Result<()> {
        let pool = &mut _ctx.accounts.pool;
        pool.amount_reward += amount;
        let cpi_accounts = Transfer {
            from: _ctx.accounts.user_vault.to_account_info(),
            to: _ctx.accounts.pool_vault.to_account_info(),
            authority: _ctx.accounts.authority.to_account_info(),
        };
        let cpi_program = _ctx.accounts.token_program.to_account_info();
        let cpi_ctx = CpiContext::new(cpi_program, cpi_accounts);
        token::transfer(cpi_ctx, amount)?;

        Ok(())
    }
```

```
lib.rs - Line 85:
      pub fn stake(_ctx: Context<Stake>, amount: u64) -> Result<()> {
       let pool = &mut _ctx.accounts.pool;

       require!(amount >= pool.min_stake_amount,
          ErrorMsg::BelowMinStakeAmount
       );

       let reward_amount = pool.get_reward_amount(amount) as u64;
       let reward_amount_reserved = pool.amount_reward_reserved +
reward_amount;
       require!(reward_amount_reserved <= pool.amount_reward,
          ErrorMsg::OverflowReservedReward
       );
```

```
 let staked_info = &mut _ctx.accounts.staked_info;
staked_info.amount = amount;
staked_info.staked_time = _ctx.accounts.clock.unix_timestamp;
staked_info.pool = pool.key();
staked_info.authority = _ctx.accounts.authority.key();
staked_info.stake_index = pool.inc_stakes;
staked_info.reward_amount = reward_amount;

pool.inc_stakes += 1;
pool.count_stakes += 1;
pool.amount_reward_reserved = reward_amount_reserved;
pool.amount_staked += amount;
```

```
lib.rs - Line 150:
    pub fn claim_stake(_ctx: Context<Unstake>) -> Result<()> {
        let state = &_ctx.accounts.state;
        let pool = &mut _ctx.accounts.pool;
        let staked_info = &_ctx.accounts.staked_info;

        require!(
            staked_info.staked_time
                .checked_add(pool.lock_duration)
                .unwrap()
                <= _ctx.accounts.clock.unix_timestamp,
            ErrorMsg::UnderLocked
        );

        let amount = staked_info.amount + staked_info.reward_amount;
```

Description

Certain mathematical operations are missing overflow checks which might generate overflow errors.

Remediation

Use checked_add() to perform addition operations.

Status: Fixed

Team has fixed this issue in commit c0b95bf2e2cccf4a229483ff361373c23ef89cf7 by doing calculations using checked_add and checked_sub.

2. Missing Account Verification

```
lib.rs - Line 205:
    pub system_program: Program<'info, System>,
```

```
lib.rs - Line 257:
    pub system_program: Program<'info, System>,
```

```
lib.rs - Line 417:
    pub system_program: Program<'info, System>,
```

```
lib.rs - Line 462:
    pub system_program: Program<'info, System>,
```

Description

Certain contexts lack a safety check in the account addresses, accounts that are passed to the instruction should all be verified, otherwise, the program may have unexpected behaviors.

Remediation

It’s recommended to verify the accounts that are passed to the program including the system_program.

Status: Fixed
team has fixed this issue in commit c0b95bf2e2cccf4a229483ff361373c23ef89cf7 by adding the constraint system_program.key() == System::id()

Informational Issues

No issues were found.

Automated Tests

Soteria

```
 - ⬙ [00m:01s] Building Static Happens-Before Graph

 - ⬙ [00m:00s] Detecting Vunerabilities
detected 0 untrustful accounts in total.
detected 11 unsafe math operations in total.

