QuillAudits

Audit Report
March, 2022

For

ENREX

Contents

Scope of the Audit

The scope of this audit was to analyze and document the Enrex 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- Outdated dependencies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 behaviour.
- Token distribution and calculations are as per the intended behaviour mentioned in the whitepaper.
- Implementation of ERC-20/721 token standards.
- Efficient use of gas.
- Code is safe from re-entrancy and 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	1	0	1
Closed	0	0	2	0

Introduction

During the period of **February 28, 2022 to March 25, 2022** - QuillAudits Team performed a security audit for Enrex programs.

The code for the audit was taken from the repository of Enrex:
https://github.com/Enrex-io/token-vesting

V	Date	Commit Hash
1	February	acb6901dbba3f6c0a564ab7d6e525b7c35c368d5
2	March 14	1a09c90f985132cd9d217fa9c05791d53c9f1527
3	March 25	483a7b9af55d47805fcd49b924b6e409eef4b051

A. Program – processor.rs

Issues Found – Code Review / Manual Testing

High severity issues

No issues were found.

Medium severity issues

1. Address not guaranteed to be a valid program address

```
processor.rs - Line 44
        let vesting_account_key = Pubkey::create_program_address(&[&seeds],
&program_id).unwrap();
        if vesting_account_key != *vesting_account.key {
            msg!("Provided vesting account is invalid");
            return Err(ProgramError::InvalidArgument);
        }
```

```
processor.rs - Line 88
        let vesting_account_key = Pubkey::create_program_address(&[&seeds],
program_id)?;
        if vesting_account_key != *vesting_account.key {
            msg!("Provided vesting account is invalid");
            return Err(ProgramError::InvalidArgument);
        }
```

```
processor.rs - Line 198
        let vesting_account_key = Pubkey::create_program_address(&[&seeds],
&program_id).unwrap();
        if vesting_account_key != *vesting_account.key {
            msg!("Provided vesting account is invalid");
            return Err(ProgramError::InvalidArgument);
        }
```

```
processor.rs - Line 285
        let vesting_account_key = Pubkey::create_program_address(&[&seeds],
program_id)?;
        let state = VestingScheduleHeader::unpack(
            &vesting_account.data.borrow()[..VestingScheduleHeader::LEN],
        )?;

        if vesting_account_key != *vesting_account.key {
            msg!("Invalid vesting account key");
            return Err(ProgramError::InvalidArgument);
        }
```

Description

The address generated using create_program_address is not guaranteed to be a valid program address off the curve. Program addresses does not lie on the ed25519 curve and therefore has no valid private key associated with it, and thus generating a signature for it is impossible. There is about a 50/50 chance of this happening for a given collection of seeds and program id.

Remediation

To generate a valid program address using a specific seed, use find_program_address function, which iterates through multiple bump seeds until a valid combination that does not lie on the curve is found.

Status: Acknowledged

Low severity issues

2. Missing signer check

```
processor.rs - Line 52
        let init_vesting_account = create_account(
            &payer.key,
            &vesting_account_key,
            rent.minimum_balance(state_size),
            state_size as u64,
            &program_id,
        );
```

Description

If an instruction should only be available to a restricted set of entities, the program should verify that the call has been signed by the appropriate entity.

Remediation

Verify that the payer account is a signer using the is_signer() function.

Status: Fixed

The Enrex team has solved the issue by verifying that the payer is the signer of the transaction.

3. Missing overflow check

```
processor.rs - Line 230
        for s in schedules.iter_mut() {
            if clock.unix_timestamp as u64 >= s.release_time {
                total_amount_to_transfer += s.amount;
                s.amount = 0;
            }
        }
```

Description
The addition operation is missing an overflow check, if the value overflows, an error should be thrown.

Remediation
The addition operation should be checked for overflows using the checked_add() function.

Status: Fixed
The Enrex team has solved the issue by using the checked_add() function to perform addition operations.

Informational issues

4. Errors should be more specific

Description
There is only one error struct and the same error is returned in every case scenario.

Remediation
Error messages should be specific to the case that caused the issue.

Status: Acknowledged
The Enrex team has acknowledged the issue.

Functional Tests

Cargo test

```
    Finished test [unoptimized + debuginfo] target(s) in 3m 05s
     Running unittests (target/debug/deps/token_vesting-73172e146af3fd59)

running 2 tests
test instruction::test::test_instruction_packing ... ok
test state::tests::test_state_packing ... ok

test result: ok. 2 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out; finished in 0.00s

     Running tests/functional.rs (target/debug/deps/functional-ace302d356aa2dd0)

running 0 tests

test result: ok. 0 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out; finished in 0.00s

   Doc-tests token-vesting

running 0 tests

test result: ok. 0 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out; finished in 0.00s
```

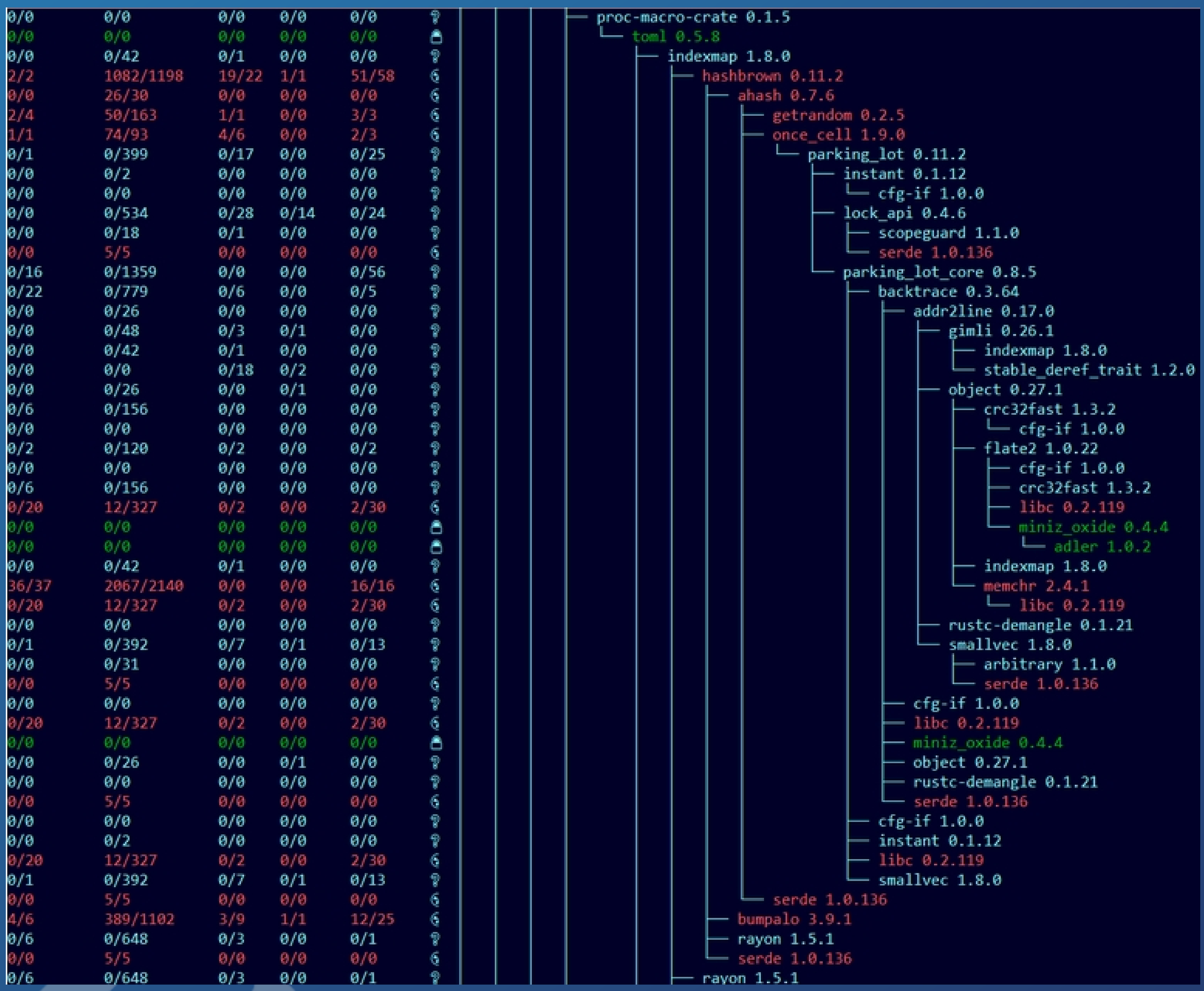
Automated Tests

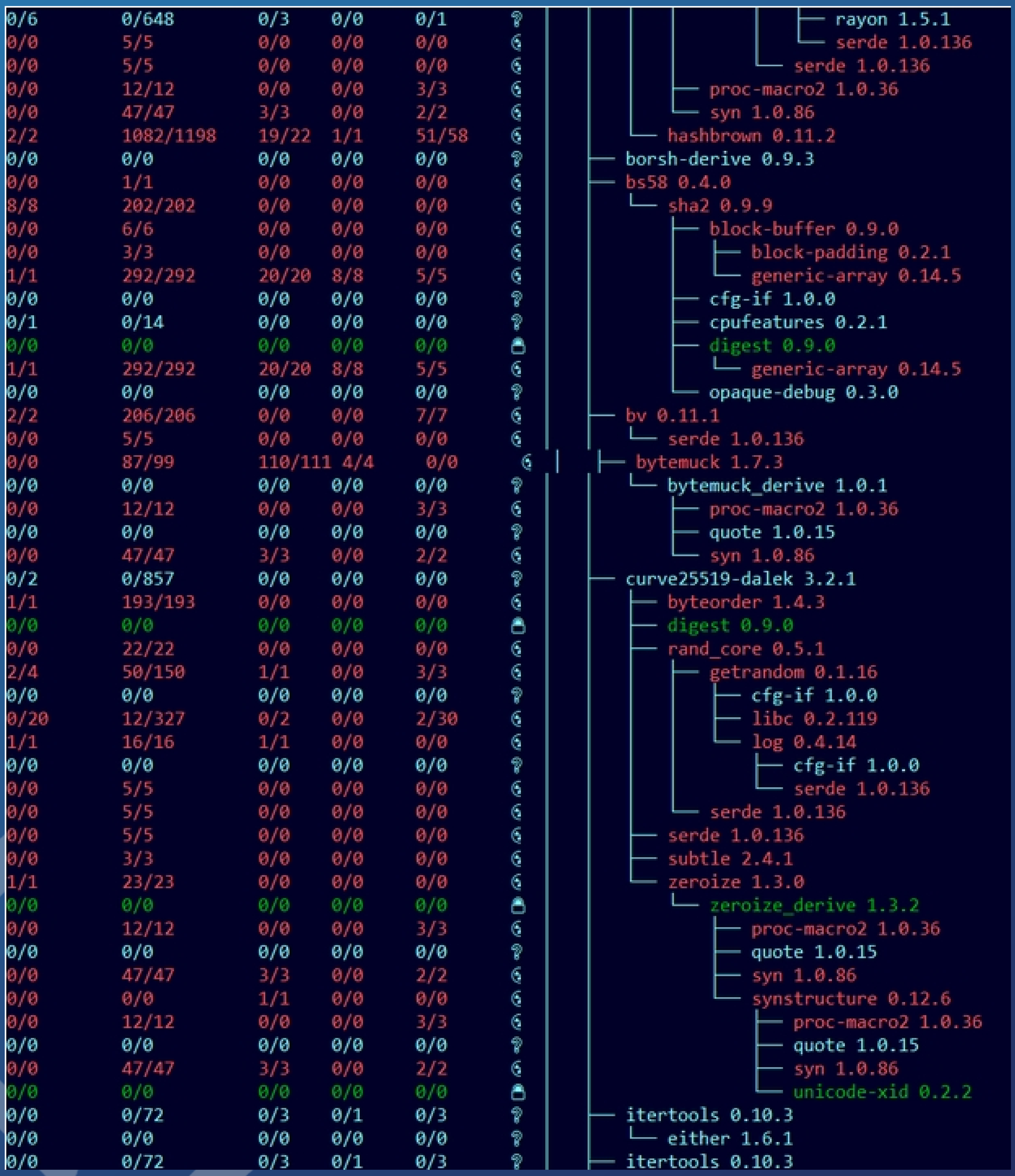
Cargo-geiger

```
    Scanning done
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/program/target/debug/build/libsecp256k1-5431544d48f177ec/out/const_gen.rs
WARNING: Dependency file was never scanned: /root/Enrex/program/target/debug/build/rustversion-2eb2b30e6ec73d94/out/version.rs
WARNING: Dependency file was never scanned: /root/Enrex/program/target/debug/build/libsecp256k1-5431544d48f177ec/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      ❓  token-vesting 0.1.0
0/0        0/2          0/0    0/0     0/0      ❓  ├── arbitrary 0.4.7
0/0        0/0          0/0    0/0     0/0      ❓  │   └── derive_arbitrary 0.4.7
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      ❓  │       ├── 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
0/0        0/0          0/0    0/0     0/0      ❓  ├── arrayref 0.3.6
0/0        0/10         0/0    0/0     0/0      ❓  ├── honggfuzz 0.5.54
0/0        0/31         0/0    0/0     0/0      ❓  │   └── arbitrary 1.1.0