--------The summary of potential vulnerabilities in all.ll--------

        11 unsafe arithmetic issues
```

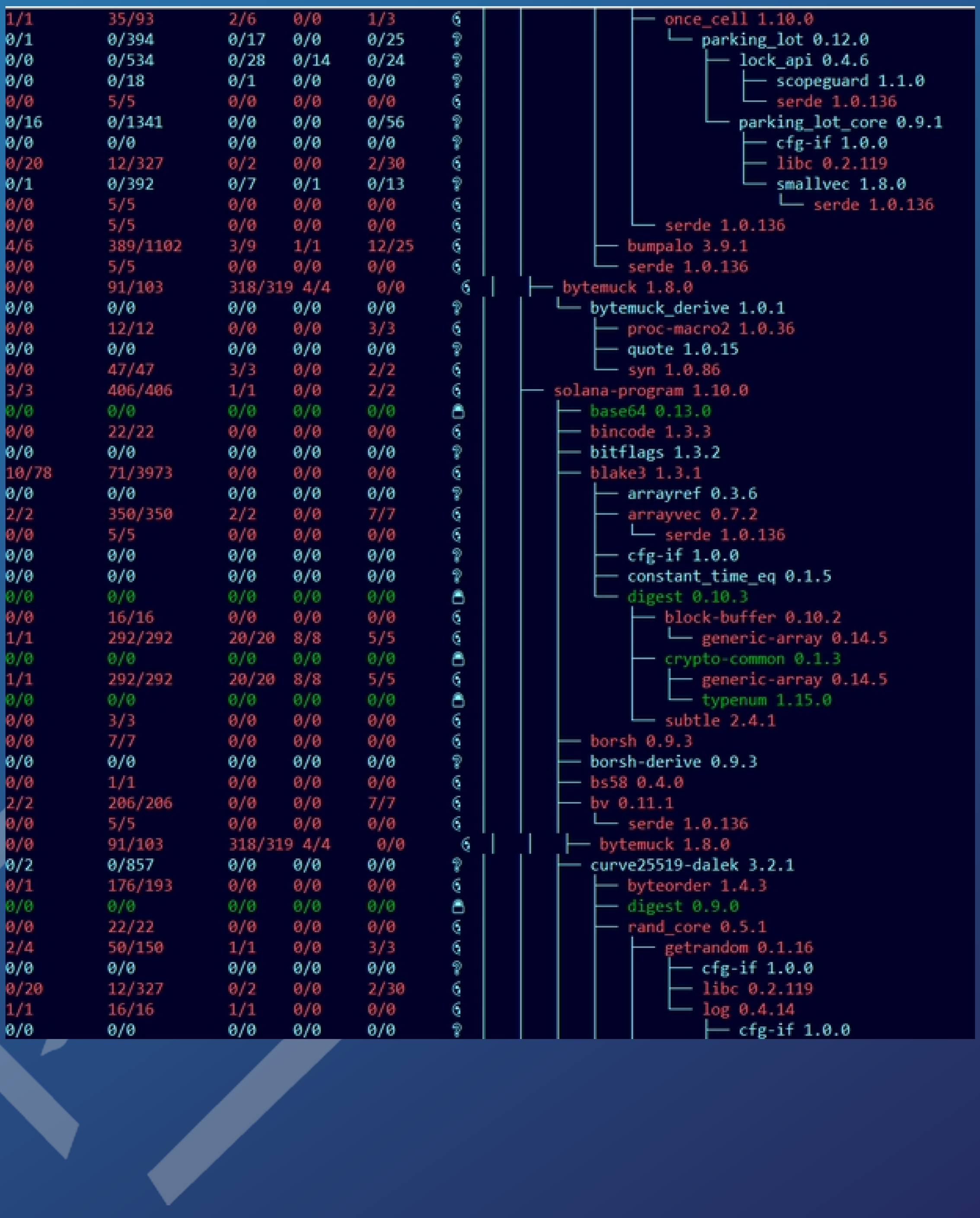
Cargo-geiger

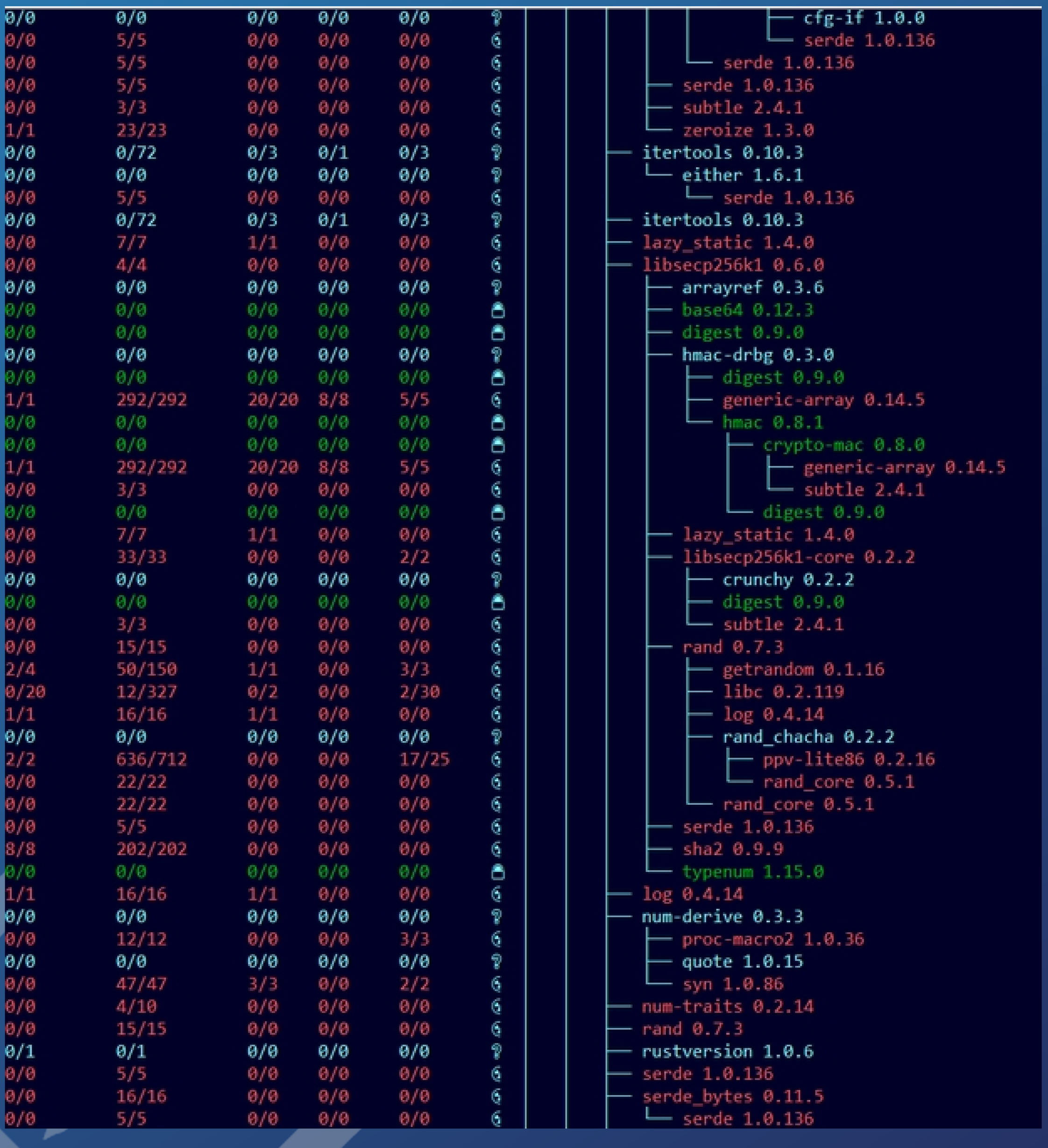
```
    Scanning done
WARNING: Dependency file was never scanned: /root/Enrex-staking/target/debug/build/rustversion-2eb2b30e6ec73d94/out/version.rs
WARNING: Dependency file was never scanned: /root/Enrex-staking/target/debug/build/typenum-d66e1a3a0eae4933/out/op.rs
WARNING: Dependency file was never scanned: /root/Enrex-staking/target/debug/build/libsecp256k1-85a3a82d632b52ac/out/const_gen.rs
WARNING: Dependency file was never scanned: /root/Enrex-staking/target/debug/build/crunchy-c7f9bbb18abff656/out/lib.rs
WARNING: Dependency file was never scanned: /root/Enrex-staking/target/debug/build/typenum-d66e1a3a0eae4933/out/consts.rs
WARNING: Dependency file was never scanned: /root/.cargo/registry/src/github.com-1ecc6299db9ec823/bumpalo-3.9.1/README.md
WARNING: Dependency file was never scanned: /root/Enrex-staking/target/debug/build/libsecp256k1-85a3a82d632b52ac/out/const.rs