0/0        0/0          0/0    0/0     0/0      ❓  ├── num-derive 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        4/10         0/0    0/0     0/0      ☢  ├── num-traits 0.2.14
3/3        405/405      1/1    0/0     2/2      ☢  ├── solana-program 1.9.9
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        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        0/0          0/0    0/0     0/0      ❓  │   ├── bitflags 1.3.2
10/78      71/3973      0/0    0/0     0/0      ☢  │   ├── blake3 1.3.1
0/0        0/0          0/0    0/0     0/0      ❓  │   │   ├── arrayref 0.3.6
2/2        350/350      2/2    0/0     7/7      ☢  │   │   ├── arrayvec 0.7.2
0/0        5/5          0/0    0/0     0/0      ☢  │   │   │   └── serde 1.0.136
0/0        0/0          0/0    0/0     0/0      ❓  │   │   ├── cfg-if 1.0.0
```

```
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     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     
1/1     292/292 20/20  8/8    5/5     
0/0     0/15    0/0    0/0    0/0     
2/4     50/163  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    
0/0     5/5     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     
0/6     0/648   0/3    0/0    0/1     
0/0     0/451   0/6    0/0    0/6     
0/0     0/0     0/0    0/0    0/0     
0/3     0/430   0/9    0/0    0/26    
0/0     0/0     0/0    0/0    0/0     
0/4     0/85    0/14   0/0    0/2     
0/0     0/0     0/0    0/0    0/0     
0/0     7/7     1/1    0/0    0/0     
0/0     0/49    0/6    0/0    0/3     
0/0     7/7     1/1    0/0    0/0     
0/0     0/0     0/0    0/0    0/0     
0/0     0/18    0/1    0/0    0/0     
0/4     0/85    0/14   0/0    0/2     
0/0     0/0     0/0    0/0    0/0     
0/0     5/5     0/0    0/0    0/0     
0/5     0/488   0/2    0/0    0/20    
0/2     0/518   0/7    0/0    0/14    
0/0     0/0     0/0    0/0    0/0     
0/4     0/85    0/14   0/0    0/2     
0/0     0/451   0/6    0/0    0/6     
0/4     0/85    0/14   0/0    0/2     
0/0     7/7     1/1    0/0    0/0     
0/0     0/72    0/0    0/0    0/0     
0/20    12/327  0/2    0/0    2/30    
0/0     7/7     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     
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     
```

```
├── constant_time_eq 0.1.5
├── digest 0.10.3
│   ├── block-buffer 0.10.2
│   │   └── generic-array 0.14.5
│   │       ├── serde 1.0.136
│   │       └── typenum 1.15.0
│   ├── crypto-common 0.1.3
│   │   ├── generic-array 0.14.5
│   │   └── rand_core 0.6.3
│   │       ├── getrandom 0.2.5
│   │       │   ├── cfg-if 1.0.0
│   │       │   └── libc 0.2.119
│   │       └── serde 1.0.136
│   │       └── typenum 1.15.0
│   └── subtle 2.4.1
└── rayon 1.5.1
    ├── crossbeam-deque 0.8.1
    │   ├── cfg-if 1.0.0
    │   ├── crossbeam-epoch 0.9.7
    │   │   ├── cfg-if 1.0.0
    │   │   ├── crossbeam-utils 0.8.7
    │   │   │   ├── cfg-if 1.0.0
    │   │   │   └── lazy_static 1.4.0
    │   │   │       └── spin 0.5.2
    │   │   ├── lazy_static 1.4.0
    │   │   ├── memoffset 0.6.5
    │   │   └── scopeguard 1.1.0
    │   └── crossbeam-utils 0.8.7
    ├── either 1.6.1
    │   └── serde 1.0.136
    └── rayon-core 1.9.1
        ├── crossbeam-channel 0.5.2
        │   ├── cfg-if 1.0.0
        │   └── crossbeam-utils 0.8.7
        ├── crossbeam-deque 0.8.1
        ├── crossbeam-utils 0.8.7
        ├── lazy_static 1.4.0
        └── num_cpus 1.13.1
            └── libc 0.2.119
├── borsh 0.9.3
│   ├── borsh-derive 0.9.3
│   │   ├── borsh-derive-internal 0.9.3
│   │   │   ├── proc-macro2 1.0.36
│   │   │   ├── quote 1.0.15
│   │   │   └── syn 1.0.86
│   │   ├── borsh-schema-derive-internal 0.9.3
│   │   │   ├── proc-macro2 1.0.36
│   │   │   ├── quote 1.0.15
│   │   │   └── syn 1.0.86
│   │   ├── proc-macro-crate 0.1.5
```