Metric output format: x/y
    x = unsafe code used by the build
    y = total unsafe code found in the crate

Symbols:
    🔒  = No `unsafe` usage found, declares #![forbid(unsafe_code)]
    ❓  = No `unsafe` usage found, missing #![forbid(unsafe_code)]
    ☢  = `unsafe` usage found

Functions  Expressions  Impls  Traits  Methods  Dependency

0/0        0/0          0/0    0/0     0/0      ❓  enrex_stake 0.1.0
0/0        0/0          0/0    0/0     0/0      ❓  ├── anchor-lang 0.22.1
0/0        0/0          0/0    0/0     0/0      ❓  │   ├── anchor-attribute-access-control 0.22.1
0/0        8/8          0/0    0/0     0/0      ☢  │   │   ├── anchor-syn 0.22.1
15/18      442/449      3/3    0/0     11/11    ☢  │   │   │   ├── anyhow 1.0.55
0/0        1/1          0/0    0/0     0/0      ☢  │   │   │   ├── bs58 0.3.1
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │   ├── heck 0.3.3
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │   │   └── unicode-segmentation 1.9.0
0/0        12/12        0/0    0/0     3/3      ☢  │   │   │   ├── proc-macro2 1.0.36
0/0        0/0          0/0    0/0     0/0      🔒  │   │   │   │   └── unicode-xid 0.2.2
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │   ├── proc-macro2-diagnostics 0.9.1
0/0        12/12        0/0    0/0     3/3      ☢  │   │   │   │   ├── proc-macro2 1.0.36
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │   │   ├── quote 1.0.15
0/0        12/12        0/0    0/0     3/3      ☢  │   │   │   │   │   └── proc-macro2 1.0.36
0/0        47/47        3/3    0/0     2/2      ☢  │   │   │   │   ├── syn 1.0.86
0/0        12/12        0/0    0/0     3/3      ☢  │   │   │   │   │   ├── proc-macro2 1.0.36
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │   │   │   ├── quote 1.0.15
0/0        0/0          0/0    0/0     0/0      🔒  │   │   │   │   │   └── unicode-xid 0.2.2
3/3        34/34        0/0    0/0     0/0      ☢  │   │   │   │   └── yansi 0.5.0
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │   └── quote 1.0.15
0/0        5/5          0/0    0/0     0/0      ☢  │   │   ├── serde 1.0.136
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │   └── serde_derive 1.0.136
0/0        12/12        0/0    0/0     3/3      ☢  │   │   │       ├── proc-macro2 1.0.36
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │       ├── quote 1.0.15
0/0        47/47        3/3    0/0     2/2      ☢  │   │   │       └── syn 1.0.86
0/0        4/7          0/0    0/0     0/0      ☢  │   │   ├── serde_json 1.0.79
0/0        7/7          0/0    0/0     0/0      ☢  │   │   │   ├── itoa 1.0.1
7/9        587/723      0/0    0/0     2/2      ☢  │   │   │   ├── ryu 1.0.9
0/0        5/5          0/0    0/0     0/0      ☢  │   │   │   └── serde 1.0.136
8/8        202/202      0/0    0/0     0/0      ☢  │   │   └── sha2 0.9.9
```

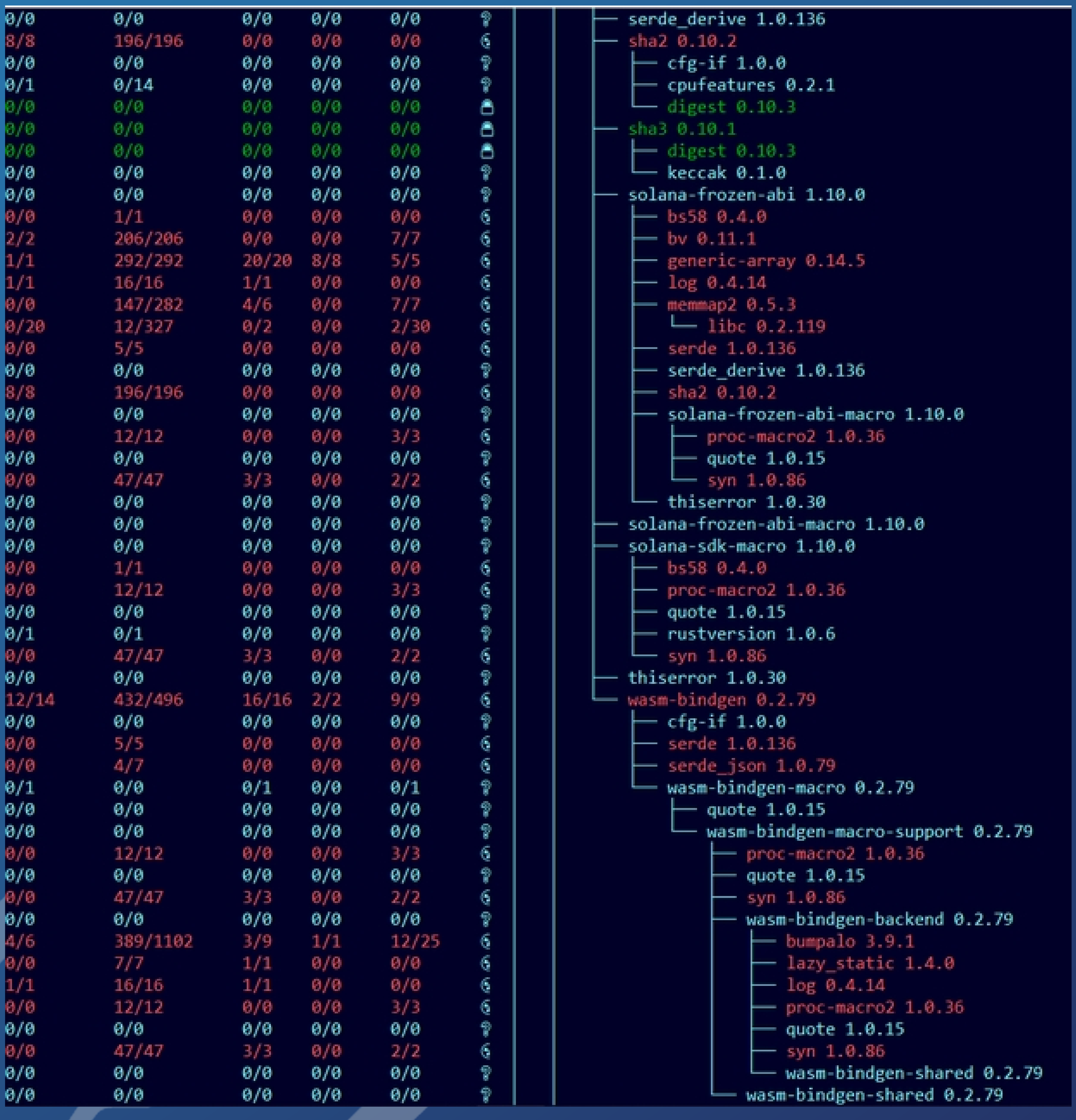
```
8/8       202/202   0/0    0/0    0/0
0/0       6/6       0/0    0/0    0/0
1/1       292/292   20/20  8/8    5/5
0/0       5/5       0/0    0/0    0/0
0/0       0/0       0/0    0/0    0/0
0/0       0/0       0/0    0/0    0/0
0/1       0/14      0/0    0/0    0/0
0/0       0/0       0/0    0/0    0/0
1/1       292/292   20/20  8/8    5/5
0/0       0/0       0/0    0/0    0/0
0/0       47/47     3/3    0/0    2/2
0/0       0/0       0/0    0/0    0/0
0/0       12/12     0/0    0/0    3/3
0/0       0/0       0/0    0/0    0/0
0/0       47/47     3/3    0/0    2/2
15/18     442/449   3/3    0/0    11/11
0/0       12/12     0/0    0/0    3/3
0/0       0/0       0/0    0/0    0/0
0/0       34/34     1/2    0/0    2/2
19/19     678/678   0/0    0/0    22/22
36/37     2067/2140 0/0    0/0    16/16
0/20      12/327    0/2    0/0    2/30
36/37     2067/2140 0/0    0/0    16/16
0/0       0/0       0/0    0/0    0/0
0/0       47/47     3/3    0/0    2/2
0/0       0/0       0/0    0/0    0/0
0/0       8/8       0/0    0/0    0/0
15/18     442/449   3/3    0/0    11/11
0/0       1/1       0/0    0/0    0/0
8/8       202/202   0/0    0/0    0/0
0/0       12/12     0/0    0/0    3/3
0/0       0/0       0/0    0/0    0/0
0/1       0/1       0/0    0/0    0/0
0/0       47/47     3/3    0/0    2/2
0/0       0/0       0/0    0/0    0/0
0/0       8/8       0/0    0/0    0/0
0/0       12/12     0/0    0/0    3/3
0/0       47/47     3/3    0/0    2/2
0/0       0/0       0/0    0/0    0/0
0/0       8/8       0/0    0/0    0/0
0/0       12/12     0/0    0/0    3/3
0/0       0/0       0/0    0/0    0/0
0/0       47/47     3/3    0/0    2/2
0/0       0/0       0/0    0/0    0/0
0/0       8/8       0/0    0/0    0/0
15/18     442/449   3/3    0/0    11/11
0/0       12/12     0/0    0/0    3/3
0/0       0/0       0/0    0/0    0/0
0/0       47/47     3/3    0/0    2/2
```

```
├── sha2 0.9.9
│   ├── block-buffer 0.9.0
│   │   └── generic-array 0.14.5
│   │       ├── serde 1.0.136
│   │       └── typenum 1.15.0
│   ├── cfg-if 1.0.0
│   ├── cpufeatures 0.2.1
│   ├── digest 0.9.0
│   │   └── generic-array 0.14.5
│   └── opaque-debug 0.3.0
├── syn 1.0.86
└── thiserror 1.0.30
    └── thiserror-impl 1.0.30
        ├── proc-macro2 1.0.36
        ├── quote 1.0.15
        └── syn 1.0.86
├── anyhow 1.0.55
├── proc-macro2 1.0.36
├── quote 1.0.15
├── regex 1.5.4
│   ├── aho-corasick 0.7.18
│   │   └── memchr 2.4.1
│   │       └── libc 0.2.119
│   ├── memchr 2.4.1
│   └── regex-syntax 0.6.25
└── syn 1.0.86
├── anchor-attribute-account 0.22.1
│   ├── anchor-syn 0.22.1
│   ├── anyhow 1.0.55
│   ├── bs58 0.4.0
│   │   └── sha2 0.9.9
│   ├── proc-macro2 1.0.36
│   ├── quote 1.0.15
│   ├── rustversion 1.0.6
│   └── syn 1.0.86
├── anchor-attribute-constant 0.22.1
│   ├── anchor-syn 0.22.1
│   ├── proc-macro2 1.0.36
│   └── syn 1.0.86
├── anchor-attribute-error 0.22.1
│   ├── anchor-syn 0.22.1
│   ├── proc-macro2 1.0.36
│   ├── quote 1.0.15
│   └── syn 1.0.86
├── anchor-attribute-event 0.22.1
│   ├── anchor-syn 0.22.1
│   ├── anyhow 1.0.55
│   ├── proc-macro2 1.0.36
│   ├── quote 1.0.15
│   └── syn 1.0.86
```