0/0 0/0 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 0/42 0/1 0/0 0/0
2/2 1082/1198 19/22 1/1 51/58
0/0 26/30 0/0 0/0 0/0
2/4 50/163 1/1 0/0 3/3
1/1 74/93 4/6 0/0 2/3
0/1 0/399 0/17 0/0 0/25
0/0 0/2 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
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 0/1359 0/0 0/0 0/56
0/22 0/779 0/6 0/0 0/5
0/0 0/26 0/0 0/0 0/0
0/0 0/48 0/3 0/1 0/0
0/0 0/42 0/1 0/0 0/0
0/0 0/0 0/18 0/2 0/0
0/0 0/26 0/0 0/1 0/0
0/6 0/156 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/2 0/120 0/2 0/0 0/2
0/0 0/0 0/0 0/0 0/0
0/6 0/156 0/0 0/0 0/0
0/20 12/327 0/2 0/0 2/30
0/0 0/0 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 0/42 0/1 0/0 0/0
36/37 2067/2140 0/0 0/0 16/16
0/20 12/327 0/2 0/0 2/30
0/0 0/0 0/0 0/0 0/0
0/1 0/392 0/7 0/1 0/13
0/0 0/31 0/0 0/0 0/0
0/0 5/5 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/20 12/327 0/2 0/0 2/30
0/0 0/0 0/0 0/0 0/0
0/0 0/26 0/0 0/1 0/0
0/0 0/0 0/0 0/0 0/0
0/0 5/5 0/0 0/0 0/0
0/0 0/0 0/0 0/0 0/0
0/0 0/2 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
4/6 389/1102 3/9 1/1 12/25
0/6 0/648 0/3 0/0 0/1
0/0 5/5 0/0 0/0 0/0
0/6 0/648 0/3 0/0 0/1
proc-macro-crate 0.1.5
toml 0.5.8
indexmap 1.8.0
hashbrown 0.11.2
ahash 0.7.6
getrandom 0.2.5
once_cell 1.9.0
parking_lot 0.11.2
instant 0.1.12
cfg-if 1.0.0
lock_api 0.4.6
scopeguard 1.1.0
serde 1.0.136
parking_lot_core 0.8.5
backtrace 0.3.64
addr2line 0.17.0
gimli 0.26.1
indexmap 1.8.0
stable_deref_trait 1.2.0
object 0.27.1
crc32fast 1.3.2
cfg-if 1.0.0
flate2 1.0.22
cfg-if 1.0.0
crc32fast 1.3.2
libc 0.2.119
miniz_oxide 0.4.4
adler 1.0.2
indexmap 1.8.0
memchr 2.4.1
libc 0.2.119
rustc-demangle 0.1.21
smallvec 1.8.0
arbitrary 1.1.0
serde 1.0.136
cfg-if 1.0.0
libc 0.2.119
miniz_oxide 0.4.4
object 0.27.1
rustc-demangle 0.1.21
serde 1.0.136
cfg-if 1.0.0
instant 0.1.12
libc 0.2.119
smallvec 1.8.0
serde 1.0.136
bumpalo 3.9.1
rayon 1.5.1
serde 1.0.136
rayon 1.5.1