```
0/0     0/0        0/0    0/0  0/0    ?  │   ├── anchor-attribute-interface 0.22.1
0/0     8/8        0/0    0/0  0/0    ☢  │   │   ├── anchor-syn 0.22.1
15/18   442/449    3/3    0/0  11/11  ☢  │   │   ├── anyhow 1.0.55
0/0     0/0        0/0    0/0  0/0    ?  │   │   ├── heck 0.3.3
0/0     12/12      0/0    0/0  3/3    ☢  │   │   ├── proc-macro2 1.0.36
0/0     0/0        0/0    0/0  0/0    ?  │   │   ├── quote 1.0.15
0/0     47/47      3/3    0/0  2/2    ☢  │   │   └── syn 1.0.86
0/0     0/0        0/0    0/0  0/0    ?  │   ├── anchor-attribute-program 0.22.1
0/0     8/8        0/0    0/0  0/0    ☢  │   │   ├── anchor-syn 0.22.1
15/18   442/449    3/3    0/0  11/11  ☢  │   │   ├── anyhow 1.0.55
0/0     12/12      0/0    0/0  3/3    ☢  │   │   ├── proc-macro2 1.0.36
0/0     0/0        0/0    0/0  0/0    ?  │   │   ├── quote 1.0.15
0/0     47/47      3/3    0/0  2/2    ☢  │   │   └── syn 1.0.86
0/0     0/0        0/0    0/0  0/0    ?  │   ├── anchor-attribute-state 0.22.1
0/0     8/8        0/0    0/0  0/0    ☢  │   │   ├── anchor-syn 0.22.1
15/18   442/449    3/3    0/0  11/11  ☢  │   │   ├── anyhow 1.0.55
0/0     12/12      0/0    0/0  3/3    ☢  │   │   ├── proc-macro2 1.0.36
0/0     0/0        0/0    0/0  0/0    ?  │   │   ├── quote 1.0.15
0/0     47/47      3/3    0/0  2/2    ☢  │   │   └── syn 1.0.86
0/0     0/0        0/0    0/0  0/0    ?  │   ├── anchor-derive-accounts 0.22.1
0/0     8/8        0/0    0/0  0/0    ☢  │   │   ├── anchor-syn 0.22.1
15/18   442/449    3/3    0/0  11/11  ☢  │   │   ├── anyhow 1.0.55
0/0     12/12      0/0    0/0  3/3    ☢  │   │   ├── proc-macro2 1.0.36
0/0     0/0        0/0    0/0  0/0    ?  │   │   ├── quote 1.0.15
0/0     47/47      3/3    0/0  2/2    ☢  │   │   └── syn 1.0.86
0/0     0/0        0/0    0/0  0/0    ?  │   ├── arrayref 0.3.6
0/0     0/0        0/0    0/0  0/0    🔒 │   ├── base64 0.13.0
0/0     22/22      0/0    0/0  0/0    ☢  │   ├── bincode 1.3.3
0/0     5/5        0/0    0/0  0/0    ☢  │   │   └── serde 1.0.136
0/0     7/7        0/0    0/0  0/0    ☢  │   ├── borsh 0.9.3
0/0     0/0        0/0    0/0  0/0    ?  │   │   ├── borsh-derive 0.9.3
0/0     0/0        0/0    0/0  0/0    ?  │   │   │   ├── borsh-derive-internal 0.9.3
0/0     12/12      0/0    0/0  3/3    ☢  │   │   │   │   ├── proc-macro2 1.0.36
0/0     0/0        0/0    0/0  0/0    ?  │   │   │   │   ├── quote 1.0.15
0/0     47/47      3/3    0/0  2/2    ☢  │   │   │   │   └── syn 1.0.86
0/0     0/0        0/0    0/0  0/0    ?  │   │   │   ├── borsh-schema-derive-internal 0.9.3
0/0     12/12      0/0    0/0  3/3    ☢  │   │   │   │   ├── proc-macro2 1.0.36
0/0     0/0        0/0    0/0  0/0    ?  │   │   │   │   ├── quote 1.0.15
0/0     47/47      3/3    0/0  2/2    ☢  │   │   │   │   └── syn 1.0.86
0/0     0/0        0/0    0/0  0/0    ?  │   │   │   ├── proc-macro-crate 0.1.5
0/0     0/0        0/0    0/0  0/0    🔒 │   │   │   │   └── toml 0.5.8
0/0     5/5        0/0    0/0  0/0    ☢  │   │   │   │       └── serde 1.0.136
0/0     12/12      0/0    0/0  3/3    ☢  │   │   │   ├── proc-macro2 1.0.36
0/0     47/47      3/3    0/0  2/2    ☢  │   │   │   └── syn 1.0.86
2/2     1082/1198  19/22  1/1  51/58  ☢  │   │   └── hashbrown 0.11.2