0/6 0/648 0/3 0/0 0/1
0/0 5/5 0/0 0/0 0/0
0/0 5/5 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
2/2 1082/1198 19/22 1/1 51/58
0/0 0/0 0/0 0/0 0/0
0/0 1/1 0/0 0/0 0/0
8/8 202/202 0/0 0/0 0/0
0/0 6/6 0/0 0/0 0/0
0/0 3/3 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
0/1 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
2/2 206/206 0/0 0/0 7/7
0/0 5/5 0/0 0/0 0/0
0/0 87/99 110/111 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
0/2 0/857 0/0 0/0 0/0
1/1 193/193 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
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 0/0 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 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 0/72 0/3 0/1 0/3
0/0 0/0 0/0 0/0 0/0
0/0 0/72 0/3 0/1 0/3
rayon 1.5.1
serde 1.0.136
serde 1.0.136
proc-macro2 1.0.36
syn 1.0.86
hashbrown 0.11.2
borsh-derive 0.9.3
bs58 0.4.0
sha2 0.9.9
block-buffer 0.9.0
block-padding 0.2.1
generic-array 0.14.5
cfg-if 1.0.0
cpufeatures 0.2.1
digest 0.9.0
generic-array 0.14.5
opaque-debug 0.3.0
bv 0.11.1
serde 1.0.136
bytemuck 1.7.3
bytemuck_derive 1.0.1
proc-macro2 1.0.36
quote 1.0.15
syn 1.0.86
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
serde 1.0.136
serde 1.0.136
subtle 2.4.1
zeroize 1.3.0
zeroize_derive 1.3.2
proc-macro2 1.0.36
quote 1.0.15
syn 1.0.86
synstructure 0.12.6
proc-macro2 1.0.36
quote 1.0.15
syn 1.0.86
unicode-xid 0.2.2
itertools 0.10.3
either 1.6.1
itertools 0.10.3

```
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
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     0/0     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     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
0/0     0/0     0/0   0/0   0/0
8/8     202/202 0/0   0/0   0/0
0/0     14/14   0/0   0/0   0/0
0/0     6/6     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
```

```
├── 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
│   │   └── rand_pcg 0.2.1
│   │       ├── rand_core 0.5.1
│   │       └── serde 1.0.136
│   ├── serde 1.0.136
│   ├── sha2 0.9.9
│   └── typenum 1.15.0
├── log 0.4.14
├── num-derive 0.3.3
├── 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
├── serde_derive 1.0.136
├── sha2 0.9.9
├── sha3 0.9.1
│   ├── block-buffer 0.9.0
│   ├── digest 0.9.0
│   ├── keccak 0.1.0
│   └── opaque-debug 0.3.0
└── solana-frozen-abi 1.9.9
    ├── bs58 0.4.0
    └── bv 0.11.1
```