0/0     26/30      0/0    0/0  0/0    ☢  │   │       ├── ahash 0.7.6
2/4     50/163     1/1    0/0  3/3    ☢  │   │       │   ├── getrandom 0.2.5
0/0     0/0        0/0    0/0  0/0    ?  │   │       │   │   ├── cfg-if 1.0.0
0/20    12/327     0/2    0/0  2/30   ☢  │   │       │   │   └── libc 0.2.119
1/1     35/93      2/6    0/0  1/3    ☢  │   │       │   ├── once_cell 1.10.0
```


1/1 35/93 2/6 0/0 1/3
0/1 0/394 0/17 0/0 0/25
0/0 0/534 0/28 0/14 0/24
0/0 0/18 0/1 0/0 0/0
0/0 5/5 0/0 0/0 0/0
0/16 0/1341 0/0 0/0 0/56
0/0 0/0 0/0 0/0 0/0
0/20 12/327 0/2 0/0 2/30
0/1 0/392 0/7 0/1 0/13
0/0 5/5 0/0 0/0 0/0
0/0 5/5 0/0 0/0 0/0
4/6 389/1102 3/9 1/1 12/25
0/0 5/5 0/0 0/0 0/0
0/0 91/103 318/319 4/4 0/0
0/0 0/0 0/0 0/0 0/0
0/0 12/12 0/0 0/0 3/3
0/0 0/0 0/0 0/0 0/0
0/0 47/47 3/3 0/0 2/2
3/3 406/406 1/1 0/0 2/2
0/0 0/0 0/0 0/0 0/0
0/0 22/22 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
10/78 71/3973 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
2/2 350/350 2/2 0/0 7/7
0/0 5/5 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 16/16 0/0 0/0 0/0
1/1 292/292 20/20 8/8 5/5
0/0 0/0 0/0 0/0 0/0
1/1 292/292 20/20 8/8 5/5
0/0 0/0 0/0 0/0 0/0
0/0 3/3 0/0 0/0 0/0
0/0 7/7 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 1/1 0/0 0/0 0/0
2/2 206/206 0/0 0/0 7/7
0/0 5/5 0/0 0/0 0/0
0/0 91/103 318/319 4/4 0/0
0/2 0/857 0/0 0/0 0/0
0/1 176/193 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 22/22 0/0 0/0 0/0
2/4 50/150 1/1 0/0 3/3
0/0 0/0 0/0 0/0 0/0
0/20 12/327 0/2 0/0 2/30
1/1 16/16 1/1 0/0 0/0
0/0 0/0 0/0 0/0 0/0
once_cell 1.10.0
parking_lot 0.12.0
lock_api 0.4.6
scopeguard 1.1.0
serde 1.0.136
parking_lot_core 0.9.1
cfg-if 1.0.0
libc 0.2.119
smallvec 1.8.0
serde 1.0.136
serde 1.0.136
bumpalo 3.9.1
serde 1.0.136
bytemuck 1.8.0
bytemuck_derive 1.0.1
proc-macro2 1.0.36
quote 1.0.15
syn 1.0.86
solana-program 1.10.0
base64 0.13.0
bincode 1.3.3
bitflags 1.3.2
blake3 1.3.1
arrayref 0.3.6
arrayvec 0.7.2
serde 1.0.136
cfg-if 1.0.0
constant_time_eq 0.1.5
digest 0.10.3
block-buffer 0.10.2
generic-array 0.14.5
crypto-common 0.1.3
generic-array 0.14.5
typenum 1.15.0
subtle 2.4.1
borsh 0.9.3
borsh-derive 0.9.3
bs58 0.4.0
bv 0.11.1
serde 1.0.136
bytemuck 1.8.0
curve25519-dalek 3.2.1
byteorder 1.4.3
digest 0.9.0
rand_core 0.5.1
getrandom 0.1.16
cfg-if 1.0.0
libc 0.2.119
log 0.4.14
cfg-if 1.0.0


0/0 0/0 0/0 0/0 0/0
0/0 5/5 0/0 0/0 0/0
0/0 5/5 0/0 0/0 0/0
0/0 5/5 0/0 0/0 0/0
0/0 3/3 0/0 0/0 0/0
1/1 23/23 0/0 0/0 0/0
0/0 0/72 0/3 0/1 0/3
0/0 0/0 0/0 0/0 0/0
0/0 5/5 0/0 0/0 0/0
0/0 0/72 0/3 0/1 0/3
0/0 7/7 1/1 0/0 0/0
0/0 4/4 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
1/1 292/292 20/20 8/8 5/5
0/0 0/0 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
1/1 292/292 20/20 8/8 5/5
0/0 3/3 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 7/7 1/1 0/0 0/0
0/0 33/33 0/0 0/0 2/2
0/0 0/0 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 3/3 0/0 0/0 0/0
0/0 15/15 0/0 0/0 0/0
2/4 50/150 1/1 0/0 3/3
0/20 12/327 0/2 0/0 2/30
1/1 16/16 1/1 0/0 0/0
0/0 0/0 0/0 0/0 0/0
2/2 636/712 0/0 0/0 17/25
0/0 22/22 0/0 0/0 0/0
0/0 22/22 0/0 0/0 0/0
0/0 5/5 0/0 0/0 0/0
8/8 202/202 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
1/1 16/16 1/1 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 12/12 0/0 0/0 3/3
0/0 0/0 0/0 0/0 0/0
0/0 47/47 3/3 0/0 2/2
0/0 4/10 0/0 0/0 0/0
0/0 15/15 0/0 0/0 0/0
0/1 0/1 0/0 0/0 0/0
0/0 5/5 0/0 0/0 0/0
0/0 16/16 0/0 0/0 0/0
0/0 5/5 0/0 0/0 0/0
cfg-if 1.0.0
serde 1.0.136
serde 1.0.136
serde 1.0.136
subtle 2.4.1
zeroize 1.3.0
itertools 0.10.3
either 1.6.1
serde 1.0.136
itertools 0.10.3
lazy_static 1.4.0
libsecp256k1 0.6.0
arrayref 0.3.6
base64 0.12.3
digest 0.9.0
hmac-drbg 0.3.0
digest 0.9.0
generic-array 0.14.5
hmac 0.8.1
crypto-mac 0.8.0
generic-array 0.14.5
subtle 2.4.1
digest 0.9.0
lazy_static 1.4.0
libsecp256k1-core 0.2.2
crunchy 0.2.2
digest 0.9.0
subtle 2.4.1
rand 0.7.3
getrandom 0.1.16
libc 0.2.119
log 0.4.14
rand_chacha 0.2.2
ppv-lite86 0.2.16
rand_core 0.5.1
rand_core 0.5.1
serde 1.0.136
sha2 0.9.9
typenum 1.15.0
log 0.4.14
num-derive 0.3.3
proc-macro2 1.0.36
quote 1.0.15
syn 1.0.86
num-traits 0.2.14
rand 0.7.3
rustversion 1.0.6
serde 1.0.136
serde_bytes 0.11.5
serde 1.0.136


0/0 0/0 0/0 0/0 0/0
8/8 196/196 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/1 0/14 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 1/1 0/0 0/0 0/0
2/2 206/206 0/0 0/0 7/7
1/1 292/292 20/20 8/8 5/5
1/1 16/16 1/1 0/0 0/0
0/0 147/282 4/6 0/0 7/7
0/20 12/327 0/2 0/0 2/30
0/0 5/5 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
8/8 196/196 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 12/12 0/0 0/0 3/3
0/0 0/0 0/0 0/0 0/0
0/0 47/47 3/3 0/0 2/2
0/0 0/0 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 1/1 0/0 0/0 0/0
0/0 12/12 0/0 0/0 3/3
0/0 0/0 0/0 0/0 0/0
0/1 0/1 0/0 0/0 0/0
0/0 47/47 3/3 0/0 2/2
0/0 0/0 0/0 0/0 0/0
12/14 432/496 16/16 2/2 9/9
0/0 0/0 0/0 0/0 0/0
0/0 5/5 0/0 0/0 0/0
0/0 4/7 0/0 0/0 0/0
0/1 0/0 0/1 0/0 0/1
0/0 0/0 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 12/12 0/0 0/0 3/3
0/0 0/0 0/0 0/0 0/0
0/0 47/47 3/3 0/0 2/2
0/0 0/0 0/0 0/0 0/0
4/6 389/1102 3/9 1/1 12/25
0/0 7/7 1/1 0/0 0/0
1/1 16/16 1/1 0/0 0/0
0/0 12/12 0/0 0/0 3/3
0/0 0/0 0/0 0/0 0/0
0/0 47/47 3/3 0/0 2/2
0/0 0/0 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
├── serde_derive 1.0.136
├── sha2 0.10.2
│ ├── cfg-if 1.0.0
│ ├── cpufeatures 0.2.1
│ └── digest 0.10.3
├── sha3 0.10.1
│ ├── digest 0.10.3
│ └── keccak 0.1.0
├── solana-frozen-abi 1.10.0
│ ├── bs58 0.4.0
│ ├── bv 0.11.1
│ ├── generic-array 0.14.5
│ ├── log 0.4.14
│ ├── memmap2 0.5.3
│ │ └── libc 0.2.119
│ ├── serde 1.0.136
│ ├── serde_derive 1.0.136
│ ├── sha2 0.10.2
│ ├── solana-frozen-abi-macro 1.10.0
│ │ ├── proc-macro2 1.0.36
│ │ ├── quote 1.0.15
│ │ └── syn 1.0.86
│ └── thiserror 1.0.30
├── solana-frozen-abi-macro 1.10.0
├── solana-sdk-macro 1.10.0
│ ├── bs58 0.4.0
│ ├── proc-macro2 1.0.36
│ ├── quote 1.0.15
│ ├── rustversion 1.0.6
│ └── syn 1.0.86
├── thiserror 1.0.30
└── wasm-bindgen 0.2.79
├── cfg-if 1.0.0
├── serde 1.0.136
├── serde_json 1.0.79
└── wasm-bindgen-macro 0.2.79
├── quote 1.0.15
└── wasm-bindgen-macro-support 0.2.79
├── proc-macro2 1.0.36
├── quote 1.0.15
├── syn 1.0.86
└── wasm-bindgen-backend 0.2.79
├── bumpalo 3.9.1
├── lazy_static 1.4.0
├── log 0.4.14
├── proc-macro2 1.0.36
├── quote 1.0.15
├── syn 1.0.86
└── wasm-bindgen-shared 0.2.79
└── wasm-bindgen-shared 0.2.79