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	0/0	0/18	0/2	0/0	?
0/0	5/5	0/0	0/0	0/0	✓
0/0	0/0	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	?
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	?
2/2	45/45	0/0	0/0	0/0	✓
0/20	12/327	0/2	0/0	2/30	✓
0/0	0/0	0/0	0/0	0/0	🔒
1/1	16/16	1/1	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	✓
36/37	2067/2140	0/0	0/0	16/16	✓
0/0	0/0	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	✓
1/1	16/16	1/1	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	✓
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	0/7	0/0	0/0	0/0	?
0/0	0/42	0/1	0/0	0/0	?
0/0	0/7	0/0	0/0	0/0	?
0/9	0/723	0/0	0/0	0/2	?

```
├── solana-frozen-abi 1.9.9
│   ├── 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
│   │   └── stable_deref_trait 1.2.0
│   ├── serde 1.0.136
│   ├── serde_derive 1.0.136
│   ├── sha2 0.9.9
│   ├── solana-frozen-abi-macro 1.9.9
│   │   ├── proc-macro2 1.0.36
│   │   ├── quote 1.0.15
│   │   └── syn 1.0.86
│   ├── solana-logger 1.9.9
│   │   └── env_logger 0.9.0
│   │       ├── atty 0.2.14
│   │       │   └── libc 0.2.119
│   │       ├── humantime 2.1.0
│   │       ├── log 0.4.14
│   │       ├── regex 1.5.4
│   │       │   ├── aho-corasick 0.7.18
│   │       │   │   └── memchr 2.4.1
│   │       │   ├── memchr 2.4.1
│   │       │   └── regex-syntax 0.6.25
│   │       └── termcolor 1.1.2
│   │   ├── lazy_static 1.4.0
│   │   └── log 0.4.14
│   └── thiserror 1.0.30
│       └── thiserror-impl 1.0.30
│           ├── proc-macro2 1.0.36
│           ├── quote 1.0.15
│           └── syn 1.0.86
├── solana-frozen-abi-macro 1.9.9
├── solana-logger 1.9.9
├── solana-sdk-macro 1.9.9
│   ├── 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
    │   ├── indexmap 1.8.0
    │   ├── itoa 1.0.1
    │   ├── ryu 1.0.9
```

```
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         0/7          0/0     0/0     0/0     ?
0/0         0/42         0/1     0/0     0/0     ?
0/0         0/7          0/0     0/0     0/0     ?
0/9         0/723        0/0     0/0     0/2     ?
0/0         5/5          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     ?
0/0         0/0          0/0     0/0     0/0     🔒
3/3         405/405      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         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         405/405      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     ?

111/290     7804/21833   188/339 16/36   174/434

error: Found 4 warnings

        ├── 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
        │   ├── indexmap 1.8.0
        │   ├── itoa 1.0.1
        │   ├── ryu 1.0.9
        │   └── serde 1.0.136
        └── 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
├── spl-associated-token-account 1.0.3
    ├── solana-program 1.9.9
    └── spl-token 3.3.0
        ├── arrayref 0.3.6
        ├── num-derive 0.3.3
        ├── num-traits 0.2.14
        ├── num_enum 0.5.6
        │   └── num_enum_derive 0.5.6
        │       ├── 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 1.9.9
        └── thiserror 1.0.30
├── spl-token 3.3.0
└── thiserror 1.0.30
```

Cargo-tarpaulin

```
    Finished test [unoptimized + debuginfo] target(s) in 4m 37s
Mar 02 01:48:15.234  INFO cargo_tarpaulin::process_handling::linux: Launching test
Mar 02 01:48:15.234  INFO cargo_tarpaulin::process_handling: running /root/Enrex/program/target/debug/deps/functional-ace302d356aa2dd0

running 0 tests

test result: ok. 0 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out; finished in 0.00s

Mar 02 01:48:15.494  INFO cargo_tarpaulin::process_handling::linux: Launching test
Mar 02 01:48:15.494  INFO cargo_tarpaulin::process_handling: running /root/Enrex/program/target/debug/deps/token_vesting-73172e146af3fd59

running 2 tests
test state::tests::test_state_packing ... ok
test instruction::test::test_instruction_packing ... ok

test result: ok. 2 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out; finished in 0.01s

Mar 02 01:48:16.861  INFO cargo_tarpaulin::report: Coverage Results:
|| Tested/Total Lines:
|| src/entrypoint.rs: 0/6
|| src/error.rs: 0/4
|| src/instruction.rs: 82/130
|| src/processor.rs: 0/178
|| src/state.rs: 66/73
||
37.85% coverage, 148/391 lines covered
```

Closing Summary

Overall, programs are very well written and adhere to guidelines.
Many issues were discovered during the initial audit. Most of the issues have been Fixed by the Exrex Team.

Disclaimer

Quillhash audit is not a security warranty, investment advice, or an endorsement of the Enrex 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
March, 2022

For

ENREX

QuillAudits

Canada, India, Singapore, United Kingdom

audits.quillhash.com

audits@quillhash.com