```
0/0         0/0          0/0    0/0    0/0     ?
0/0         0/0          0/0    0/0    0/0     ?
0/0         0/0          0/0    0/0    0/0     ?
3/3         406/406      1/1    0/0    2/2     
0/0         0/0          0/0    0/0    0/0     
3/3         406/406      1/1    0/0    2/2     
0/0         0/0          0/0    0/0    0/0     ?
0/0         0/0          0/0    0/0    0/0     ?
0/0         0/0          0/0    0/0    0/0     ?
0/0         4/10         0/0    0/0    0/0     
0/0         0/0          0/0    0/0    0/0     ?
0/0         0/0          0/0    0/0    0/0     ?
0/0         0/0          0/0    0/0    0/0     ?
0/0         0/0          0/0    0/0    0/0     ?
0/0         0/0          0/0    0/0    0/0     
0/0         12/12        0/0    0/0    3/3     
0/0         0/0          0/0    0/0    0/0     ?
0/0         47/47        3/3    0/0    2/2     
3/3         406/406      1/1    0/0    2/2     
0/0         0/0          0/0    0/0    0/0     ?
0/0         0/0          0/0    0/0    0/0     ?

141/267     8970/18443   396/472 16/32   186/366

    └── thiserror 1.0.30
└── anchor-spl 0.22.1
    ├── anchor-lang 0.22.1
    ├── solana-program 1.10.0
    ├── spl-associated-token-account 1.0.3
    │   ├── solana-program 1.10.0
    │   └── spl-token 3.3.0
    │       ├── arrayref 0.3.6
    │       ├── num-derive 0.3.3
    │       ├── num-traits 0.2.14
    │       ├── num_enum 0.5.7
    │       │   └── num_enum_derive 0.5.7
    │       │       ├── proc-macro-crate 1.1.3
    │       │       │   ├── thiserror 1.0.30
    │       │       │   └── toml 0.5.8
    │       │       ├── proc-macro2 1.0.36
    │       │       ├── quote 1.0.15
    │       │       └── syn 1.0.86
    │       ├── solana-program 1.10.0
    │       └── thiserror 1.0.30
    └── spl-token 3.3.0
```

Closing Summary

Overall, programs are very well written and adhere to guidelines.
The best practices were already followed, and the logic of the program was verified to not contain any critical issues, and all the issues discovered during the audit phase were fixed by the Enrex team.

Disclaimer

Quillhash audit is not a security warranty, investment advice, or an endorsement of the Enrex Staking Programs. This audit does not provide a security or correctness guarantee of the audited programs. The statements made in this document should not be interpreted as investment or legal advice, nor should its authors be held accountable for decisions made based on them. Securing programs is a multistep process. One audit cannot be considered enough. We recommend that the Enrex Team put in place a bug bounty program to encourage further analysis of the programs by other third parties.

Audit Report
April, 2022

For

ENREX

QuillAudits

Canada, India, Singapore, United Kingdom

audits.quillhash.com

audits@quillhash.com